

# Cisco

## Exam Questions 300-735

Automating and Programming Cisco Security Solutions (SAUTO)



#### NEW QUESTION 1

Which description of synchronous calls to an API is true?

- A. They can be used only within single-threaded processes.
- B. They pause execution and wait for the response.
- C. They always successfully return within a fixed time.
- D. They can be used only for small requests.

**Answer: B**

#### NEW QUESTION 2

```
import requests

headers = {
    'Authorization': 'Bearer ' + investigate_api_key
}

domains=["cisco.com", "google.com", "xreddfr.df"]

investigate_url= "https://investigate.api.umbrella.com/domains/categorization/"
values = str(json.dumps(domains))
response = requests.post(investigate_url, data=values, headers=headers)
```

Refer to the exhibit.

What does the response from the API contain when this code is executed?

- A. error message and status code of 403
- B. newly created domains in Cisco Umbrella Investigate
- C. updated domains in Cisco Umbrella Investigate
- D. status and security details for the domains

**Answer: D**

#### NEW QUESTION 3

Refer to the exhibit. A network operator must generate a daily flow report and learn how to act on or manipulate returned data. When the operator runs the script, it returns an enormous amount of information. Which two actions enable the operator to limit returned data? (Choose two.)

- A. Add recordLimit
- B. followed by an integer (key:value) to the flow\_data.
- C. Add a for loop at the end of the script, and print each key value pair separately.
- D. Add flowLimit, followed by an integer (key:value) to the flow\_data.
- E. Change the startDateTime and endDateTime values to include smaller time intervals.
- F. Change the startDate and endDate values to include smaller date intervals.

**Answer: AB**

#### NEW QUESTION 4

When the URI "/api/fmc\_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies" is used to make a POST request, what does "e276abec-e0f2-11e3-8169- 6d9ed49b625f" represent?

- A. API token
- B. domain UUID
- C. access policy UUID
- D. object UUID

**Answer: B**

#### NEW QUESTION 5

DRAG DROP

Drag and drop the code to complete the curl command to query the Cisco Umbrella Investigate API for the umbrella popularity list. Not all options are used. Select and Place:

```
curl -H "Authorization:  %YourToken%"
"https://investigate.api.umbrella.com/
```

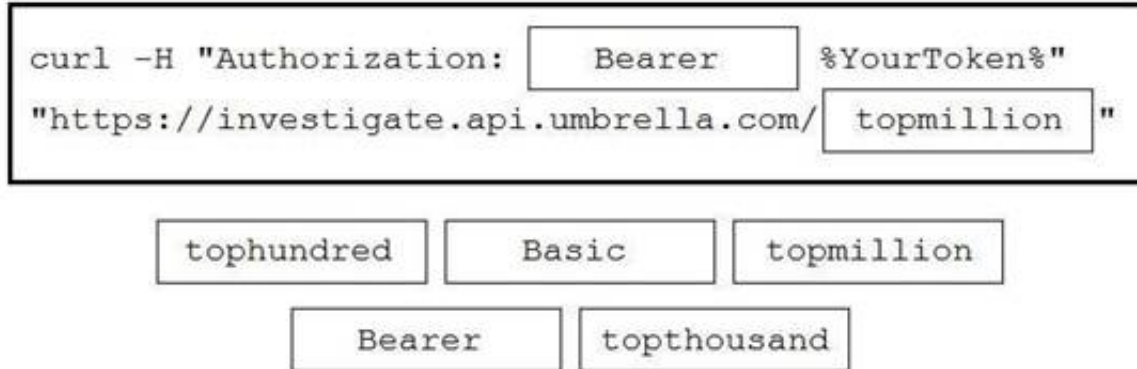
tophundred   Basic   topmillion

Bearer   topthousand

- A. Mastered
- B. Not Mastered

**Answer: A**

Explanation:



#### NEW QUESTION 6

Refer to the exhibit.

Which URL returned the data?

