

# DevNet Associate (Version 1.0) – Module 6 Exam Answers

 [itexamanswers.net/devnet-associate-version-1-0-module-6-exam-answers.html](https://itexamanswers.net/devnet-associate-version-1-0-module-6-exam-answers.html)

January 17, 2021

## Module 6: Application Deployment and Security 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 6 Exam Answers

### 1. Which technique is used to help mitigate SQL injection attacks?

- using the same owner or admin account in the web applications to connect to the database
- **limiting the read access to specific fields of a table or joins of tables**
- using stored procedures with the “db\_owner” default role
- assigning DBA or admin access rights to the application account

**Explanation:** Recommended practices for defending against SQL injection include the following:

Not assigning DBA or admin type access rights to application accounts

Avoid using the same owner/admin account in the web applications to connect to the database

Limiting the read access to specific fields of a table or joins of tables

Not assigning db\_owner rights to stored procedures

### 2. Which security device is used to make responses to client requests look like they all come from the same server?

- stateful firewall
- forward proxy
- **reverse proxy**
- jump box

**Explanation:** The job of a reverse proxy is to make sure responses look like they all come from the same server. This is the opposite of a forward proxy, which makes requests from multiple computers look like they all come from the same client.

### **3. What is a characteristic of a virtual machine running on a PC?**

- A virtual machine needs a physical network adapter to connect to the Internet.
- **A virtual machine runs its own operating system.**
- The number of virtual machines that can be made available depends on the software resources of the host machine.
- A virtual machine is not susceptible to threats and malicious attacks.

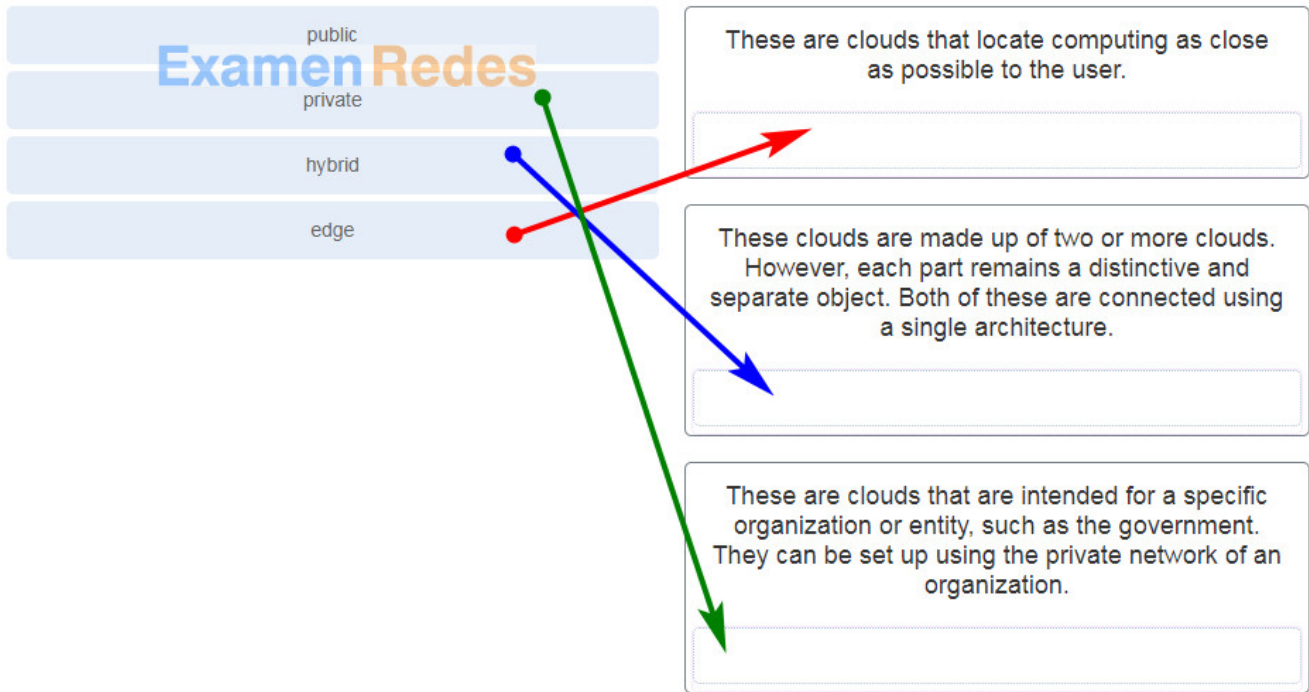
**Explanation:** Each virtual machine runs its own operating system. The number of virtual machines that can be made available depends on the hardware resources of the host machine. Virtual machines are susceptible to threats and malicious attacks, like physical computers. To connect to the Internet, a virtual machine uses a virtual network adapter, that acts like a physical adapter in a physical computer, connecting through the physical adapter on the host to establish a connection to the Internet.

