Storage Basics

Storage Basics

- Storing data digitally.
- 3 major keywords:
  - Availability
  - Integrity
  - Security

Types of storage

- Primary storage
  - RAM
  - Cache
- Secondary storage
  - HDD
  - SSD
  - NVMe
- Long-term storage
  - Tape drives
  - CD/DVD
  - Blu-rays
- Cloud storage
  - AWS → S3 bucket
  - Azure → Azure storage account
  - Google → Google cloud storage

Storage Architecture

- DAS
- NAS
- SAN

Storage Architecture - DAS

- Direct Attached Storage (DAS)
  - it will be connected directly to the server/machine
  - using a small, single cable.
  - ex:
    - External HDD
    - External SSD
    - Pen drives
  - Scalability is the issue

Storage Architecture - NAS

- Network-Attached Storage (NAS)
  - Dedicated storage within the network
  - Uses file-based storage

1. NFS - Network File Share
   - Used for transferring data between linux to linux & windows to windows
   - L <--> L
   - W <--> W

2. SMB - Samba server
   - mostly used in cloud technologies
   - current version: 4.0
   - cross platform
   - L <--> W
   - W <--> L
   - L <--> L

Storage Architecture - SAN

- Storage Area Network (SAN)
- high speed, good performance storage designed for production
- it uses block level storage
  - iSCSI
  - Fiber channel
- it is scalable, supports virtualization, Expensive & complex
- Components of SAN
  1. storage devices
  2. server
  3. networking hardware
  4. software
- it works on MPIO (MultiPath Input Output)
- 3 types of SANs:
  - Fibre Channel
  - IP SAN (iSCSI)
  - Hybrid SAN

Storage virtualization

- Logical instance of physical storage to improve manageability
- technologies:
  - VMWare vSAN
  - Microsoft Storage Spaces
  - Linux LVM (Logical Volume Manager)

RAID – Redundant Array of Independent Disks

Performance & redundancy

- Different levels:
  - **RAID 0**
    - works on Striping
    - useful in storing data faster
    - no fault tolerance
  - **RAID 1**
    - works on mirroring concept.
    - has fault tolerance.
    - we are using only 50% of actual disk.
  - **RAID 5**
    - works on striping with parity
    - used for higher redundancy
    - even if one disk crashes, we can still recover the crashed disk information
    - Minimum 3 disks of equal sizes are required.
  - **RAID 6**
    - works on striping with dual parity
    - used for high redundancy
    - minimum 4 disks are required
  - **RAID 10**
    - Mirroring (RAID 1) + Striping (RAID 0)
    - used for high speed & redundancy
    - its n expensive solution

Storage Protocols

- **Fiber Channel (FC)**
  - high speed network, used in SAN
- **iSCSI**
  - Internet Small Computer System Interface
  - used in TCP/IP for storage
- **NFS**
  - used in Linux/Unix/Windows
- **SMB**
  - Server Message Block
  - used in windows infra.
  - used in multi-platform network.
- **NVMe-oF**
  - NVMe Over Fabrics
  - high performance protocol for remote flash storage

FreeNAS

- FreeNAS, now rebranded as TrueNAS CORE.
- FreeNAS was rebranded as TrueNAS CORE in 2020.
  - open-source, free Network-Attached Storage (NAS) operating system based on FreeBSD.
- It is widely used for creating enterprise-grade storage solutions on commodity hardware.
- FreeNAS Hardware Requirements:
  - **CPU**: 64-bit processor (Intel or AMD).
  - **RAM**: Minimum 8GB RAM (recommended 16GB+ for ZFS).
  - **Storage**: At least one dedicated hard drive (SSD recommended for caching).
  - **Network**: Gigabit Ethernet or higher for optimal performance.

