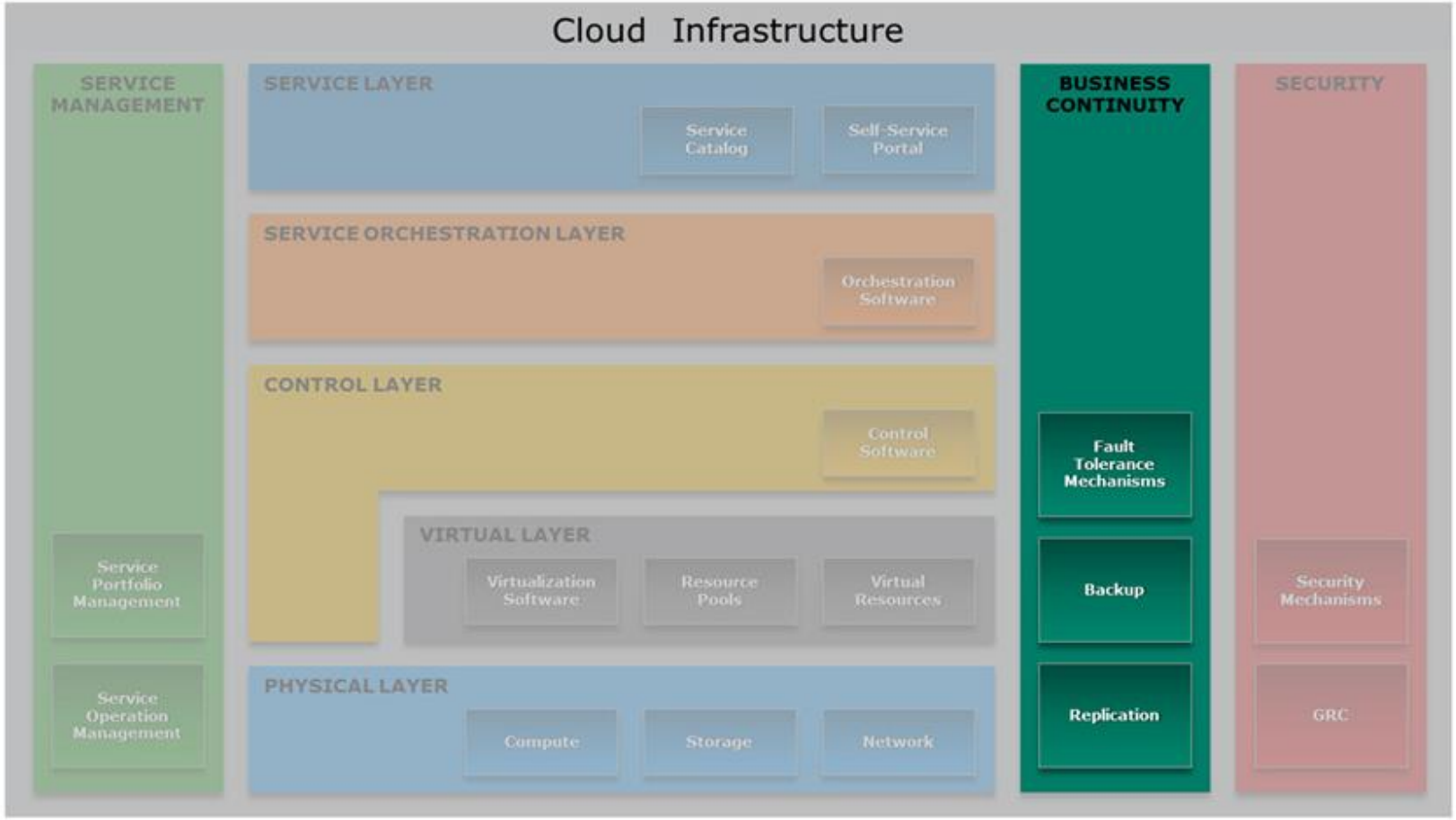
IT496: Cloud Computing

MODULE 7: BUSINESS CONTINUITY

LECTURE 12

Based on EMC course materials

Business continuity cross-layer function



Lecture Outline:

- Part One: Business continuity Overview
- Part Two: Building Fault Tolerance Cloud Infrastructure -1
- Part Three: Building Fault Tolerance Cloud Infrastructure -2
- Part Four: Data Protection Solution - Backup

Lecture Outline:

Part one: Business Continuity Overview

- covers the causes of service unavailability and the impact due to service unavailability.

What is Business Continuity?

- Business Continuity is preparing for, **responding** to, and **recovering** from an **application outage** that adversely affects business operations
- Business Continuity solutions address **unavailability and degraded** application performance
- BC enables continuous availability of cloud services in the event of **failure**
  - Helps to meet the required **service level**

What is Business Continuity?

- BC involves various **proactive and reactive** measures

- **Disaster recovery** is a part of BC, which coordinates the process of **restoring** infrastructure, including data
  - Required to support ongoing cloud services, after a disaster occurs

Cloud service availability

- Refers to the **ability** of a cloud service to perform its **agreed function** according to ***business requirements*** and ***customer expectations*** during its operation.
- Cloud service providers need to design and build their infrastructure to **maximize the availability** of the service

Cloud service availability

$$\textbf{Service Availability} = \frac{\boldsymbol{Agreed\ Service\ time - Downtime}}{\boldsymbol{Agreed\ service\ time}}$$

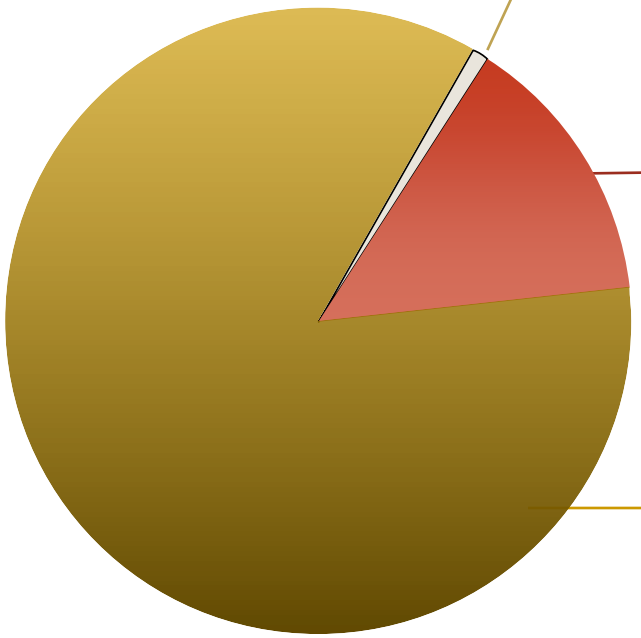
Availability Measurement – Levels of ‘9s’ Availability

% Uptime	% Downtime	Downtime per Year	Downtime per Week
98%	2%	7.3 days	3hrs 22 min
99%	1%	3.65 days	1 hr 41 min
99.8%	0.2%	17 hrs 31 min	20 min 10 sec
99.9%	0.1%	8 hrs 45 min	10 min 5 sec
99.99%	0.01%	52.5 min	1 min
99.999%	0.001%	5.25 min	6 sec
99.9999%	0.0001%	31.5 sec	0.6 sec

Causes of Cloud Service unavailability

- Application failure
  For example, due to catastrophic exceptions caused by bad logic
- Data loss
- Infrastructure component failure
- Failure of dependent services
- Data center or site down
- Refreshing IT infrastructure

Causes of Information Unavailability



Disaster (<1% of Occurrences)

Natural or man made

- Flood, fire, earthquake
- Contaminated building

Unplanned Outages (20%)

Failure

- Database corruption
- Component failure
- Human error

Planned Outages (80%)

Competing workloads

- Backup, reporting
- Data warehouse extracts
- Application and data restore

Impact of Downtime

Know the downtime costs (per hour, day, two days...)

