9.5.3 Cloud Security Controls Facts

Most organizations rely on cloud services or will in the future. Cloud services provide many benefits, but there are risks involved when data security is the responsibility of an outside source. To safeguard against vulnerabilities, implement a cloud security strategy.

This lesson covers the following topics:

- Cloud security concepts
- Network security concepts
- Cloud access

Cloud Security Concepts

The following table describes cloud security concepts.

Cloud Security Concept	Description
High availability across zones	Cloud service providers replicate data in multiple zones and within zones to provide high availability. Replication: ▪ Helps eliminate downtime (the time your data is unavailable). ▪ Redirects to another availability zone, when a zone fails. To determine the best provider for your organization, compare cloud service providers' availability percentages. ▪ Availability percentage = uptime/uptime + downtime. ▪ The higher the percentage, the more resilient and reliable a provider is.
Integration	Cloud integration is the system that connects application repositories, systems, and IT environments in a way that allows access and exchange of data over a network by multiple devices and locations. This can include: ▪ Cloud-to-on-premises integration ▪ Cloud-to-cloud integration ▪ Both cloud-to-on-premises integration and cloud-to-cloud integration Your organization’s systems must be tightly integrated to the cloud provider to preserve secure communication in the digital system.
Encryption	Cloud service providers protect a customer’s data by changing it to ciphertext. It is your responsibility to: ▪ Be familiar with your cloud service provider's encryption services. Some cloud service providers offer encryption before the data is transferred to the cloud, some do not, and some offer end-to-end encryption only for sensitive data. ▪ Familiarize yourself with your provider’s encryption policies and procedures to ensure they meet your security requirements. ▪ Encrypt your data in-house before it’s transferred to the cloud if encryption is not part of the service you chose.

Instance awareness	Instance awareness is the ability to apply cloud security within an application that has rules specific to an instance. This tool allows the user to set security rules for an instance of an app interacting with one organization and a different security rules for an instance of the app is interacting with another organization.
Virtual private cloud (VPC) endpoint	A *VPC endpoint* is a virtual device that provides a private connection between virtual private clouds and a cloud provider's services. A VPC keeps traffic secure with a private link resource. VPC endpoints improve cloud security because VPC resources never traverse the internet to reach a service.
Cloud security infrastructure	To ensure your cloud service provider has and maintains a strong security infrastructure: ▪ Verify the provider's firewall protection from external sources. If the firewall is inadequate, provide your own. ▪ Verify the log monitoring and analysis tools offered by your provider.
Cloud auditing	Cloud auditors evaluate: ▪ Security controls ▪ Performance ▪ Communication ▪ Risk management ▪ Data management ▪ Vulnerability and remediation management ▪ Privacy of cloud provider's services ▪ Compliance with regulation and security policies
Application programming interfaces (API) inspections and integration	APIs are the software that allows applications and cloud computing systems to communicate with each other. You should regularly inspect the API integration points to: ▪ Ensure authentication is required from the end user before access is given. ▪ Determine the functions or operations necessary for each user and authorize only those functions or operations. ▪ Restrict users from using unnecessary roles. ▪ Scan payloads and validate API schemas to prevent injection attacks or man-in-the-middle attacks.

Network Concepts

To understand how to secure your applications and data in the cloud, it helps to understand network concepts that enhance security.

Network Concepts	Description
Virtual	

networks	Virtual networks connect virtual machines and devices through software. Network virtualization can also include combining network hardware resources and network software resources into one unit.
	▪ Virtual networks have a physical underlay that is made of physical servers and routers. Underlays use bridges and routers for traffic.
	▪ Virtual networks also have overlays that are connected to the underlay through a router. Overlays have virtual routers and bridges that connect the virtual machines within the virtual network.
	▪ Tunnel endpoints (TEPs) connect encapsulated data from the virtual network to physical network servers.
	▪ Segments are used in the virtual network to reduce traffic and keep areas within the virtual network separate.
	▪ Firewalls can also be used in the virtual network to protect segments through micro segmentation.
	▪ Virtual networks provide limited access to resources because most of the network functions in an isolated environment.
	▪ Virtual networks:
	  ▪ Limit costs.
	  ▪ Allow you to create the virtual machines, routers, bridges, and firewalls to suit your needs.

Public and private subnets	Subnets are subdivisions of an IP network. ▪ Public subnets can send outbound traffic directly to the internet. ▪ Private subnets access the internet through a network address translation (NAT) gateway within a public subnet. Database servers can connect to the internet through a NAT gateway, but internet connections are not established directly to the database servers. Subnets, give you greater control over who has access to your network. Dividing your network limits traffic, exposure, and potential damage from an attack. For example, if an attacker gains access or inserts malicious code into one subnet, the attack is confined to that subnet.
Segmentation	*Segmentation* divides a network into network segments using a Virtual Local Area Network (VLAN) and firewalls. To protect segments, filter traffic between segments with a deny all statement and then add rules to allow necessary traffic. Segmentation: ▪ Aids in monitoring traffic for security issues. ▪ Limits any damage to the compromised segment.

Cloud Storage Access

Standard security access measures are even more important when using cloud computing. The following table describes security access measures to implement when using cloud computing.

Security groups	A *security group* is a group of files that is assigned a unique name. The security group is controlled through permissions and works like a firewall that controls traffic to and from

	instances. Security groups use restrictive access control lists (ACLs) to allow ingress traffic only from specific IPs and to specific ports that are prepared through an application for connection. When using security groups: ▪ Regularly check security group policies to ensure they are allowing traffic only from acceptable addresses based on the organization's policies and purposes. ▪ Never allow incoming traffic to connect to the SSH port 22. ▪ Never allow incoming traffic to connect to RDP port 3389.
Container security	A *container* holds the complete runtime environment including an application, its dependencies, libraries, other binaries, and configuration files, all in one unit. Benefits of containers include: ▪ Containers allow software to function properly when moved from one computing environment to another. ▪ Multiple applications within containers can run on a server using the same operating system. ▪ Each container shares the OS kernel with the other containers. This requires fewer resources than a virtual machine.
Root account security	To secure the root account: ▪ Create an administrative group and assign rights to it. ▪ Do not give rights to any other groups or individual users. ▪ Use groups to control the level of access to files and programs.

Secrets management	Secrets management is the method for managing authentication credentials which can include passwords, encryption keys, usernames, email addresses, and private certificates. To secure secrets:
	
	▪ Centralize all secrets across your network using one tool for management.
	▪ Ensure password security through:
	  ▪ Regular rotation
	  ▪ Complexity
	  ▪ Password expirations
	▪ Remove default and hardcoded credentials from:
	  ▪ Applications
	  ▪ Code files
	  ▪ Test builds
	  ▪ Production builds

Permission management	Configuring permissions is essential in cloud data security. ▪ To manage permissions, you can use buckets, which are containers that store your data. ▪ Applying permissions to a bucket can help you manage who has access to sets of data. For example, a bucket may need to be globally readable at the first stage of a project, but it will need tighter permissions at the next stage. Remember to always practice the principle of least privilege with cloud storage.