# Cisco Certified DevNet Associate (200-901 DEVASC) Practice Test (Sample)

## Study Guide


**Everything you need from our exam experts!**

# Questions

**1. What do SSL and TLS primarily provide?**

**A. Encryption of database access**

**B. Data transfer authentication**

**C. User authentication for websites**

**D. Network monitoring and analysis**

**2. What kind of data can you pass to a remote server using Curl's -d option?**

**A. Only text data**

**B. Only binary data**

**C. JSON formatted data**

**D. Both strings and files**

**3. What does the 'from' keyword indicate when importing in Python?**

**A. It allows module renaming**

**B. It suggests importing all available methods**

**C. It specifies a subset of a module to import**

**D. It restricts access to private methods**

**4. How do you verify that a specific error is raised in unittest?**

**A. assertError(ValueError)**

**B. self.assertRaises(ValueError, function)**

**C. self.checkRaises(ValueError, function)**

**D. assertRaises(ValueError, function)**

**5. What role does the CDB play in Cisco NSO?**

**A. It provides a secure logging system**

**B. It stores critical operations**

**C. It maintains all platform data in a RAM database**

**D. It functions as a user interface**

**6. What best describes XML?**

**A. HyperText Markup Language**

**B. Extensible Markup Language**

**C. Database Query Language**

**D. Simple Markup Language**

**7. What is the term for applying Lean principles to software development?**

**A. Scrum**

**B. Kanban**

**C. Agile**

**D. Extreme Programming**

**8. What transport protocol does DHCP utilize?**

**A. TCP**

**B. UDP**

**C. SCTP**

**D. ICMP**

**9. Which component of Cisco SD-WAN is responsible for managing the control plane?**

**A. vManage**

**B. vEdge**

**C. vSmart**

**D. vBond**

**10. What type of attack does CSRF qualify as?**

**A. Data breach attack**

**B. Unauthorized access attack**

**C. Session hijacking attack**

**D. Injection attack**

# Answers

**1. B**
**2. D**
**3. C**
**4. B**
**5. C**
**6. B**
**7. C**
**8. B**
**9. C**
**10. C**

# Explanations

## 1. What do SSL and TLS primarily provide?

**A. Encryption of database access**

**B. Data transfer authentication**

**C. User authentication for websites**

**D. Network monitoring and analysis**

**SSL (Secure Sockets Layer) and TLS (Transport Layer Security) primarily provide data transfer authentication along with encryption to ensure secure communication over a network, typically the internet. They are cryptographic protocols designed to protect data transmitted between clients and servers, ensuring that the data remains confidential and intact during transfer. When SSL and TLS are implemented, they authenticate the identity of the communicating parties through certificates, helping to prevent impersonation (man-in-the-middle attacks). This validation process allows clients to verify the legitimacy of the server they are connecting to, establishing trust in secure transactions, such as online banking or shopping. While SSL and TLS contribute to user authentication indirectly—by ensuring that only legitimate parties can communicate—they do not directly provide user authentication in the way that, for example, username and password mechanisms do. Instead, their primary role is in securing the data as it moves across the network while authenticating the sender and receiver of that data, reinforcing trust in the connection.**

## 2. What kind of data can you pass to a remote server using Curl's -d option?

**A. Only text data**

**B. Only binary data**

**C. JSON formatted data**

**D. Both strings and files**

**Using Curl's -d option allows you to send both strings and files to a remote server. The -d flag is typically used to send data in a POST request when communicating with a web server. The data you pass can be in various formats, including plain text strings, URL-encoded strings, or even the contents of files when specified correctly. For example, if you use the -d option with text data, such as key-value pairs ("key=value"), it sends that data as part of the request body. Additionally, you can specify files to be uploaded as well, enhancing the breadth of scenarios where -d can be utilized. This flexibility ensures that developers can work with various data types and use cases, making Curl a powerful tool for HTTP requests and interactions with APIs.**