### **4. What is a characteristic of the blue-green upgrade deployment strategy?**

- **A new environment is created with the new code in it, while the old environment is held in reserve in case users experience problems.**
- The code changes are periodically rolled out in such a way that they do not impact current users.
- The new code is deployed all at once to the old environment. If users experience no issues, it is then moved to the new environment.
- The new code version is first rolled out to a subset of users. Changes can then be rolled back if the users experience any problems.

**Explanation:** With a blue-green deployment, an entirely new environment (blue) is created with the new code in it. The old environment (green) is held in reserve so if users in the new environment experience problems, traffic can be diverted back to the original environment. If there are no problems, the new environment becomes the production environment.

### **5. Match the cloud model to its description. (Not all options are used.)**



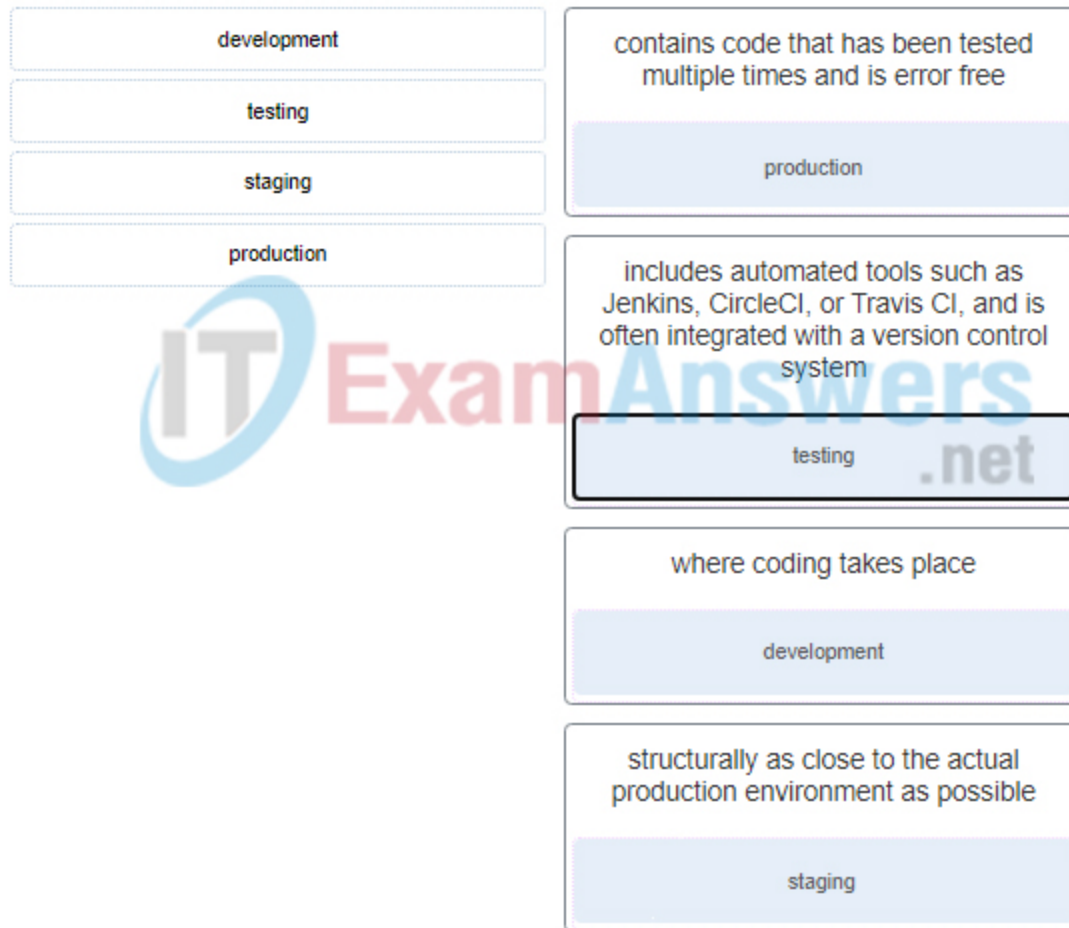
DevNet Associate (Version 1.0) – DevNet Associate Module 6 Exam 1