Lost Productivity

- Number of employees impacted (x hours out * hourly rate)

Lost Revenue

- Direct loss
- Compensatory payments
- Lost future revenue
- Billing losses
- Investment losses

Damaged Reputation

- Customers
- Suppliers
- Financial markets
- Banks
- Business partners

Financial Performance

- Revenue recognition
- Cash flow
- Lost discounts (A/P)
- Payment guarantees
- Credit rating
- Stock price

Other Expenses

Temporary employees, equipment rental, overtime costs, extra shipping costs, travel expenses...

Methods to Achieve Required Cloud Service Availability

- Building resilient cloud infrastructure **facilitates meeting the required service availability**
- Building resilient cloud infrastructure requires **various high availability solutions**
  - Implementing **fault tolerance** mechanisms (Part 2)
  - Deploying **data protection solutions** such as backup and replication
  - Implementing **automated cloud** service failover
  - Architecting resilient cloud applications

Lecture Outline:

Part two: Building Fault Tolerance Cloud Infrastructure -1

- covers identifying and avoiding single points of failure.
- fault tolerance mechanisms at the cloud infrastructure component level.

Single Points of failure

- Refers to any **individual component or aspect** of an infrastructure whose failure can make the entire system or service unavailable.
- Single points of failure may occur at:-
  - Component level
  - Site or data center level

Avoiding Single Points of Failure

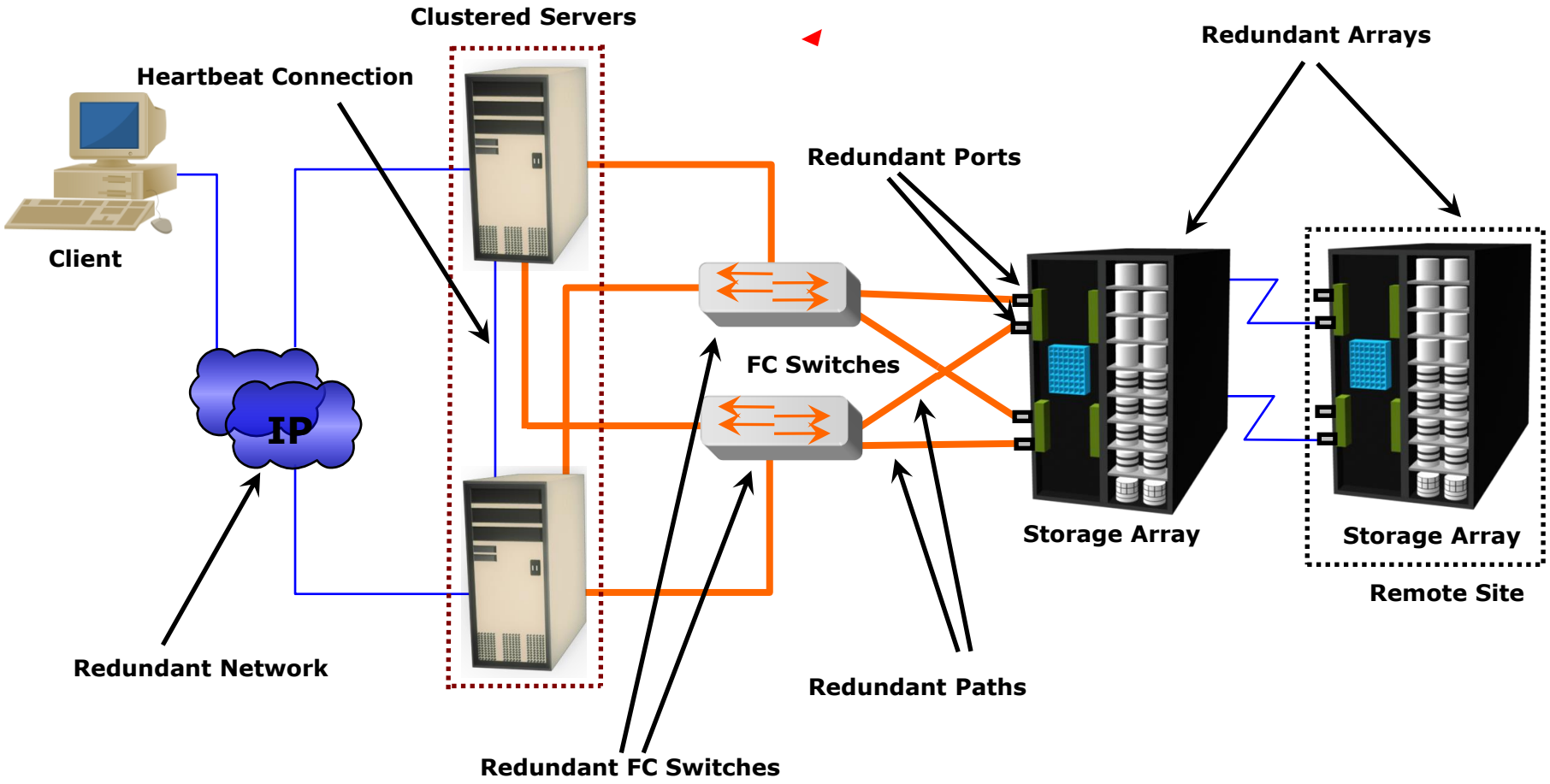
- Single points of failure can be avoided by implementing **fault tolerance** mechanisms such as **redundancy**
- Implement redundancy at component level
  - Compute
  - Storage
  - Network

Avoiding Single Points of Failure

- Implement multiple **service availability zones**
  - Avoids single points of failure at data center (site) level
  - Enable service failover globally

- It is important to have ***high availability mechanisms*** that enable **automated service failover**

Resolving Single Points of Failure



Compute Clustering

- A technique where at least two compute systems (or nodes) work together and are viewed as a **single compute system** to provide ***high availability and load balancing.***
- Enables service **failover** in the event of compute system failure to another system to minimize or avoid any service outage
- Two common clustering implementations are:
  - Active/active
  - Active/passive

Compute Clustering

- **Hypervisor cluster** is a common clustering implementation in cloud environment
- Clustering can be implemented between multiple physical compute systems, or between multiple VMs, or between VM and physical compute system, or between multiple hypervisors.

Compute Clustering

- Clustering uses a ***heartbeat mechanism*** to determine the health of each node in the cluster.

- The exchange of heartbeat signals, usually happens over a ***private network***, allows participating cluster members to **monitor** one another's status.

Compute Clustering Active/active

- The nodes in a cluster are **all active participants** and run the same service of their clients. active/active cluster balances requests for service among the nodes.
- If one of the nodes fails, the surviving nodes take the load of the failed one.
- **Active/Active clustering** only one node can write or update the data in a **shared** file system or database at a ***given time***.

Compute Clustering Active/passive

- The service runs on one or more nodes, and the passive node just **waits** for a failover.
- If and when the active node fails, the service that had been running on the active node is failed over to the passive node.
- Active/passive clustering **does not provide performance improvement** like active/active clustering.

