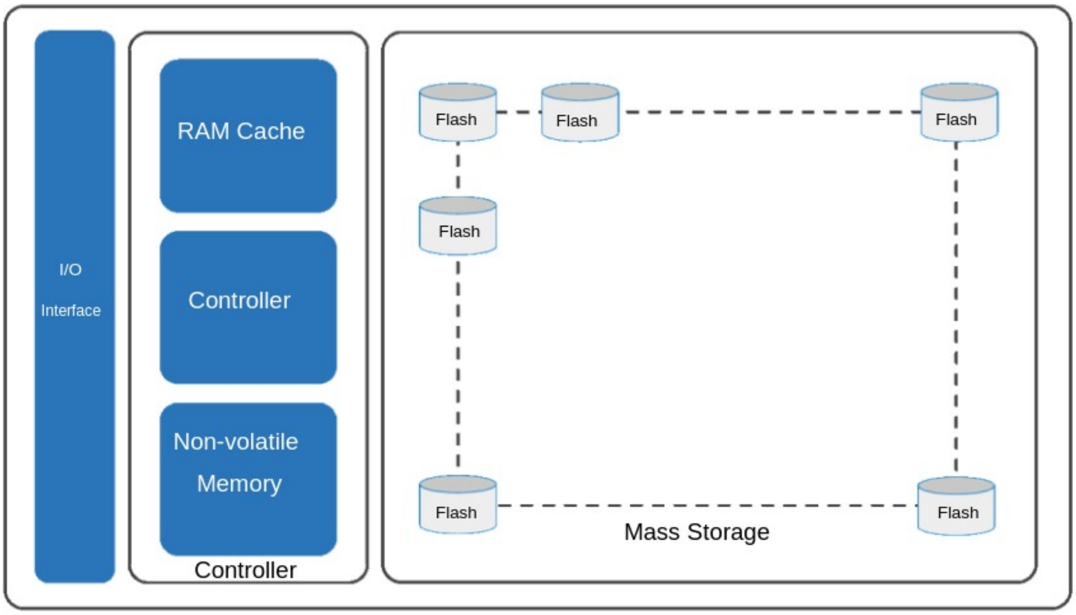
Storage

businesses today are driven by data, and to store that data a lot of storage is needed, also part of the data is processed in real time which requires a lot of I/O operations per seconds, for that there are lots of storage devices and protocols

Hard Disk Drive

This is a metal disk that is polarized, when an the I/O arm moves above the disk it can read or right to it, the disk is spinning so the arm can reach all of the disk.
This is a very slow method and it releases a lot of heat and has moving parts which is not good.

Solid State Drive



This is multiple non volatile flash memory that is controlled in the same interface as the HDD so for the computer there is no difference, there are no moving parts so this memory is much faster and can work in parallel and excels at random access unlike HDD which needs to wait for the disk to spin to the right place.

Non Volatile Memory Express

This is an SSD with a PCI interface which is much faster, offering even more speed

Redundant Array Independent Disks (RAID)

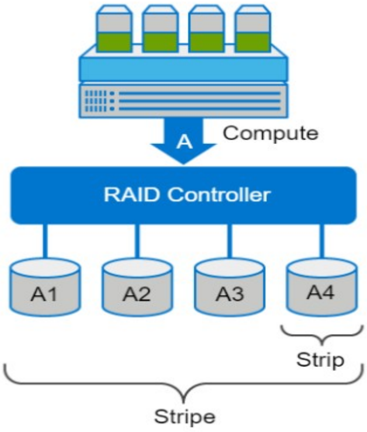
This is a technique that combines multiple disks into one logical unit and also provide data protection against drive failiures.

This improves performance because files can be saved on multiple disks, thus performing the I/O simultaneously on those disks.

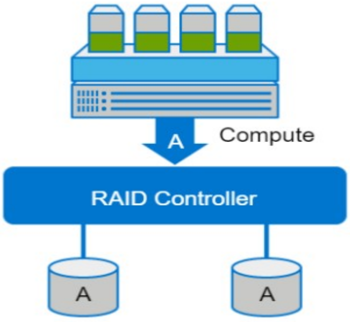
RAID is most of the time implemented on the computer that writes to the disks or on the storage system. This can be implemented in software.

RAID provides some techniques

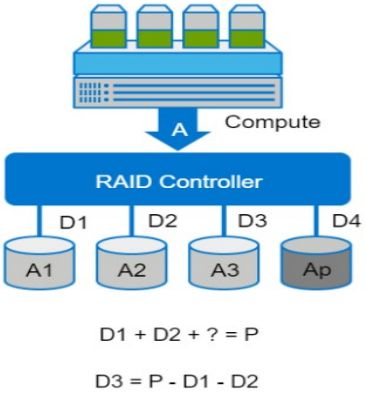
Stripping – this is the technique that is used to store file in multiple disks, when saving a file the raid controller takes the file size and divides it into the strip size and then saves each strip on different disks so of the strip size is 64KB and the file is the size of 256KB, then each disk will save on strip of the file, so the file I/O is 4 times faster.
This does not provide any data protection.



Mirroring – This is a technique where the data is stored on two or more disks, this provides backup in the cost of more resources. If one disk fails, there is also the other disk for backup, and this also provides performance benefits for read but slower for right, **Most of the time it is done only on very important data because of the high resource price.**



Parity – Method to protect stripped data without the cost of mirroring. An additional drive is added to hold the parity. The parity can help calculate the value of one of the disks if it is not available, for example it will store the sum of the rows of D1-D3 in a row of D4, so if one of the disks fails, it can calculate the row. And it can also be a XOR operation.



Raid levels

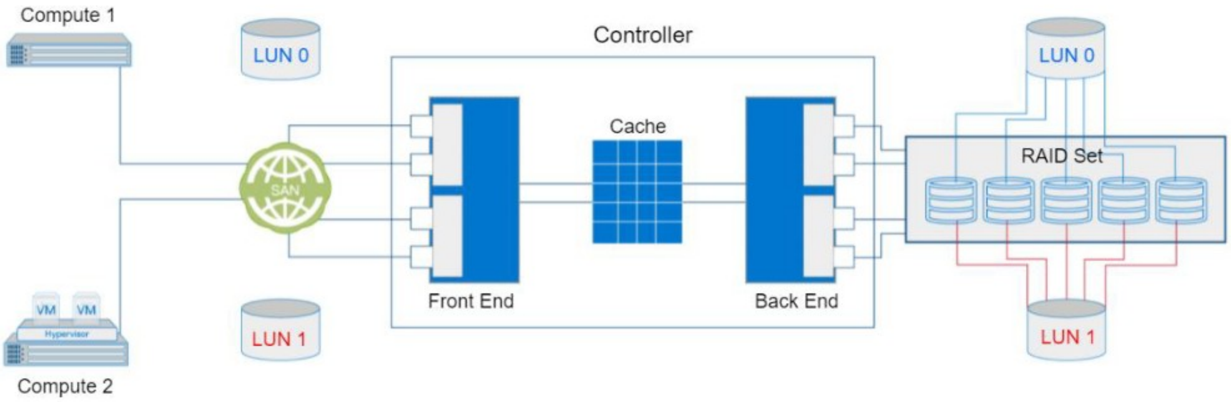
0 – stripped set without fault tolerance,
1 – Disk mirroring, set of two that one is a mirror.
0 + 1 – Mirroring and stripping.
5 – Stripped set with independent disk access, and distributed parity.
6 - stripped set with independent disk access and dual distributed parity.

RAID Level	Minimum Number of Disks	Available Storage Capacity (%)	Write Penalty	Protection
1	2	50	2	Mirror
1 + 0	4	50	2	Mirror
5	3	[(n-1)/n] * 100	4	Parity (Supports single disk failure)
6	4	[(n-2)/n] * 100	6	Dual Parity (Supports two disk failures)

Storage Provisioning

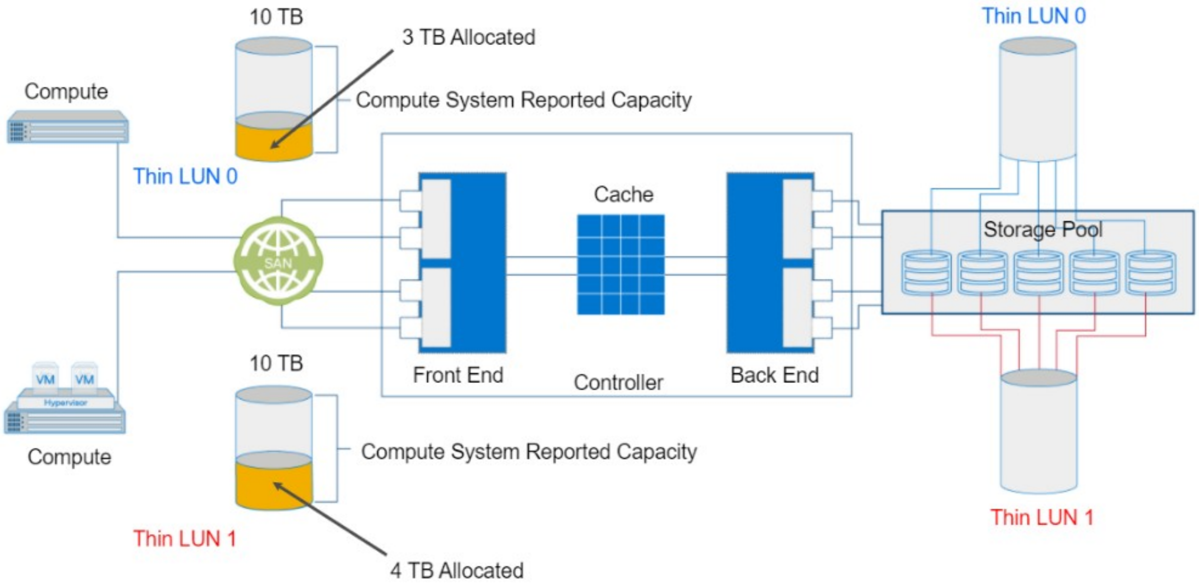
This is a concept of assigning storage to a system based on it’s need from a pool of storage.
Storage is provided with “LUNs”, which is logical unit of storage that is given to a machine.

Traditional Provisioning



With traditional provisioning the disks are partitioned and sliced into two LUNs, LUN1 and LUN2, these are then given into the compute units that require the storage.
These LUNs are considered THICK because they demand all the space of the LUN

Virtual Provisioning

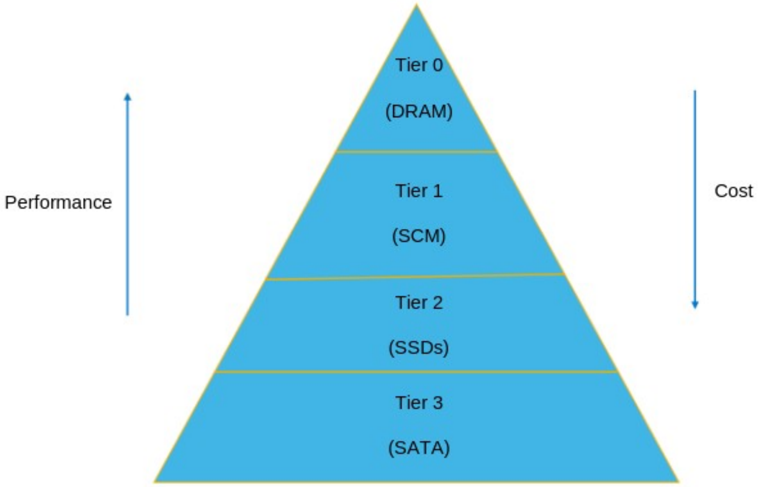


This method provides a way to create LUNs with more capacity then there available on the disk, the capacity is shared from a big pool and each LUN can be as big as the pool size, and they acquire more “thick” space on demand, this is called thin lun

Storage Tiering

This concept helps to manage storage, high and expensive storage used to store frequently accessed data, gets a low tier while slow storage gets a higher number tier.

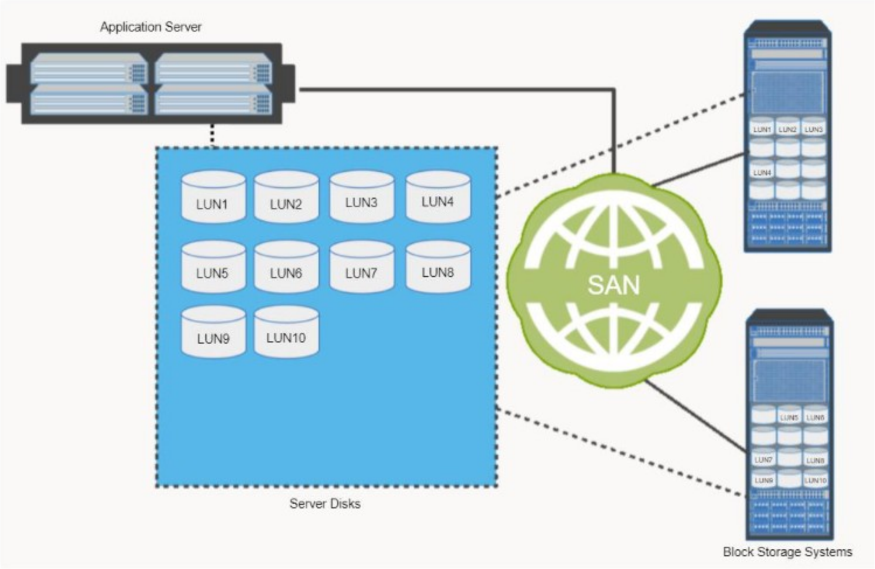
Each tier has different performance and cost.



DRAM is the fastest and the most expensive while SATA is much slower and way cheaper

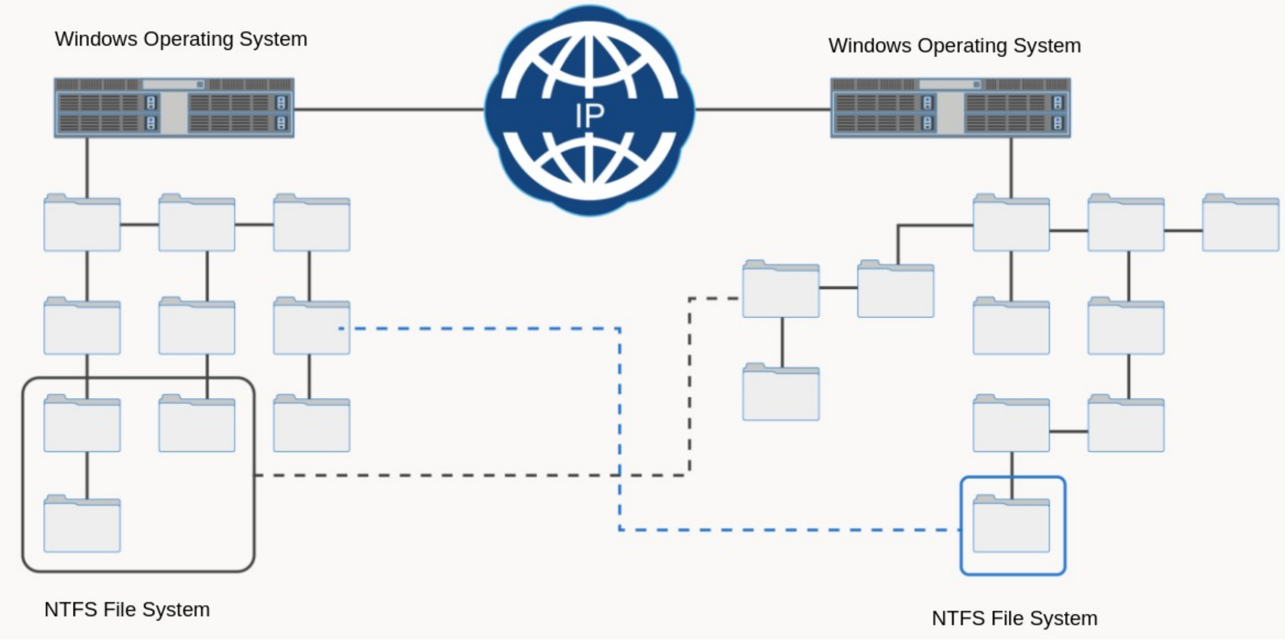
Block Base Storage System

This is a pool of storage that is divided into consistent size LUNS, then when a device wants storage, it is asking from the storage system a block, and it is up to the device to put there a storage system



File Based Storage System

This storage system shares files instead of space, this can be done because files has metadata, so the system knows how to interpret the raw bytes the files are shared over the network and collisions in editing should be handles which adds more complexity, this method lacks scalability, and windows operating system don’t understand linux operating system



Storage Area Network
this is a common name for general block storage system, this is using protocols like ISCSI for sharing blocks of storage

Network Attached Storage
this is a common name for file storage system that is used to share files and not blocks, common protocols are CIFS/SMB for windows and NFS for linux
S3 is a NAS that is provided by the aws cloud

Object Based Storage System
this type of storage system is needed, because there is a very large exponential growth of data each year, this data must be instantly available from anywhere, traditional storage solutions are inefficient in managing this data, and in handling the growth.
In addition there is a change in how people expect to see the data, from anywhere and on every type of device.
Traditional solutions like NAS that add overhead in managing large number of permissions and nested directories.
NAS performance degrades as there are more users that access the data and increased metadata is needed.
Object based systems are ment to solve these challenges which will introduce lower cost growth, increased metadata

The basic unit of object file system is an object, this can contain metadata, user information.

