



## 4.0 Operations and Support

**4.1** Given a scenario, configure logging, monitoring, and alerting to maintain operational status.

### • Logging

- Collectors
  - Simple network management protocol (SNMP)
  - Syslog
- Analysis
- Severity categorization
- Audits
- Types
  - Access/authentication
  - System
  - Application
- Automation
- Trending

### • Monitoring

- Baselines
- Thresholds
- Tagging
- Log scrubbing
- Performance monitoring
  - Application
  - Infrastructure components
- Resource utilization
- Availability
  - SLA-defined uptime requirements
- Verification of continuous monitoring activities
- Service management tool integration

### • Alerting

- Common messaging methods
- Enable/disable alerts
  - Maintenance mode
- Appropriate responses
- Policies for categorizing and communicating alerts

**4.2** Given a scenario, maintain efficient operation of a cloud environment.

### • Confirm completion of backups

### • Life-cycle management

- Roadmaps
- Old/current/new versions
- Upgrading and migrating systems
- Deprecations or end of life

### • Change management

### • Asset management

- Configuration management database (CMDB)

### • Patching

- Features or enhancements
- Fixes for broken or critical infrastructure or applications
- Scope of cloud elements to be patched
  - Hypervisors
  - VMs
  - Virtual appliances

### • Networking components

- Applications
- Storage components
- Firmware
- Software
- OS
- Policies
  - n-1
- Rollbacks

### • Impacts of process improvements on systems

### • Upgrade methods

- Rolling upgrades
- Blue-green
- Canary
- Active-passive
- Development/QA/production/DR

### • Dashboard and reporting

- Tagging
- Costs
  - Chargebacks
  - Showbacks
- Elasticity usage
- Connectivity
- Latency
- Capacity
- Incidents
- Health
- Overall utilization
- Availability



### 4.3 Given a scenario, optimize cloud environments.

- **Right-sizing**
  - Auto-scaling
  - Horizontal scaling
  - Vertical scaling
  - Cloud bursting
- **Compute**
  - CPUs
  - GPUs
  - Memory
  - Containers
- **Storage**
  - Tiers
    - Adaptive optimization
  - IOPS
  - Capacity
  - Deduplication
  - Compression
- **Network**
  - Bandwidth
  - Network interface controllers (NICs)
  - Latency
  - SDN
- Edge computing
  - CDN
- **Placement**
  - Geographical
  - Cluster placement
  - Redundancy
  - Colocation
- **Device drivers and firmware**
  - Generic
  - Vendor
  - Open source

### 4.4 Given a scenario, apply proper automation and orchestration techniques.

- **Infrastructure as code**
  - Infrastructure components and their integration
- **Continuous integration/continuous deployment (CI/CD)**
- **Version control**
- **Configuration management**
  - Playbook
- **Containers**
- **Automation activities**
  - Routine operations
  - Updates
  - Scaling
  - Shutdowns
  - Restarts
  - Create internal APIs
- **Secure scripting**
  - No hardcoded passwords
  - Use of individual service accounts
  - Password vaults
  - Key-based authentication
- **Orchestration sequencing**

### 4.5 Given a scenario, perform appropriate backup and restore operations.

- **Backup types**
  - Incremental
  - Differential
  - Full
  - Synthetic full
  - Snapshot
- **Backup objects**
  - Application-level backup
  - Filesystem backup
  - Database dumps
  - Configuration files
- **Backup targets**
  - Tape
  - Disk
  - Object
- **Backup and restore policies**
  - Retention
  - Schedules
  - Location
  - SLAs
  - Recovery time objective (RTO)
  - Recovery point objective (RPO)
- Mean time to recovery (MTTR)
- 3-2-1 rule
  - Three copies of data
  - Two different media
  - One copy off site
- **Restoration methods**
  - In place
  - Alternate location
  - Restore files
  - Snapshot