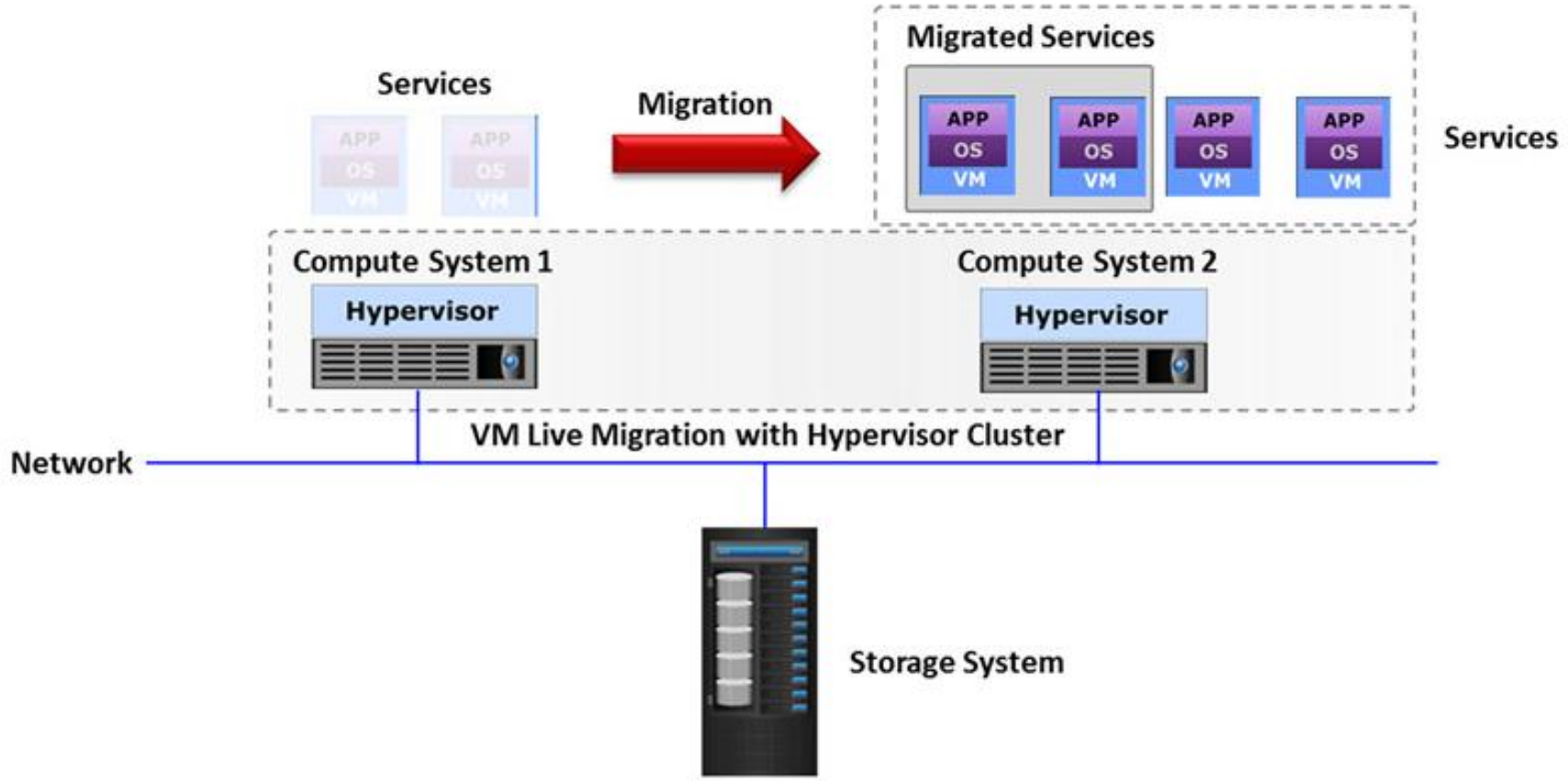
Hypervisor cluster

- **Multiple hypervisors** running on ***different*** compute systems are clustered.
- Provides continuous availability of services running on VMs even if a ***physical compute system*** or a ***hypervisor fails***
- This method provides rapid recovery of services running on VMs in the event of compute system failure.

Virtual Machine Live Migration

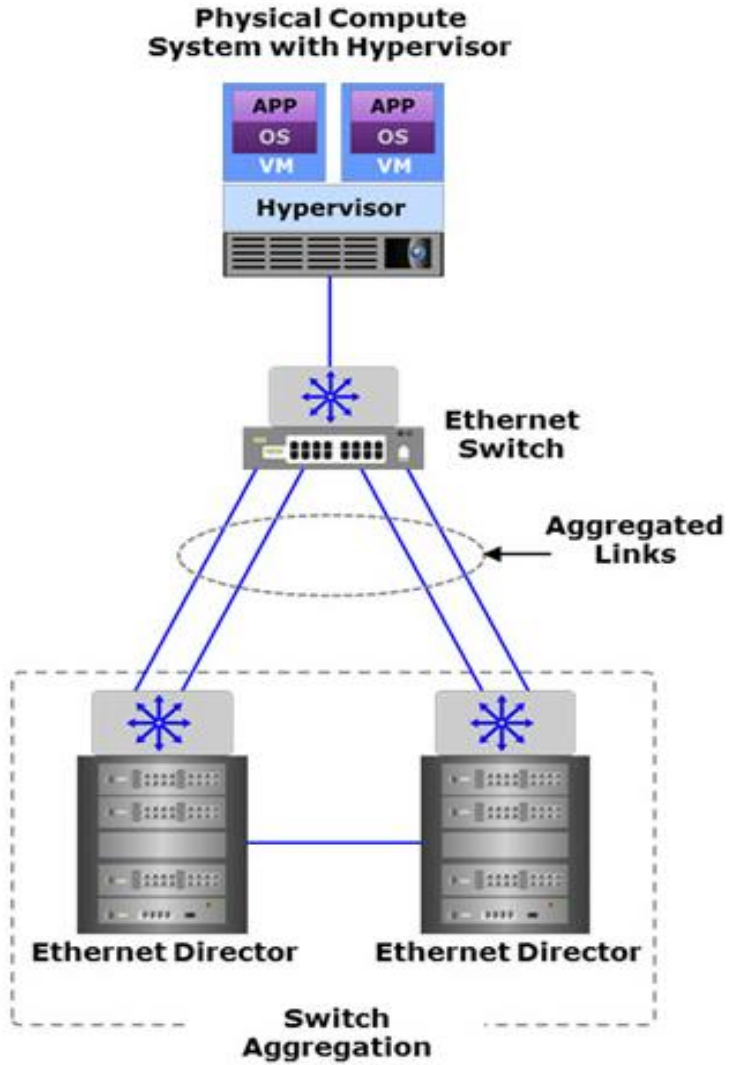
- Running services on VMs are moved from one physical compute system to another without any downtime
  - Allows scheduled maintenance without any downtime
  - Facilitates ***VM load balancing***
- Performing VM live migration requires a ***high speed network*** connection.

