Chapter 9

Troubleshooting Cloud Solutions

Episode 9.01

Troubleshooting Methodology

Quick Review

- Troubleshooting should always begin by identifying the actual problem
- A plan of action determines the methods you will use to solve the problem
- Full system functionality should always be verified before closing a problem ticket
- Documentation, while often overlooked, is important in the troubleshooting process

Episode 9.02

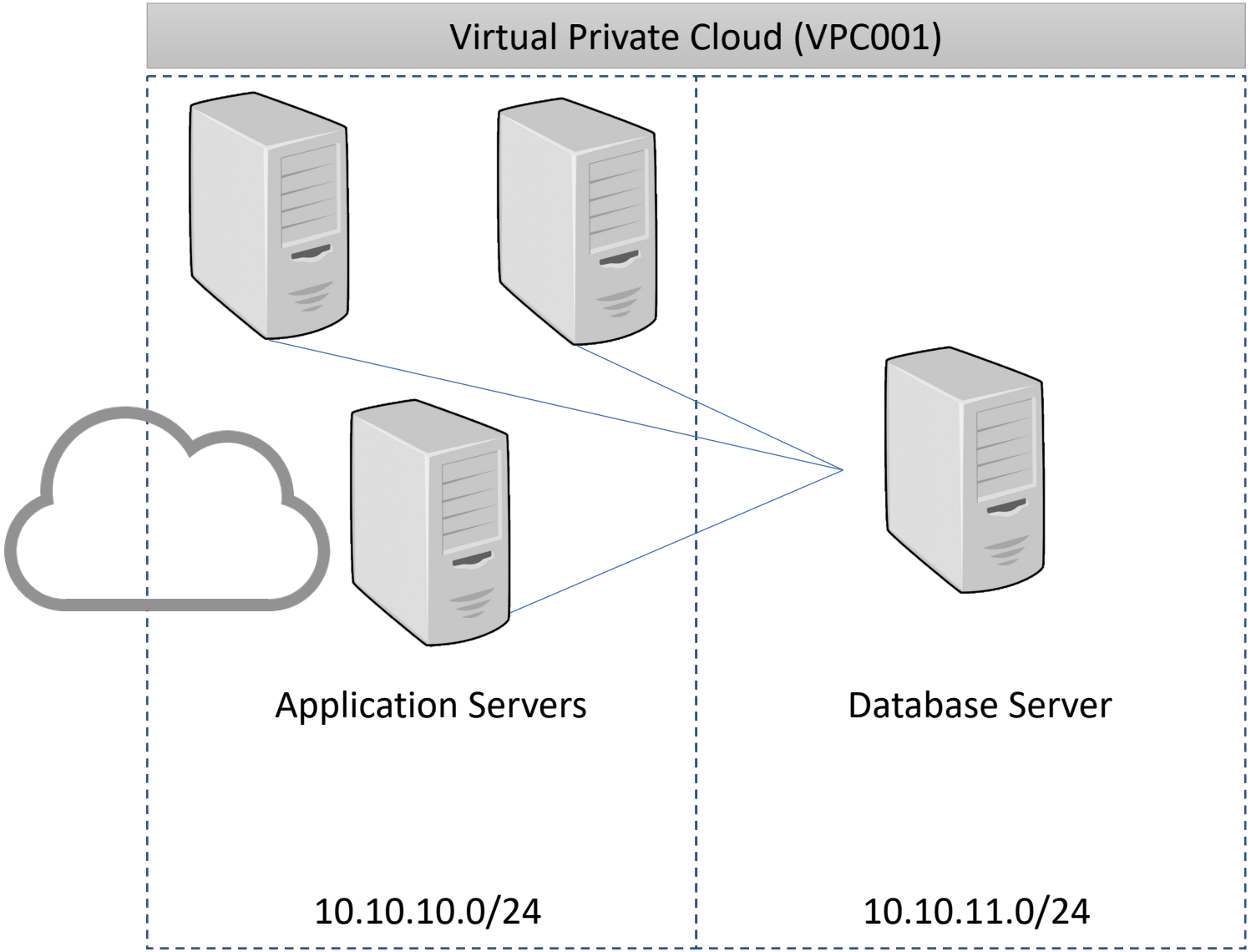
Troubleshooting Deployment

Common Deployment Issues

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

Scenario

- Users reporting they can access applications in the cloud, but receiving errors when accessing data
- Errors include “database unavailable” error
- Cloud management platform reports the database server instance is running
- Use the methodology to troubleshoot this problem