- A. <https://api.amp.cisco.com/v1/computers>
- B. <https://api.amp.cisco.com/v0/computers>
- C. <https://amp.cisco.com/api/v0/computers>
- D. <https://amp.cisco.com/api/v1/computers>

Answer: A

#### NEW QUESTION 7

```
def query(config, secret, url, payload):
    print('query url=' + url)
    print(' request=' + payload)
    handler = urllib.request.HTTPSHandler(context=config.get_ssl_context())
    opener = urllib.request.build_opener(handler)
    rest_request = urllib.request.Request(url=url, data=str.encode(payload))
    rest_request.add_header('Content-Type', 'application/json')
    rest_request.add_header('Accept', 'application/json')
    b64 = base64.b64encode((config.get_node_name() + ':' + secret).encode()).decode()
    rest_request.add_header('Authorization', 'Basic ' + b64)
    rest_response = opener.open(rest_request)
    print(' response status=' + str(rest_response.getcode()))
    print(' response content=' + rest_response.read().decode())
```

Refer to the exhibit. A Python function named "query" has been developed and the goal is to use it to query the service "com.cisco.ise.session" via Cisco pxGrid 2.0 APIs. How is the function called, if the goal is to identify the sessions that are associated with the IP address 10.0.0.50?

- A. `query(config, secret, "getSessionByIpAddress/10.0.0.50", "ipAddress")`
- B. `query(config, "10.0.0.50", url, payload)`
- C. `query(config, secret, url, "10.0.0.50")`
- D. `query(config, secret, url, '{"ipAddress": "10.0.0.50"}')`

Answer: D

#### NEW QUESTION 8

Which two API capabilities are available on Cisco Identity Services Engine? (Choose two.)

- A. Platform Configuration APIs
- B. Monitoring REST APIs
- C. Performance Management REST APIs
- D. External RESTful Services APIs
- E. Internal RESTful Services APIs

Answer: BD

#### NEW QUESTION 9

If the goal is to create an access policy with the default action of blocking traffic, using Cisco Firepower Management Center REST APIs, which snippet is used?

- A.
 

```
- API PATH:
/api/fmc_config/v1/domain/<domain_uuid>/object/accesspolicies

- METHOD:
POST

- INPUT JSON:
{
  "type": "AccessPolicy",
  "name": "AccessPolicy-test-1",
  "defaultAction": {
    "action": "BLOCK"
  }
}
```
- B.

```
- API PATH:
/api/fmc_config/v1/domain/<domain_uuid>/object/securityzones

- METHOD:
POST

- INPUT JSON:
{
  "type": "AccessPolicy",
  "name": "AccessPolicy-test-1",
  "defaultAction": {
    "action": "BLOCK"
  }
}
```

- C.
- ```
- API PATH:
/api/fmc_config/v1/domain/<domain_uuid>/object/accesspolicies

- METHOD:
PUT

- INPUT JSON:
{
  "type": "AccessPolicy",
  "name": "AccessPolicy-test-1",
  "defaultAction": {
    "action": "BLOCK"
  }
}
```
- D.
- ```
- API PATH:
/api/fmc_config/v1/domain/<domain_uuid>/object/accesspolicies

- METHOD:
POST

- INPUT JSON:
{
  "type": "AccessPolicy",
  "name": "AccessPolicy-test-1",
  "action": "FASTPATH"
}
```

**Answer: D**

#### NEW QUESTION 10

Which API is designed to give technology partners the ability to send security events from their platform/service/appliance within a mutual customer's environment to the Umbrella cloud for enforcement?

- A. Cisco Umbrella Management API
- B. Cisco Umbrella Security Events API
- C. Cisco Umbrella Enforcement API
- D. Cisco Umbrella Reporting API

**Answer: C**

#### NEW QUESTION 10

Which curl command lists all tags (host groups) that are associated with a tenant using the Cisco Stealthwatch Enterprise API?

