14.4.9 Lesson Review

Candidate: Richard Habib (richard_habib1)
Date: 12/3/2024, 9:59:46 AM • **Time Spent:** 19:49

Score: 100%

Passing Score: 80%

Question 1. ✓ Correct

Why is Infrastructure as Code important for cloud technologies?

○ It simplifies the physical maintenance of cloud servers.

○ It reduces the bandwidth required for cloud services.

○ It enables manual configurations to be more reliable.

→ ● It encourages the use of scripted approaches to provisioning.

Explanation

IaC is crucial for cloud technologies because it leverages scripted, automated approaches for provisioning and managing cloud resources. This ensures faster, more reliable, and consistent deployments compared to manual configurations.

IaC deals with virtual rather than physical aspects of cloud servers.

IaC aims to replace manual configurations with automation for reliability.

IaC's importance lies in automation and efficiency, not in reducing bandwidth usage.

References

14.4.1 Infrastructure as Code

q_iac_cloud_technology_n09.question.fex

Question 2. ✓ Correct

What is the role of automation playbooks in Infrastructure as Code?

○ To document manual configuration steps for engineers

→ ● To automate configuration or build tasks using code blocks

○ To increase the need for human intervention in automated processes

○ To provide a graphical interface for infrastructure management

Explanation

Automation playbooks in IaC are used to script configuration or build tasks, allowing for automation and standardization. These playbooks take standard arguments and perform tasks in a consistent manner, reducing errors and ensuring compliance with policies.

Playbooks are used for automation, not for documenting manual steps.

Playbooks are code-based tools for automation, not graphical interfaces.

The aim of automation playbooks is to reduce, not increase, the need for human intervention.

References

14.4.1 Infrastructure as Code

q_iac_playbook_role_n09.question.fex

Question 3. ✓ Correct

Why are upgrades considered complex in infrastructure as code environments?

○ They require manual intervention.

→ ● They can introduce unforeseen impacts.

○ They are less secure.

○ They are time-consuming.

Explanation

Upgrades can change system behavior in unexpected ways, affecting compatibility and functionality. This complexity necessitates careful planning and testing.

Automation can reduce the need for manual work in upgrades.

While they can be time-consuming, the complexity and potential for unforeseen impacts are more significant concerns.

Security levels depend on the specific changes made during an upgrade, not the upgrade process itself.

References

14.4.2 Uses for Infrastructure as Code

q_automation_upgrades_complex_n09.question.fex

Question 4. ✓ Correct

What does a pull request in source control signify?

- ○ A request for increasing storage space on the repository server
- → ● A request to merge branch code back into the main branch
- ○ A request to delete a branch
- ○ A request to pull the latest version from the repository

Explanation

A pull request is issued by a developer when they want to merge their branch code back into the main branch. It is a key part of the collaborative development process, allowing for code review and validation before merging.

A pull request is not a request to delete a branch but to merge changes.

Pulling the latest version from the repository is a different action and does not involve merging code.

Requests for increasing storage space on the repository server are administrative tasks unrelated to the function of a pull request.

References

14.4.3 Source Control

q_source_control_pull_request_n09.question.fex

Question 5. ✓ Correct

Which server is commonly used to maintain source code in software development environments?

→ ● Repository Server

○ Email Server

○ Web Server

○ FTP Server

Explanation

A repository server, such as Git, is used in software development environments to maintain and manage source code. It allows developers to commit changes, track versions, and collaborate effectively.

FTP servers are used for file transfers and not specifically for maintaining source code.

Email servers manage email communications and are not used for source code management.

Web servers host websites and web applications but do not serve as the central system for source code management.

References

14.4.3 Source Control

q_source_control_repository_server_n09.question.fex

Question 6. ✓ Correct

Which of the following best describes the function of the Northbound API in SDN architecture?

- ○ It is used for peer-to-peer network communication.
- ○ It encrypts data traffic between different network layers.
- → ● It facilitates communication between the SDN controller and network applications.
- ○ It connects the SDN controller to the physical network devices.

Explanation

The Northbound API in SDN architecture is designed to enable communication between the SDN controller and higher-level network applications or business logic. This API allows applications to request network services (such as the creation of a new network segment or the application of specific policies) from the SDN controller, which then translates these requests into configurations for the network devices via the Southbound API.