Each object is identified with a unique ID, the object metadata and attributes are used for optimized search, and automated deletion of objects.

The object ID is generated by an algorithm for the actual that the object contains, so each change in data changes the ID, and each object, has a unique ID.

Hierarchical VS Flat

Instead of hierarchical order that data is stored on a flat repository.

Objects cannot be placed on another objects.

There is no limit on the number of files per directory.

OSD allows to store large number of objects without having to maintain an absolute path to each object.

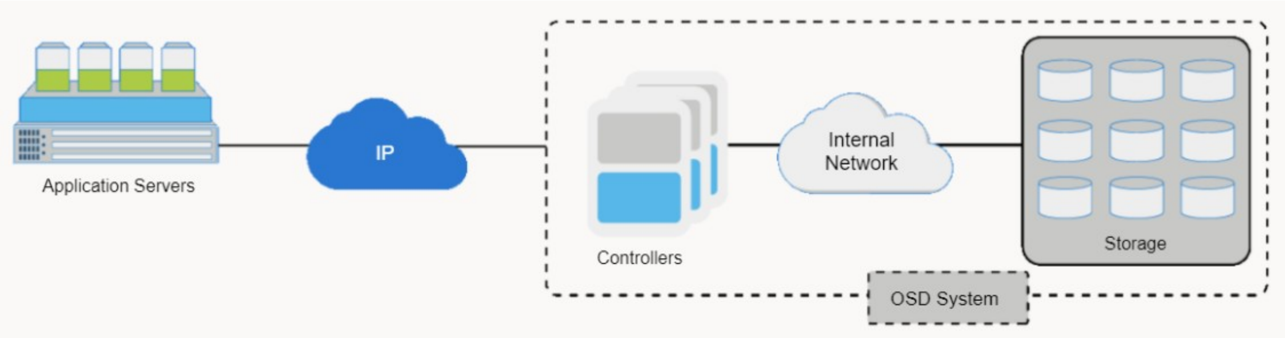
Components of Object-Based Storage Device (OSD)

<u>Key Components -</u>

Controller

Network

Storage

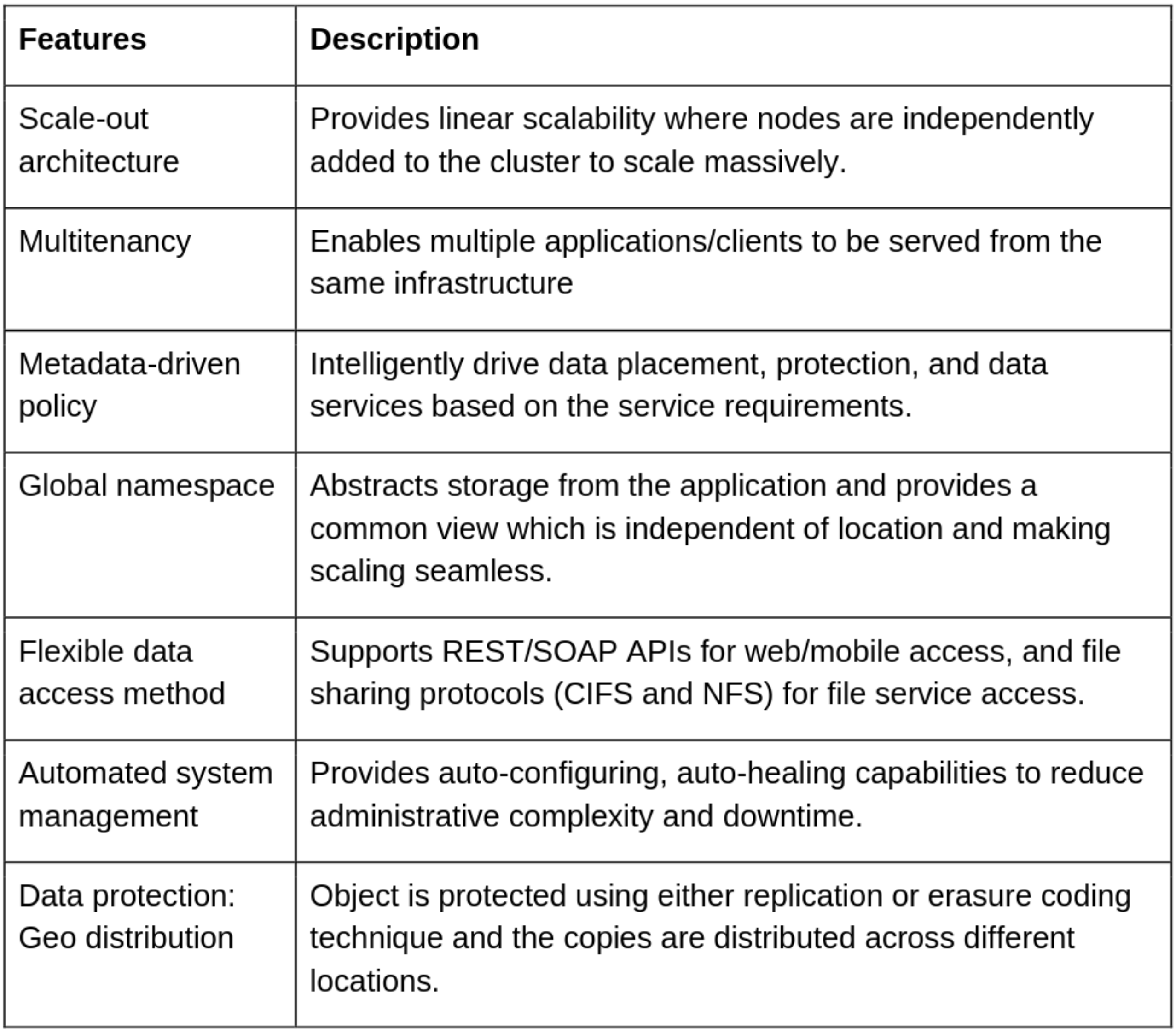


A controller is a server that run the OSD environment, it is a software service that allows to store, retrieve, and manage data in the system.

<u>Metadata Service</u> – this service is responsible for generating the unique ID of the object and also may include attribute data. It also maintains the mapping of the object IDs and the file system name space

<u>Storage Service</u> – This service manages the disk I/O

The Controller is connected to the storage via local network



Features	Description
Scale-out architecture	Provides linear scalability where nodes are independently added to the cluster to scale massively.
Multitenancy	Enables multiple applications/clients to be served from the same infrastructure
Metadata-driven policy	Intelligently drive data placement, protection, and data services based on the service requirements.
Global namespace	Abstracts storage from the application and provides a common view which is independent of location and making scaling seamless.
Flexible data access method	Supports REST/SOAP APIs for web/mobile access, and file sharing protocols (CIFS and NFS) for file service access.
Automated system management	Provides auto-configuring, auto-healing capabilities to reduce administrative complexity and downtime.
Data protection: Geo distribution	Object is protected using either replication or erasure coding technique and the copies are distributed across different locations.

Notes

Object file system can scale to petabytes and even exabytes

Object file system can serve multiple users and not give access to each other data

Provides global namespace for clients

Provides data protection and auto configuration

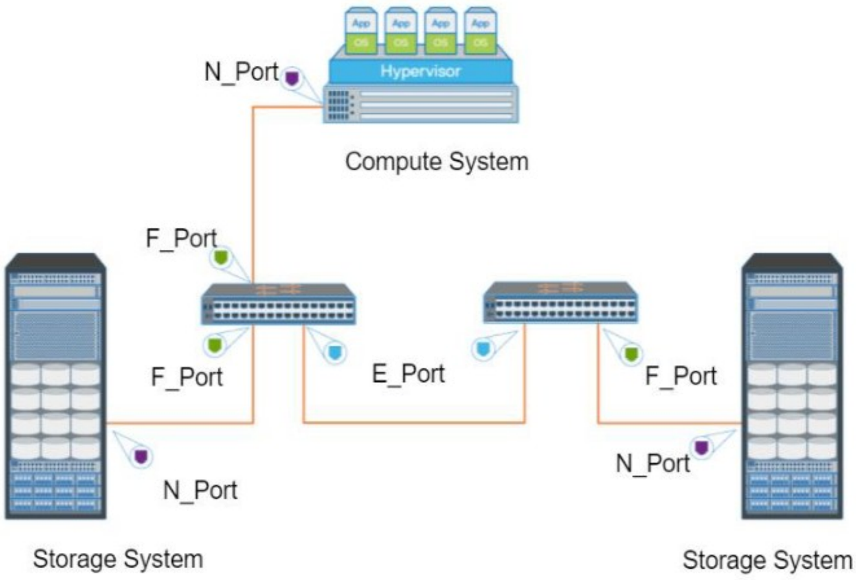
Unified Storage Systems

This is a system that provides a tool for managing all the types of storage systems.

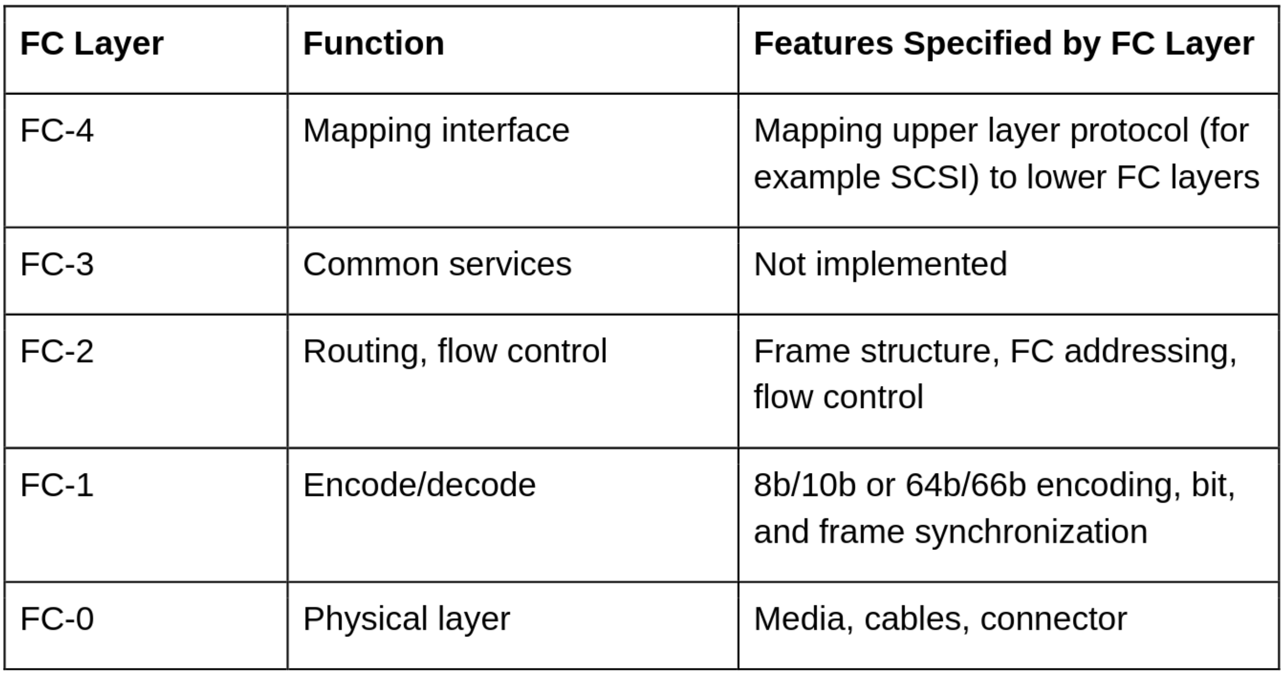
Fiber Channel SAN

This is a SAN over a fiber channel network allowing fast reliable file transporting.

Ports:
N_PORT – this is used in the end devices
E_PORT – this is used to expend, and connect switch to switch
F_PORT – this is used to connect an end device to the switch
G_PORT – this is a general purpose port and can be E or F



Fiber Channel Protocol Stack



FC Layer	Function	Features Specified by FC Layer
FC-4	Mapping interface	Mapping upper layer protocol (for example SCSI) to lower FC layers
FC-3	Common services	Not implemented
FC-2	Routing, flow control	Frame structure, FC addressing, flow control
FC-1	Encode/decode	8b/10b or 64b/66b encoding, bit, and frame synchronization
FC-0	Physical layer	Media, cables, connector

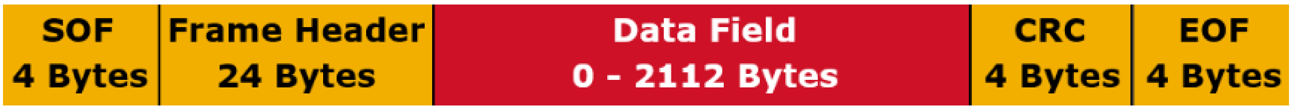
Layer 4 this is the uppermost layer in the protocol stack, it defines the application interfaces, and the way upper layer protocols are mapped to the lower layer. The standard defines the protocols, SCSI, HIPPI, ESCON, ATM, IP.

Layer 2 Provides addressing, structure and organization of data. It also defines fabric services, flow control and routing.

Layer 1 defines how data is encoded prior to transmission.

Layer 0 This layer defines the physical interface, media and transmission. And it also includes the cables connector.

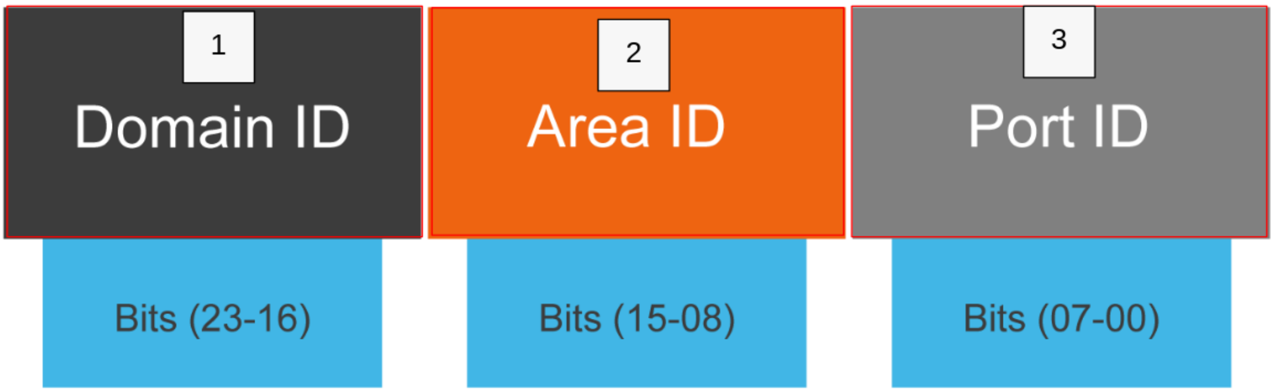
Fiber Channel Frame



SOF 4 Bytes	Frame Header 24 Bytes	Data Field 0 - 2112 Bytes	CRC 4 Bytes	EOF 4 Bytes

The frame consists start of frame, the frame header, data field, cyclic redundant check, end of frame.

