5.0 Troubleshooting

5.1 Given a scenario, troubleshoot a deployment issue.

- **Common issues in the deployments**
    - Breakdowns in the workflow
    - Integration issues related to different cloud platforms
    - Resource contention
    - Connectivity issues
    - Cloud service provider outage
    - Licensing issues
    - Template misconfiguration
    - Time synchronization issues
    - Language support
    - Automation issues

5.2 Given a scenario, troubleshoot common capacity issues.

- **Exceeded cloud capacity boundaries**
    - Compute
    - Storage
    - Networking
        - IP address limitations
        - Bandwidth limitations
    - Licensing
    - Variance in number of users
    - API request limit
    - Batch job scheduling issues
- **Deviation from original baseline**
- **Unplanned expansions**

5.3 Given a scenario, troubleshoot automation/orchestration issues.

- **Breakdowns in the workflow**
    - Account mismatch issues
    - Change management failure
    - Server name changes
    - IP address changes
    - Location changes
    - Version/feature mismatch
    - Automation tool incompatibility
    - Job validation issue

5.4 Given a scenario, troubleshoot connectivity issues.

- **Common networking issues**
    - Incorrect subnet
    - Incorrect IP address
    - Incorrect gateway
    - Incorrect routing
    - DNS errors
    - QoS issues
    - Misconfigured VLAN or VXLAN
    - Misconfigured firewall rule
    - Insufficient bandwidth
    - Latency
    - Misconfigured MTU/MSS
    - Misconfigured proxy
- **Network tool outputs**
- **Network connectivity tools**
    - ping
    - tracert/traceroute
    - telnet
    - netstat
    - nslookup/dig
    - ipconfig/ifconfig
    - route
    - arp
    - ssh
    - tcpdump
- **Remote access tools for troubleshooting**

5.5 Given a scenario, troubleshoot security issues.

- Authentication issues
  - Account lockout/expiration
- Authorization issues
- Federation and single sign-on issues
- Certificate expiration
- Certification misconfiguration
- External attacks
- Internal attacks
- Privilege escalation
- Internal role change
- External role change
- Security device failure
- Incorrect hardening settings
- Unencrypted communication
- Unauthorized physical access
- Unencrypted data
- Weak or obsolete security technologies
- Insufficient security controls and processes
- Tunneling or encryption issues

5.6 Given a scenario, explain the troubleshooting methodology.

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

1. Identify the problem
   - Question the user and identify user changes to computer and perform backups before making changes
2. Establish a theory of probable cause (question the obvious)
   - If necessary, conduct internal or external research based on symptoms
3. Test the theory to determine cause
   - Once theory is confirmed, determine the next steps to resolve the problem
   - If the theory is not confirmed, reestablish 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 findings, actions, and outcomes