Key Features of FreeNAS / TrueNAS CORE

- **Open-Source & Free**
  - Developed by iXsystems, FreeNAS is completely open-source and free to use.
- **ZFS (Zettabyte File System) Support**
  - Uses ZFS, an advanced file system that provides:
    - Data integrity (checksumming to prevent data corruption).
    - Snapshots & Clones for data recovery.
    - RAID-Z for redundancy and fault tolerance.
- **Easy-to-Use Web GUI**
  - Web-based management (no CLI required for most tasks).
  - Allows users to configure storage, permissions, and network settings easily.

Key Features of FreeNAS / TrueNAS CORE

- **File Sharing & Protocol Support**
  - NFS (for Linux/Unix systems)
  - SMB/CIFS (for Windows)
  - AFP (for macOS)
  - iSCSI (for block storage and virtualization)
  - FTP/SFTP (for remote access)
- **Virtualization & Docker Support**
  - Built-in bhyve hypervisor for running virtual machines.
  - Can run Docker containers via RancherOS or a VM.
- **Backup & Replication**
  - Supports snapshot replication between NAS servers.
  - Can be used for offsite backup and disaster recovery.
- **Encryption & Security**
  - Supports disk encryption for data protection.
  - User authentication via Active Directory (AD), LDAP, and local accounts.
  - Two-Factor Authentication (2FA) available.

Introduction to backups

What is a Backup?

- A backup is a copy of data that is stored separately to protect against
  - data loss,
  - corruption, or
  - cyber threats.
- It ensures
  - data availability,
  - integrity, and
  - recoverability

  in case of accidental deletion, hardware failure, ransomware attacks, or natural disasters.

Why is Backup Important?

- **Data Protection**: Prevents loss due to hardware failures or accidental deletions.
- **Disaster Recovery**: Ensures business continuity after system failures or cyberattacks.
- **Compliance**: Meets legal and industry regulations for data retention.
- **Security**: Guards against ransomware, malware, and insider threats.

Types of Backup

- **Full Backup**
  - Creates a complete copy of all data.
  - Pros: Easy recovery.
  - Cons: Time-consuming, high storage usage.
- **Incremental Backup**
  - Saves only the changes made since the last backup.
  - Pros: Faster, uses less storage.
  - Cons: Recovery takes longer (requires full + incremental backups).

Types of Backup

- **Differential Backup**
  - Saves changes since the last full backup.
  - Pros: Faster restore than incremental.
  - Cons: Larger storage usage than incremental.
- **Mirror Backup**
  - Creates a real-time exact replica of data.
  - Pros: Fast recovery.
  - Cons: Does not keep old versions, high storage needs.
- **Snapshot Backup**
  - Captures a point-in-time state of data (used in virtualization and cloud storage).
  - Pros: Fast, minimal downtime.
  - Cons: Short-term solution, not ideal for long-term archiving

Backup Storage Types

- **Local Backup**
  - Stored on physical media (external HDD, NAS, SAN).
    - Pros: Fast access, no internet needed.
    - Cons: Vulnerable to physical damage (fire, theft, failure).
- **Cloud Backup**
  - Stored on remote servers (AWS, Azure, Google Cloud, Backblaze).
    - Pros: Scalable, offsite protection, automated.
    - Cons: Internet dependency, ongoing cost.
- **Hybrid Backup**
  - Combines local + cloud storage for best performance and security.
    - Example: Store daily backups locally, weekly backups in the cloud.

Backup Strategies

1. **3-2-1 Backup Rule**
   - 3 copies of data
   - 2 different storage types
   - 1 offsite backup
2. **Grandfather-Father-Son (GFS)**
   - Uses daily (son), weekly (father), and monthly (grandfather) backups for retention.
3. **Continuous Data Protection (CDP)**
   - Real-time backups whenever a change occurs

Backup Technologies & Tools

- **Windows Backup:**
  - Windows Server Backup, Veeam, Acronis.
- **Linux Backup:**
  - Rsync, Bacula, Amanda, Timeshift.
- **Cloud Backup:**
  - AWS Backup, Azure Backup, Google Cloud Backup.
- **Enterprise Backup:**
  - Veritas NetBackup, Commvault, IBM Spectrum Protect.

