DevNet Associate (Version 1.0) – Module 8 Exam Answers

itexamanswers.net/devnet-associate-version-1-0-module-8-exam-answers.html

January 17, 2021

Module 8: Cisco Platforms and Development Exam Answers

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

DevNet Associate (Version 1.0) – DevNet Associate Module 8 Exam Answers

1. Which underlying technology makes it possible for Cisco Umbrella to prevent a user from accessing a blocked site?

- **DNS**
- HTTP and HTTPS
- Cisco Firewall
- DHCP

Explanation: Cisco Umbrella uses Domain Name Servers (DNS) to enforce security on the network. Umbrella blocks access to malicious domains, URLs, IPs, and files. The system looks at the nature of any DNS requests and takes an action based on its threat intelligence, which is a large-scale repository of historical data about threats. These requests can be deemed safe and allowed, malicious and blocked, or risky and sent to a proxy server for deeper inspection.

2. Which language is used by the NETCONF protocol to encode both the configuration data and protocol messages?

- **XML**
- YAML
- HTML
- JSON

Explanation: The NETCONF protocol uses an Extensible Markup Language (XML) based data encoding for both the configuration data and the protocol messages.

3. What are the three main capabilities provided by Cisco AMP? (Choose three.)

- annihilation
- **detection**
- **responses and automation**
- redirection
- relaying
- **prevention**

Explanation: There are three main categories of capabilities that AMP offers:
Prevention – protects against identified threats in malware files by preventing breaches
Detection – continuously monitors and records all file activity to detect malware
Responses and automation – accelerates investigations and automatically remediates malware across PCs, Macs, Linux, servers, and mobile devices (Android and iOS).

4. Which three functions are provided by Cisco Finesse REST APIS? (Choose three.)

- **They can be used to integrate into existing applications to add contact center functionality.**
- They can be used to get termination call detail (TCD) reports.
- They can be used to get the call history of an agent.
- **They can be used to build a fully functioning agent desktop.**
- They can be used to build custom OpenSocial gadgets.
- **They can be used to build a script to automate tasks.**

Explanation: The Finesse REST APIs can be used to build a fully functioning agent desktop, integrate into existing applications to add contact center functionality, and build a script to automate tasks.

5. Which two benefits are provided by the Python-based WebEx Teams SDK? (Choose two.)

- It integrates with the Webex Devices API.
- **It provides error reporting.**
- It provides access to more API calls within Webex Teams.
- **It manages requests with pagination.**
- It is better supported than the Webex Teams APIs.

Explanation: The SDK, available at GitHub as webexteamssdk, automatically handles pagination, simplifies authentication, provides built-in error reporting, and manages file attachments.

6. Refer to the exhibit. Which data format is used to describe the list of interfaces?

- JSON
- **YANG**
- XML
- YAML

```
list interface {
     key "name";
     leaf name {
            type string;
     }
     leaf speed {
            type enumeration {
                enum 10m;
                enum 100m;
                enum auto;
            }
     }
     leaf observed-speed {
            type uint32;
            config false;
     }
}
```


Explanation: YANG models use a tree structure. Within that structure, the models are similar in format to XML and are constructed in modules. These modules are hierarchical in nature and contain all the different data and types that make up a YANG device model.

7. Which two statements describe the usage of Cisco Finesse JavaScript APIs? (Choose two.)

- They can be used to get the call history of an agent.
- They can be used to build custom gadgets to be placed into applications other than Finesse.
- **They can be used to embed existing web pages into a custom gadget.**
- **They can be used to build a custom gadget for the agent state workflow.**
- They can be used to build a fully functioning agent desktop.

Explanation: The Finesse JavaScript APIs can be used to embed existing web pages into a custom gadget and build a custom gadget for the agent state workflow. The Finesse JavaScript APIs can only be used for gadgets in the out-of-the-box Finesse agent and supervisor desktop.

8. Why does the Meraki dashboard API return a 404 rather than a 403 code in response to a request with an invalid API key?

- The 404 return code determines whether unauthorized users will try again.
- The 403 return code would indicate that the client definitely has an invalid API key.
- **The 404 return code prevents the system from indicating the existence of resources to unauthorized users.**

- The 403 return code would indicate that there are no resources at that endpoint but the API key could be correct.

Explanation: Fo the Meraki Dashboard API, every request must specify an API key via a request header. The API will return a 404 (rather than a 403) code in response to a request with a missing or incorrect API key. This behavior prevents leaking even the existence of resources to unauthorized users.