Quick Review

- To utilize cloud services, connectivity is a first priority requirement
- When running applications in the cloud, proper licensing is still required
- It is important to configure time zone settings correctly in the cloud so that time synchronization is accurate with the local network

Episode 9.03

Troubleshooting Capacity

Common Capacity Issues

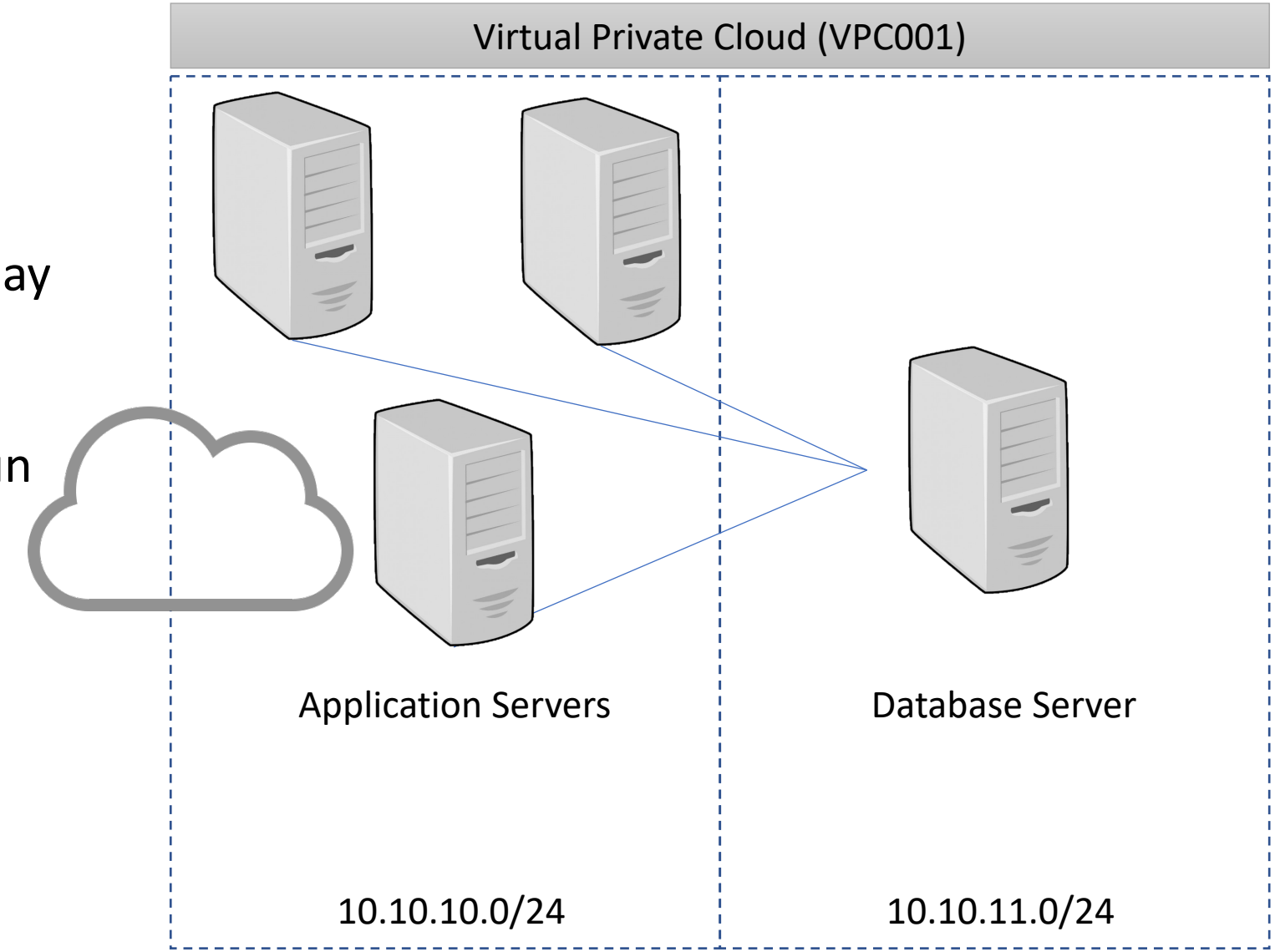
- Exceeding cloud capacity boundaries
  - Compute
  - Storage
  - Networking
    - IP address limitations
    - Bandwidth limitations
  - Licensing
  - Variance in the number of users
  - API request limit
  - Batch job scheduling issues