Fiber Channel addressing
this address is assigned to each proto
main purpose is routing data through the fabric
this address size is 24



1	2	3
Domain ID	Area ID	Port ID
Bits (23-16)	Bits (15-08)	Bits (07-00)

Address contains Domain ID which is the ID switch on the fiber network, each switch has a unique one.

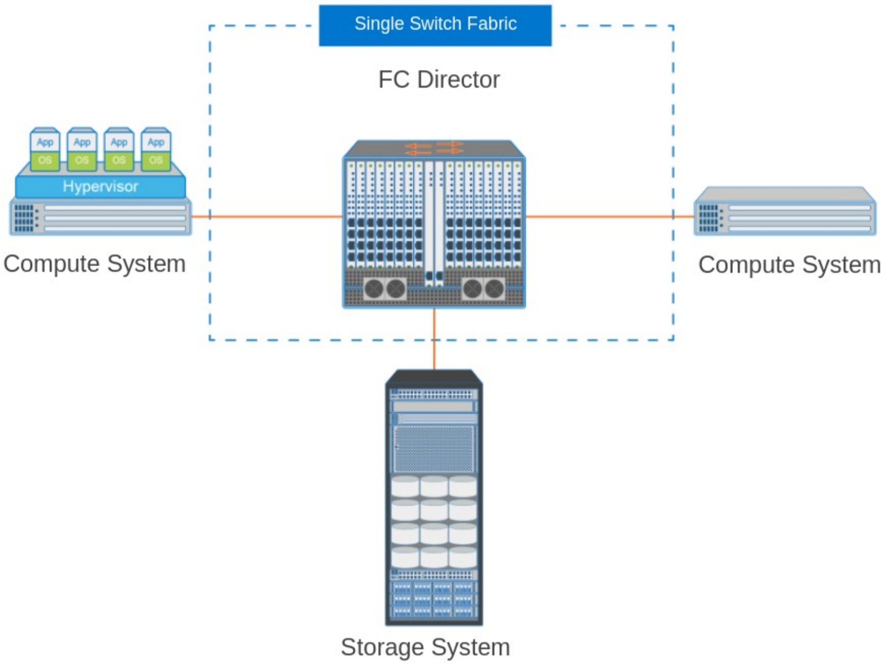
The area ID which contains the group of switch ports for the connection, and the port ID to identify the port in the group

Fiber Channel San Topologies

<u>Single Switch Fabric</u>
The fabric contains a single switch

Both the compute system and the Storage connect to the same switch

Every switch port is usable for node connectivity

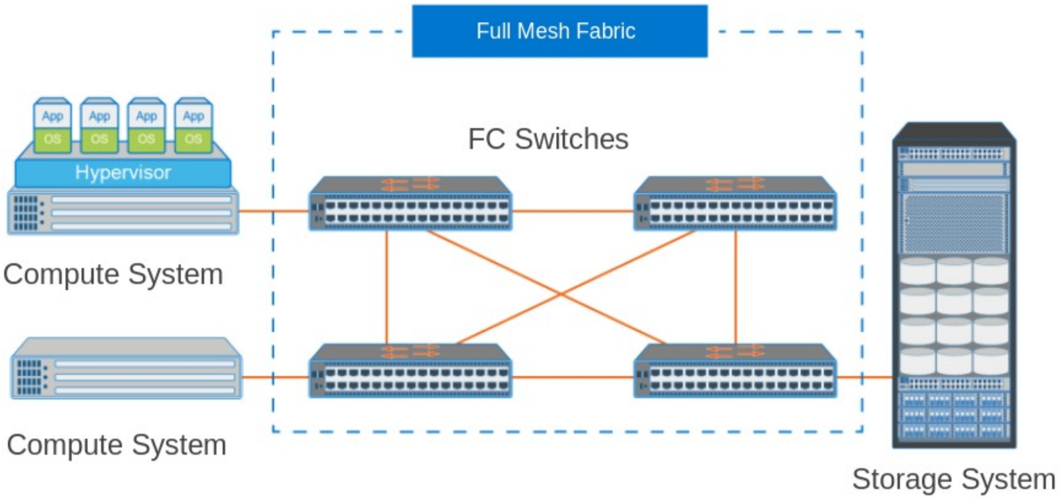


Full Mesh Topology

Each switch is connected to all the switches

Compute system and storage are connected to any switch

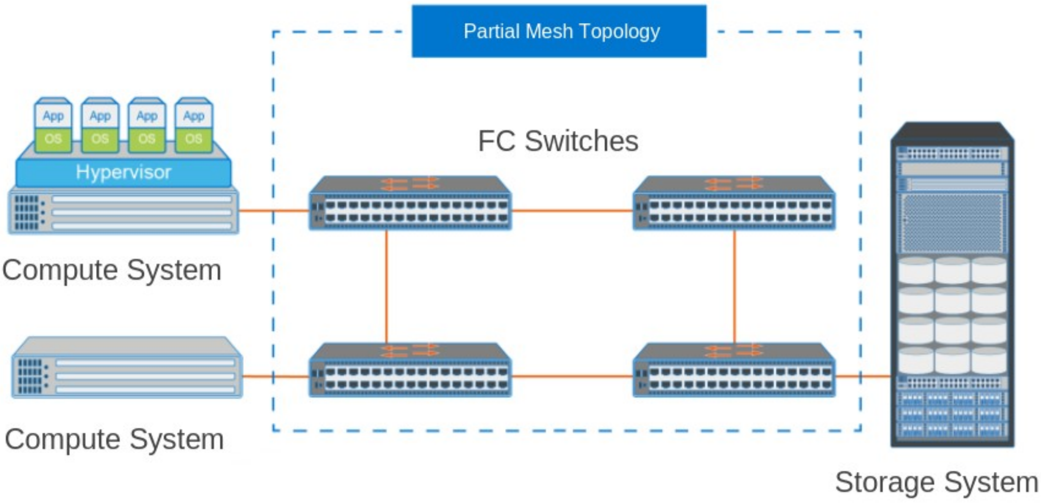
Maximum of One Inter Switch Link is required



Partial Mesh Topology

Not all switches are connected

Several ISLs are required

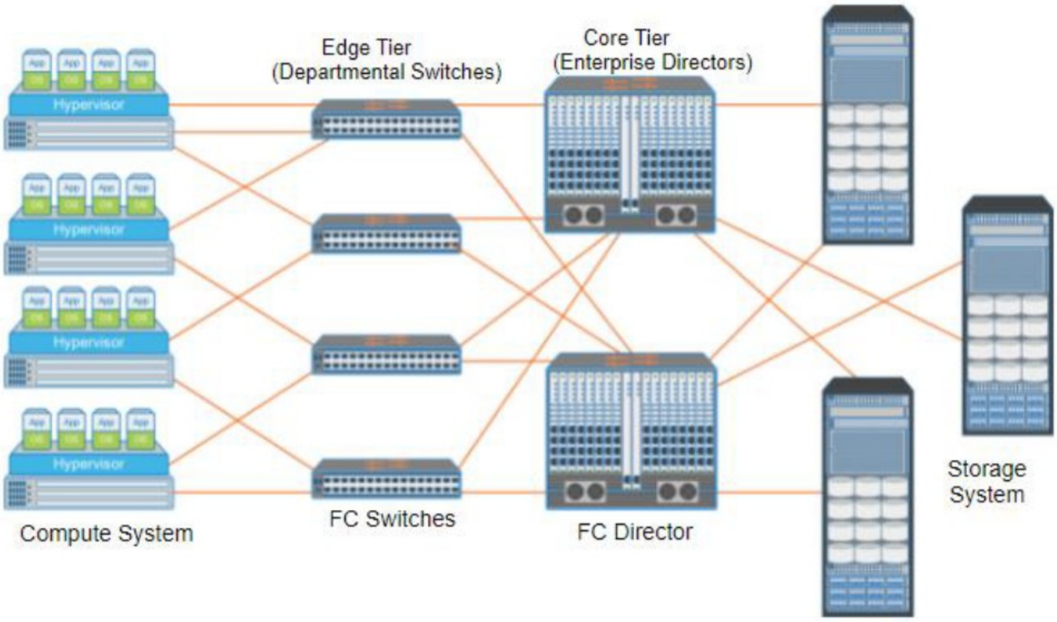


Core Edge Topology

Edge tier is composed from departmental switches and offer inexpensive approach for adding more compute systems in the fabric

The edge tier switches are not connected to each other, and must be connected into a director switch

Compute systems that require high performance may be connected directly to the core tier to avoid Inter switch link delay



Zoning

logical private path between nodes

provides access control so only members of the zone can talk to each other.

WWN Zoning zones by utilizing the world wide names which are like MAC addresses

Port Zoning zones by port numbers

SAN Virtualization

Provides a virtualization layer in the SAN which Abstracts away storage systems.

Aggregates LUNs to create storage pools

Virtual volumes from a storage pools are assigned to compute systems.

Virtual map assigns virtual volumes to LUNs

This allows online expansion of virtual volumes, and non disruptive data migration.

VSAN

enables a group of nodes to communicate with each other using virtual topology that is defined on the physical SAN

multiple VSANs may be created on a single physical SAN

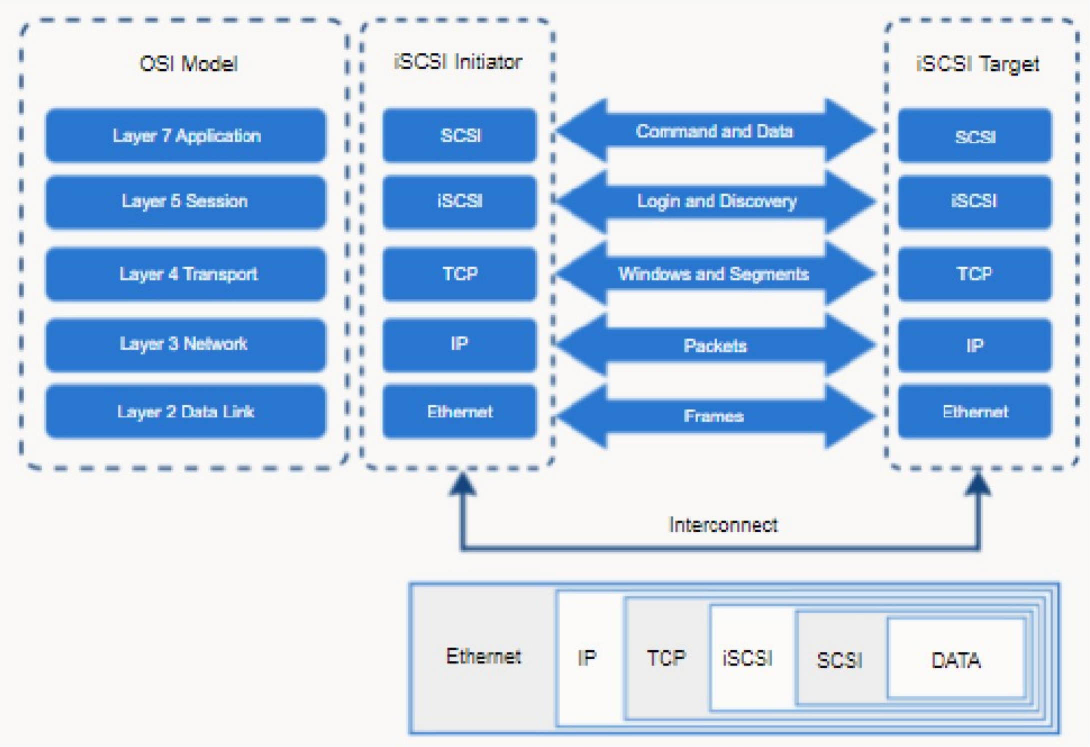
each VSAN behaves as an independent fabric

each VSAN has its own configuration

This method improves security, scalability, availability manageability

iSCSI
This is basically a SAN over regular IP network, which add a massive overload on the network.

There are hardware devices that lowers the load of the protocol from the computer CPU



iSCSI Addressing and Naming

iSCSI address is logical path into an iSCSI initiator or target, this is a combination of the IP and the TCP port. And also the iSCSI name

the iSCSI name is a unique world wide name that is used to identify initiators or targets withing the network.

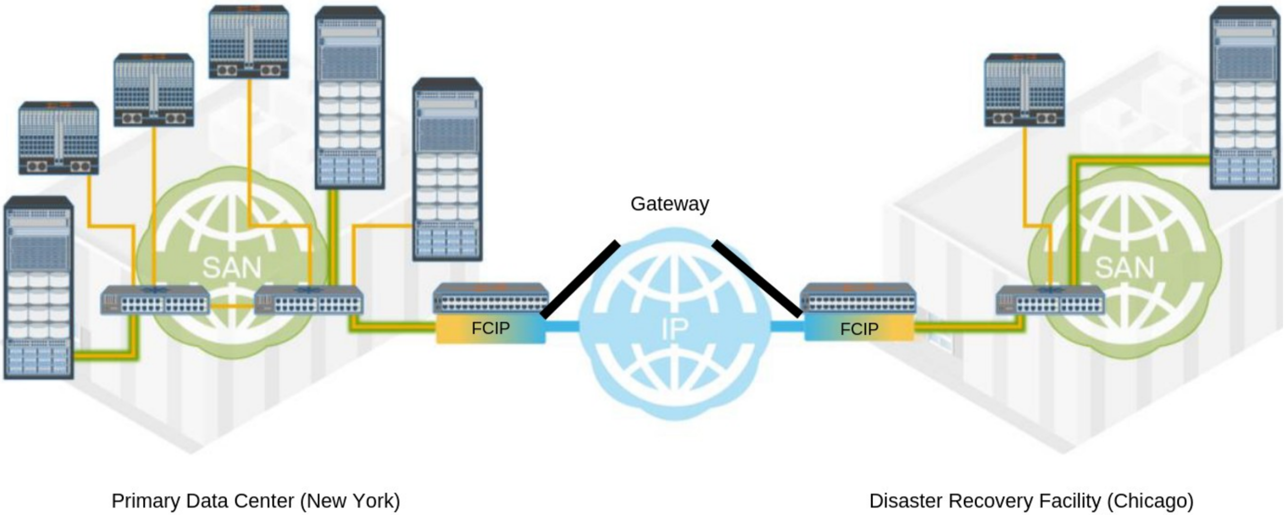
Name Conventions
iSCSI Qualified Name (IQN) this is using a domain like name for accessing targets, which allows a logical name for the target

Extended Unique Identifier EUI is a globally unique identifier based on the IEEE EUI-64 naming standard. An EUI is composed of the eui prefix followed by a 16-character hexadecimal name, such as eui.0300732A32598D26.