Virtual Machine Live Migration



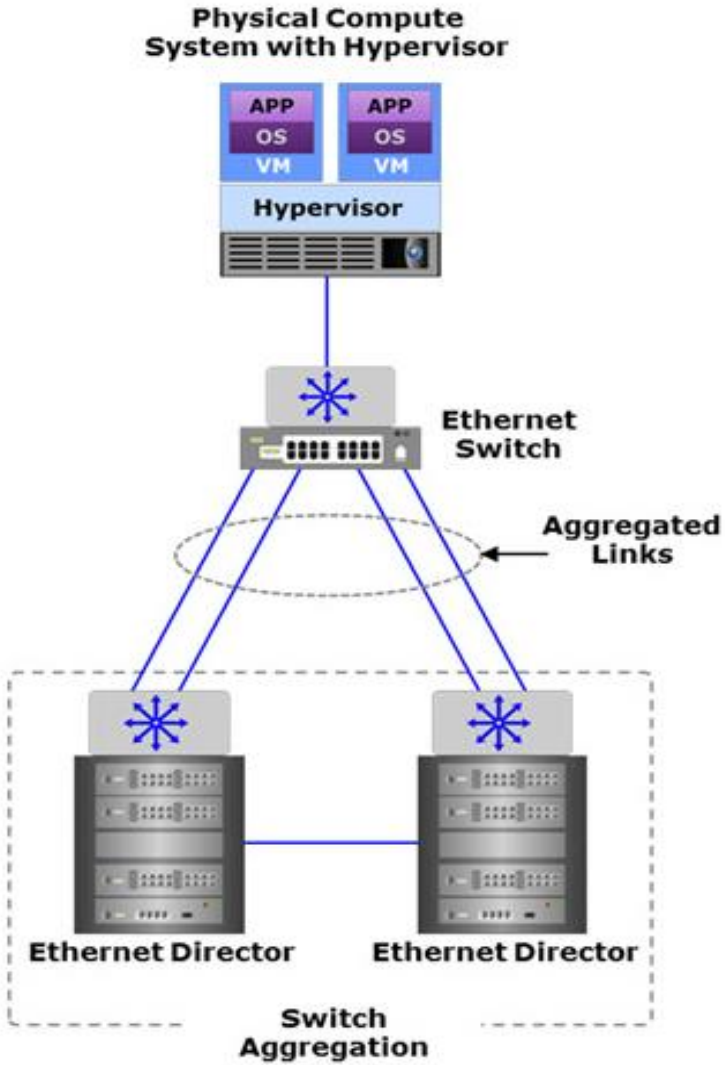
Link and Switch Aggregation

- **Link aggregation**
  - Combines links between two switches and also between a switch and a node
  - Enables network **traffic failover** in the event of a link failure in the aggregation
  - Enables distribution of **network traffic** across links in the aggregation



Link and Switch Aggregation

- **Switch aggregation**
  - Provides fault tolerance against ***switch and link failures***
  - Improves node performance by providing more ***active paths and bandwidth***



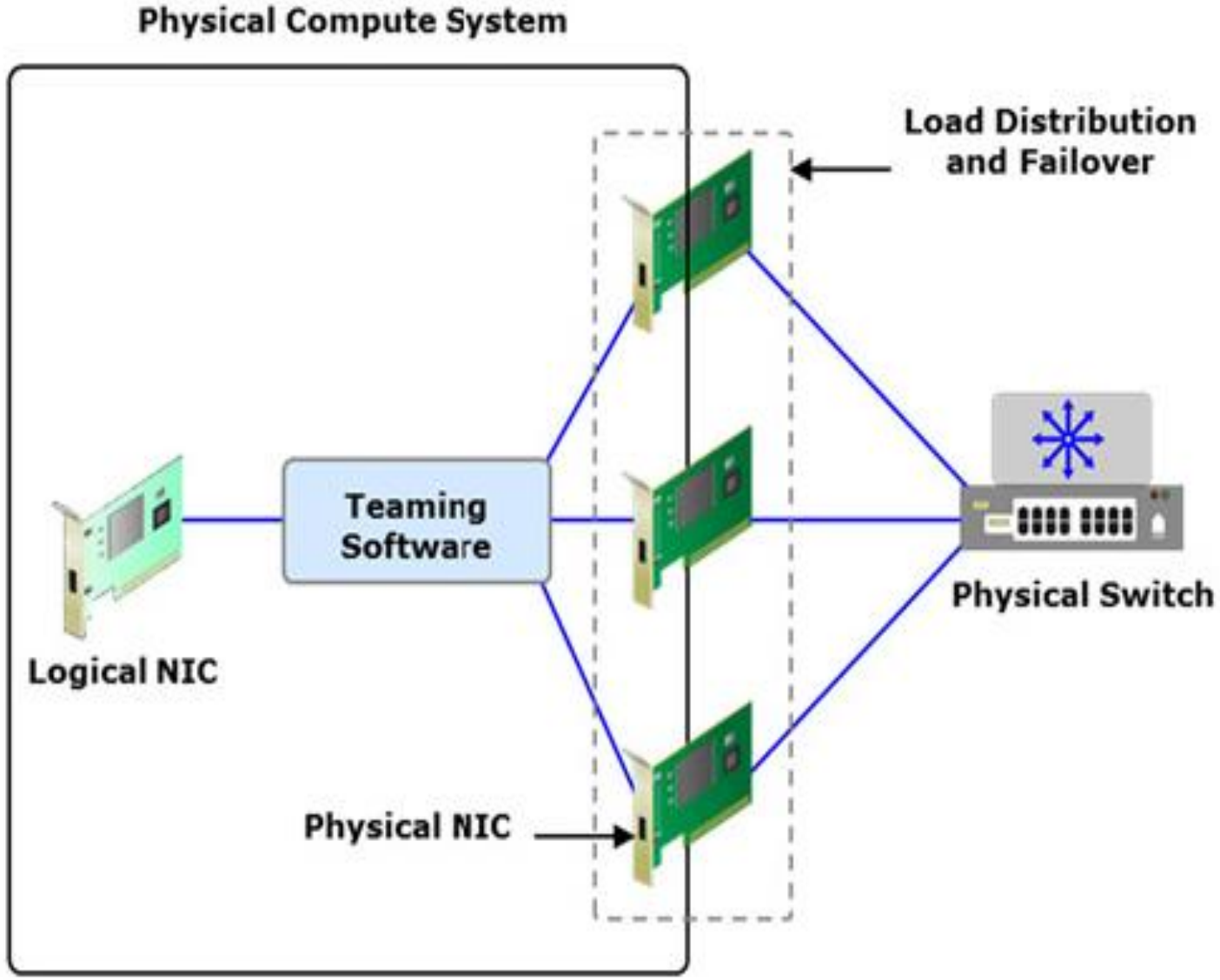
NIC teaming

- NIC teaming groups NICs (to create a NIC team) so that they appear as a single, **logical NIC** to the OS or hypervisor.
- Provides network traffic failover to prevent connectivity loss in the event of a **NIC failure** or a network link outage
- Distribution of network traffic across NICs in the team

NIC teaming

- NICs within a team can be configured as **active and standby**.
- Active NICs are used to send data packets, whereas the standby NICs remain idle.
- A standby NIC is not used for forwarding traffic unless an active NIC fails.

NIC Teaming


Physical Compute System
Load Distribution and Failover
Teaming Software
Logical NIC
Physical NIC
Physical Switch

Multipathing

- Enables a compute system to use **multiple paths** for transferring data to a LUN
- Enables failover by **redirecting I/O from a failed** path to another active path
- Performs load balancing by distributing I/O across active paths
  - Standby paths become active if one or more active paths fail

In-Service Software Upgrade (ISSU)

