5.0 Troubleshooting

5.1 Given a scenario, use the troubleshooting methodology to resolve cloud-related issues.

- **Always consider corporate policies, procedures, and impacts before implementing changes.**

1. **Identify the problem**
   - Question the user and identify user changes to the computer and perform backups before making changes
   - Inquire regarding environmental or infrastructure changes
2. **Establish a theory of probable cause (question the obvious)**
   - If necessary, conduct external or internal research based on symptoms
3. **Test the theory to determine cause**
   - Once the theory is confirmed, determine the next steps to resolve the problem
   - If the theory is not confirmed, re-establish a new theory or escalate
4. **Establish a plan of action to resolve the problem and implement the solution**
5. **Verify full system functionality and, if applicable, implement preventive measures**
6. **Document the findings, actions, and outcomes throughout the process.**

5.2 Given a scenario, troubleshoot security issues.

- **Privilege**
  - Missing
  - Incomplete
  - Escalation
  - Keys
- **Authentication**
- **Authorization**
- **Security groups**
  - Network security groups
  - Directory security groups
- **Keys and certificates**
  - Expired
  - Revoked
  - Trust
  - Compromised
  - Misconfigured
- **Misconfigured or misapplied policies**
- **Data security issues**
  - Unencrypted data
  - Data breaches
  - Misclassification
  - Lack of encryption in protocols
  - Insecure ciphers
- **Exposed endpoints**
- **Misconfigured or failed security appliances**
  - IPS
  - IDS
  - NAC
  - WAF
- **Unsupported protocols**
- **External/internal attacks**

5.3 Given a scenario, troubleshoot deployment issues.

- **Connectivity issues**
  - Cloud service provider (CSP) or Internet service provider (ISP) outages
- **Performance degradation**
  - Latency
- **Configurations**
  - Scripts
- **Applications in containers**
- **Misconfigured templates**
- **Missing or incorrect tags**
- **Insufficient capacity**
  - Scaling configurations
  - Compute
  - Storage
  - Bandwidth issues
  - Oversubscription
- **Licensing issues**
- **Vendor-related issues**
  - Migrations of vendors or platforms
  - Integration of vendors or platforms
  - API request limits
  - Cost or billing issues

5.4 Given a scenario, troubleshoot connectivity issues.

- **Network security group misconfigurations**
  - ACL
  - Inheritance
- **Common networking configuration issues**
  - Peering
  - Incorrect subnet
  - Incorrect IP address
  - Incorrect IP space
  - Routes
    - Default
    - Static
    - Dynamic
  - Firewall
    - Incorrectly administered micro-segmentation
  - Network address translation (NAT)
    - VPN
    - Source
    - Destination
  - Load balancers
    - Methods
    - Headers
    - Protocols
    - Encryption
    - Back ends
    - Front ends
  - DNS records
  - VLAN/VXLAN/GENEVE
  - Proxy
  - Maximum transmission unit (MTU)
  - Quality of service (QoS)
  - Time synchronization issues
- **Network troubleshooting tools**
  - ping
  - tracert/traceroute
  - flushdns
  - ipconfig/ifconfig/ip
  - nslookup/dig
  - netstat/ss
  - route
  - arp
  - curl
  - Packet capture
  - Packet analyzer
  - OpenSSL client

5.5 Given a scenario, troubleshoot common performance issues.

- **Resource utilization**
  - CPU
  - GPU
  - Memory
  - Storage
    - I/O
    - Capacity
  - Network bandwidth
  - Network latency
  - Replication
  - Scaling
- **Application**
  - Memory management
  - Service overload
- **Incorrectly configured or failed load balancing**

5.6 Given a scenario, troubleshoot automation or orchestration issues.

- **Account mismatches**
- **Change management failures**
- **Server name changes**
- **IP address changes**
- **Location changes**
- **Version/feature mismatch**
- **Automation tool incompatibility**
  - Deprecated features
  - API version incompatibility
- **Job validation issue**
- **Patching failure**