

1. What is meant by a public cloud?

☉ A solution hosted by a third party cloud service provider (CSP) and shared between subscribers (multi-tenant). This sort of cloud solution has the greatest security concerns.

2. What type of cloud solution would be used to implement a SAN?

☉ This would usually be described as Infrastructure as a Service (IaaS).

3. What is a Type II hypervisor?

☉ Software that manages virtual machines that has been installed to a guest OS. This is in contrast to a Type I (or "bare metal") hypervisor, which interfaces directly with the host

4. What is a VDE?

☉ A Virtual Desktop Environment (VDE) is the workspace presented when accessing an instance in a virtual desktop infrastructure (VDI) solution. VDI is the whole solution (host server and virtualization platform, connection protocols, connection/session broker, and client access devices).

5. What is the risk from a VM escaping attack?

☉ VM escaping refers to attacking other guest OSes or the hypervisor or host from within a virtual machine. Attacks may be to steal information, perform Denial of Service (DoS), infect the system with malware, and so on.

6. Describe some key considerations that should be made when hosting data or systems via a cloud solutions provider.

☉ Integrate auditing and monitoring procedures and systems with on-premises detection, identify responsibility for implementing security controls (such as patching or backup), identify performance metrics in an SLA, and assess risks to privacy and confidentiality from breaches at the service provider.

7. True or false? The account with which you register for the CSP services is not an account with root privileges.

☉ False. This account is the root account and has full privileges. It should not be used for day-to-day administration or configuration.

8. Which security attribute is ensured by monitoring API latency and correcting any problems quickly?

☉ This ensures the availability of services.

9. What format is often used to write permissions statements for cloud resource policies?

☉ JavaScript Object Notation (JSON).

10. True or false? A customer is limited to creating one VPC per account.

☉ False. There are limits to the number of virtual private clouds (VPCs) that can be created, but more than one is allowed.

11. What feature allows you to filter traffic arriving at an instance?

☉ This is accomplished by assigning the instance to a security group with the relevant policy configured.

12. What is a cloud access security broker (CASB)?

☉ Enterprise management software mediating access to cloud services by users to enforce information and access policies and audit usage.

13. A company has been using a custom-developed client-server application for customer management, accessed from remote sites over a VPN. Rapid overseas growth has led to numerous complaints from employees that the system suffers many outages and cannot cope with the increased number of users and access by client devices such as smartphones. What type of architecture could produce a solution that is more scalable?

☒ Microservices is a suitable architecture for replacing monolithic client-server applications that do not meet the needs of geographically diverse, mobile workforces. By breaking the application up into microservice components and hosting these in cloud containers, performance can scale to demand. Web-based APIs are better suited to browser-based access on different device types.

14. You have been asked to produce a summary of pros and cons for the products Chef and Puppet. What type of virtualization or cloud computing technology do these support?

☒ These are orchestration tools. Orchestration facilitates "automation of automation," ensuring that scripts and API calls are made in the right order and at the right time to support an overall workflow.

15. True or false? Serverless means running computer code on embedded systems.

☒ False. With serverless, the provision of functions running in containers is abstracted from the underlying server hardware. The point is that as a consumer, you do not perform any server management. The servers are still present, but they are operated and maintained by the cloud service provider.

16. A company's web services are suffering performance issues because updates keep failing to run on certain systems. What type of architecture could address this issue?

☒ Infrastructure as Code (IaC) means that provisioning is performed entirely from standard scripts and configuration data. The absence of manual configuration adjustments or ad hoc scripts to change settings is designed to eliminate configuration drift so that updates run consistently between the development and production environments.

17. What is SDV?

☒ Software-defined visibility (SDV) gives API-based access to network infrastructure and hosts so that configuration and state data can be reported in near real time. This facilitates greater automation in models and technologies such as zero trust, inspection of east/west data center traffic, and use of security orchestration and automated response (SOAR) tools.