## 6. Which mitigation method is effective against cross-site scripting?

- requiring multifactor authentication
- consistent hardening of systems and applications
- **sanitizing untrusted content**
- using only necessary features and secure packages downloaded from official sources and verified with a signature

**Explanation:** Cross-site scripting occurs when an attacker uses the dynamic functions of a site to inject malicious content into a page. Mitigating the attacks requires careful consideration of where untrusted content is included on a page, as well as sanitizing any untrusted content.

## 7. Match the environments in the four-tier development environment structure to the description.



**8. Which attack involves the insertion of malicious code into SQL statements?**

- **SQL injection**
- cross-site scripting
- brute force
- local file inclusion

**Explanation:** SQL injection (SQLi) is basic web application attack technique where the attacker places malicious SQL code into a field on a web page and the server-side code submits it to the database without sanitizing it first. An SQLi attack, if successful, can delete or change sensitive data or reveal it to the attacker.

**9. In software development, what is the purpose of a jump box?**

- **to act as a single trusted machine used to launch connections to sensitive systems**
- to make all requests originating from within a network look like they come from the same source IP address
- to filter packets based on Layer 3 and Layer 4 addressing
- to receive incoming requests and forward them to multiple servers

**Explanation:** A jump box is a server that users must first access in order to launch a connection to a target system. Because the jump box is the trusted machine for accessing sensitive systems, it provides an additional layer of security.

**10. Which characters are used to separate batched SQL statements?**

- **semicolons ;**
- colons :
- parentheses ()
- pound signs #

**Explanation:** A batch of SQL statements is a group of two or more SQL statements separated by semicolons.

**11. What is a philosophy for software deployment used in the field of DevOps?**

- OWASP
- DevNet
- SOAP
- **CI/CD**

**Explanation:** CI/CD (continuous integration/continuous delivery) is a philosophy for software deployment that figures prominently in the field of DevOps.

**12. Which statement is a characteristic of the broken access control threat to web applications?**

- It allows attackers to access, and potentially change, serialized versions of data and objects.
- It allows an attacker to use the dynamic functions of a site to inject malicious content into the page.
- **It allows users to circumvent existing authentication requirements.**
- It allows attackers to steal sensitive information such as passwords or personal information.

**Explanation:** Broken access control can occur if a developer builds an application that enables users to circumvent existing authentication requirements. Developers must make sure to protect all resources and functions that need to be protected on the server side, ensuring that all access is authorized.

**13. Which technology is used to containerize applications and allows them to run in a variety of environments?**

- **Docker**
- GitHub

- VirtualBox
- Cisco DNA

**Explanation:** Docker is a technology designed to make it easier to create, deploy, and run applications by using containers. Containers allow a developer to package an application with all of the parts the application needs to run in most any environment.

**14. Match the OWASP resource with a description.**

Dependency Check	explains ways to mitigate command security issues in web applications
ModSecurity Core Rule Set	Cheat Sheet Series
Cheat Sheet Series	looks for known vulnerabilities in code
DefectDojo	Dependency Check
	streamlines the code testing process
	DefectDojo
	generic attack detection rules used with web application firewalls
	ModSecurity Core Rule Set

**15. What is used to isolate the different parts of a running container?**

- wrappers
- **namespaces**
- control groups
- union file systems

**Explanation:** Containers use namespaces to define and isolate each part of an application within a container.