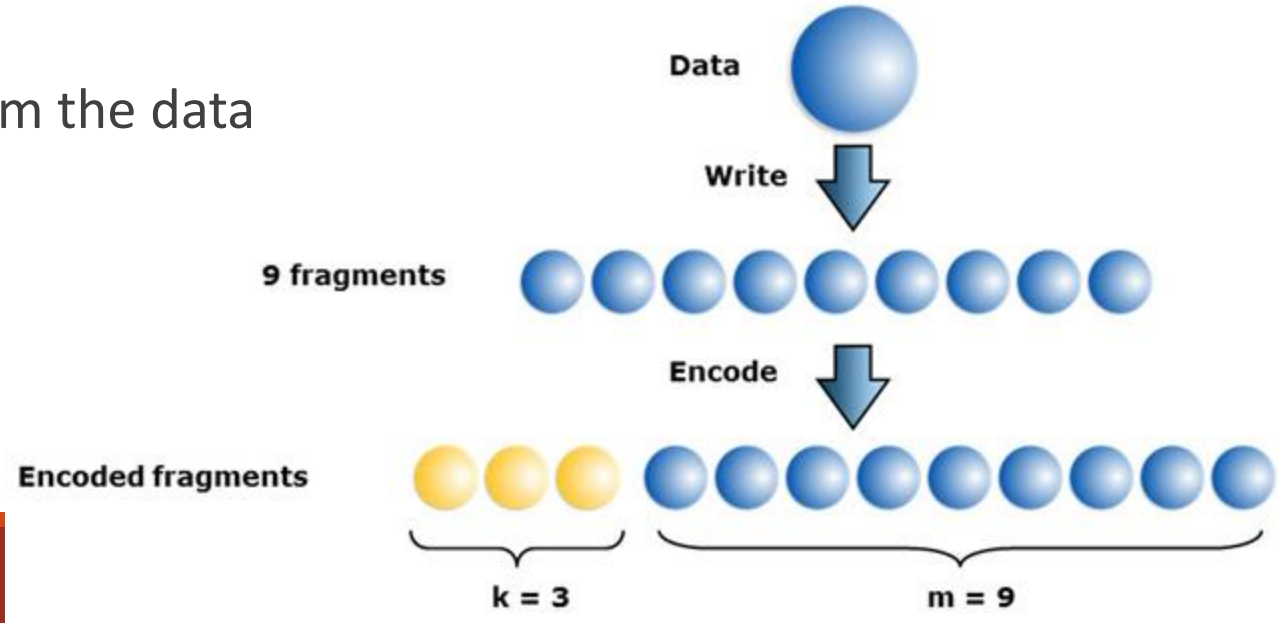
- Allows ***updating*** software on network devices (switches and routers) **without impacting the network availability**
  - Eliminates the need to stop the ongoing process on a device
  - Ensures network availability as a result of a network device maintenance or upgrade processes
- Typically requires a network device with redundant control plane elements (supervisor or routing engines)
  - This setup allows the administrator to update the software image on one engine while the other maintains network availability

RAID and Dynamic disk sparing

- RAID
  - Combines multiple drives into a logical unit called a RAID set
  - Provides data protection against drive failure
- Dynamic disk sparing
  - Automatically replaces a failed drive with a spare drive to protect against data loss
  - Multiple spare drives can be configured to improve availability

Erasure Coding

- Provides space-optimal ***data redundancy*** to protect data loss against multiple drive failure.
  - a set of n disks is divided into m disks to hold data and k disks to hold coding information
  - The coding information is calculated from the data



Lecture Outline:

Part Three: Building Fault Tolerance Cloud Infrastructure -1

- covers identifying and avoiding single points of failure. This lesson also covers the key
- fault tolerance mechanisms at the cloud infrastructure component level.

Service availability zone

- A location with its **own set of resources** and **isolated** from other zones to avoid that a failure in one zone will not impact other zones.

- A zone can be a **part** of a data center or may even be composed of the **whole** data center
  - Enables running multiple service instances within and across zones to survive data center or site failure
  - In the event of outage, the service should seamlessly failover across the zones
- Zones within a particular region are typically connected through **low-latency** network which enables **faster cloud service failover**

Automated Service Failover Across Zones

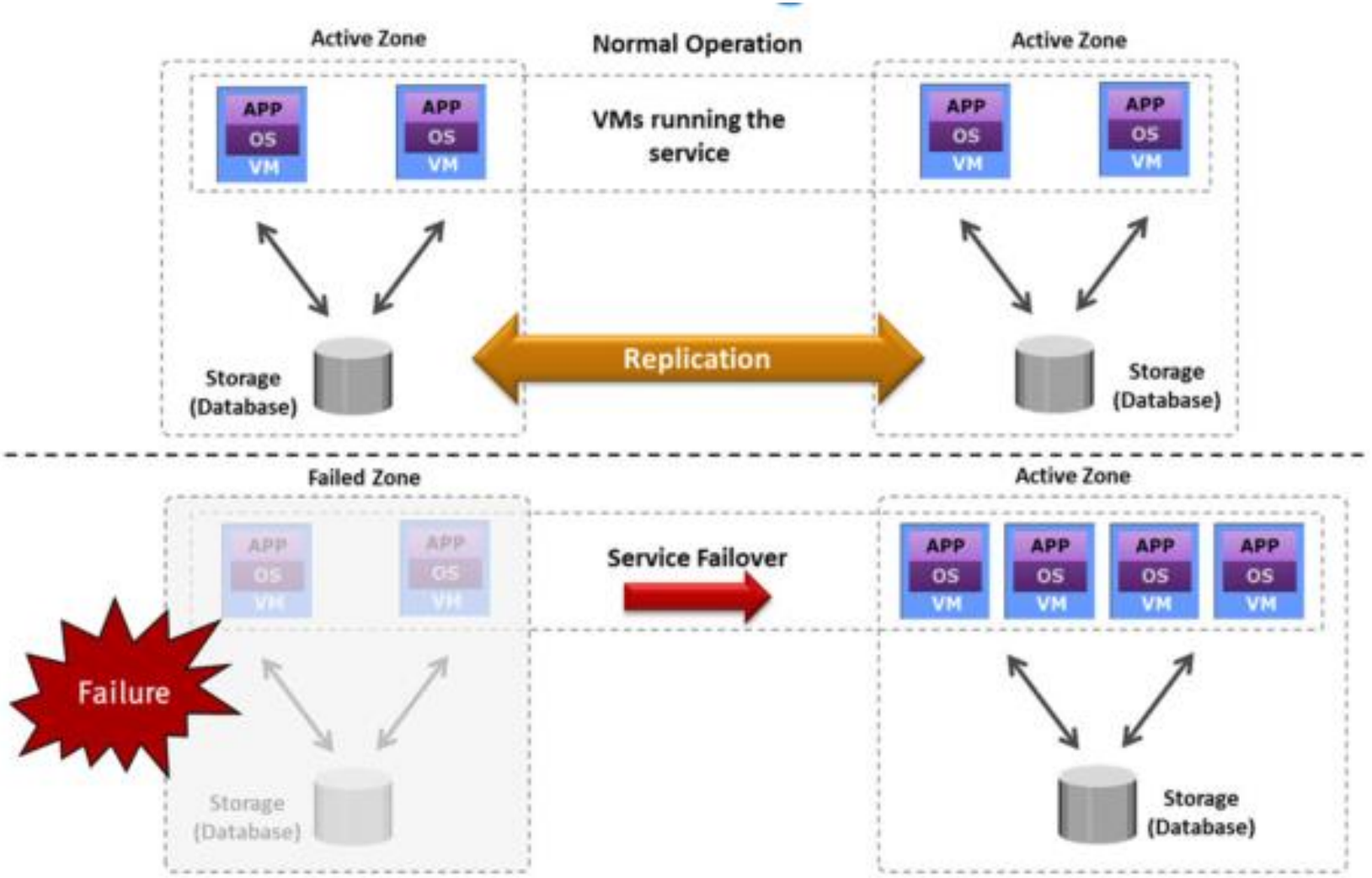
- Automated service failover
  - Ensures **robust** and consistent failover
  - Enables to meet **strict service levels**
  - Reduces **RTO**

- Why?
  - because manual steps are often **error prone** and may take **considerable time** to implement.

