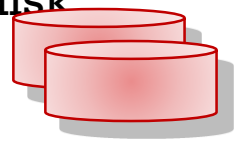
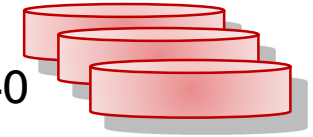
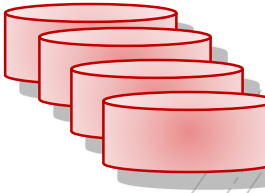
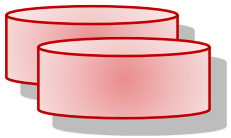
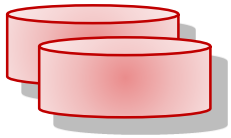
سبر 1213
Network Defense

Lecture #9 Part 2
Implementing Controls to Protect Assets

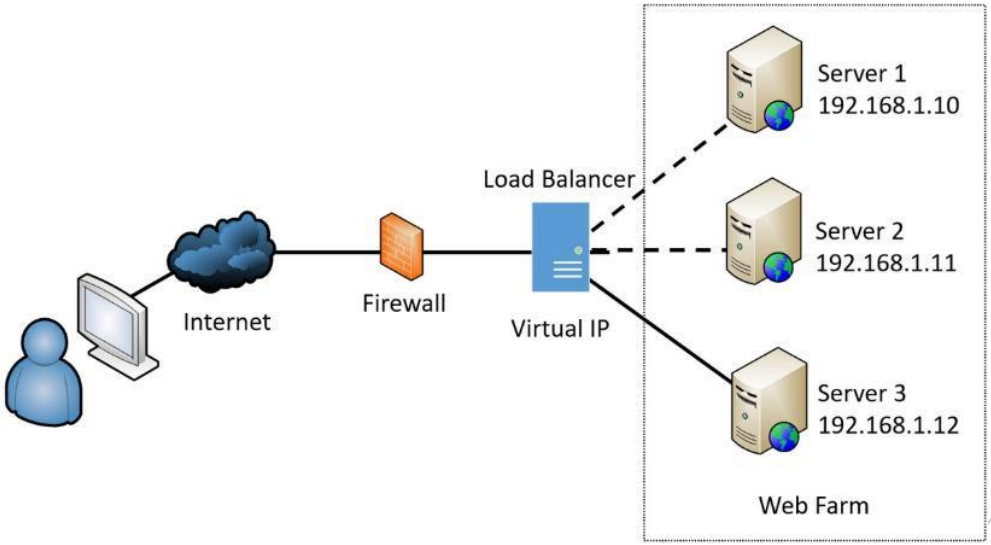
Disk Redundancies

- RAID-0 no redundancy
  - Two or more disks
- RAID-1 uses two disks as a mirror
  - Two disks
- RAID-5 can survive failure of one disk
  - Three or more disks
- RAID-6 can survive failure of two disks
  - Four or more disks
- RAID-10 combines RAID-1 and RAID-0
  - Even number of disks

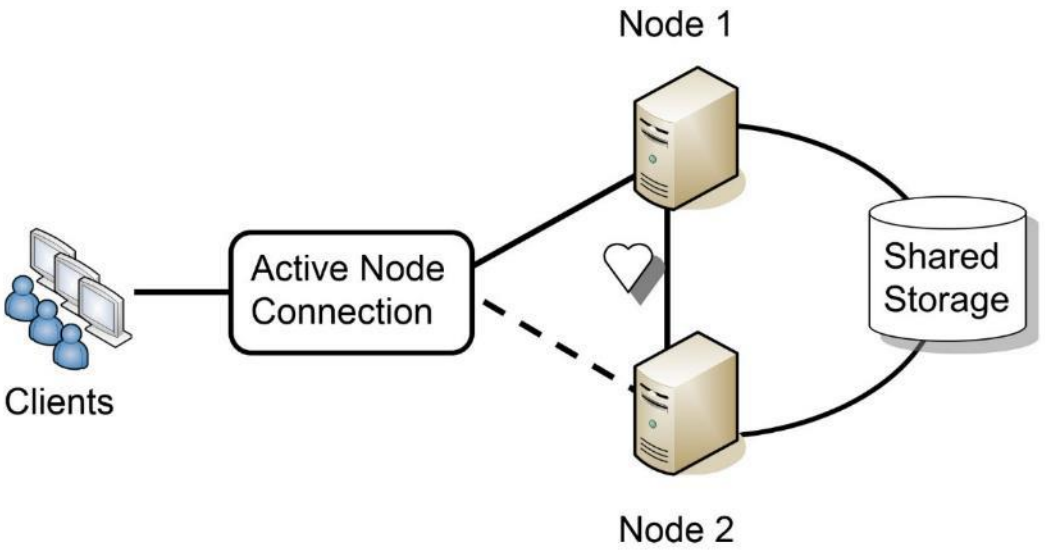
Load Balancers

- Active/active load balancer
  - Affinity



Load Balancers

- Active/passive load balancer



Power Redundancies

- **UPS**
  - **Provides short-term fault tolerance for power**
  - **Can protect against power fluctuations**
- **Dual supply**
- **Generators provide long-term fault tolerance for power**
- **Managed power distribution units**

Protecting Data with Backups

- **Backup media**
  - **Network-attached storage (NAS)**
  - **Storage area network (SAN)**
  - **Cloud**
- **Online backups**
- **Offline backups**

Backups Types

- **Full backups**
  - **Fastest recovery time**
- **Differential backup**
  - **Backs up all the data that has changed since the last full or differential backup**
- **Incremental backup**
  - **Backs up all the data that has changed since the last full or incremental backup**

Protecting Data with Backups

- Snapshot backup
- Image backup
- Copy backup
- Testing backup

Geographic Considerations

- Off-site storages
- Distance
- Location selection
- Legal implications
- Data sovereignty

Business Continuity Elements

- Protect against disasters and outages
  - Fires
  - Attacks
  - Power outages
  - Data loss from any cause
  - Hardware and software failures
  - Natural disasters, such as hurricanes, floods, tornadoes, and earthquakes

Business Continuity Elements

- Business impact analysis (BIA) identifies:
  - Systems and components that are essential to the organization's success (must continue to operate)
  - Maximum downtime limits for these systems and components
  - Scenarios that can impact these systems and components
  - Potential losses from an incident
  - Assets to include in recovery plans

Business Continuity Elements

- **Impact**
- **Recovery Time Objective (RTO)**
  - **Identifies maximum amount of *time* it should take to restore a system after an outage**
  - **Derived from maximum allowable outage *time* identified in the BIA**
- **Recovery Point Objective (RPO)**
  - **Refers to the amount of *data* an organization can afford to lose**

Risk Metrics

- Mean time between failures (MTBF)
  - Provides a measure of a system's reliability
  - Usually represented in hours
  - MTBF indicates the device can be repaired
- Mean time to recover or mean time to repair (MTTR)
  - The time it takes to restore a failed system
  - Often specified in contracts as a target

Continuity of Operations Sites

- Provides an alternate location for operations after a critical outage
- Most common sites are hot, cold, and warm sites
- Hot site
  - Includes personnel, equipment, software, and communications capabilities of the primary site
  - All the data is up to date
  - Can take over for a failed site within an hour
  - Most effective disaster recovery solution for an alternate site
  - Most expensive to maintain

Continuity of Operations Sites

- Cold site
  - Has power and connectivity needed for COOP activation, but little else
  - Least expensive and hardest to test
- Warm site
  - Compromise between a hot site and a cold site
- Order of restoration
  - Return least critical functions first