

DAY 19

DATE:19/05/2025

NAME: ANNIE JOHN

USER ID:27739

Batch: 25VID0885_DC_Batch4

TITLE: STORAGE SYSTEMS, BACKUP - POLICY AND STRATEGY AND MONITORING TOOLS

➤ **STORAGE SYSTEMS**

A storage system refers to the technology and infrastructure used to store, manage, and access digital data. It's a core part of IT environments in personal, business, and enterprise use.

➤ **Components of a Storage System**

1. Storage Devices – Physical hardware (HDDs, SSDs, tape drives, optical discs).
2. Controllers – Manage data read/write operations.
3. Interfaces – Connect storage to systems (e.g., SATA, SAS, NVMe, iSCSI, Fibre Channel).
4. Protocols – Define communication (e.g., SMB, NFS, iSCSI).
5. Software – Manages redundancy, replication, snapshots, etc.

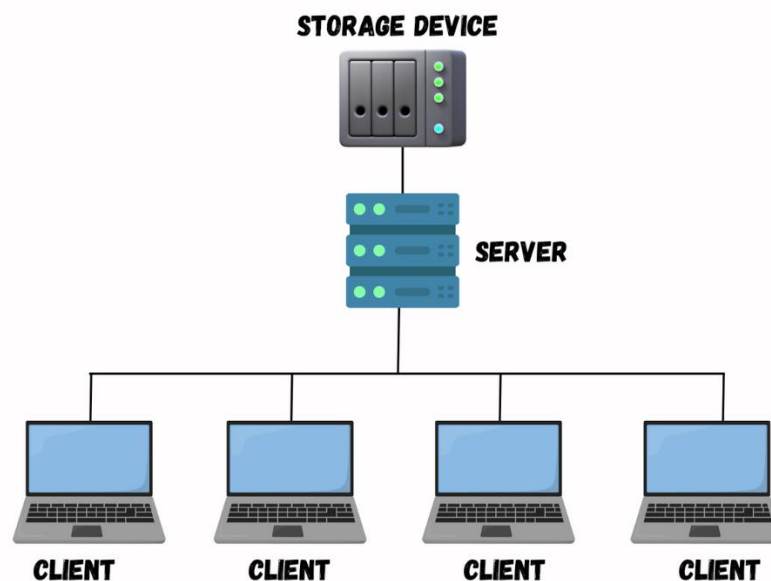
➤ **TYPES OF STORAGE SYSTEMS**

Type	Description	Best For
DAS (Direct Attached Storage)	Storage directly connected to one computer/server (e.g., USB, internal drives)	Personal, small business
NAS (Network Attached Storage)	File-level storage accessed over a network (uses SMB/NFS)	File sharing, home/office backup
SAN (Storage Area Network)	Block-level storage connected via high-speed networks (Fibre Channel/iSCSI)	Large-scale enterprise, virtualization

Type	Description	Best For
Cloud Storage	Data stored offsite on cloud providers' infrastructure	Scalable storage, remote access
Object Storage	Stores data as objects with metadata and ID (e.g., Amazon S3)	Big data, unstructured data, cloud-native apps



DAS (DIRECT ATTACHED STORAGE)



➤ **iSCSI (Internet Small Computer Systems Interface)**

iSCSI is a **network protocol** that allows block-level access to storage devices over IP networks.

Think of it like: Turning a remote storage device into a "local" hard drive over a network.

How It Works:

- Initiator (usually the server) connects to the target (iSCSI storage device).
- Server uses the remote disk **as if it were a local drive**.
- Can use standard Ethernet networks.

Key Benefits:

- **Cost-effective** compared to Fibre Channel SAN
- **Uses existing Ethernet infrastructure**
- Supports high availability and scalability
- Good for **virtualization (e.g., VMware, Hyper-V)**

Common Use Cases:

- Storage Area Networks (SANs)
- Server virtualization storage
- Backup and disaster recovery solutions

➤ **Backup**

Backup is the process of copying data from a primary location to a secondary one to protect it in case of loss, corruption, or disaster.

Why it's important:

- Recover from accidental deletion or hardware failure
- Protection against ransomware
- Disaster recovery (fires, floods, etc.)
- Compliance with data retention laws

➤ **Types of Backups**

1. Full Backup

- A complete copy of all selected data.
- **Pros:** Easiest to restore, complete snapshot.
- **Cons:** Slow and requires the most storage.

2. Incremental Backup

- Only backs up data changed **since the last backup** (either full or incremental).
- **Pros:** Fast and storage-efficient.
- **Cons:** Slower restore time, as it needs to piece together data from the full backup and each incremental one.

3. Differential Backup

- Backs up data changed **since the last full backup**.
- **Pros:** Faster than full backup, quicker restore than incremental.
- **Cons:** Grows in size over time until next full backup.

4. Mirror Backup

- An exact mirror copy of the source data.
- **Pros:** Fast recovery.

- **Cons:** Deletes mirrored files if they're deleted on the source (dangerous without versioning).

5. Cloud Backup

- Backups stored in a cloud storage provider (AWS, Google Drive, etc.).
- **Pros:** Offsite, scalable, accessible anywhere.
- **Cons:** Requires internet, recurring costs.

➤ **BACKUP POLICY**

A **backup policy** is the official set of **rules and guidelines** for creating, storing, and managing data backups in an organization.

➤ **Backup Policy Components**

1. Purpose

- The purpose of this backup policy is to ensure that all critical organizational data is regularly and securely backed up, and that data can be restored quickly and accurately in the event of data loss due to hardware failure, cyberattacks, accidental deletion, or natural disasters.
- A strong backup policy supports **business continuity**, **minimizes downtime**, and helps meet **legal and regulatory obligations**.