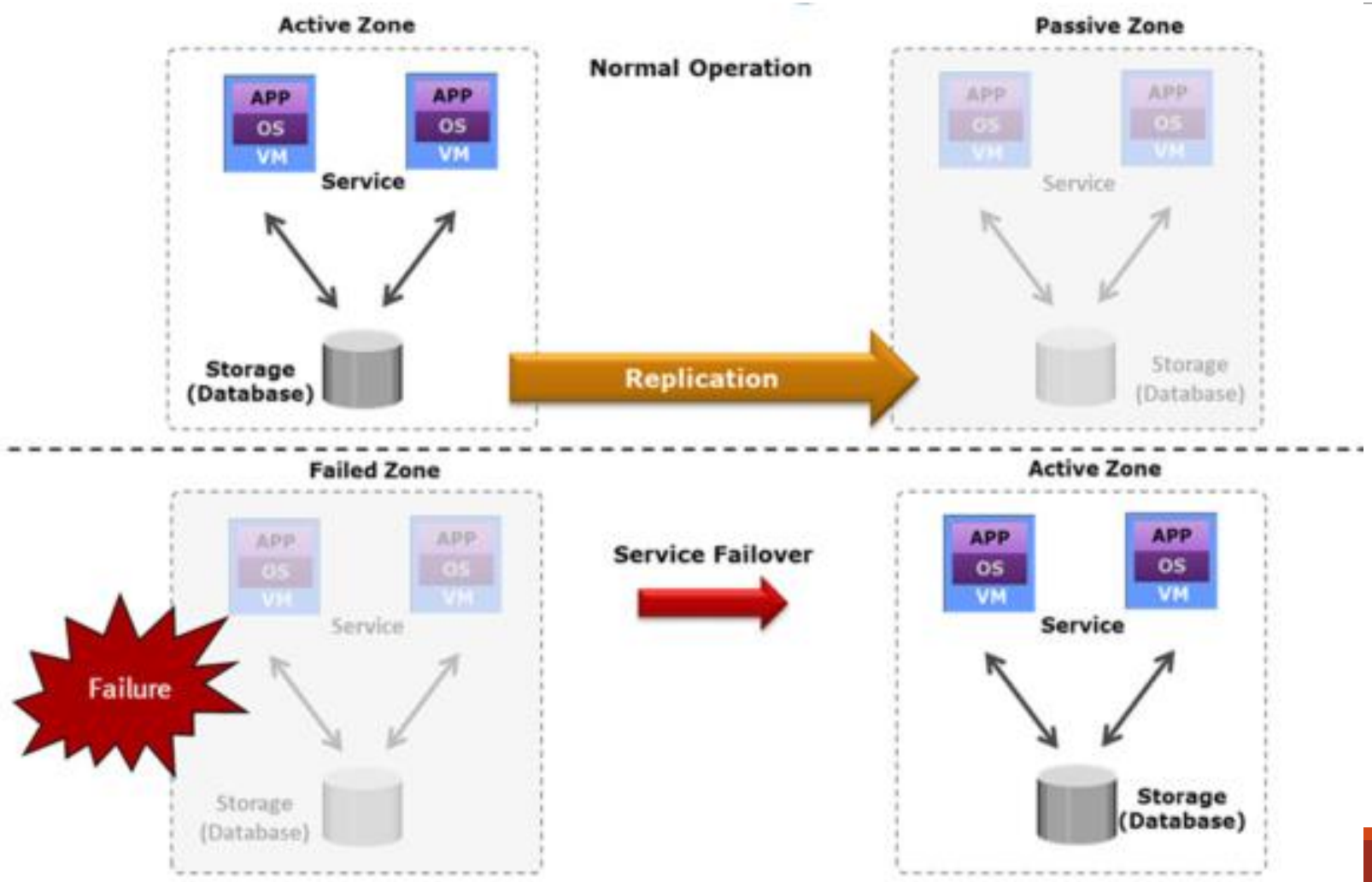
Automated Service Failover Across Zones

- Automated fail over process primarily depends on:
  - **Replication** across zones
  - **Live migration** with stretched cluster (zones in different remote locations)
  - **Reliable network** infrastructure between zones
- Zones can be configured as **active/passive** and **active/active** configurations

Active/Active Zone Configuration



Active/Passive Configuration



Lecture Outline:

Part Four: Data Protection Solution - Backup

- Backup and recovery
- Backup requirements in a cloud environment
- Guest-level and image-level backup method
- Backup as a Service
- Backup service deployment options
- Deduplication for backup environment

Data Protection Overview

- Protecting critical data ensures availability of services
  - Seamless service failover requires the availability of data
- protect the data from accidentally **deleting files**, **application crashes**, **data corruption** and **disaster**.
- Data should be protected at **local location** and as well as to a remote location to ensure the availability of service.

Data Protection Overview

- Individual services and associated data sets have different business values, require different data protection strategies
- Two common data protection solutions:
  - Backup
  - Replication

Introduction to Backup and Recovery

- A backup is an **additional copy** of production data, created and retained for the sole purpose of **recovering** the **lost** or **corrupted** data.
- RPO and RTO are the primary considerations in selecting and implementing a specific backup strategy
  - RPO specifies the time interval between two backups
  - RTO relates to the time taken to recover data from backup
    - RTO influences the type of backup target that should be used

Introduction to Backup and Recovery

- To implement a successful backup and recovery solution
  - Service providers need to evaluate the backup methods along with their recovery considerations and retention requirements

Backup Requirements in a Cloud Environment

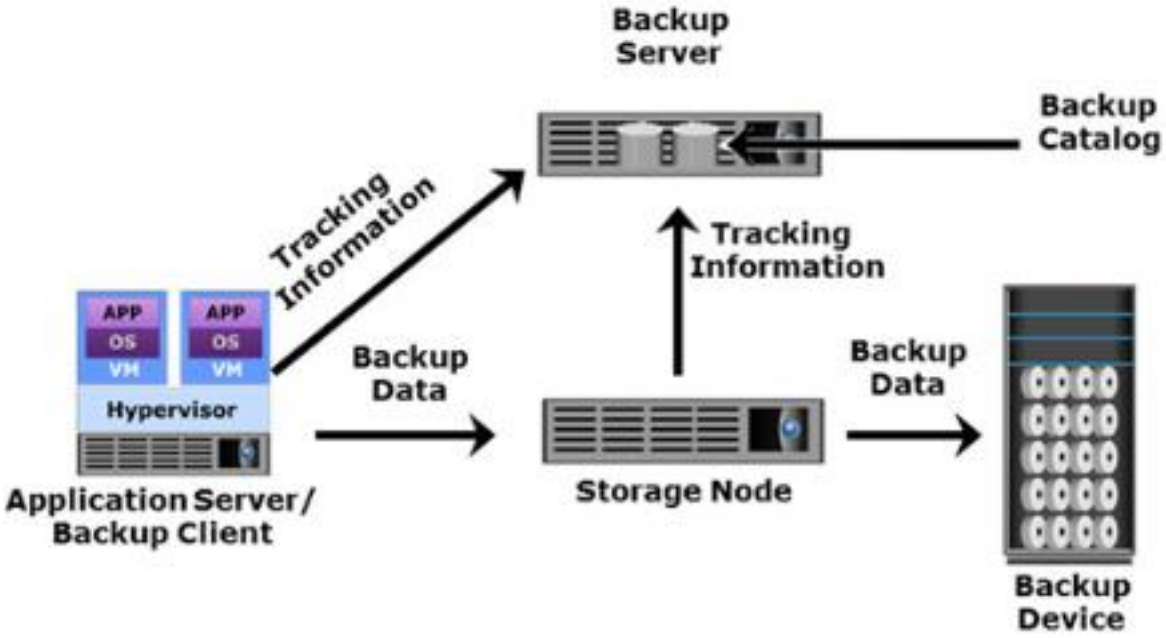
- Backup requires integration between backup application and management server of virtualized environment
- Backup requirements may differ from one service to another based on RTO and RPO
- Recovery requires file level and/or full VM recovery

Backup Requirements in a Cloud Environment

- Huge volume of redundant data in the backup environment
  - Large number of VMs having identical data and configurations
- Backing up of redundant data would significantly impact the backup window and increase the operating expenditure. Service provider needs to consider ***deduplication*** techniques to overcome these challenges.
- Backup and recovery operations need to be automated