9. What does Cisco ISE do when it identifies a user or device accessing the network?

- It logs the access attempt.
- **It automatically and securely places the device and user into the right part of the network.**
- It processes the originating IP address according to a whitelist.
- It quarantines the device and user until an administrator releases the quarantine.

Explanation: Cisco ISE identifies every single device and user accessing the network whether the device connects to a wired or wireless network or is on a remote network. Once identified, the connecting device and user are then automatically and securely placed into the right part of the network. This segmentation offers efficiency gains as one network can be used for two separate organizations. It enables secure wired access while also giving asset visibility.

10. How are service profiles used by Cisco UCS Manager?

- Cisco USC Manager uses an assigned service profile to each instance to define network policy.
- **Cisco UCS Manager uses service profiles to assign a unique identity to the server associated with each profile.**
- Cisco UCS Manager saves service profiles to recover servers in case of data loss.
- Cisco UCS Manager uses service profiles as templates to provision policies to multiple versions of the same server.

Explanation: Cisco UCS Manager uses service profiles to assign an identity to a server. Each profile can have a unique address and identifier. Each UCS server can only have one service profile association at a time.

11. Which function does the AXL interface provide for users?

- **provisions and manages objects in the Unified Communication Management Administration Console**
- looks up the top ten OWASP vulnerabilities and identifies which endpoints are vulnerable

- updates network device configurations with a rollback mechanism
- provisions Webex Devices and customizes each display

Explanation: The Administrative XML Web Service (AXL) is an XML/SOAP based interface that provides a mechanism for inserting, retrieving, updating, and removing data from the Unified Communication configuration database.

12. What are three primary YANG sources in Cisco NSO? (Choose three.)

- mapping model
- **data models from devices**
- **NSO data model**
- configuration models
- communication model
- **YANG service models**

Explanation: In Cisco NSO, there are three primary YANG sources:
NSO data model – defining the built-in functions of NSO.
Data models from devices – such as native YANG modules from NETCONF devices, generated YANG modules from SNMP MIBs, or reverse engineered YANG modules from a CLI device.
YANG service models – When developing service applications, a developer specifies the service model, such as a BGP peer, firewall setting, or MPLS VPN, in YANG.

13. What are two tasks a network administrator can perform with Cisco UCS Director? (Choose two.)

- Manage multiple Cisco UCS Manager appliances.
- **Deploy and add capacity to converged infrastructures in a consistent and repeatable manner.**
- Load-balance data traffic.
- **Create, clone, and deploy service profiles and templates for all Cisco UCS servers and compute applications.**
- Create a direct line of communication between Cisco and non-Cisco components.

Explanation: Cisco UCS Director extends the unification of computing and networking layers through Cisco UCS to provide visibility and management of data center infrastructure components. A network administrator can use Cisco UCS Director to configure, administer, and monitor supported Cisco and non-Cisco components. The administrator can use UCS Director to perform the following tasks:
Create, clone, and deploy service profiles and templates for all Cisco UCS servers and compute applications.
Monitor organizational usage, trends, and capacity across a converged infrastructure on a continuous basis.

Deploy and add capacity to converged infrastructures in a consistent, repeatable manner.
Manage, monitor, and report on data center components, such as Cisco UCS domains or Cisco Nexus network devices.
Extend virtual service catalogs to include services for your physical infrastructure.
Manage secure multitenant environments to accommodate virtualized workloads that run with nonvirtualized workloads.

14. What are two actions taken by Firepower for traffic control? (Choose two.)

- **using security intelligence data to filter traffic, including IP addresses, address blocks, domain names, and URLs**
- **controlling which websites are available to the users on the network**
- shutting down the network in the event of a DDOS attack
- directing heavy data traffic to free servers
- load balancing during high-traffic time periods

Explanation: Firepower takes multiple actions for traffic control including these:
Inspecting, logging, and acting on network traffic.
Using security intelligence data to filter traffic. A network administrator can create lists of blocked and allowed IP addresses or address blocks, domain names, or URLs.
Controlling which websites are available to users on the network.
Blocking or filtering certain files based on lists containing data about the files.
Rate limiting network traffic based on access control.
Creating protective measures to redirect traffic to a “sinkhole server”, where the firewall can fake a DNS query response for a known malicious domain.

15. What are two types of YANG models? (Choose two.)

- **native model**
- vendor model
- private model
- hybrid model
- **open model**

Explanation: There are two types of YANG models:
Open models – Developed by vendors and standards bodies, such as IETF, ITU, OpenConfig. They are designed to be independent of the underlying platform and normalize the per-vendor configuration of network devices.
Native models – Developed by vendors, such as Cisco. They relate and are designed to integrate to features or configuration only relevant to that platform.