**Module : 4 Business Continuity In The Cloude**

**1. Resource Monitoring Techniques .**

Resource monitoring involves tracking the performance and health of cloud resources. Common techniques include:

* **Agent-based Monitoring**: Installing monitoring agents on servers to gather data (e.g., Nagios, Datadog).
* **Agentless Monitoring**: Uses APIs or network protocols to monitor resources without installing software (e.g., SolarWinds).
* **Log Analysis**: Analyzing logs for system performance and security insights (e.g., Splunk, ELK Stack).
* **Real-time Alerts**: Setting thresholds for performance metrics and triggering alerts (e.g., CloudWatch for AWS).
* **Dashboarding**: Visual representation of performance metrics in tools like Grafana.

**2. How to Access Compute (Windows and Linux) from the Internet? Tools and Security .**

**Windows Compute**

* **Tools**:
  + **Remote Desktop Protocol (RDP)**: Access Windows machines using the RDP client (e.g., Microsoft Remote Desktop).
* **Security**:
  + Use strong passwords and usernames.
  + Enable network-level authentication.
  + Restrict access with IP whitelisting or VPN.
  + Use firewalls to block unnecessary ports.

**Linux Compute**

* **Tools**:
  + **Secure Shell (SSH)**: Access Linux instances via SSH clients (e.g., PuTTY, OpenSSH).
* **Security**:
  + Use SSH key pairs instead of passwords.
  + Restrict SSH access using security groups or firewalls.
  + Disable root login and use non-standard ports.
  + Use Fail2Ban to block brute force attacks.

**3. Encryption Technologies and Methods .**

* **Symmetric Encryption**: Uses the same key for encryption and decryption (e.g., AES, DES).
* **Asymmetric Encryption**: Uses public and private key pairs (e.g., RSA, ECC).
* **Hashing**: One-way encryption for data integrity (e.g., SHA-256, MD5).
* **Transport Layer Security (TLS)**: Encrypts data in transit over the internet.
* **End-to-End Encryption (E2EE)**: Ensures data is encrypted from the sender to the recipient without intermediate access.
* **Full Disk Encryption (FDE)**: Encrypts all data on a device (e.g., BitLocker, LUKS).

**4. Network Security in Cloud, Compute Security, and Storage Security .**

**Network Security in Cloud**

* Use **Virtual Private Clouds (VPCs)** to isolate network traffic.
* Implement **firewalls** and **security groups** to restrict inbound and outbound traffic.
* Use **Intrusion Detection/Prevention Systems (IDS/IPS)**.
* Encrypt network traffic with **VPNs** or **TLS**.
* Utilize **Network Access Control Lists (NACLs)** to add additional security layers.

**Compute Security**

* Secure virtual machines by updating and patching regularly.
* Use **Identity and Access Management (IAM)** to control access.
* Enable **antivirus** and **endpoint detection and response (EDR)** tools.
* Regularly monitor VM activity for anomalies.
* Apply **secure boot** and disk encryption.

**Storage Security**

* Enable **encryption at rest** using tools like AWS KMS or Azure Key Vault.
* Use **access controls** to manage who can read or write data.
* Regularly audit storage access logs.
* Use replication and backups to ensure data durability.
* Implement data classification to handle sensitive data appropriately.

4o

Top of Form

Bottom of Form