## 3. What does the 'from' keyword indicate when importing in Python?

**A. It allows module renaming**

**B. It suggests importing all available methods**

**C. It specifies a subset of a module to import**

**D. It restricts access to private methods**

**The 'from' keyword in Python is used to specify a subset of a module to import. This allows you to import specific functions, classes, or variables directly from a module rather than importing the entire module. For example, if you have a module named `math`, using 'from math import sqrt' allows you to use the `sqrt` function directly without needing to prefix it with the module name (like `math.sqrt`). By importing only the specific components you need, your code can be more efficient and clear, as it directly implies to the reader what functions or classes are being used. This also helps to avoid potential naming conflicts with other imported modules or functions. In contrast, the other options involve details that do not accurately reflect the purpose of the 'from' keyword in import statements. Renaming modules typically involves the 'as' keyword, suggesting importing all methods would use an asterisk (*) syntax, and restricting access to private methods pertains to object-oriented programming principles rather than module importation.**

## 4. How do you verify that a specific error is raised in unittest?

**A. assertError(ValueError)**

**B. self.assertRaises(ValueError, function)**

**C. self.checkRaises(ValueError, function)**

**D. assertRaises(ValueError, function)**

**To verify that a specific error is raised in Python's unittest framework, utilizing `self.assertRaises(ValueError, function)` is the correct approach. This method is designed to catch an exception during the execution of a function call and allows for verification that the expected exception is indeed raised. When `self.assertRaises` is used, you specify the type of exception you expect (in this case, `ValueError`) and then provide the function that is expected to raise this exception. If the function does raise the specified exception, the test passes. If it does not, or if it raises a different exception, the test fails. This built-in framework simplifies the process of error checking and makes your tests more readable and maintainable. The correct implementation of this functionality ensures that you not only check for errors in your code but also that your assertions are clear and aligned with Python's intended usage of exceptions. The focus here is on validating that the expected exception is raised, making it a fundamental aspect of writing robust and reliable unit tests.**

## 5. What role does the CDB play in Cisco NSO?

**A. It provides a secure logging system**

**B. It stores critical operations**

**C. It maintains all platform data in a RAM database**

**D. It functions as a user interface**

**In Cisco Network Services Orchestrator (NSO), the CDB, or the Configuration Database, serves as an essential component that maintains all platform data in a RAM database. The CDB is designed for quick access and efficient data handling, allowing NSO to effectively manage the configuration and operational state of network devices. By utilizing a RAM database, the CDB enables high-speed read and write operations, which are crucial for orchestrating network services in real-time. The use of RAM ensures that the data stored can be processed rapidly, which is vital in dynamic network environments where changes need to be enacted quickly and reliably. Furthermore, the CDB plays a pivotal role in maintaining the desired state of the network, providing a synchronized view of configurations across devices, and facilitating the automation of network tasks. This understanding highlights the importance of the CDB in the context of Cisco NSO's architecture and its functionality within network management.**

## 6. What best describes XML?

**A. HyperText Markup Language**

**B. Extensible Markup Language**

**C. Database Query Language**

**D. Simple Markup Language**

**The description of XML as Extensible Markup Language is accurate because XML is designed specifically to facilitate the transportation and storage of data in a structured format that is both human-readable and machine-readable. It allows developers to create custom tags that define the data, making it flexible for a wide array of applications. XML's extensibility is one of its key strengths, enabling users to define their own tags and structure based on the requirements of the data's context, rather than being limited to a predefined set of tags as seen in HTML. This characteristic makes XML highly suitable for data interchange between systems, allowing different applications to communicate effectively and share data regardless of their underlying platforms or technologies. The other options describe different technologies or methods: HyperText Markup Language is specific to creating and structuring content on the web, Database Query Language relates to querying databases, and Simple Markup Language does not have a defined standard in the context of structured data representation. Therefore, defining XML as Extensible Markup Language captures its primary attributes and purpose accurately.**

