20- Implementing Cybersecurity Resilience

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Outlines

20.1- Implement Redundancy Strategies

20.2- Implement Backup Strategies

Labs

Lab 27: Backing Up and Restoring Data in Windows and Linux

20.1- Implement Redundancy Strategies

20.2- Implement Backup Strategies

HIGH AVAILABILITY

- One of the key properties of a resilient system is high availability.
- Availability is the percentage of time that the system is online, measured over the defined period, typically one year.
- High availability is usually loosely described as **24x7** (24 hours per day, 7 days per week) or **24x365** (24 hours per day, 365 days per year).
- For a critical system, availability will be described as "**two-nines**" (99%) up to five- or six-nines (99.9999%).

HIGH AVAILABILITY (cont.)

Availability	Annual Downtime (hh:mm:ss)
99.9999%	00:00:32
99.999%	00:05:15
99.99%	00:52:34
99.9%	08:45:36
99%	87:36:00

POWER REDUNDANCY

- All types of computer systems require a stable power supply to operate.
- Electrical events, such as voltage spikes or surges, can crash computers and network appliances, while loss of power from blackouts will cause equipment to fail.
- Power management means deploying systems to ensure that equipment is protected against these events and that network operations can either continue uninterrupted or be recovered quickly.
- An enterprise-class server or appliance enclosure is likely to feature two or more power supply units (PSUs) for redundancy.
- A hot plug PSU can be replaced (in the event of failure) without powering down the system.

NETWORK REDUNDANCY

- Network Interface Card (NIC) Teaming
  - ✓ Network interface card (NIC) teaming, or adapter teaming, means that the server is installed with multiple NICs, or NICs with multiple ports, or both.
  - ✓ Each port is connected to separate network cabling. During normal operation, this can provide a high-bandwidth link.
  - ✓ For example, four 1 Gb ports gives an overall bandwidth of 4 Gb.
  - ✓ If there is a problem with one cable, or one NIC, the network connection will continue to work, though at just 3 Gb.
- Load Balancers
  - ✓ A load balancing switch distributes workloads between available servers.
  - ✓ A load balancing cluster enables multiple redundant servers to share data and session information to maintain a consistent service if there is failover from one server to another.

DISK REDUNDANCY

- Disk and storage resources are critically dependent on redundancy.
- While backup provides integrity for when a disk fails, to restore from backup would require installing a new storage unit, restoring the data, and testing the system configuration.
- Disk redundancy ensures that a server can continue to operate if one, or possibly more, storage devices fail.
- When a storage system is configured as a Redundant Array of Independent Disks (RAID), many disks can act as backups for each other to increase reliability and fault tolerance.
- If one disk fails, the data is not lost, and the server can keep functioning.

20.1- Implement Redundancy Strategies

20.2- Implement Backup Strategies

BACKUPS

- Every business continuity and disaster recovery plan makes use of backups, of one type or another.
- The execution and frequency of backups must be carefully planned and guided by policies.
- Backups are kept back to certain points in time.
- As backups take up a lot of space, and there is never limitless storage capacity, this introduces the need for storage management routines to reduce the amount of data occupying backup storage media while giving adequate coverage of the required recovery window.

BACKUP TYPES

- When considering a backup made against an original copy of data, the backup can usually be performed using one of three main types: **full**, **incremental**, and **differential**.

Type	Data Selection	Backup/Restore Time	Archive Attribute
Full	All selected data regardless of when it was previously backed up	High/low (one tape set)	Cleared
Incremental	New files, as well as files modified since the last backup	Low/high (multiple tape sets)	Cleared
Differential	All new and modified files since the last full backup	Moderate/moderate (no more than two sets)	Not Cleared

BACKUP TYPES (cont.)

- Assuming a backup is performed every working day, an incremental backup only includes files changed during that day, while a differential backup includes all files changed since the last full backup.
- Incremental backups save backup time but can be more time-consuming when the system must be restored.
- The system must be restored from the last full backup set and then from each incremental backup that has subsequently occurred.

Lab

Lab 27: Backing Up and Restoring Data in Windows and Linux