Connecting the SDN controller to the physical network devices is the role of the Southbound API, which facilitates communication between the SDN controller and the physical or virtual network devices to implement the network policies.

Peer-to-peer communication refers to direct data exchange between network nodes, which is not the purpose of the Northbound API.

Encryption of data traffic is a security function and not the primary role of the Northbound API, which is designed for enabling application-level requests and services.

References

14.4.4 Software-Defined Networking

q_sd_network_northbound_api_n09.question.fex

Question 7. ✓ Correct

Which of the following is a characteristic of SDN?

→ ● Transport agnostic

○ Increased need for manual reconfiguration

○ Application unaware

○ Decentralized policy management

Explanation

Being transport agnostic means that SDN can operate over any underlying network technology, such as Ethernet, Wi-Fi, or cellular networks. This characteristic is crucial for SDN's flexibility and adaptability, allowing it to support a wide range of networking environments and requirements.

SDN is characterized by centralized policy management, where policies are defined and managed centrally rather than distributed across individual devices.

One of the advantages of SDN is the reduction in the need for manual reconfiguration, thanks to centralized management and automation capabilities.

SDN networks are designed to be application-aware, allowing for more intelligent and efficient handling of different types of network traffic.

References

14.4.4 Software-Defined Networking

q_sd_network_sdn_characteristic_n09.question.fex

Question 8. ✓ Correct

How does SD-WAN facilitate secure access to the cloud?

○ By using public Internet exclusively

→ ● Using automation and orchestration

○ By requiring manual setup for each connection

○ Through direct physical connections

Explanation

SD-WAN utilizes automation and orchestration to dynamically provision network links based on application needs and network conditions, ensuring secure and efficient cloud access.

Using public Internet exclusively does not ensure secure access; SD-WAN employs a combination of underlay networks and adds security measures.

Direct physical connections are not the primary method SD-WAN uses for cloud access; it focuses on virtual, dynamic connections.

Manual setup for each connection is contrary to the automated, dynamic nature of SD-WAN.

References

14.4.5 Software-Defined WAN

q_sdwan_automation_orchestration_n09.question.fex

Question 9. ✓ Correct

What is a key feature of the routers, gateways, or VPN apps in an SD-WAN?

→ ● They are SD-WAN capable.

○ They require manual configuration for each site.

○ They function without any form of encryption.

○ They can only operate in a wired environment.

Explanation

Devices in an SD-WAN must be capable of supporting SD-WAN functions, such as dynamic path selection and secure connectivity, to fully participate in the SD-WAN architecture.

Operating only in a wired environment limits the flexibility and the potential of SD-WAN, which can also use wireless connections.

Requiring manual configuration for each site contradicts the automated, dynamic nature of SD-WAN.

Functioning without any form of encryption would compromise the security of the SD-WAN, which is not the case as security is a key feature.

References

14.4.5 Software-Defined WAN

q_sdwan_routers_gateways_sd-wan_n09.question.fex

Question 10. ✓ Correct

What protocol can be used alongside VXLAN for automated configuration and management of the overlay network?

○ SSH

→ ● EVPN

○ FTP

○ HTTP

Explanation

Ethernet VPN (EVPN) can be used with VXLAN to provide a control plane for automated configuration and management, using Border Gateway Protocol (BGP) to advertise VXLAN networks and nodes as routes.

HTTP is a protocol for transferring hypertext requests and information on the Internet, not for network configuration management.

SSH is a protocol for secure system administration and file transfers over insecure networks, not specifically for overlay network management.

FTP is used for the transfer of files between a client and server on a network, not for managing overlay networks.

References

14.4.6 Overlay Networks

q_overly_networks_vxlan_evpn_n09.question.fex

Question 11. ✓ Correct

What technology is typically used inside data centers to implement overlay networks?

→ ● VXLAN

○ BGP

○ OSPF

○ MPLS

Explanation

VXLAN (Virtual Extensible LAN) is commonly used in data centers to implement overlay networks. It allows for the creation of a logical network on top of a physical network using layer 2 encapsulation over a layer 3 IP network.