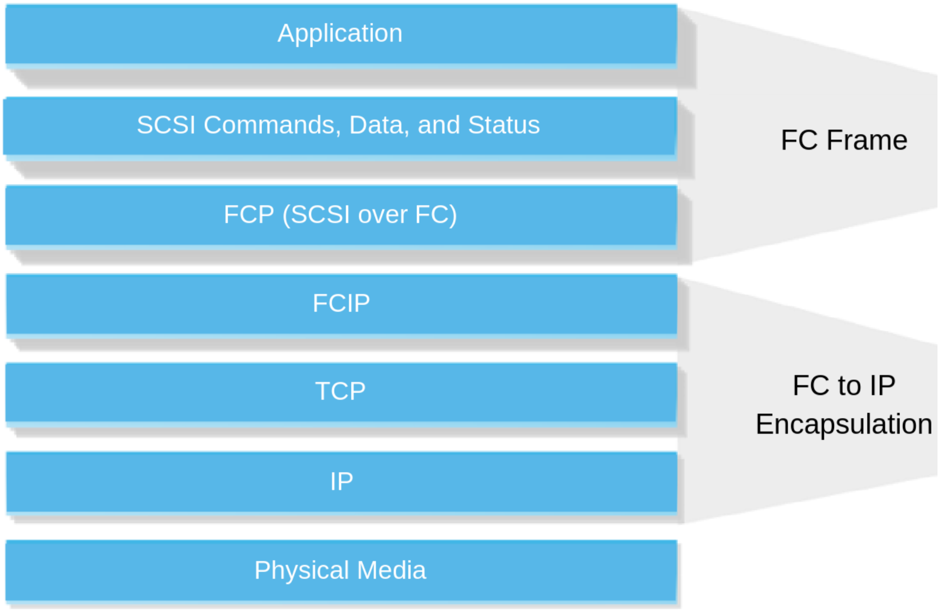
Network Address Authority another world wide unique name, and enables other port types like SAS or FC, composed by a naa prefix and a 32 hex characters

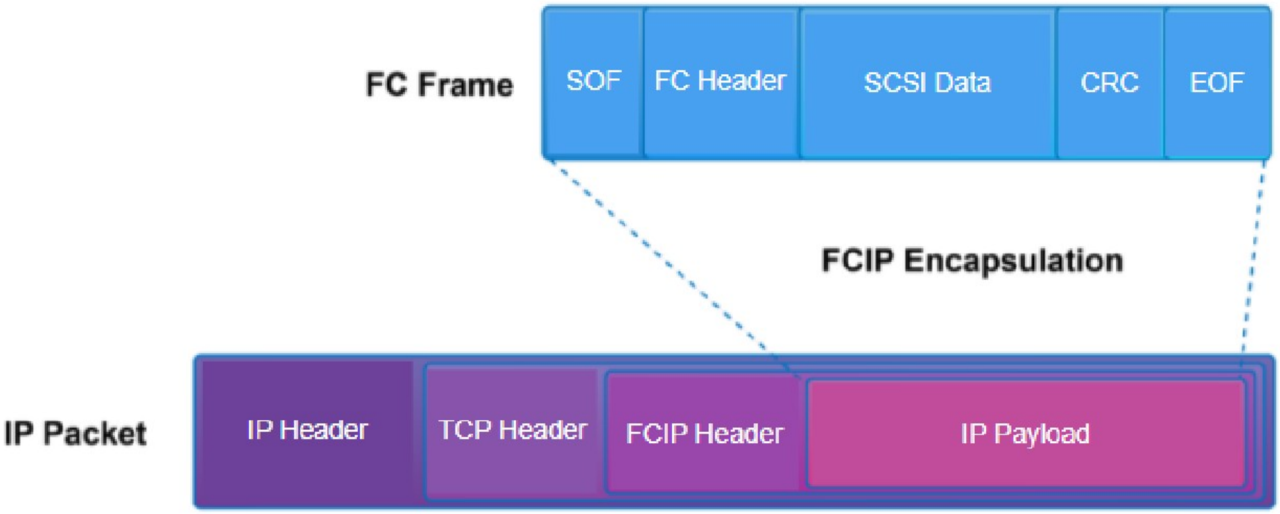
Fiber Channel Over IP

This protocol encapsulates the fiber channel packets inside the payload of the IP packet.
There is no configuration in the Fiber Channel SAN because there is a special switch called “FCIP Gateway” that is making the transfer over the IP network seemless


SAN
FCIP
Gateway
IP
FCIP
SAN
Primary Data Center (New York)
Disaster Recovery Facility (Chicago)

Protocol Stack and Frame Encapsulation



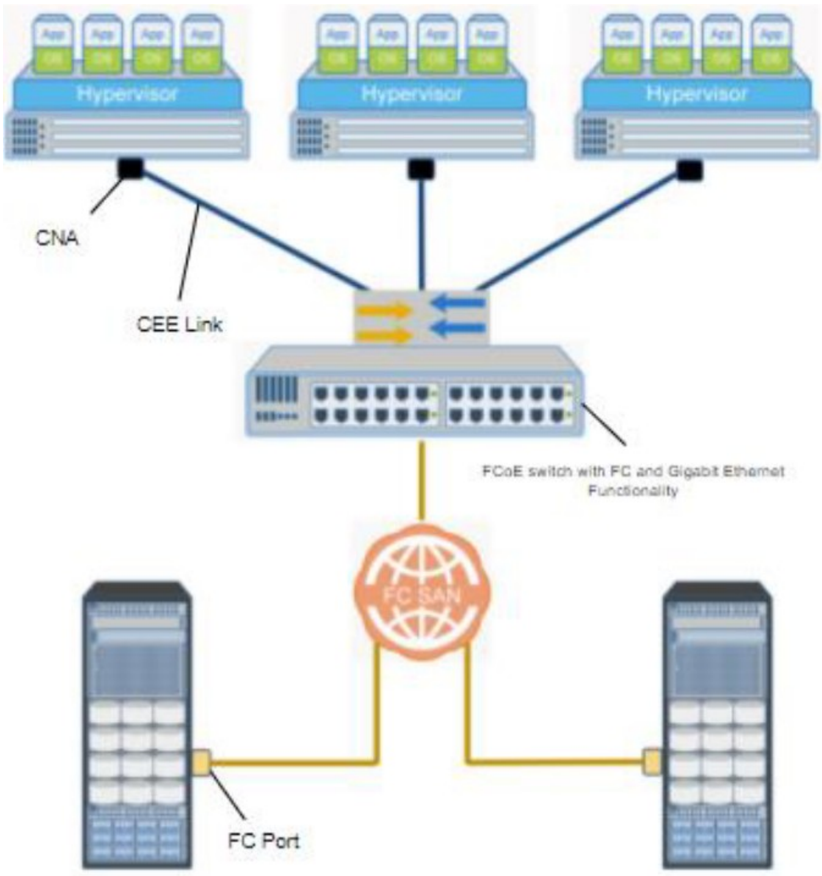


Fiber Channel Over Ethernet (FCoE)

This is a Storage Protocol that enables Fiber Channel SAN traffic over 10GB Ethernet or greater.

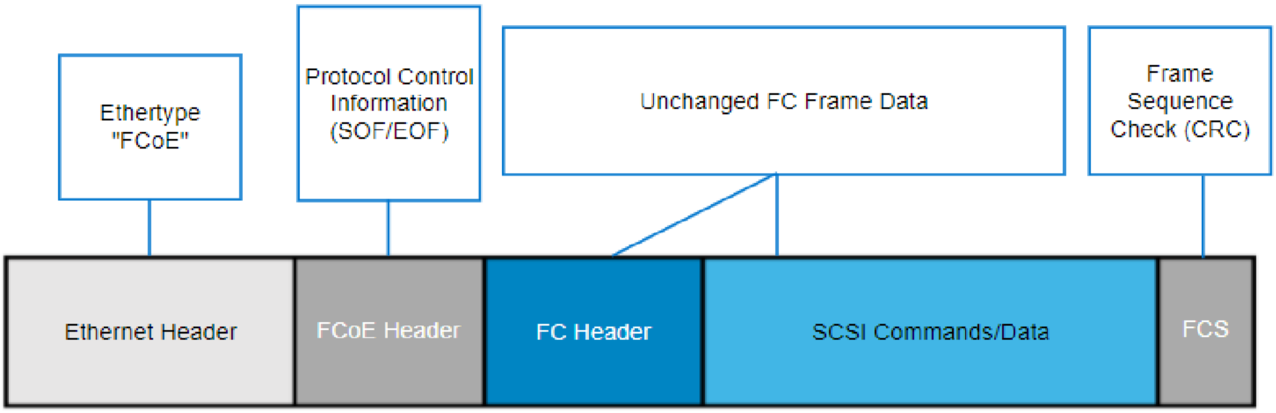
A Converged Network Adapter (CNA) that can receive the data is installed on the node machine.

The data is then transferred into a special multi protocol switch that can transfer it into the end devices.



FCoE Encapsulation

FCoE encapsulates unchanged FC frames into an ethernet frame payload.



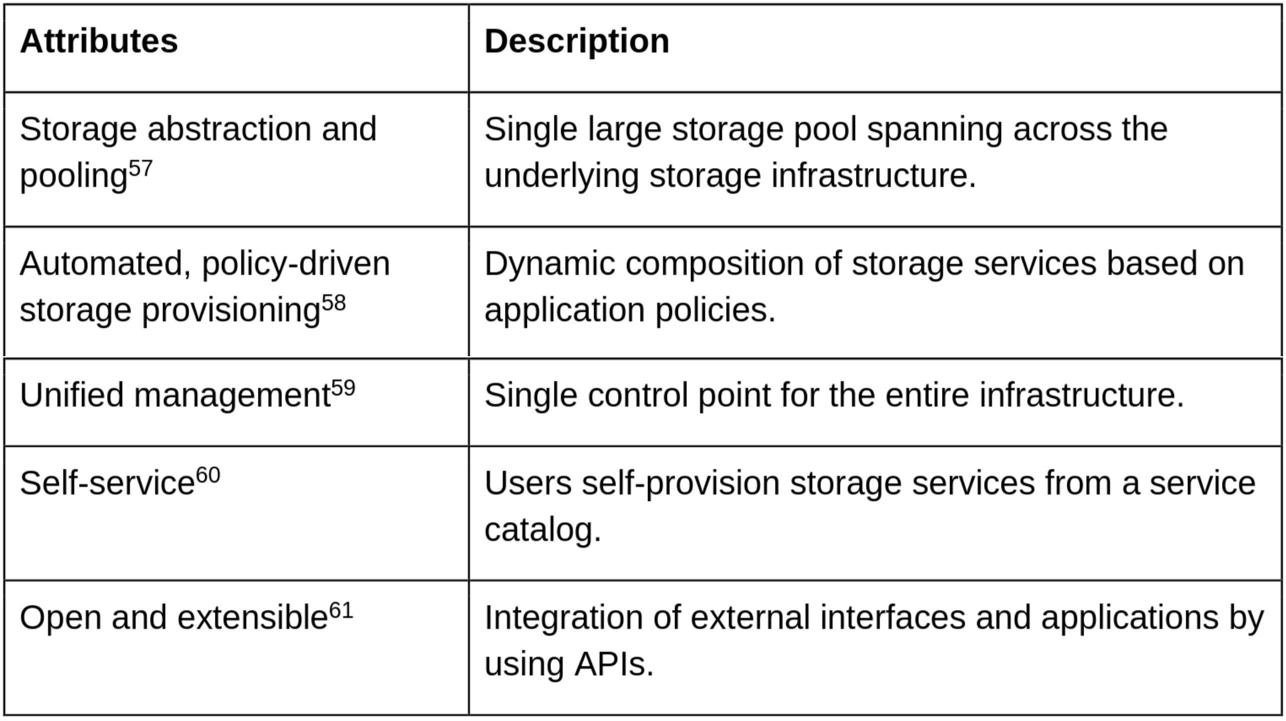
NvME over Fabric

This is the State of the art of storage, the fastest connection and the fastest hardware, which yields a massive data transfer rates. Nvme uses Nvme qualified name, which is similar IQN

Software Defined Storage

This is a storage infrastructure that is automated through software which allocates storage based on needs.

Key attributes



Attributes	Description
Storage abstraction and pooling[57]	Single large storage pool spanning across the underlying storage infrastructure.
Automated, policy-driven storage provisioning[58]	Dynamic composition of storage services based on application policies.
Unified management[59]	Single control point for the entire infrastructure.
Self-service[60]	Users self-provision storage services from a service catalog.
Open and extensible[61]	Integration of external interfaces and applications by using APIs.

Why it is needed

SDS enables organizations to build modern, hyperscale storage infrastructure in a cost-effective manner using standardized, commercial off-the-shelf components.

Key Concepts

Assets Discovery

Controller automatically detects assets when they are added to the Software Defined Storage environment

Assets that can be discovered are =>

- Storage Systems
- Storage Networks
- Compute System and Clusters
- Data Protection Solutions

Resource Abstraction and Pooling

This is a controller that exposes the storage infrastructure through a simplified model hiding and handling details such as storage system, disk selection, LUN creation and LUN masking.
Software defined storage abstracts storage across physical systems and manages individual components, this functionality enables administrators and users to treat storage as a large resource

Service Catalog and Self Service

Administrators creates storage services and organizes then in a service catalog.

- services include block, file and object data services.
- users place services request through user interface.

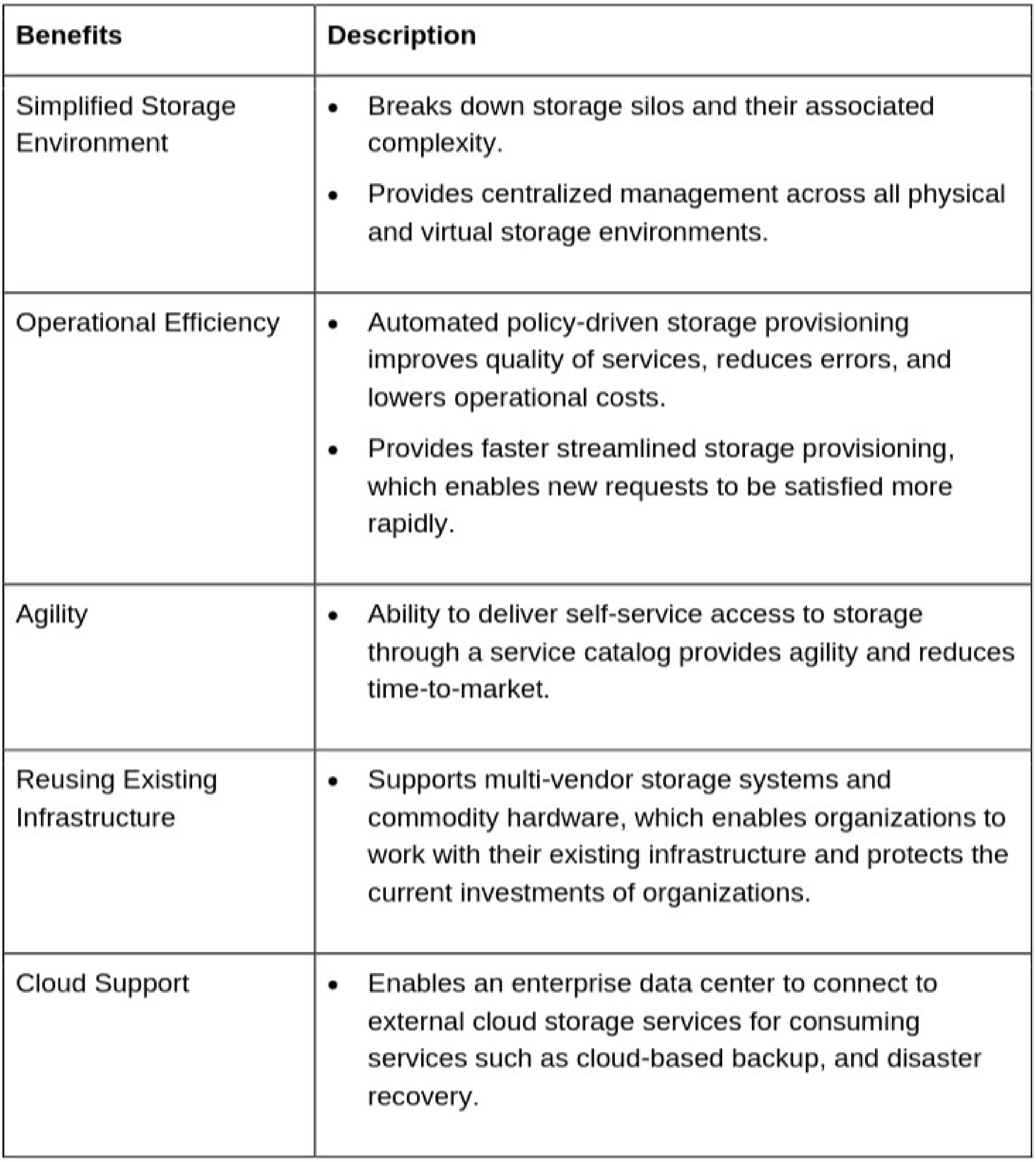
This is automates the provisioning of resources

Block Data Service

Provides block volume of required size, performance and protection levels.

