VCE & PDF
https://www.pass4itsure.com/cv0-003.html
Pass4itSure.com

CV0-003^{Q&As}

CompTIA Cloud+ Certification

Pass CompTIA CV0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/cv0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

A company has moved all on-premises workloads into a public cloud. After some time, the cloud engineer starts noticing time drifts on the VMs and suspects an NTP issue. Time drifts were not an issue when all the workloads were on-premises.

Which of the following describes how the cloud engineer should resolve the issue?

A. Implement Coordinated Universal Time on all workloads

B. Point all workloads back to an on-premises NTP server

C. Point all workloads to a stratum 2 within the public cloud provider

D. Configure all of the VMs as NTP servers within the public cloud provider

Correct Answer: A

QUESTION 2

A user reports a poor-quality remote VDI session. Which of the following should the help desk technician do FIRST to troubleshoot the issue?

A. Check the FAQ section of the vendor\'s documentation.

B. Ask the user if the client device or access location has changed.

C. Reboot the user\'s virtual desktop.

D. Request permission to log in to the device remotely.

Correct Answer: B

Asking the user if the client device or access location has changed is what the help desk technician should do first to troubleshoot poor-quality remote VDI (Virtual Desktop Infrastructure) session. VDI is a technology that allows users to access virtual desktops hosted on remote servers over a network or internet connection. VDI can provide users with flexibility, mobility, and security, but it may also introduce quality issues depending on various factors, such as: The client device: This is the device that users use to access their virtual desktops, such as a laptop, tablet, smartphone, etc. The client device can affect VDI quality by determining how well it can support and display virtual desktop applications and services, as well as how fast it can process and send data over a network or internet connection. The access location: This is where users access their virtual desktops from, such as home, office, public place, etc. The access location can affect VDI quality by determining how stable and secure their network or internet connection is, as well as how much latency or interference they may experience. Asking the user if these factors have changed can help to troubleshoot poor-quality remote VDI session by identifying any potential causes or sources of quality issues, as well as suggesting any possible solutions or alternatives.

QUESTION 3

Which of the following is relevant to capacity planning in a SaaS environment?

A. Licensing

B. A hypervisor

C. Clustering

D. Scalability

Correct Answer: D

Scalability is the ability of a system or service to handle increased workload or demand by adding or removing resources or capacity as needed. Scalability is relevant to capacity planning in a SaaS environment, as it can affect the performance, availability, and cost of the SaaS service. Scalability can help optimize the capacity planning process by ensuring that the SaaS service has enough resources or capacity to meet the current and future needs of the customers without wasting or underutilizing resources or capacity. References: CompTIA Cloud+ Certification Exam Objectives, page 12, section 2.2

QUESTION 4

A systems administrator is working within a private cloud environment. Over time. random 4K read/write speeds on all VMS in the environment slow down until the VMS are completely unusable, with disk speeds of less than 1MBps. The

administrator has gathered the information below:

There is no correlation between the slowdown and VM/hypervisor resource utilization.

The network is rated to 40Gbps and utilization is between 1--5%.

The hypervisors use hundreds of NFSv3 mounts to the same storage appliance, one per VM.

The VMS on each hypervisor become unresponsive after two weeks of uptime.

The unresponsiveness is resolved by moving slow VMS onto a rebooted hypervisor.

Which of the following solutions will MOST likely resolve this issue?

A. Increase caching on the storage appliance.

B. Configure jumbo frames on the hypervisors and storage.

C. Increase CPU/RAM resources on affected VMS.

D. Reduce the number of NFSv3 mounts to one.

Correct Answer: D

Explanation: The correct answer is D. Reduce the number of NFSv3 mounts to one.

NFSv3 is a network file system protocol that allows clients to access files stored on a remote server. NFSv3 uses TCP or UDP as the transport layer protocol, and typically runs on port 20491. One of the known issues with NFSv3 mounts is that they can cause performance degradation and unresponsiveness on the client side if there are too many mounts or if there are network connectivity problems. This is because NFSv3 does not handle connection failures or timeouts gracefully, and may keep retrying to access the server indefinitely, blocking other processes or threads. This can result in slow disk speeds, high CPU usage, and system hangs23. Therefore, one of the possible solutions to this issue is to reduce the number of NFSv3 mounts to one per hypervisor, instead of one per VM. This way, the hypervisor can manage the access to the shared storage appliance more efficiently, and avoid creating too many TCP connections or UDP packets that may overload the network or the server. Reducing the number of NFSv3 mounts can also simplify the

configuration and troubleshooting of the network file system. Increasing caching on the storage appliance may improve the read performance of the NFSv3 mounts, but it will not solve the underlying issue of connection failures or timeouts. Caching may also introduce data inconsistency or corruption issues if the cache is not synchronized with the server. Configuring jumbo frames on the hypervisors and storage may improve the network throughput and efficiency of the NFSv3 mounts, but it will not solve the underlying issue of connection failures or timeouts. Jumbo frames are larger than standard Ethernet frames, and require that all devices on the network path support them. Jumbo frames may also introduce fragmentation or compatibility issues if they are not configured properly. Increasing CPU/RAM resources on affected VMs may improve their performance in general, but it will not solve the underlying issue of connection failures or timeouts. Increasing CPU/RAM resources may also be costly and wasteful if they are not needed for other purposes.

QUESTION 5

A cloud administrator is having difficulty correlating logs for multiple servers. Upon inspection, the administrator finds that the time-zone settings are mismatched throughout the deployment. Which of the following solutions can help maintain time synchronization between all the resources?

A. DNS

B. IPAM

C. NTP

D. SNMP

Correct Answer: C

Explanation: The correct answer is C. NTP.

NTP stands for Network Time Protocol, which is a standard protocol for synchronizing the clocks of computers over a network. NTP uses a hierarchical, client-server architecture, where a client requests the current time from a server, and the server responds with a timestamp. The client then adjusts its own clock to match the server\\'s time, taking into account the network delay and clock drift. NTP can achieve sub-millisecond accuracy over local area networks and a few milliseconds over the internet12. NTP can help maintain time synchronization between all the resources in a distributed cloud environment, as it allows each resource to get the accurate time from a reliable source. This can help with correlating logs, auditing, security, and other time-sensitive operations. NTP can also handle different time zones, as it uses Coordinated Universal Time (UTC) as the reference time, and each resource can convert UTC to its local time zone12. DNS stands for Domain Name System, which is a protocol for resolving domain names into IP addresses. DNS does not provide any functionality for time synchronization3. IPAM stands for IP Address Management, which is a method for planning, tracking, and managing the IP address space used in a network. IPAM does not provide any functionality for time synchronization. SNMP stands for Simple Network Management Protocol, which is a protocol for collecting and organizing information about managed devices on a network. SNMP can be used to monitor the performance, availability, configuration, and security of network devices, but it does not provide any functionality for time synchronization.

CV0-003 PDF Dumps   CV0-003 VCE Dumps   CV0-003 Practice Test