Common Capacity Issues

- Deviation from original baseline
- Unplanned expansions

Scenario

- Users reporting performance is degraded when accessing accounting servers every Thursday afternoon
- They can still perform their operations, but the processes run more slowly



Quick Review

- Known the boundaries for capacity of your cloud provider and contract is important
- Deviation from the original or planned baseline can result in problems
- Unplanned expansions can result in inferior performance

Episode 9.04

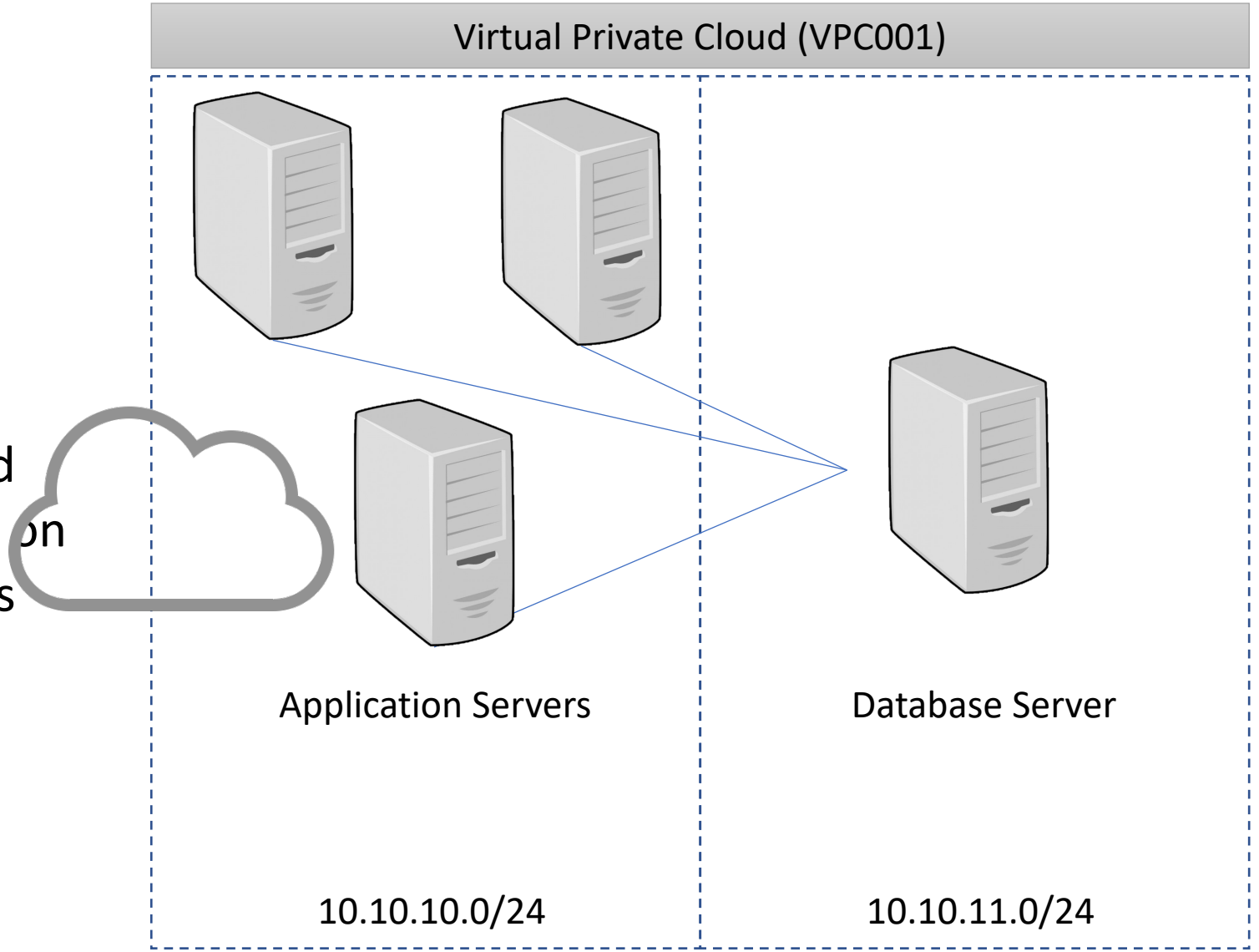
Troubleshooting Automation and Orchestration