Key Backup Components

- Backup client
  - Gathers the data that is to be backed up
  - Sends the data to the storage node
- Backup server
  - Manages backup operations
  - Maintains backup catalog
- Storage node
  - Responsible for writing data to backup device
- Backup device (backup target)
  - Tape library, disk library, and virtual tape library



Backup Targets

Backup Targets	Description
Tape Library	• Tapes are portable and can be used for long term offsite storage • Must be stored in locations with a controlled environment • Not optimized to recognize **duplicate** content • Data **integrity and recoverability** are major issues with tape-based backup media
Disk Library	• Enhanced backup and recovery performance • Disks also offer faster recovery when compared to tapes • Disk-based backup appliance includes features such as **deduplication**. **compression**, **encryption**, and **replication** to support business objectives
Virtual Tape Library	• Disks are **emulated and presented as** tapes to backup software • Does not require any additional modules or changes in the legacy backup software • Provides better **performance and reliability** over physical tape • Does not require the usual maintenance tasks associated with a physical tape drive, such as periodic cleaning and drive calibration

Backup Methods

- Two key backup methods:
  - Guest-level
  - image-level

Guest-level Backup

- Backup agent is installed on each VM
  - Performs file-level backup and recovery
  - Does not backup VM configuration files

- Performing backup on multiple VMs on a compute system may **consume more resources** and lead to **resource contention**
  - Impacts performance of applications running on VMs

Image-level Backup

- Creates a copy of the **entire virtual disk** and **configuration data** associated with a particular VM
  - Backup is saved as a **single entity** called a **VM image**
  - No backup agent is required inside the VM to backup

Backup as a Service

- Enables consumers to procure **backup services on demand**
  - Provides **offsite** backup for consumer desktops, laptops, and application servers
  - Backs up data to the cloud storage
- Reduces the backup management overhead
  - Pay-per-use/subscription-based pricing
- Gives consumers the flexibility to select a **backup technology** based on their current requirements

Backup Service Deployment Options

- Managed backup service
  - suitable when a **cloud service provider already hosts** consumer applications and data
  - Backup is offered by the **provider** to protect consumers data
  - Back up is managed by the service **provider**
- Replication Backup service
  - Service provider only **manages data replication** and IT infrastructure at the disaster recovery site
  - Local backup is managed by the consumers
- Remote backup service
  - Service provider receives data from consumer.
  - Backup is managed by service provider.

Introduction to Data Deduplication

- Deduplication is the **process of detecting and identifying** the unique data segments (chunk) within a given set of data to eliminate redundancy.

- Data deduplication operates by **segmenting a dataset** into blocks and identifying redundant data and **writing the unique** blocks to a backup target.

Introduction to Data Deduplication

- To identify redundant blocks in the backup data, the data deduplication system creates a **hash value** or **digital signature**—like a fingerprint—for each data block and an index of the signatures for a given repository.

- When the data deduplication system sees a block it has processed before, instead of storing the block again, it **inserts a pointer** to the original block in the repository.

Deduplication Granularity Level

- File-level deduplication
  - Detects and removes redundant copies of **identical files**
  - Only one copy of the file is stored; the subsequent copies are replaced with a pointer to the original file
    - Does not address the problem of duplicate content inside the files
  - For example, two 10-MB presentations with a difference in just the title page are not considered as duplicate files, and each file is stored separately.
- Sub-file level deduplication
  - Breaks files down to **smaller segments**
    - Detects redundant data within and across files
  - Two methods:
    - Fixed-length block
    - fixed-length block deduplication divides the files into fixed length blocks and uses a hash algorithm to find duplicate data.
    - Variable-length block

Deduplication Method

- Source-based deduplication
  - Eliminates redundant data at the **source** (backup client)
  - Client sends only **new, unique segments** across the network
  - Reduces **storage and network bandwidth** requirements
  - Increases **overhead** on the backup client

- Target-based deduplication
  - **Offloads** deduplication process from the backup client
  - Data is deduplicated at the target either inline or post-process
  - backup application sends data to the target backup device where the data is deduplicated

Lecture Outline:

Part Four: Building Fault Tolerance Cloud Infrastructure -1

- Replication and its types
- Snapshot and mirroring
- Disaster Recovery as a Service (DRaaS)

Introduction to Replication

- Process of creating an **exact copy** (replica) of the data for ensuring availability of services.
- Replica copies are used to **restore and restart services** if data loss occurs
  - Based on the SLA for the service being offered to the consumers, data can be replicated to **one or more locations**
- Replication can be classified
  - Local replication
    - Snapshot and mirroring
  - Remote replication
    - Synchronous and asynchronous

Backup vs Replication

- Replicas are **immediately accessible** by the application, but a backup copy must be restored by backup software to make it accessible to applications.
- Backup is always a **point-in-time** copy, but a replica can be a **point-in-time** copy or continuous.
- Backup is typically used for **operational or disaster recovery** but replicas can be used for **recovery and restart**.
- Replicas typically provide **faster RTO** compared to recovery from backup.