Example Services:
Create and Delete block volume
Bind and Unbind volume to computer
Mount and Unmount a block volume
Expend and Shrink volume

Benefits



Benefits	Description
Simplified Storage Environment	• Breaks down storage silos and their associated complexity. • Provides centralized management across all physical and virtual storage environments.
Operational Efficiency	• Automated policy-driven storage provisioning improves quality of services, reduces errors, and lowers operational costs. • Provides faster streamlined storage provisioning, which enables new requests to be satisfied more rapidly.
Agility	• Ability to deliver self-service access to storage through a service catalog provides agility and reduces time-to-market.
Reusing Existing Infrastructure	• Supports multi-vendor storage systems and commodity hardware, which enables organizations to work with their existing infrastructure and protects the current investments of organizations.
Cloud Support	• Enables an enterprise data center to connect to external cloud storage services for consuming services such as cloud-based backup, and disaster recovery.

Software Defined Networking

Software Defined Networking is an approach to abstract and separate the control plane from the data plane.

Instead of the control being in the components, the control functions are from an external devices which are called network controllers.

Benefits

Centralized Control

- Single point of control for the entire network and infrastructure
- Helps to manage traffic and network with software.

Policy Based Automation

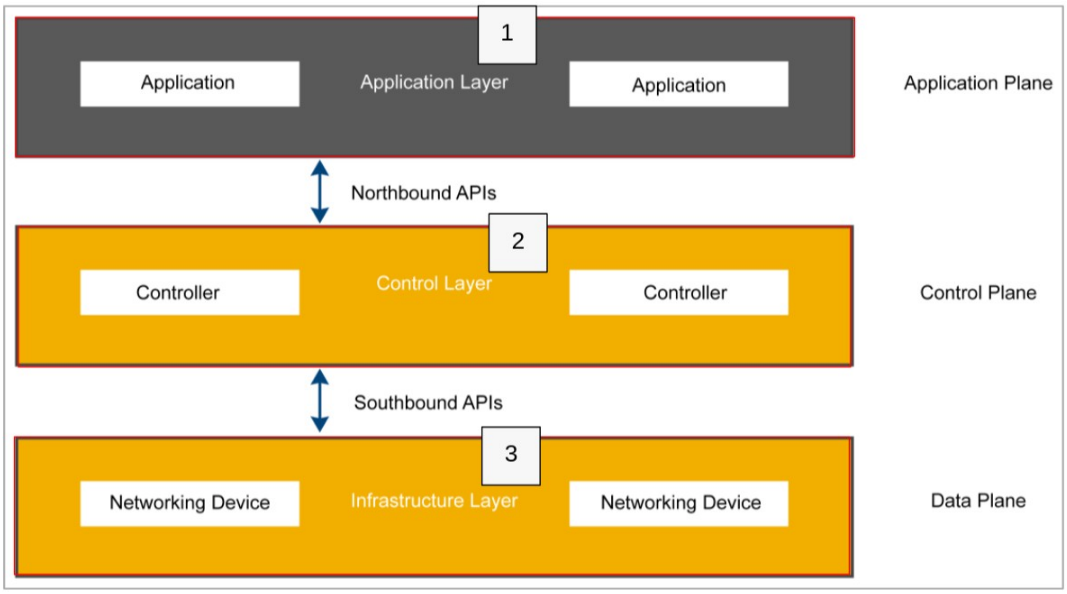
- Hardware-based network management like zoning can be automated.
- Management operations can be programmed on the controller

Agile Management

- Management functions are available in simplified form.
- Makes it easier to configure and modify network configuration

Software Defined Networking Architecture

The architecture contains three layers that communicate between them with APIs



Layer 1 – Mostly APIs and user interfaces
Layer 2 – Controller logic with policies and
Layer 3 – Consists the lateral networking devices

Use Case

Data Center Security

- Security against lateral movement techniques, like pass the hash, pass the ticket
- Security Policies

Automation

- Automated network provisioning
- Programmatically control entire network environment

Business Control

- Hybrid cloud initiatives
- Disaster recovery

Business Continuity

This is a set of processes that includes all the activities business must to mitigate planned and unplanned down time, and it ensures a business critical functions can continue after and during a disaster

This involves proactive measurements, such as business impact analysis, risk assessment to build resilient IT infrastructure.

Information Availability

This is the ability of an IT infrastructure to function according to business requirements, and customer expectations during the time of operation.

Accessibility

Information should be accessible to the right user when required

Reliability

Information should be reliable and correct in all aspects.

Timelines

Defines the time window during which information must be accessible. For example from 8:00 to 22:00

Causes to Information Unavailability

1) Catastrophic exceptions caused by bad logic
2) Multiple drive failure without any redundant paths
3) Network switch failure without redundant paths
4) Power failure or disaster
5) Scheduled maintenance requiring downtime

Impact of Data Unavailability

<u>Lost of Productivity</u>

Number of employees can’t work

<u>Damaged Reputation</u>

Customers

Suppliers

<u>Lost Revenue</u>

Direct Loss

Compensatory payments

Billing losses

<u>Financial Performance</u>

Revenue recognition

Cash flow

Credit rating

Stock Price

How to measure

Uptime / Uptime + Downtime is the amount of percentage of time the information is available.

Recovery Point Objective This is the point in time which data must be recovered after an outage. It defines the amount of data loss a business can endure, based on this organization define replications, backup etc.

Recover Time Objective The time within which systems and applications must be recovered after an outage. The downtime an organization can survive

Disaster Recovery This is a set of policies involved that makes a disaster less impactful by for example replicating.

How to ensure business continuity

Implementing fault tolerance

Deploying data protection solutions

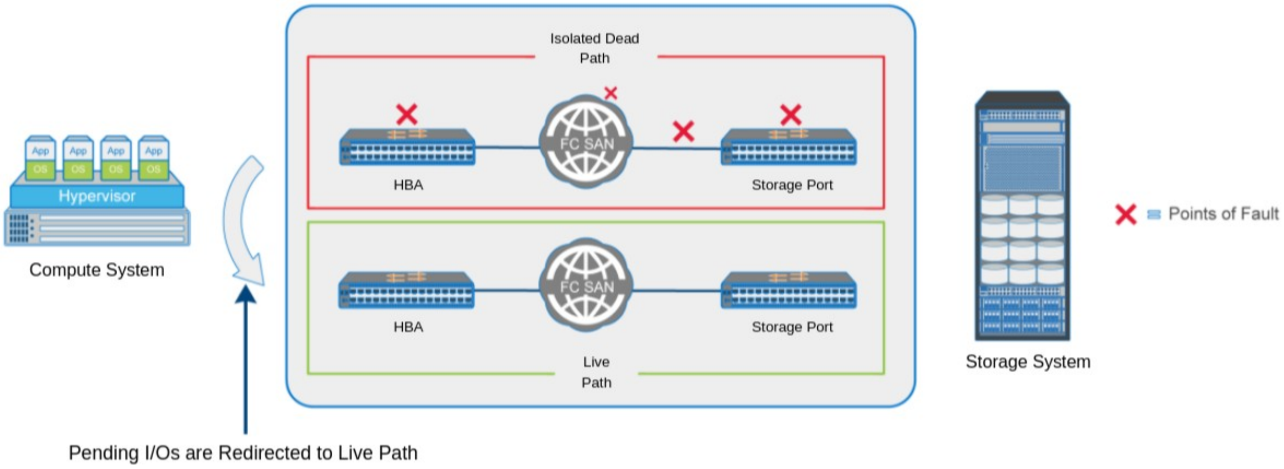
Atomic fail-over mechanisms

Architecting resilient modern applications

Fault Tolerance Infrastructure
This is the ability of an IT system to continue functioning in the event of a failure
A fault may cause complete outage, or only to certain components.
This is mostly happening because software bug, hardware defect or administrator or user error.

Requirements
Fault Isolation and Eliminating Single Point of Failure

Fault Isolation
Fault Isolation contains the scope of fault so other areas of a system are not implemented by the fault.
It does not prevent the fault of a system, but it ensures the failure doesn't impact the system as a whole.



Single Point of Failure
This is a single component or aspect of a system whose failure can disrupt the entire system

Eliminating Single Point of Failure
Single points of failure can be avoided by implementing fault tolerance mechanisms.

Implement redundancy at component level

- Compute
- Network
- Storage

Avoid singe points of failure at data center (site) level

Compute Cluster

Compute systems are combined in a cluster, when a computation is needed, the computation is done on the cluster.

Between the computers in a cluster, a heartbeat is sent between them to, which is a signal of health, if the signal is not sent from one cluster to the others after a period of time it counts as dead, so the computations that were on him are moved into other clusters.

Network Fault Tolerance Mechanisms

A short network interruption could impact plenty of service running in a data center environment.

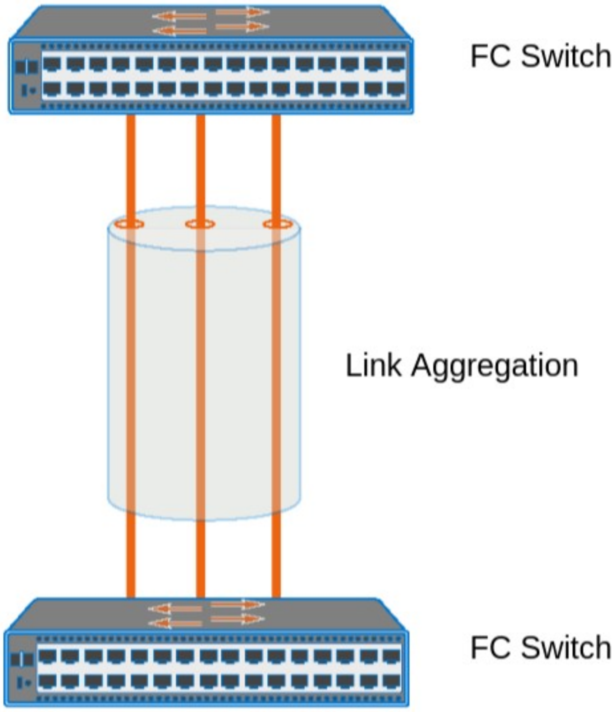
So the network infrastructure must be fully redundant and highly available.

Techniques

<u>Link aggregation</u>

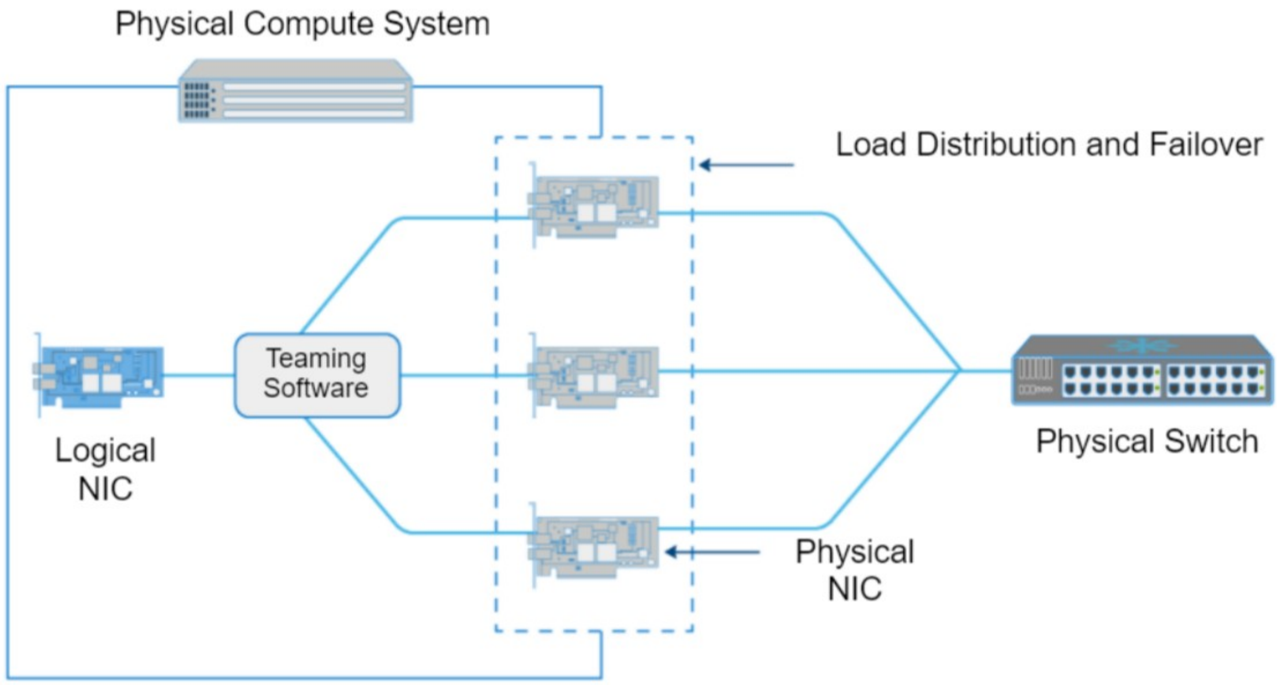
Combines links between two switches and also between a switch and a node.

Enables network traffic fail-over in the event of a link failure in the aggregation



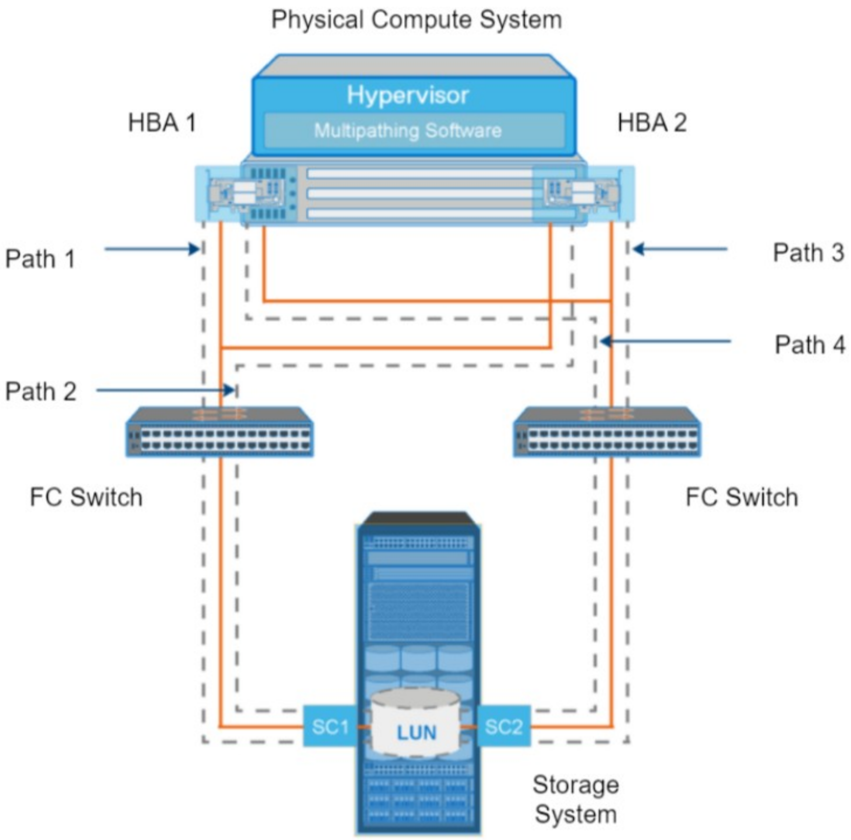
NIC Teaming

When the service on the cluster wants to send information, it sends it through a virtual link. The virtual NIC is then connected to multiple physical NICs, with this method, the NICs can load balance the sending rate between each other, and in case one NIC falls, the other NICs are still alive and can send information without him