- A. curl -X PUT "Cookie:{Cookie Data}"https://{stealthwatch\_host}/smc-configuration/rest/v1/tenants/{tenant\_id}/tags
- B. curl -X POST -H"Cookie:{Cookie Data}"https://{stealthwatch\_host}/smc-configuration/rest/v1/tenants/tags
- C. curl -X GET -H"Cookie:{Cookie Data}"https://{stealthwatch\_host}/smc-configuration/rest/v1/tenants/{tenant\_id}/tags
- D. curl -X GET -H"Cookie:{Cookie Data}"https://{stealthwatch\_host}/smc- configuration/rest/v1/tenants/tags

**Answer: C**

#### NEW QUESTION 13



```
curl -X PUT \
--header "Accept: application/json" \
--header "Authorization: Bearer ${ACCESS_TOKEN}" \
--header "Content-Type: application/json" \
-d '{
  "id": "XXXXXXXXXX",
  "ruleAction": "DENY",
  "eventLogAction": "LOG_FLOW_START",
  "type": "accessrule",
}' \
"https://${HOST}:${PORT}/api/fdm/v3/policy/accesspolicies
/{parentId}/accessrules/{objId}"
```

Refer to the exhibit. The security administrator must temporarily disallow traffic that goes to a production web server using the Cisco FDM REST API. The administrator sends an API query as shown in the exhibit. What is the outcome of that action?

- A. The given code does not execute because the mandatory parameters, source, destination, and services are missing.
- B. The given code does not execute because it uses the HTTP method "PUT". It should use the HTTP method "POST".
- C. The appropriate rule is updated with the source, destination, services, and other fields set to "Any" and the action set to "DENY". Traffic to the production web server is disallowed, as expected.
- D. A new rule is created with the source, destination, services, and other fields set to "Any" and the action set to "DENY". Traffic to the production web server is disallowed, as expected.

**Answer: C**

#### NEW QUESTION 17

##### DRAG DROP

A Python script is being developed to return the top 10 identities in an organization that have made a DNS request to "www.cisco.com". Drag and drop the code to complete the Cisco Umbrella Reporting API query to return the top identities. Not all options are used. Select and Place:

```
import requests

URL = 'https://reports.api.umbrella.com/v1/organizations/fe4936f9/
[ ] / [ ] / [ ]',

HEADERS = {'Authorization': 'Basic aGVsb29oYXViYnd5YXNk'}

response = requests.get(URL, headers=HEADERS)
```

security-activity

destinations

activity

www.cisco.com

identities

topIdentities

- A. Mastered
- B. Not Mastered

**Answer: A**

##### Explanation:

```
import requests

URL = 'https://reports.api.umbrella.com/v1/organizations/fe4936f9/
destinations / www.cisco.com / activity',

HEADERS = {'Authorization': 'Basic aGVsb29oYXViYnd5YXNk'}

response = requests.get(URL, headers=HEADERS)
```

security-activity

destinations

activity

www.cisco.com

identities

topIdentities

#### NEW QUESTION 19

Which two destinations are supported by the Cisco Security Management Appliance reporting APIs? (Choose two.)

- A. email
- B. Microsoft Word file
- C. FTP
- D. web
- E. csv file

**Answer: AD**

### NEW QUESTION 22

What are two capabilities of Cisco Firepower Management Center eStreamer? (Choose two.)

- A. eStreamer is used to get sources for intelligence services.
- B. eStreamer is used to send malware event data.
- C. eStreamer is used to get a list of access control policies.
- D. eStreamer is used to send policy data.
- E. eStreamer is used to send intrusion event data.

**Answer: BE**

### NEW QUESTION 25

```
import requests

URL =
'https://sma.cisco.com:6080/sma/api/v2.0/reporting/web_malware_category_malware_name_user_detail/
blocked_malware?startDate=2019-03-14T02:00+00:00&endDate=2019-04-14T01:00+00:00&
filterValue=23&filterBy=na&filterOperator=is&device_type=wsa'

HEADERS = {'Authorization': "Basic Y2hlcGFLYWJSQSZe"}

response = requests.get(URL, headers=HEADERS)
```

Refer to the exhibit.

What must be present in a Cisco Web Security Appliance before the script is run?

- A. reporting group with the name web\_malware\_category\_malware\_name\_user\_detail
- B. data for specified dates
- C. reporting group with the name blocked\_malware
- D. data in the queried category

**Answer: A**

### NEW QUESTION 27

The Cisco Security Management Appliance API is used to make a GET call using the URI  
 /sma/api/v2.0/reporting/mail\_incoming\_traffic\_summary/detected\_amp?startDate=2016-09-10T19:00:00.000Z&endDate=2018-0924T23:00:00.000Z&device\_type=esa&device\_name=esa01.