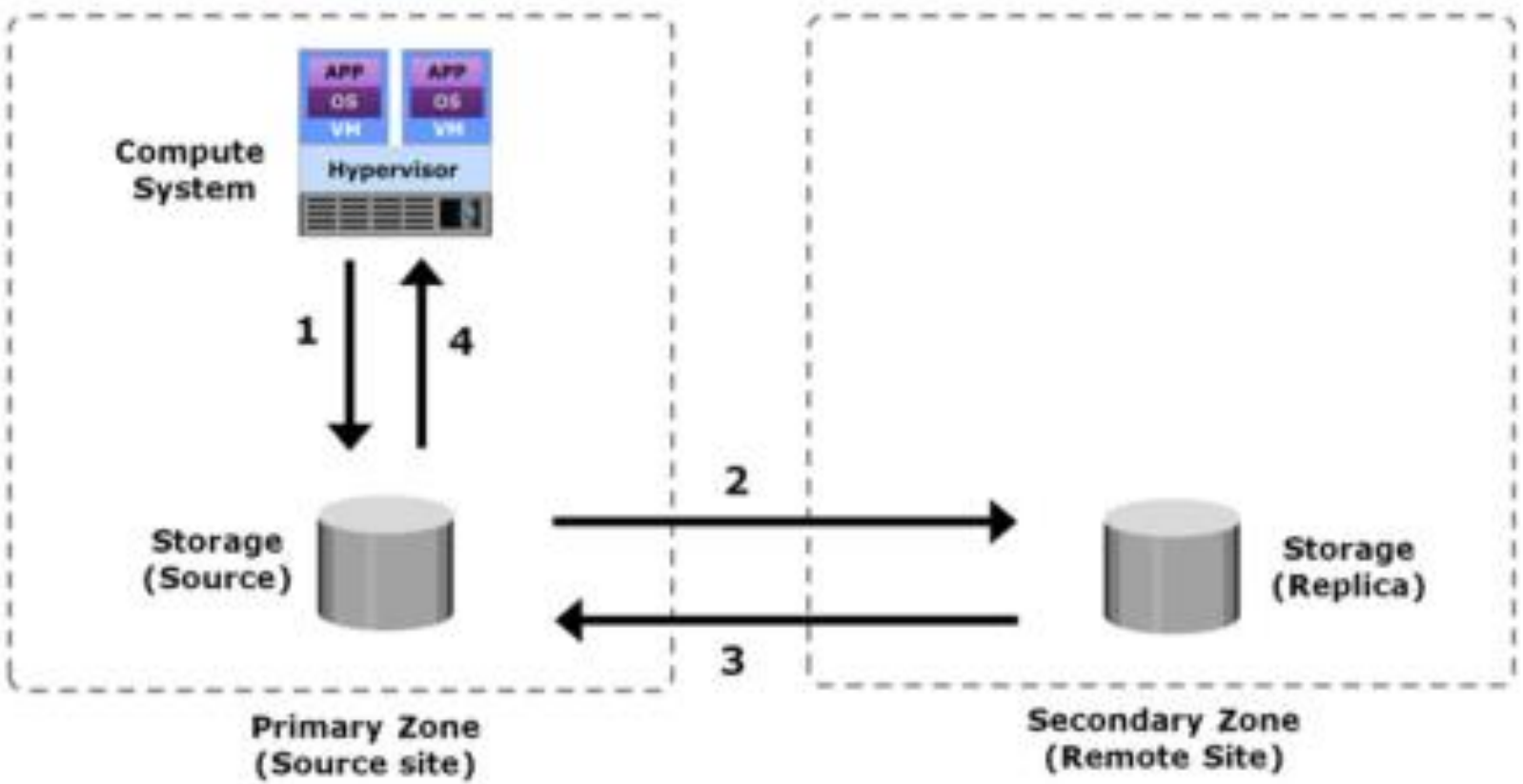
Local Replication: Snapshot

- A virtual copy of a **set of files**, or volume as they appeared in a particular PIT (point in time)
  - Provides the ability to restore the files or volumes if there is a data loss or corruption
- Virtual machine snapshot is a common snapshot technique, that preserves the **state and data** of a VM at a specific PIT
  - Snapshots hold **only changed** blocks
  - The VM state includes VM files, such as BIOS, VM configurations, and its power state
  - This VM snapshot is useful for quick restore of a VM

Remote Replication: Synchronous

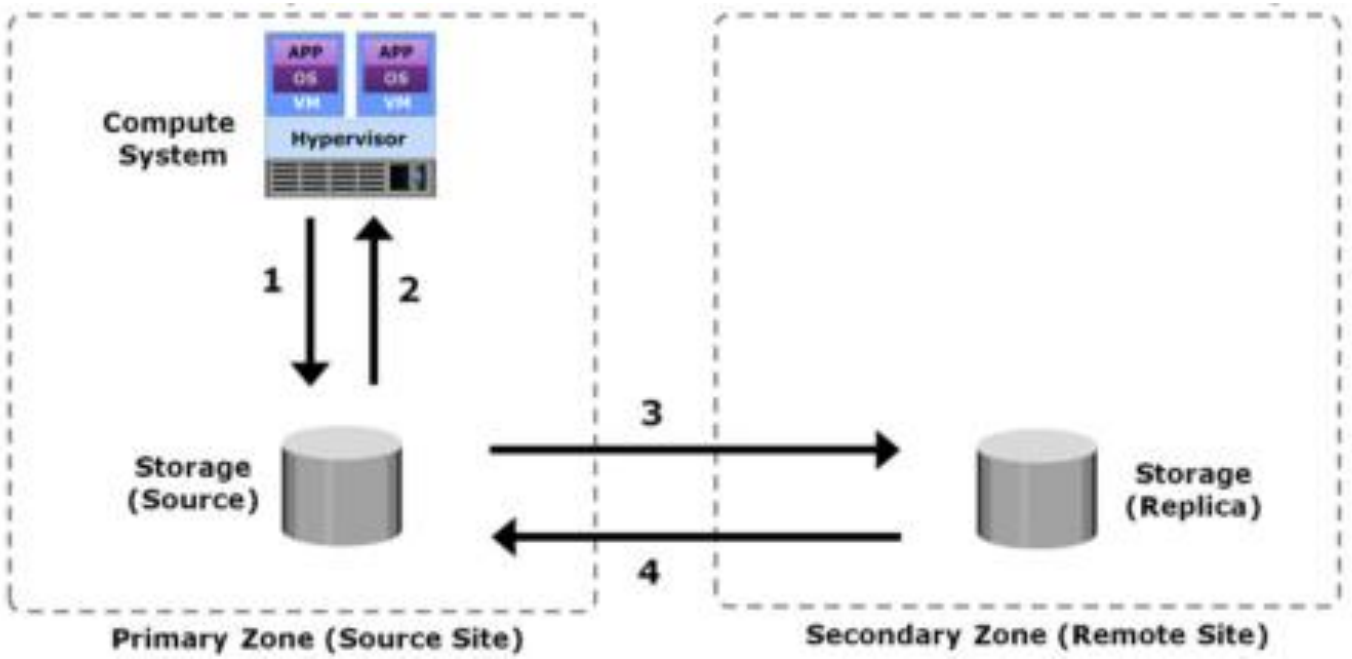
- Write is committed to both the **source and the remote replica** before it is **acknowledged** to the compute system
- Ensures that the source and the replica have identical data at all times
  - Provides near zero RPO
- *Application response time is increased with synchronous remote replication because writes must* **be committed on both the source and the target** *before sending the "write complete" acknowledgment to the compute system.*

Remote Replication: Synchronous



Remote Replication: Asynchronous

- A write is committed to the source and immediately acknowledged to the compute system
- Data is buffered at the source and transmitted to the remote site later
- Replica will be behind the source by a finite amount (finite RPO)

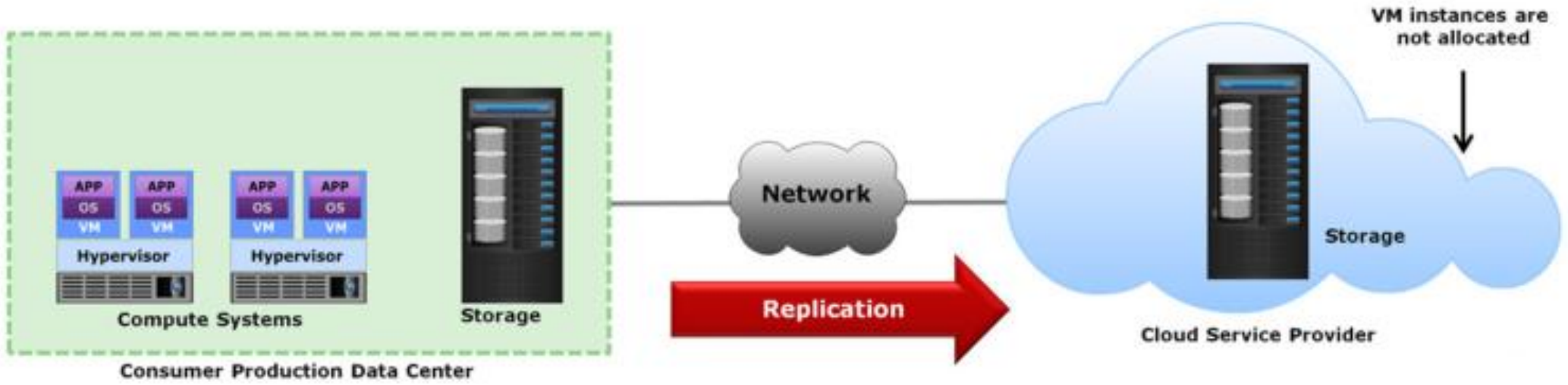


Replication Use Case: DRaaS

- Service provider offers resources to enable consumers to run their IT services in the event of a disaster
  - Resources at the service provider location can be ***dedicated to the consumer*** or they can be shared
- Replication is a key technique used by the service provider in order to offer DRaaS to the consumers
- Service provider should design, implement, and document a DRaaS solution specific to the customer's infrastructure

DRaaS - Normal Production Operation

- IT services run at the consumer's production data center
- Replication occurs from the consumer production environment to the service provider's data center over the network
- Data is usually encrypted while replicating to the provider's location



DRaaS - Business Disruption

- Business operations failover to the provider's infrastructure in the event of a disaster at consumer's data center
  - Users at the consumer organization are redirected to the cloud
- Typically VM instances are created from a pool of compute
  - Connect replicated storage to each of the newly activated VMs