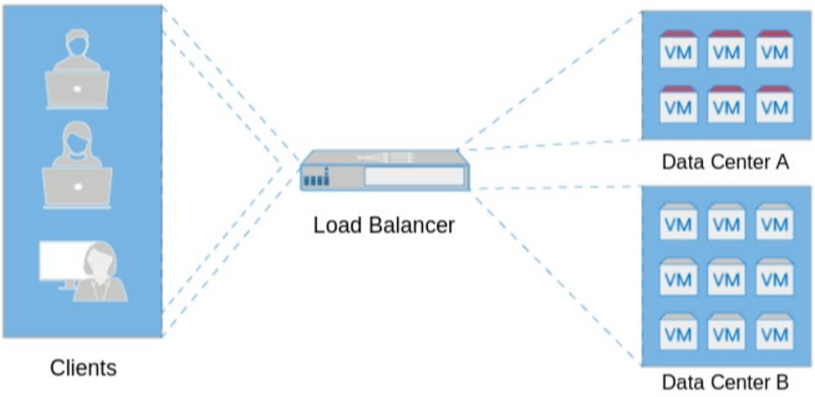
Multipathing

Enables a compute system multiple paths to transfer data to a LUN
Enables failover by redirecting I/O from failed path to an active one
Perform load balancing across active paths



Elastic Load Balancing

- Enables dynamic distribution of applications and I/O traffic
- Dynamically scales resources (VM instances) to meet demands
- Provides fault tolerance capabilities by detecting unhealthy VM instances and automatically redirect I/O to a healthy VM



Storage Fault Tolerance Mechanisms

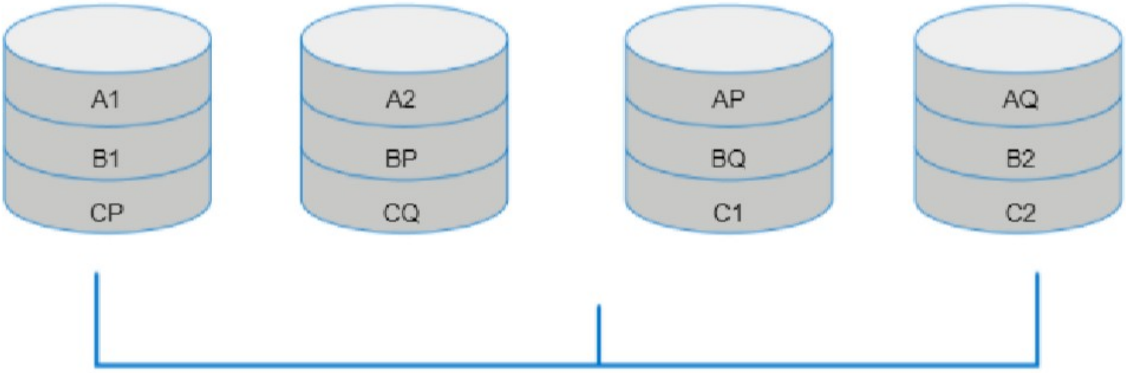
Data centers comprise storage many large disks. If some of those disks fail data can be destroyed.
To prevent this some methods of data protection were developed

Raid

This is a method that provides data protection against one or two driver failures

This method combines physical drivers into a RAID set which is a logical unit that can be accessed as one driver.

Almost all RAID types provide driver protection



RAID 6 - Dual Distributed Parity

Erasure Coding
Provides space optimal data redundancy to prevent data loss against disk drive failures.
- A set of n disks are divided into m disks that hold data and k disks that a redundant. Where m+k=n. This method can behold k faults.

Coding information is calculated from data.

Dynamic Disk Sparing
Automatically replaces a failed drive with spare driver to protect against data loss.

Multiple spare drives can be configured to be available

When disk recoverable error rates for a disk exceed predetermined threshold, the disk subsystem tries to copy data from the failing disk to the spare drive automatically

Availability Zones
This is a location with its own set of resources isolated from other zones.

Although this is isolated from resources from other zones, they are still connected through low latency links.

In the case of a zone falling, services on that zone may failover to another zone.

Data Replication
Copying data from one target into another, while there is a complete and regular functioning.

This is an alternative to backup

Provides a fast recovery if the source falls because there is the replication.

Provides near production testing environment

Local Replication

Replicating data withing the same location
- Withing a Data center
- Withing a storage system

It is typically used for operational restore of data when there is a data loss.

Remote Replication

Replicating data to remote locations (Geographically far)
Data can be synchronously or asynchronously replicated
Enables users to replicate data to cloud.

Local Replication: Snapshot

Virtual Copy of a file system or VM

VM snapshot

Copying the state of the VM (The file that makes it) and when applying changes, we can always restore the state. This is a ?hard copy? And not considered a backup because it is not on the same disk.

<u>Copy on Write</u>

When the snapshot is taken nothing really happens. If a file is changes it is firstly copied and then changed

<u>Redirect on Write</u>

Changes are written to another place on the disk an when reading the file the changes are applied to it, similar to git changes.

Storage System Based Snapshot

This is a virtual copy of the file system as they appeared at a specific point in time.
This is not a hard copy or a backup, it is just coping the pointers to the files. When a file is overwritten just the pointer is over written to the new file data. When the snapshot is reverted the old set of pointers is then restored so the data returns to the previous state

Local Replication: Clone

Cloning provides the ability to create fully populated point-in-time copies of LUNs withing a storage system or create a copy of an existing VM.

Clone of a storage volume
- Initial synchronization is performed between the source LUN and the replica

- During sync the replica is not available for any compute system, once sync finished there is no difference between the replica and the source

Clone of a VM

- Clone is a copy of an existing VM (Parent VM).
- Typically clones are deployed when many identical VMs are required which reduces the time that is required to deploy a new VM

Linked Clone – It is created from a snapshot of the parent VM
Full Clone – This is an independent copy of the VM that shares no resources from the original one.

Remote Replication – Synchronous

Write is committed to both the source and the remote replicate before it is acknowledged to the compute system

Synchronous replication enables restarting business operations at a remote site with zero data loss and provides near zero

Remote Replication – Asynchronous

- A write is committed to the source and immediately acknowledged to the compute system
- Data is buffered at the source and sent t the remote site periodically
- Replica is behind the source by a finite amount

Continuous Data Protection
Continuous Data Protection provides the capability to restore data and VMs to any previous point in time

- Data changes are continuously captured and std at a separate location from the production volume so that the data can be restored to any previous point in time.

Key attributes

Continuous Replication

Continuous Data Protection provides continuous replication, which tracks all the changes to the production volumes that enable to recover to any point in time

Supports Heterogeneous Storage Systems

Continuous Data Protection solutions have the capability to replicate data across heterogeneous systems

Support Both Local And Remote Replications

Continuous Data Protection support both local and remote replication of data and VMs to meet operational and disaster re

Support WAN Optimization techniques

Continuous Data Protection supports various WAN optimization techniques (deduplication, compression, and fast write) to reduce bandwidth requirements and also optimally uses the available bandwidth

Multi-Site Support

Continuous Data Protection supports multi site replication, where the data can be replicated to more than two sites using synchronous and asynchronous replication.

Key Components

Journal Volume

- Contains all the data that has changed from the time the replication session started.
- The amount of space that is configured for the journal determines how far back the recovery points can go.

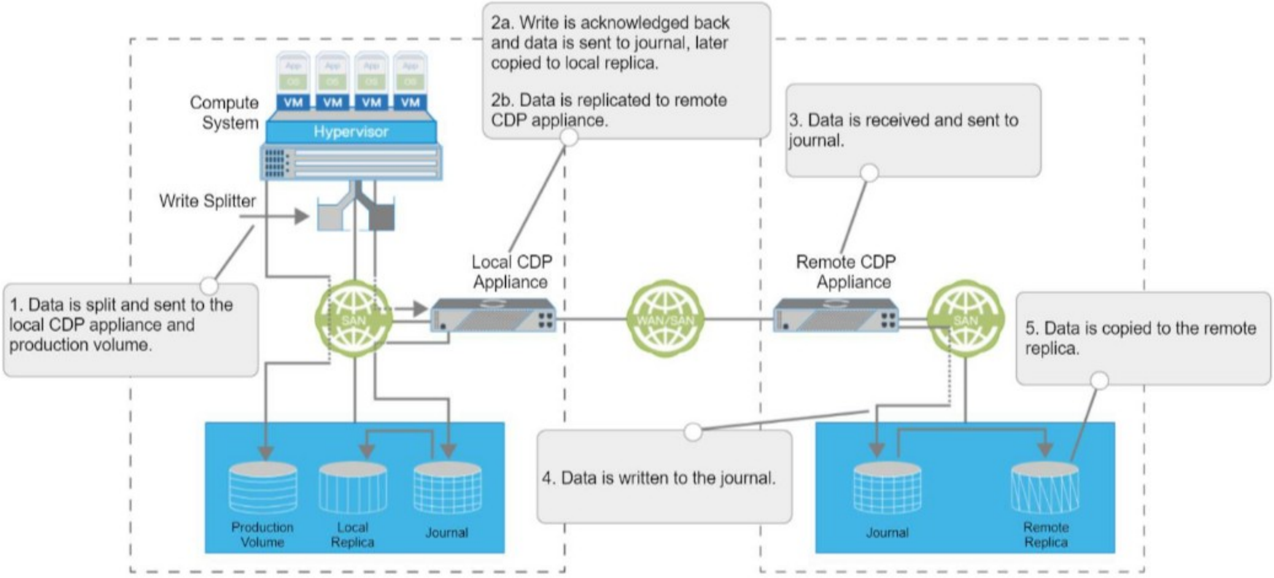
Continuous Data Protection Appliance

- Intelligent hardware platform that runs the Continuous Data Protection software.
- Manages both the local and remote replications
- Appliance can also be virtual

Write Splitter

- Intercepts writes to the production volume and splits each write into two copies
- Can be implemented at the compute, fabric, or storage system

Local and Remote Replication


2a. Write is acknowledged back and data is sent to journal, later copied to local replica.
2b. Data is replicated to remote CDP appliance.
Compute System
App
OS
VM
Hypervisor
Write Splitter
3. Data is received and sent to journal.
Local CDP Appliance
Remote CDP Appliance
1. Data is split and sent to the local CDP appliance and production volume.
SAN
WAN/SAN
SAN
5. Data is copied to the remote replica.
4. Data is written to the journal.
Production Volume
Local Replica
Journal
Journal
Remote Replica

<u>Data Backup</u>

A backup is an additional copy of production data, which is create and retained for the sole purpose of recovering lost or corrupted data

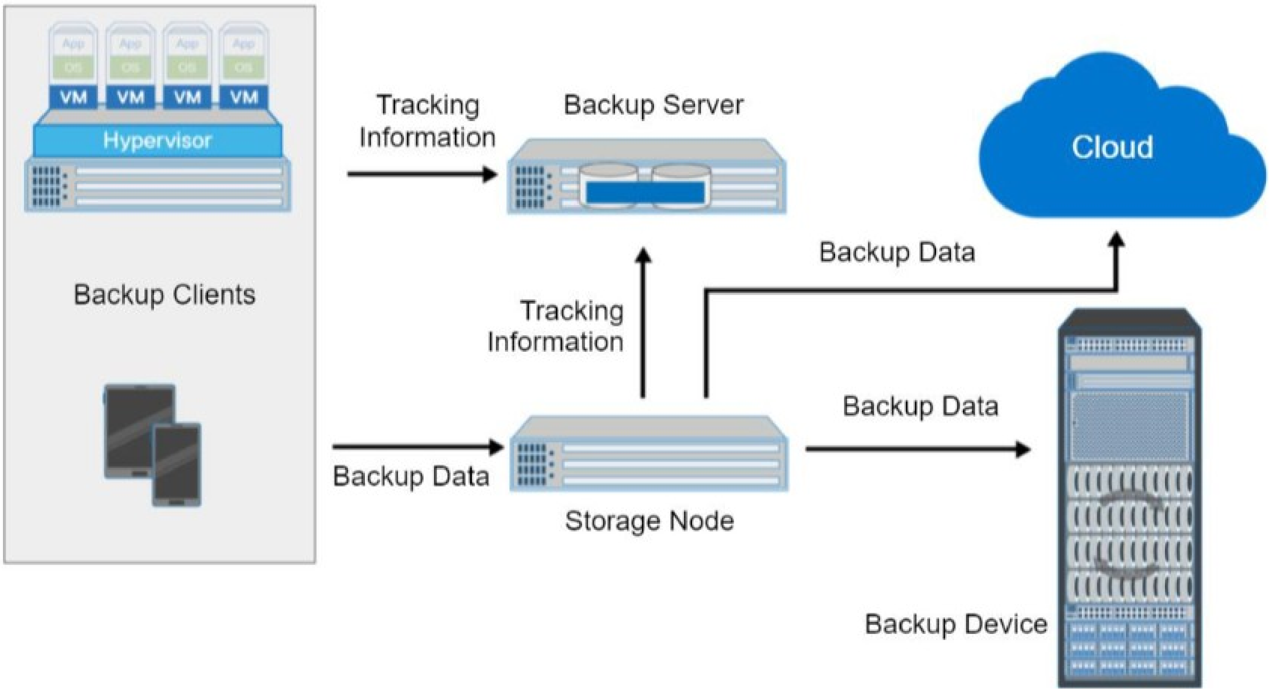
Organizations implement backups in order to protect the data from accidental deletion, application crashes, data corruption and disaster.

<u>Organizations backup data to:</u>

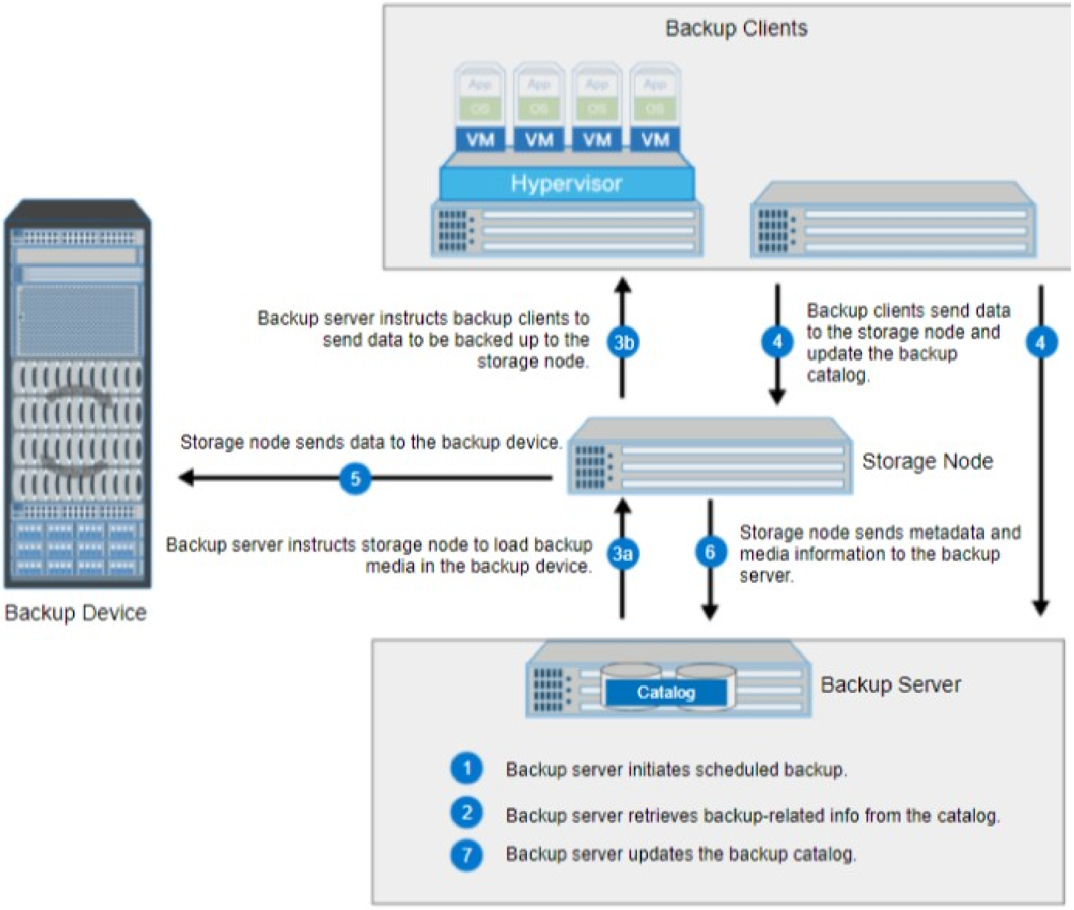
- Recover the lost or corrupted data for smooth functioning of business operation
- Comply with regulatory requirements
- Avoid financial and business loss

Backup Architecture

In a backup architecture environment, the common backup components are Backup Client, Backup Server, Storage Node and Backup Target



Backup Operation


Backup Clients
App
OS
VM
Hypervisor
Backup Device
Backup server instructs backup clients to send data to be backed up to the storage node.
3b
4
Backup clients send data to the storage node and update the backup catalog.
4
Storage node sends data to the backup device.
5
Storage Node
Backup server instructs storage node to load backup media in the backup device.
3a
6
Storage node sends metadata and media information to the backup server.
Catalog
Backup Server
1
Backup server initiates scheduled backup.
2
Backup server retrieves backup-related info from the catalog.
7
Backup server updates the backup catalog.