Automation and Orchestration Issues

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

Scenario

- Application was upgraded on an application servers
- Users can connect to the application, but data can’t be accessed
- User performing the upgrade said everything was configured based on documentation created two years ago



Quick Review

- Many times, accounts are modified after automation and this can break the workflow
- If IP addresses are hard coded in automation scripts, the change of an IP address can break the workflow
- If DNS names are used to process automation scripts, the change of a server name can break the workflow

Episode 9.05

Troubleshooting Connectivity

Networking Issues

- Incorrect subnet
- Incorrect IP address
- Incorrect gateway
- Incorrect routing
- DNS errors
- QoS issues

Networking Issues

- Misconfigured VLAN or VXLAN
- Misconfigured firewall rule
- Insufficient bandwidth
- Latency
- Misconfigured MTU/MSS
- Misconfigured proxy

Networking Tools

- Network tool outputs
- Connectivity tools
  - ping/traceroute/tracert
  - arp
  - ipconfig/ifconfig
  - nslookup/dig
  - netstat
  - telnet/ssh
  - route
  - tcpdump
- Remote access tools (RDP/VNC/SSH)

Quick Review

- An incorrect gateway configuration can cause communications outside of the subnet to fail
- When real-time applications suffer in performance, Quality of Service (QoS) configuration should be validated
- Latency is the delay in network communications and high latency values can cause problems for real-time applications

Episode 9.06

Network Troubleshooting Lab

Demo

- PING
- PATHPING
- TRACERT
- NETSTAT
- IPCONFIG
- WIRESHARK

Episode 9.07

Troubleshooting Security

Security Breach Issues

- External attacks
- Internal attacks
- Privilege escalation
- Internal role change
- External role change
- Security device failure

Security Breach Issues

- Incorrect hardening settings
- Unencrypted communication
- Unauthorized physical access
- Unencrypted data
- Weak or obsolete security technologies
- Insufficient security controls and processes

Problems Related to Security Solutions

- Authentication issues
  - Account lockout/expiration
- Authorization issues
- Federation and single sign-on issues
- Certificate expiration
- Certification misconfiguration
- Tunneling or encryption issues

Quick Review

- Implementing a compute instance with incorrect hardening settings can weaken the security of an entire cloud deployment
- Unencrypted communications can result in the exposure of sensitive data
- With several failed login attempts, a cloud account may be locked

Episode 9.08

Disaster Recovery

Documentation

- Network diagrams
- Playbooks
- Disaster Recovery kits
- Corporate guidelines
- Network configurations
- Geographical datacenter requirements

Selecting DR Solutions

- On-premises and cloud sites
  - Hot
  - Warm
  - Cold
- Replication
- Requirements
  - Recovery Point Objective (RPO)
  - Recovery Time Objective (RTO)
  - Service Level Agreement (SLA)

Failure Response

- Failover
- Failback
- Restore backups

Episode 9.09

Troubleshoot a Capacity Problem

Scenario

You have implemented a cloud solution for an Internet of Things (IoT) deployment. The deployment consists of hundreds of IoT devices sensing environmental conditions (humidity, temperature, air quality, light, etc.) and machine operations. The devices use an MQTT service in the cloud to publish sensor readings and other statistics about the devices. MQTT is a publish/subscribe protocol where publishers submit publications (messages) to the broker and subscribers receive them. After deployment, it has been determined that the MQTT broker, which is running on an AWS instance of Linux, is not keeping up with the workload. The instance currently has 4 GB of RAM and uses a moderate processor virtualization setting. What options are available in most cloud service providers to improve the capacity of this solution?

Possible Solution

- Increase the amount of RAM
- Increase the CPU capability
- Increase the Internet speed of the cloud connection
- Horizontally scale the MQTT server instance
  - Load balancing
  - Configuration-based distribution