2. Scope

This policy applies to:

- All **production systems, databases, and applications**
- **User workstations, file servers, email systems**
- **Cloud services** (if storing company data)
- **Virtual machines, network configurations, and system settings**
- Employees, contractors, and any other parties with access to the organization's data

3. Roles and Responsibilities

Role	Responsibility
IT Administrator	Configure and monitor backup jobs; perform test restores
Backup Operator	Run scheduled backups, manage storage media
Data Owners	Identify what data needs to be backed up

Role	Responsibility
Compliance Officer	Ensure policy aligns with legal and regulatory requirements
Management	Approve the policy; allocate resources for backup infrastructure
Users	Save data to designated backup locations (e.g., mapped drives or folders)

4. Compliance and Legal Requirements

The organization must ensure backups comply with relevant **laws, regulations, and industry standards**:

Regulation	Requirement
GDPR (EU)	Right to access, erase, and recover data
HIPAA (US)	Secure storage and restoration of health data
SOX (US)	Retention and integrity of financial records
ISO 27001	Backup controls for information security

Backups must be **encrypted, access-controlled, and retained** for the legally required time periods.

5. Documentation and Logging

Proper records must be maintained for transparency, audits, and troubleshooting:

A. Backup Documentation Includes:

- Backup schedule (what, when, where)
- Tools/software used
- Retention periods
- Recovery procedures
- Encryption and storage methods
- Access control measures

B. Logging Includes:

- Backup success/failure logs
- Restore attempt logs
- Changes to backup configurations

- Alerts or errors during backup jobs
- User access to backup data

➤ **Backup Strategy**

This strategy defines **how** backups are carried out to ensure the availability, security, and recoverability of business-critical data.

1. Frequency

The frequency defines **how often** data is backed up, based on the data's importance and how frequently it changes.

Data Type	Backup Frequency
Critical databases	Real-time or every 1–4 hours
File servers	Daily incremental + weekly full backup
User workstations	Daily or weekly
System configurations	Weekly or after any major changes

2. Storage Location

Data should be stored in **multiple, redundant locations** to reduce risk.

Storage Location	Description
On-site Storage	Local NAS, external drives, backup servers
Off-site Storage	Another physical location (e.g., branch office)
Cloud Backup	AWS S3, Azure Blob, Google Cloud Storage
Hybrid Backup	Combines local speed with off-site safety

3. Retention Policy

Defines **how long backups are kept**, based on business needs and legal requirements.

Backup Type	Retention Period
Daily	7–14 days
Weekly	1–3 months
Monthly	1–2 years
Yearly/Archive	5–7+ years (for compliance or tax records)

Use **automated retention policies** to delete old backups and manage storage costs.

4. Encryption and Security

Security ensures backups are **protected from unauthorized access or data breaches**.

Security Measure	Description
At-Rest Encryption	Encrypt backup files using AES-256 or higher
In-Transit Encryption	Use SSL/TLS for data transfer
Access Control	Role-based access, admin-only write access
MFA (Multi-Factor Auth)	Required for accessing backup systems
Immutable Backups	Prevent deletion/modification for ransomware protection

Always test encryption key management and recovery access.

5. Disaster Recovery Integration

Backups must be an active part of the **disaster recovery (DR)** and **business continuity plan**.

Integration Aspect	Description
Recovery Time Objective (RTO)	How quickly systems must be restored (e.g., 4 hours)
Recovery Point Objective (RPO)	How much data loss is acceptable (e.g., 15 minutes)
Restore Testing	Monthly restore tests to verify backup integrity
DR Runbooks	Step-by-step recovery documentation for critical systems
Failover Plan	For cloud or hybrid systems, ensure auto-failover options






















Regularly simulate disasters (e.g., server crash) to test full backup-to-recovery flow.

➤ MONITORING TOOL

A **monitoring tool** is a software application used in computer systems to track various metrics such as CPU load, network bandwidth, server services, and disk space to detect issues and alert administrators before users are affected. **Splunk** is one of the **most famously used** tools in IT and cybersecurity.

Monitoring tools

From sources across the web

 Datadog	▼	 New Relic	▼	 Dynatrace	▼
 Zabbix	▼	 AppDynamics	▼	 Nagios	▼
 Prometheus	▼	 Paessler PRTG	▼	 Performance monitoring	▼
 Database monitoring	▼	 ManageEngine Site24x7	▼	 Grafana	▼
 Kibana	▼	 ManageEngine OpManager	▼	 Splunk	▼
 Security monitoring	▼	 WhatsUp Gold	▼	 Checkmk	▼
 Stackdriver	▼	 Infrastructure monitoring	▼	 Log monitoring	▼

➤ What Is an SLA?

SLA stands for **Service Level Agreement** — it is a **formal contract** between a **service provider** and a **customer** that defines the **expected level of service**.

➤ Why SLAs Are Important

- Sets clear expectations between customers and providers
- Protects both parties legally
- Measures performance with clear metrics
- Improves accountability and customer satisfaction
- Provides remedies if commitments aren't met

➤ What Is Ticketing in IT?

Ticketing refers to the process of **tracking and managing IT issues, requests, and tasks** using a software system called a **ticketing system** or **help desk system**.

Each issue or request is recorded as a **ticket**, which contains important details like:

- Who reported the issue
- What the issue is
- When it occurred
- Current status (open, in progress, resolved)
- Priority and assigned technician