Recovery Operation
After the data is backed up, it can be restored when required. A recovery operation restores data to its original state at a specific Point In Time. Typically, backup applications support restoring one or more individual files, directories or VMs

Full Backup – Full copy of the data
Incremental Backup – Copy of the changes of data since last backup
Agent Backup – An agent continuously sends backup data to server
Image Backup – The VM is backed up as a single image file

Data Deduplication

This is the process of detecting and identifying the unique data segments withing a given set of data to eliminate redundancy

Basically removing duplicate backup data.

Key Benefits

1) Eliminating backup data from the backup, the infrastructure that in needed in requirement is minimized reducing costs.

2) Daily backups can include more data from the users

3) Eliminated redundant content of backup.

4) When used on the client, duplicate data isn’t sent over the network reducing bandwidth

Source Based Deduplication

Data is deduplicated at the source
Backup client sends only new, unique segments across the network

Target Based Deduplication

Data is deduplicated at the target
Offload the backup client from the process
Requires sufficient network bandwidth
Reduces the burden on the target
Improves the overall backup performance

Data Archiving

Moves fixed size content that is no longer actively accessed to a separate, low-cost archive storage system for long-term retention and future reference.

- Data archiving saves primary storage capacity
- Data archiving reduces backup window and backup storage cost.

Fixed Data is a data that is not changing for a long time but is still needed because applications and users read from it.

Data Migration

This is a special replication technique that enables moving data from one system to another withing a data center, between data centers or between clouds.

Pros

Data center maintenance without down time
Avoid production impacts due to natural disasters
Facilitate technology upgrades and refreshes
Load balance across data centers

VM Migrations

In this type of migration, virtual machines are moved from one physical compute system to another without any downtime.

VM Storage Migration

VM files are moved from one storage system to another system without any down time or service disruption

Simplifies array migration and storage upgrades
Dynamically optimizes storage I/O performance
Efficiently manages storage capacity

Storage Based Data Migration

SAN-Based Migration

SAN-Based migration moves block-level data between heterogeneous storage systems over SAN

Storage system that performs migration is called the control storage system

NAS-Based Migration

NAS-Based migration moves file-level data between NAS system over LAN or WAN.

Concepts In Practice

vSphere High Availability (HA)
This method leverages multiple EXSi hosts that are configured as a cluster to provied rapid recovery from outages.
- Provides high availability for application running in virtual machine
- Protect against a server failure by restarting the virtual machines on other hosts withing the cluster.
- Protects against application failure by continuously monitoring a virtual machine and resetting it if a failure is detected

vSphere Fault Tolerance (FT)
- Enables users to protect any virtual machine from a host failure with no loss of data, transactions or connections.
- Provides continuous availability by ensuring that the states of the primary and the secondary VMs are identical at any point in time

Storage Information Security

Set of practices that protect data and information systems form unauthorized disclosure, access, use, destruction, deletion, modification, and disruption

Involves implementing safeguards or controls in order to lessen the risk of an exploitation or vulnerability in the information system.

Deploy tools that protect both data and infrastructure from unauthorized access, modification and deletion.

Goals of information security

Confidentiality
Provides the required secrecy of information to ensure that only authorized users have access to data

Integrity
Ensure that unauthorized changes to information are not allowed.

Availability
Ensure that unauthorized users have reliable and timely access to compute, storage, network, application, and data resources

Accountability
The process where the users or applications are responsible for the actions or events that are executed on the systems. Can be achieved by auditing logs.

Governance Risk and Compliance (GRC)
GRC is a term encompassing processes that help an organization to ensure that their acts are ethically correct and in the accordance with their:

Risk appetite (The risk level an organization willing to take)
Internal policies
External regulations

Governance =>
The Authority for making policies
Governance determines the purpose, strategy and operational rules by which companies are directed and managed.
Risk Management =>
Restricting access to certain users
A systematic process of assessing its assets placing a realistic valuation on each asset, and creating a risk profile that is rationalized for each information asset across the business
Compliance
Assures that the policies are being enforced
This is an act of sticking to corporate laws and policies and external laws and regulations

Authentication Authorization and Auditing

Authentication
A process to ensure that users or assets are who they claim to be by verifying their identity credentials
Authorization
A process determining whether and in which manner, a user, device , application or process is allowed to access only the particular service or resource
Auditing
Refers to the logging of all transactions for the purpose of assessing the effectiveness of security mechanisms
Helps to validate the behavior of the infrastructure components and to perform forensics, debugging and monitoring activities.

Security Concepts

Assets
Includes information, hardware, and software
Security considerations

- Must provide easy access to authorized users
- Must be difficult for potential attackers to compromise
- Cost of securing the assets should be cheap

Security Threats
Potential attacks that can be carried out
Attacks can be classified as:
- Passive attacks attempt to gain unauthorized access to the system
- Active attacks attempt data modifications or DoS attack

Security Vulnerabilities
Weaknesses that an attacker exploits to carry out attacks
Three security considerations:
- Attack Surface → The various enrty points that an attacker can use to launch an attack, which includes people, process, and technology
- Attack Vectors → Step or series of steps necessery to complete an attack.
- Work Factors → The amount of time and effort required to exploit an attack vector

Managing vulnerabilities
- Minimize the attack surface
- Maximize the work factor
- Install security controls

Security Control Catagories

Security controls reduce the exploitation of security vulnerabilities and any subsequent impact.

Preventive – Avoid a vulnerability from being exploited
Detective – Identifies when a vulnerability has been exploited
Corrective – Reduces the impact of an explited vulnerability

Controls can be technical such as Anti-Virus, Firewalls, and Intrusion Detection and Prevention Systems.
And non technical such as Administrative policies and physical controls

Key Security Threats
Denial of Service
Orevents legitamte users from accessing resources or services
- Exhosting network bandwidth or CPU cycles
- Target compute systems, network or storage resources

Distributed DoS
- Several systems launch a coordinated DosS attack on target.
- Attacker multiplies the effectiveness of the DoS attack by harnessing the reources of multiple collaborating attack systems,

Malicous Insider
A malicious insider is an organiation’s current or former employee, contractr or other business partner, who has or had authorized access to an organizaitions compute systems, network or storage
Control Measures:
- Strict access control policies
- Security audit and data encryption
- Disable employee accounts immediately after seperation

Man-in-the-middle Attack
The attacker eavedrops-overhears the conversation on the network channel berween two sites

Account Hijacking
Scenario where an attacker gains access to an administartor’s or user’s account(s)

Methods →
Phishing is a social engineering attack that is used to deceive users. Phising are typically carried by spoofing mail

Keystroke logging malware The attacker captures the user’s credentials

Shared Technology vulnerabilities
An attacker may exploit the vulnerabilities of tools used to enable multi-tenant evnironements
- Failure of controls that provide separation of memory and storage
- Hyperjacing attack involves installing rougue hypervisor that takes contols of compute system

Fileless Attacks

Fileless attacks fall are low-observable characteristics (LOC) attacks that avoids detection by most security solutionss

- Fileless attacks are not based on new files and d not install net software on that target machine

- Filelesee infections goes strighat into memory and the maliciouse content never touches the harddrive

- Fileless malware controls whitelisted applications that are already approved by an IT organization

Example – Web browser vulnerability are exploited to run malicious code

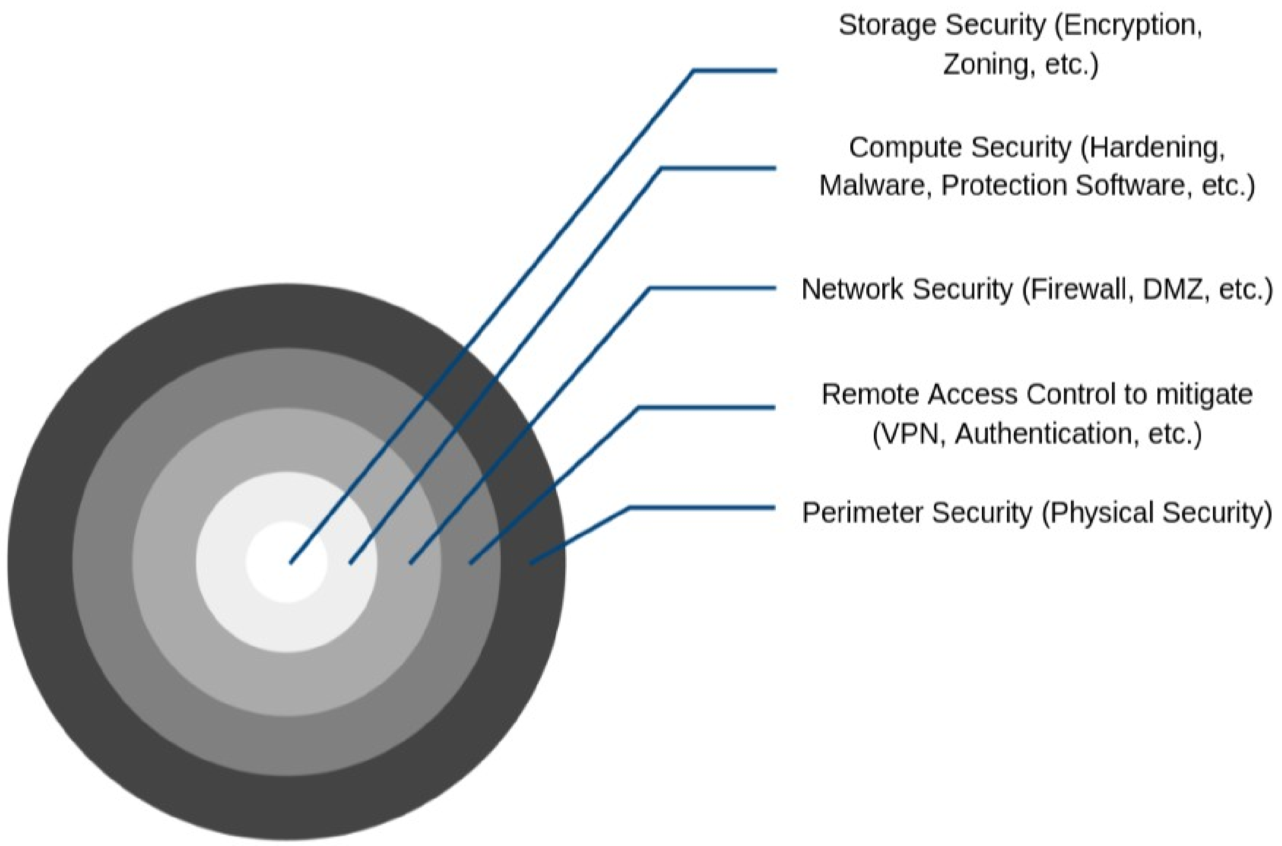
Insecure APIs

APIs are used in modern data cetner environment to perform various activities such as resouce provisioning, configuration, monitoring, management and orchestration

Attacker may exploit an API vulnerability to carry out an attack

Control measures :
- Authentication, authorization, encryption, and avoiding buffer overflows
- Periodic security reviews of APIs
- Restrict access to the API only to authorized users

Defense in Depth


Storage Security (Encryption, Zoning, etc.)
Compute Security (Hardening, Malware, Protection Software, etc.)
Network Security (Firewall, DMZ, etc.)
Remote Access Control to mitigate (VPN, Authentication, etc.)
Perimeter Security (Physical Security)

A multilayered security mechanism is deployed throughout the infrastructure to mitigate security risk if one layer of the defense is compromised

Defense in depth increases the barriers to exploitation
- An attacker must breach each layer of defense t obe successful
- Provides additional time to detect and respond to an attacker
- Reduces the scope of the security breach

Security Controls

Firewall

Security control system that is designed to examine data packets traversing a network and comapre them to a set of a filtering rules

- Rules can be set for both the incoming and the outgoing traffic
- Effectiveness of a firewall depends on how roubstly and extensively the security rules are defined

Demilitarized Zone
A control to secure internal assets while allowing Internet-based access to selected resources

In a DMZ environment sercers that need Internet access are placed between two firewalls

Servers in DMZ may or may not be allowed to communicate with internal resources

Application specific ports such as those designated for HTTP or FTP traffic are allowed thourgh the firewall to the DMZ

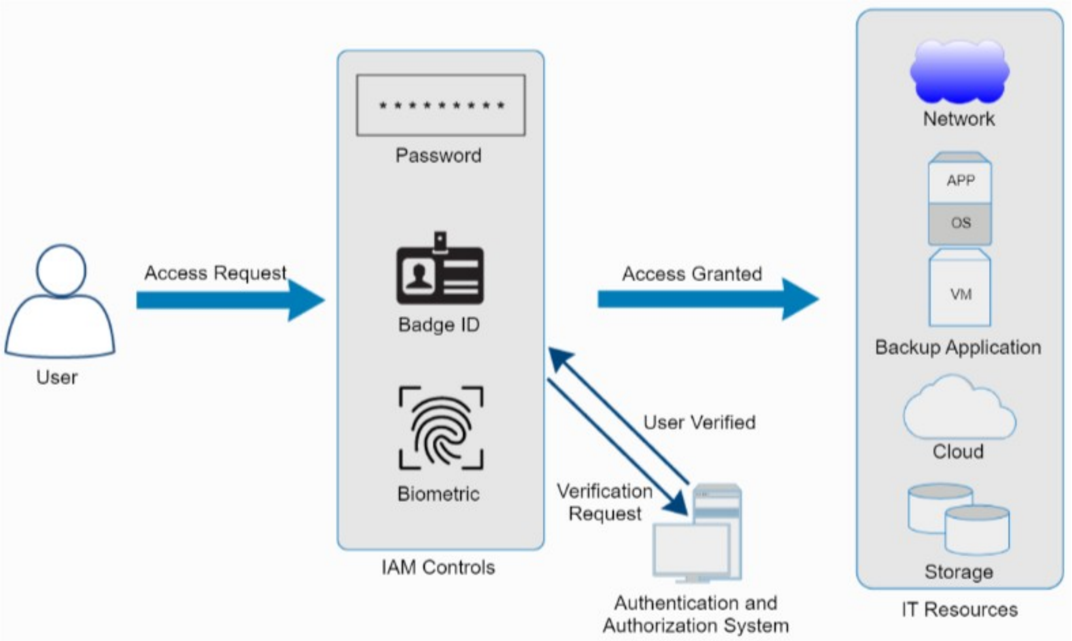
IDPS
Intrusion detection is the process of detecting events that can compromise the confidentiality, integrity, or availability of IT resources

Virtual Private Network
A VPN is a secure connection to the IT resource in the modern data protection environment

- Enables secure site connection between primary site when performing replication

- Secure site to site connection between an organization’s data center and cloud when performing cloud-based backup and replication

Identity and Access Management (IAM)

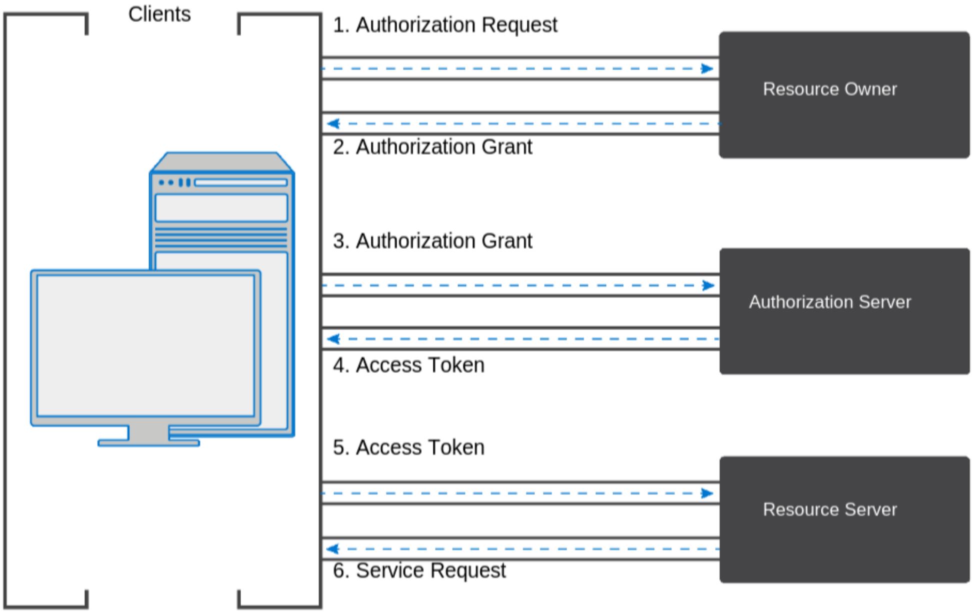


This is the process of:
- Managing user’s idetifiers and their authentication and authorization to access IT infrastructure resources

- Controlling access to resources by placing restrictions based on user identities

- Identifying the user and the privileges assigned to the user

OAuth and OpenID



An open authorization control enables a client to access protected resources from a resoucre server on behalf of a reouscre owner.