What does this GET call return?

- A. values of all counters of a counter group, with the device group name and device type for web
- B. value of a specific counter from a counter group, with the device name and type for email
- C. value of a specific counter from a counter group, with the device name and type for web
- D. values of all counters of a counter group, with the device group name and device type for email

**Answer: D**

### NEW QUESTION 32

DRAG DROP

Drag and drop the code to complete the Cisco Umbrella Investigate WHOIS query that returns a list of domains that are associated with the email address "admin@example.com". Not all options are used.

Select and Place:

"https://investigate.api.umbrella.com/  /

/  "

email	emails	WHOIS
admin@example.com	whois	{admin@example.com}

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

"https://investigate.api.umbrella.com/ WHOIS /

emails / admin@example.com "

email	emails	WHOIS
admin@example.com	whois	{admin@example.com}

**NEW QUESTION 36**

Which two commands create a new local source code branch? (Choose two.)

- A. git checkout -b new\_branch
- B. git branch -b new\_branch
- C. git checkout -f new\_branch
- D. git branch new\_branch
- E. git branch -m new\_branch

**Answer:** AD

**NEW QUESTION 39**

Which header set should be sent with all API calls to the Cisco Stealthwatch Cloud API?

- A. Content-Type: application/json  
Accept: application/json  
Authorization: Bearer <api\_key>
- B. Content-Type: application/json  
Accept: application/json  
Authorization: ApiKey <username>:<api\_key>
- C. Content-Type: application/json  
Accept: application/json  
Authorization: Basic <api\_key>
- D. Content-Type: application/json  
Accept: application/json  
Authorization: <username>:<api\_key>

**Answer:** B

**NEW QUESTION 40**

Refer to the exhibit. A network operator wrote a Python script to retrieve events from Cisco AMP.

```
import requests
CLIENT_ID = 'a1b2c3d4e5f6g7h8i9j0'
API_KEY = 'a1b2c3d4-e5f6-g7h8-i9j0-k112m3n4o5p6'
----MISSING CODE----
URL = BASE_URL+'v1/events'
request = requests.get(url, auth=(amp_client_id, amp_api_key))
```

Against which API gateway must the operator make the request?

- A. BASE\_URL = "https://api.amp.cisco.com"
- B. BASE\_URL = "https://amp.cisco.com/api"
- C. BASE\_URL = "https://amp.cisco.com/api/"
- D. BASE\_URL = "https://api.amp.cisco.com/"

**Answer:** A

**NEW QUESTION 43**

What is the purpose of the snapshot APIs exposed by Cisco Stealthwatch Cloud?

- A. Report on flow data during a customizable time period.
- B. Operate and return alerts discovered from infrastructure observations.
- C. Return current configuration data of Cisco Stealthwatch Cloud infrastructure.
- D. Create snapshots of supported Cisco Stealthwatch Cloud infrastructure.

**Answer:** B

**NEW QUESTION 44**

Which query parameter is required when using the reporting API of Cisco Security Management Appliances?

- A. device\_type
- B. query\_type
- C. filterValue
- D. startDate + endDate

**Answer:** D

**NEW QUESTION 46**

Which step is required by Cisco pxGrid providers to expose functionality to consumer applications that are written in Python? A. Look up the existing service using the /pxgrid/control/ServiceLookup endpoint.

- A. Register the service using the /pxgrid/control/ServiceRegister endpoint.
- B. Configure the service using the /pxgrid/ise/config/profiler endpoint.
- C. Expose the service using the /pxgrid/ise/pubsub endpoint.

**Answer:** D

**NEW QUESTION 50**

.....



## 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

### 300-735 Practice Exam Features:

- \* 300-735 Questions and Answers Updated Frequently
- \* 300-735 Practice Questions Verified by Expert Senior Certified Staff
- \* 300-735 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* 300-735 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 300-735 Practice Test Here](#)**