MPLS is used for creating efficient, scalable networks, not specifically for data center overlay networks.

OSPF is a routing protocol, not a technology for implementing overlay networks.

BGP is used for routing decisions on the Internet and within large networks; while it can work with overlay networks (e.g., with EVPN), it is not the technology that implements the overlay itself.

References

14.4.6 Overlay Networks

q_overly_networks_vxlan_overlay_networks_n09.question.fex

Question 12. ✓ Correct

In ZTA, what does the separation of the control and data planes achieve?

○ Increases the complexity of network management.

→ ● Segregating policy decision-making from data transfer.

○ Enhances the scalability of network infrastructure.

○ Reduces the need for continuous monitoring.

Explanation

This separation ensures that policy decisions are made in a secure environment, isolated from the data plane where data transfer occurs, thereby enhancing the overall security posture.

Increasing the complexity of network management is a potential challenge but not the purpose of the separation.

Enhancing the scalability of network infrastructure, while possible, is not the primary reason for this architectural choice.

Reducing the need for continuous monitoring misinterprets the proactive and dynamic nature of security in ZTA.

References

14.4.7 Zero Trust Architecture

q_zero_trust_control_data_plane_separation_n09.question.fex

Question 13. ✓ Correct

What are the two subsystems of the policy decision point in ZTA?

→ ● Policy engine and policy administrator

○ Data plane and control plane

○ Authentication server and authorization server

○ Threat intelligence and behavioral analytics

Explanation

The policy engine and policy administrator subsystems work together to dynamically make and enforce access decisions, with the policy engine evaluating requests and the policy administrator managing access tokens and sessions.

Data plane and control plane describe the overall architecture of ZTA, not the components of the policy decision point.

Authentication and authorization servers are broader concepts that do not specifically represent the two subsystems within the policy decision point.

Threat intelligence and behavioral analytics are tools used by the policy engine, not separate subsystems of the policy decision point.

References

14.4.7 Zero Trust Architecture

q_zero_trust_decision_point_subsystems_n09.question.fex

Question 14. ✓ Correct

Which of the following is a function of a Cloud Access Security Broker (CASB)?

→ ● Monitors and audits user and resource activity

○ Reduces the cost of cloud storage

○ Directly improves the performance of SD-WAN connections

○ Increases the speed of cloud services

Explanation

Monitoring and auditing user and resource activity is the correct answer. One of the key functions of a CASB is to provide visibility into cloud application usage, monitor user activities, and audit resource accesses. This is crucial for detecting and responding to security threats, ensuring compliance with data protection regulations, and preventing data leaks.

CASBs primarily focus on security aspects rather than enhancing the speed of cloud services. Their role is to enforce security policies between cloud users and cloud applications, which includes monitoring, compliance, and threat protection, but not directly increasing service speeds.

While CASBs can help organizations use cloud services more securely and efficiently, their primary function is not to reduce the cost of cloud storage. They are security tools that manage and protect cloud environments rather than tools designed for cost optimization of storage resources.

CASBs do not directly improve the performance of SD-WAN connections. Their role is to secure access to cloud services by mediating between users and cloud applications, implementing security policies, and providing threat protection. While they may work alongside SD-WAN technologies in a Secure Access Service Edge (SASE) architecture, their primary focus is on security rather than enhancing network performance.

References

14.4.8 Secure Access Service Edge

q_secure_edge_casb_function_n09.question.fex

Question 15. ✓ Correct

How can CASBs be implemented?

○ Only through forward proxies

○ Only through reverse proxies

→ ● Through forward proxies, reverse proxies, and APIs

○ Through VPNs only

Explanation

CASBs can be deployed in various configurations, including forward proxies, reverse proxies, and APIs, to suit different security needs and architectures.

While forward proxies are one method, they are not the only way CASBs can be implemented.

Reverse proxies are another method but not the sole option for CASB deployment.

VPNs are not a method of CASB implementation; they are a separate technology for secure connectivity.

References

14.4.8 Secure Access Service Edge

q_secure_edge_casb_implementation_n09.question.fex

Copyright © The Computing Technology Industry Association, Inc. All rights reserved.