This can be used to secure application access domain
- Example: giving LinkdedIn permission to access Facebook

There are four entities involved in the authorization control
- Resource owner
- Resource server
- Client
- Authorization server

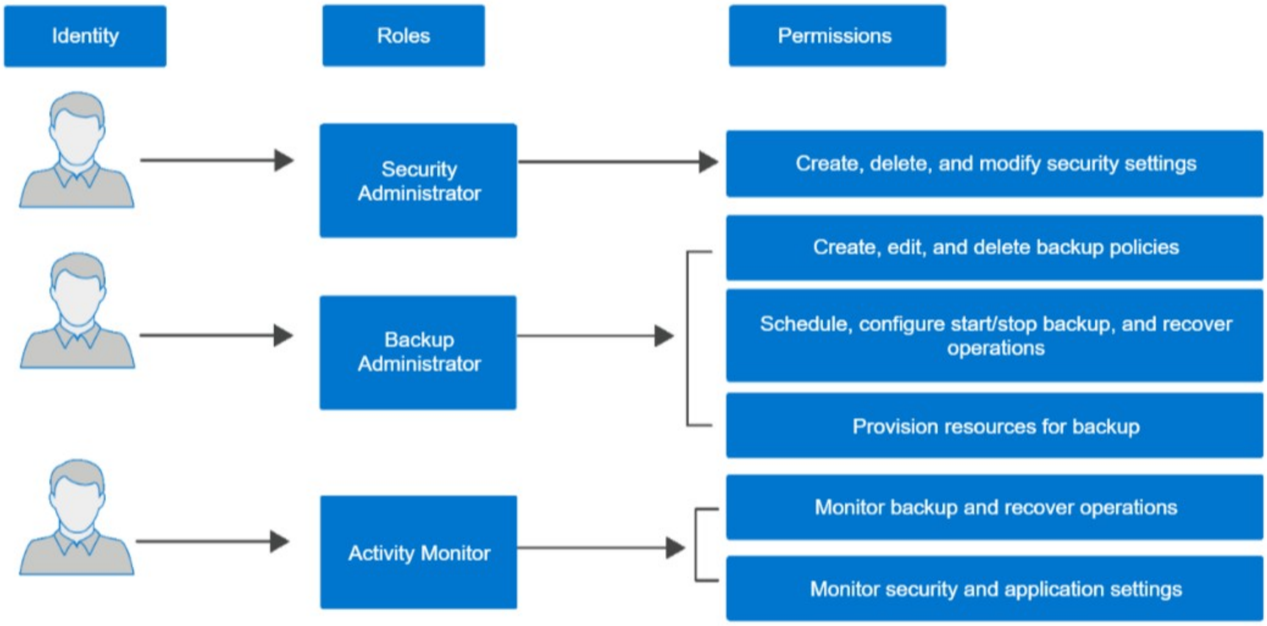
OpenID is an open standard for authentication in which an organization uses authenctication services from an OpenID third-party provider

The organization is known as the relying party and the OpenID provider is known as the identity provider

The user creates an OpenID with an OpenID provider, this OpenID can be used to sign on to any organization (relying party) that accpets OpenID authentication

Control can be used in the modern environment to secure application access domain.

Role Based Access Control


Identity
Roles
Permissions
Security Administrator
Backup Administrator
Activity Monitor
Create, delete, and modify security settings
Create, edit, and delete backup policies
Schedule, configure start/stop backup, and recover operations
Provision resources for backup
Monitor backup and recover operations
Monitor security and application settings

Role Based Access Control is an approach to restirct access to the authorized users based pm their respective roles
- Minimum privileges are assigned to a role that is required to perform the tasks associated with that role

Malware protection sofware

Signiture Based Detection Scan files and determine signatures based on known malware

Heuristic Can be used to detect malware by examining the behavior of program

Malware detection program

This is a program installed on a compute system or mobile device to detect, prevent and remove malware and malicious programs such as viruses, worms, trojan horses, key loggers, and spyware

Uses various techniques to detect malware

Data Encryption

Data encryption is a cryptographic technique in which data is encoded and made indecipherable to evasdroppers or hackers

Provides protection from threats such as:

- Tampering with data which violates data integrity
- Media theft which compromises data availability
- Sniffing attacks which compromise confidentiality

Data encryption is one of the most important controls for securing data in-flight and at-rest in a modern data center environment.

Data Shredding

A process of deleting data or residual representations of data which makes it unrecoverable

When data is deleted, sometimes the actual strings of binary data may remain on the storage device.

On magetic media, magnetic residuals can remain after deleting data.

Cyber Recovery

True information protection emphasizes keeping an isolated copy of your critical data sich as essential applications and itellectual property off the network

Cyber recovery architecture

- Maintains critical business data and technology configuration in a secure air-gapped 'vault' environment that can be used for recovery or analysis

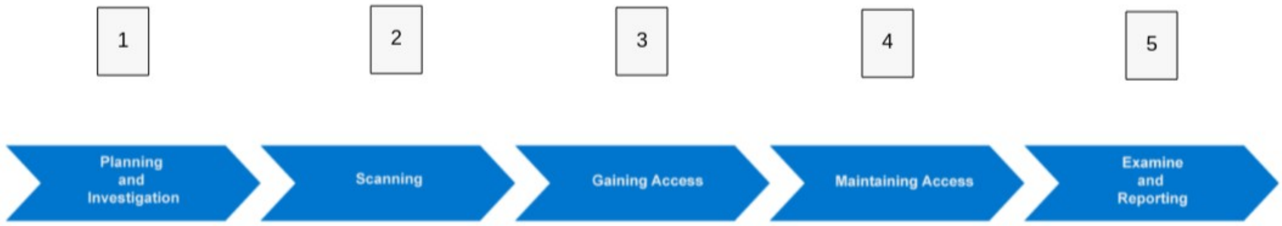
- Isolated data to ensure an uncompromised copy always exists

- Creates point in time retention locked copies that can be validated and then used for recovery of the production system

Penetration Testing

Penetration testing evaluates systems, networks, and applications to find vulnerabilities and threates that an attacker could exploit.

Penetration testing is performed through several stages as shown in the image



1) Goals and priorities of an organization. Investigation includes collecting information about active and passive network, domains and mails of the target system or network

2) Examine and Test the system, network, and application against attacks and automated intrusion attempts

3) Third stage collects the evidence of the exploited vulnerabilities and determines if presistenve access can be maintained

4) Collects the evidence of the exploited vulnerabilities and determines if persistence access can be maintained

5) In the fifth stage, the identified findings are documented:
- Approvals made in previous stages
- Risk levels by exploited vulnerabilities
- Sensitive data that was breached
- Total engaged time of pen-tester
- Find recommendations for future security

Virtual Machine Hardening

Process of securing VMs, this includes →
- Changes the default configuration of the VM
- Disconnection of the virtual components that are not required
- Ensuring that the security mechanisms are enabled and updated
- Isolation of the VM network using VLANs
- Creation of the virtual machine from a secure VM template

Operating System Hardening

Process of securing the operating system
- Deletion of unused files and programs
- Installtion of current OS updates and patches
- Performing vulnerability scanning and penetration testing

Application Hardening

Process of securing an application
- Identify security policies and procedures
- Examine transmission of credentials over the network
- Implement Access Control List to restict applications
- Secure thired party applications and tools
- Install application updates and patches

<u>Storage Infrastructure Management</u>

A process ensures the proper and cost effective use of the available storage resoures to meet the business needs

- Helps IT organizations to achieve their strategic business needs
- Aligns the storage resources with the performance needs of the applications
- Ensures better utilization of the existing storage resources to reduce unnecessary infrastructure investments

Key Characteristics

Service Focused approach
Modern storage infrastructure management has a service based focus. It is linked to the service requiremetns and service level agreement (SLA).
This Includes →
- Determining the optimal amount of storage space needed in a backup storage system to meet the capacity requirement of a service
- Creating a disaster recovery plan to meet the recovert time objective of services
- Ensuring that the management processes, management tools, and staffing are appropriate to provide a data archiving service

Software Defined Data Center Aware

- Software defomed data cemter management is more efficient over hardware specific management
- Many common repeatable, hardware-sepcific management tasks are automated. Management is focused on strategic, value-driven activities
- Management functions move to an external software controller
- Management operations become independent of underlying hardware

End to End Visibility

- Provides detailed information on configuration, connectivity, capacity, performance and interrelationship between components

- Enables Report conodilation, correlating issues to find root cause and tracking migration of data and services

Storage Management Function

Infrastructure Discovery
- Discovery provides visibility inot each infrastructure compnenet. Discoverd inforamation helps in monitoring and management
- Discovery tool interacts and collects information from components
- Discovery is typically scheduled to occur periodically. May aso be initiated by an administrator or triggered by an orchestator

Monitoring Alerts and Reporting
- Monitoring provides visibility into the storage infrastructure and froms the vasis for performing management operations
- Alerting provides inforamtion about events or impending threats or issues
- Reporting involves gathering information from various components and operations management processes

Operations Management
- Involves on going management activities to maintain the IT infrastructure and the deployed services
- Ensures that the services and service levels are deivered as committed
- Ideally, operations management should be automated to ensure the operational agility. Management tools are usually capable of automating many management operations
Further, the automated operations of management tools can also be logically integrated and sequemced through orchestration

Monitoring
Monitoring provides visibility into the storage information health and involves the following activities

- Tracks the performance and availability status of components and services
- Measures the utilization and consumption of resources
- Tracks environmental parameters such as heating, ventilating, and air-conditioning
- Triggers alerts when thresholds are reached, security policies are violated or service performance deviates from SLA

Monitoring Parameters
Configuration
Involves tracking changes and deployment of storage infrastructure components and services
Detects configuration errors, non-compliance with configuration policies and unauthorized configruation changes

Availability
Monitor the availability of hardware components.
Involves monitoring of the errors generated by the ingrastrcture compnents
Identifies the failure of any component that may lead to data and service unavailability or defraded performance

Capacity
Monitor capacity of storage and raise notifications when reaching certain points of free space.

Alerts
Used to inform that something is wrong, like a driver fell down,

Change Management

Standardizes change related procedures in a data protection environment for prompt handling of all changes with minimal impact on data protection operations and service quality

Examples of change:
- Introduction to a new data replication service
- Replacing an archive storage system
- Expansion of a storage pool
- Upgrade of backup application

Capacity Management

Ensure that data prortection environment is able to meet the required capacity demands for protection operations and services in a cost effective and timely manner

Example of capacity management:
- Addomg new nodes to a scale-out NAS
- Expanding a storage pool and setting utilization threshold
- Forecasting the usage of storage media

Performance Management

Ensures the optimal operational efficiency of all infrastructure components so that data protection operations and services can meet or exceed the required performance level.

Example of Performance Management:
- Adjusting conflicting backup schedules
- Fine tuning file system configuration
- Adding new VM or allocating more resources

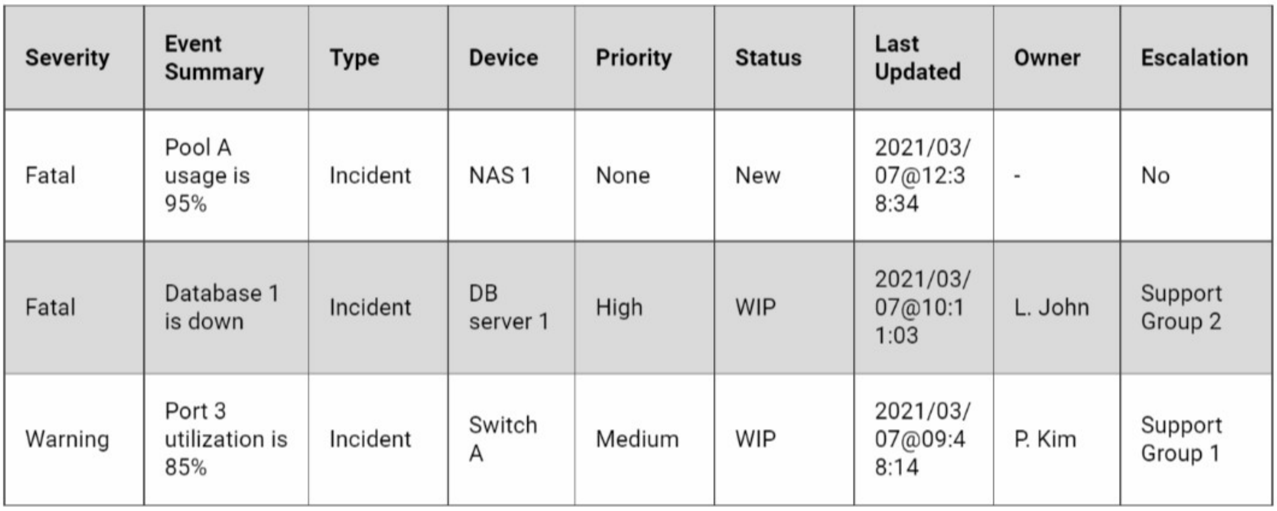
Availability Management

Ensures that the availability requirements of data protection operations and services are consistently net

Examples of Availability
- Deploying redundant, fault-tolerant, and hot swappable components.
- Implementing compute cluster, VM live shadow copy, and multi pathing solutions

Incident Management

Responsible for detecting and recording all incidents in a data protection environment. It investigates the incidents and provides appropriate solutions to resolve them.
Example of incident detection:



Severity	Event Summary	Type	Device	Priority	Status	Last Updated	Owner	Escalation
Fatal	Pool A usage is 95%	Incident	NAS 1	None	New	2021/03/07@12:38:34	-	No
Fatal	Database 1 is down	Incident	DB server 1	High	WIP	2021/03/07@10:11:03	L. John	Support Group 2
Warning	Port 3 utilization is 85%	Incident	Switch A	Medium	WIP	2021/03/07@09:48:14	P. Kim	Support Group 1

Problem Management

Prevents incidents that share common symptoms or root cause for reoccurring, and minimizes the adverse impcat of incidents that cannot be prevented

Problem management examples:
- Reviews of incident history to detect problems in a data protection environment
- Identifies the underlying root cause that creates a problem
- Uses integrated incident and problem management tools to mark specific incidents as problems and perform root cause analysis

Security Management
prevents occurrence of security related incidents or activities. These incidents or activities. These incidents adversely affect the confidentiality, integrity and availability of organizations. Data security management ensures the regulatory or compliance requirements for data protection of organizations are met for protecting data at reasonable costs.

Example of security management:
- Managing user accounts and access policies
- Implementing controls at multiple levels
- Scanning applications and databases
- Configuration zoning, LUN masking, and data enctyption services