Granularity of backup

- The granularity of backup refers to the level of detail at which data is backed up and can be restored.
- It determines how much data can be recovered in a single restore operation.
- Backup granularity can range from entire systems to individual files or even application-specific objects.

Types of Backup Granularity

- **Full System Backup (Coarse Granularity)**
  - Includes the entire operating system, applications, settings, and user data.
  - Typically used for disaster recovery (DR).
  - Example: Image-based backup of a server using Veeam or Commvault.
- **Volume/Partition-Level Backup**
  - Backs up entire logical or physical disks.
  - Useful for restoring a specific drive without affecting others.
  - Example: Windows Volume Shadow Copy or LVM snapshots in Linux.
- **File-Level Backup**
  - Backs up individual files or directories.
  - Provides flexibility for recovering specific files rather than restoring an entire system.
  - Example: Traditional file-based backups using tools like Rsync or Windows Backup.

Types of Backup Granularity

- **Application-Level Backup**
  - Targets specific applications like databases, email systems, or virtual machines.
  - Ensures application consistency using APIs like VSS (Windows) or RMAN (Oracle).
  - Example: Microsoft Exchange mailbox backup or SQL database backup.
- **Object-Level Backup (Fine Granularity)**
  - Allows restoration of specific database tables, emails, or SharePoint objects.
  - Used in enterprise backup solutions.
  - Example: Restoring a single email from a Veeam Exchange backup.

Choosing the Right Granularity

- **For Disaster Recovery** → Full system or image-based backups.
- **For File Servers** → File-level or volume-level backups.
- **For Databases & Applications** → Application or object-level backups.
- **For Compliance & Archival** → Granular file and object-level backups for long-term storage.

Backups, Redundancy, and the Cloud

Aspect	Backup	Redundancy
Purpose	Protects against data loss by keeping copies	Ensures system availability with duplicate resources
Data Versioning	Maintains historical copies	Only mirrors or replicates current data
Use Case	Restoring lost, deleted, or corrupted files	Preventing downtime from hardware failures
Location	Can be local, offsite, or in the cloud	Usually on-premises or in a cloud region
Examples	Veeam, Commvault, NetBackup, Azure Backup	RAID, Load Balancers, Multi-AZ deployment in AWS

- **Key Takeaway:**
  - **Backups** help you recover data after corruption, accidental deletion, or ransomware attacks.
  - **Redundancy** ensures high availability but does **not** protect against accidental file deletions or cyber threats.

Cloud Backup Strategies

Types of Cloud Backups

- **Cloud-Native Backup (Backup directly to the cloud)**
  - Example: Azure Backup, AWS Backup, Google Cloud Backup
  - Best for: Workloads running in the cloud
- **Hybrid Backup (On-premise + Cloud)**
  - Example: Veeam Cloud Connect, Commvault Cloud Storage
  - Best for: Businesses needing local backups with cloud as a secondary copy
- **Cloud-to-Cloud (C2C) Backup**
  - Example: SaaS backups for Microsoft 365, Google Workspace
  - Best for: Protecting cloud applications

Combine Backup & Redundancy for Full Protection

- Use **redundancy** for uptime and availability.
- Use **backups** for data protection and recovery.
- Use **cloud** for scalability and offsite resilience.