## 7. What is the term for applying Lean principles to software development?

**A. Scrum**

**B. Kanban**

**C. Agile**

**D. Extreme Programming**

**The term for applying Lean principles to software development is Agile. Agile is a methodology that emphasizes flexibility, collaboration, and customer-centric development, which aligns closely with Lean principles that focus on minimizing waste and maximizing value. Agile promotes iterative development, allowing for incremental delivery and ongoing feedback, which helps teams adapt quickly to changes and improve the efficiency of their workflows. The root philosophies of Lean thinking, such as reducing cycle times and improving overall quality, are fundamental to Agile practices. This methodology encourages a mindset of continuous improvement, mirroring the Lean approach. While other methodologies like Scrum and Kanban are frameworks within Agile, they are not synonymous with Lean principles themselves. Scrum is a specific Agile framework that uses fixed-length iterations, while Kanban focuses on visualizing work and managing flow, making them tools to implement Agile rather than definitions of the Lean approach to software development. Extreme Programming (XP) involves Agile practices but also introduces specific engineering techniques, dressing it up in a unique set of practices. Overall, Agile as a whole is the broader category that encompasses Lean principles applied to software development.**

## 8. What transport protocol does DHCP utilize?

**A. TCP**

**B. UDP**

**C. SCTP**

**D. ICMP**

**Dynamic Host Configuration Protocol (DHCP) uses the User Datagram Protocol (UDP) as its transport protocol. The reason for using UDP is that DHCP is designed to be a lightweight protocol that facilitates the assignment of IP addresses and configuration settings to devices on a network. UDP is a connectionless protocol, which means it allows for faster transmission without the overhead of establishing a connection, making it suitable for the quick request-response nature of DHCP operations. Specifically, DHCP operates over UDP using port 67 for the server and port 68 for the client. This allows client devices to send packets to the server without requiring a prior handshake, enabling rapid deployments of network configurations. This efficiency is vital in environments where devices frequently connect and disconnect from the network. The other transport protocols listed are not suitable for the design and functioning of DHCP. TCP, which is connection-oriented, would introduce unnecessary overhead for the simple task of lease requests and responses. SCTP is also a connection-oriented protocol that is used in more complex situations, while ICMP is primarily used for error reporting and diagnostic functions within IP networks, such as in ping operations and not suited for carrying DHCP messages.**

## 9. Which component of Cisco SD-WAN is responsible for managing the control plane?

**A. vManage**

**B. vEdge**

**C. vSmart**

**D. vBond**

**The component responsible for managing the control plane in Cisco SD-WAN is the vSmart controller. The vSmart controllers are the central entities that manage the distribution of information about network paths, topology, and security policies throughout the SD-WAN. They facilitate secure communication between the devices in the network by establishing and maintaining control plane connections. In the role of control plane management, the vSmart controllers handle tasks such as maintaining routing information and providing the necessary configurations to the vEdge routers, which are the data plane components. This separation of control and data planes helps to optimize performance and security in the network. Understanding this functionality is critical because it distinguishes between the various components in the Cisco SD-WAN architecture. While other components like vManage focus on network management and monitoring, and vBond assists in the initial establishment of secure connections between devices, it is the vSmart controllers that fundamentally manage the control plane, ensuring efficient communication and policy enforcement across the entire SD-WAN infrastructure.**

## 10. What type of attack does CSRF qualify as?

**A. Data breach attack**

**B. Unauthorized access attack**

**C. Session hijacking attack**

**D. Injection attack**

**Cross-Site Request Forgery (CSRF) is categorized as a session hijacking attack. In CSRF, an attacker tricks a victim into unknowingly submitting a request to a web application where they are authenticated, effectively making the request with the victim's credentials or session. This manipulation occurs without the victim's consent, leading to actions being executed in the context of their active session, hence "hijacking" their session to perform unauthorized actions. Understanding CSRF's nature as a session hijacking attack is critical in web security. It exploits the trust that a site has in an authenticated user rather than directly targeting the user's data, unlike a data breach. While data breaches focus on unauthorized access to sensitive data, unauthorized access attacks typically involve gaining entry to a system or network without permission but do not necessarily involve exploiting an existing authenticated session. Similarly, injection attacks involve inserting malicious code into an application, which is a different vector than what CSRF employs. Therefore, recognizing CSRF as a session hijacking attack clarifies its mechanisms and highlights the importance of implementing anti-CSRF measures, like token validation, to protect against such vulnerabilities.**