Backup Software - Enterprise Backup Solutions

Software	Key Features	Best For
Veeam Backup & Replication	Agentless VM backups, Instant Recovery, Ransomware protection	VMware, Hyper-V, Cloud workloads
Commvault	End-to-end data protection, multi-cloud support, deduplication	Large enterprises, hybrid cloud
Veritas NetBackup	High-performance backup, tape support, cloud integration	Legacy systems, multi-site backup
IBM Spectrum Protect	Scalable, policy-based data management, multi-platform	Large organizations with complex storage needs
Rubrik	API-driven, immutable backups, ransomware recovery	Cloud-native and hybrid environments

Backup Software - Cloud-Native Backup Solutions

Software	Cloud Provider	Best For
AWS Backup	AWS	Backing up EC2, RDS, EFS, S3
Azure Backup	Azure	Azure VMs, SQL, SAP HANA
Google Cloud Backup & DR	Google Cloud	Cloud VMs, Kubernetes, Databases
Druva Phoenix	Multi-Cloud	Endpoint & cloud workload backup
HYCU	Nutanix, Google Cloud	SaaS-based, agentless backup

Backup Software - Open-Source & Free Backup Software

Software	Cloud Provider	Best For
Bacula	Enterprise-grade, multi-client backup	Image and file backups, web-based interface
Amanda	Network-wide backup, open-source	Linux and UNIX systems
Restic	Deduplication, encryption, cloud-friendly	Cloud backups
Duplicati	Encrypts and stores backups on cloud storage	Personal/small business use
UrBackup	Image and file backups, web-based interface	Small businesses

Symantec Netbackup 7.5 Overview

- Symantec NetBackup 7.5 was a widely used enterprise backup and recovery solution that provided **centralized, scalable, and high-performance** data protection for physical, virtual, and cloud environments.
- It was released in 2012 and included key improvements over previous versions.
- NetBackup 7.5 Architecture
  - **Master Server** – Controls backup policies, scheduling, and reporting.
  - **Media Server** – Handles data movement between clients and storage devices.
  - **Client** – The system where files, applications, or databases are backed up.
  - **Storage Targets** – Includes disk, tape, deduplication appliances, or cloud storage

Key Features of NetBackup 7.5

- **Intelligent Deduplication**
  - Built-in deduplication at the source, media server, and target storage.
  - Reduces storage costs and speeds up backups.
- **V-Ray for Virtualized Environments**
  - Agentless backups for VMware vSphere and Microsoft Hyper-V.
  - Supports Granular Recovery Technology (GRT) for VM restores.
- **Auto Image Replication (AIR)**
  - Automates replication of backup images across multiple sites.
  - Helps with disaster recovery and business continuity.
- **Accelerator Technology**
  - Speeds up full backups by tracking and backing up only changed blocks.
  - Reduces backup windows significantly.

Key Features of NetBackup 7.5

- **Operational Restore for Databases & Applications**
  - Oracle, SQL Server, Exchange, SharePoint, SAP, and DB2 support.
  - Granular recovery for individual database objects.
- **NetBackup OpsCenter**
  - Provides centralized reporting, analytics, and monitoring.
  - Helps IT teams optimize backup performance.
- **Cloud Storage Integration**
  - Supports Amazon S3, Google Cloud Storage, and Azure Blob Storage as backup targets.
  - Reduces reliance on on-premises storage

Supported Platforms & Storage

- **Operating Systems:**
  - Windows, Linux, AIX, Solaris, HP-UX
- **Backup Targets**:
  - Disk, Tape Libraries, Deduplication Appliances
- **Cloud Integration**:
  - Amazon S3, Google Cloud, Microsoft Azure

Strengths & Limitations

- **Pros**:
  - Enterprise-grade scalability and high performance
  - Unified management for physical, virtual, and cloud backups
  - Advanced deduplication to reduce storage costs
  - Built-in disaster recovery features like Auto Image Replication (AIR)
- **Cons**:
  - Complex setup and management compared to modern backup solutions
  - High licensing costs for enterprises
  - Legacy UI (OpsCenter) compared to newer versions
  - Slower backup speeds compared to modern incremental forever backups

NetBackup 7.5 End of Life (EOL)

- NetBackup 7.5 reached End of Support in 2016.
- Organizations should upgrade to newer versions (like **NetBackup 10.5**) for security patches and cloud-native features.


That's all Folks!