MODULE 5

SECURING AND MANAGING STORAGE INFRASTRUCTURE

5.1 Information Security Framework

The basic information security framework is built to achieve four security goals: confidentiality, integrity, and availability (CIA), along with accountability. This framework incorporates all security standards, procedures, and controls, required to mitigate threats in the storage infrastructure environment.

- **Confidentiality:** Provides the required secrecy of information and ensures that only authorized users have access to data. This requires authentication of users who need to access information.
- **Integrity:** Ensures that the information is unaltered. Ensuring integrity requires detection of and protection against unauthorized alteration or deletion of information. Ensuring integrity stipulates measures such as error detection and correction for both data and systems.
- **Availability**: This ensures that authorized users have reliable and timely access to systems, data, and applications residing on these systems. Availability requires protection against unauthorized deletion of data and denial of service. Availability also implies that sufficient resources are available to provide a service.
- **Accountability service**: Refers to accounting for all the events and operations that take place in the data center infrastructure. The accountability service maintains a log of events that can be audited or traced later for the purpose of security.

5.2 Risk Triad

Risk triad defines risk in terms of threats, assets, and vulnerabilities. They are considered from the perspective of risk identification and control analysis.

5.2.1 Assets

- Information is one of the most important assets for any organization. Other assets include hardware, software, and other infrastructure components required to access the information.

- To protect these assets, organizations must develop a set of parameters to ensure the availability of the resources to authorized users and trusted networks. These parameters apply to storage resources, network infrastructure, and organizational policies.
- Security methods have two objectives.
  - The first objective is to ensure that the network is easily accessible to authorized users. It should also be reliable and stable under disparate environmental conditions and volumes of usage.
  - The second objective is to make it difficult for potential attackers to access and compromise the system.
- The security methods should provide adequate protection against unauthorized access, viruses, worms, trojans, and other malicious software programs.
- Security measures should also include options to encrypt critical data and disable unused services to minimize the number of potential security gaps.
- The security method must ensure that updates to the operating system and other software are installed regularly

5.2.2 Security Threats

- Threats are the potential attacks that can be carried out on an IT infrastructure.
- Attacks can be classified as active or passive.
  - ***Passive attacks*** are attempts to gain unauthorized access into the system. They pose threats to confidentiality of information.
  - ***Active attacks*** include data modification, denial of service (DoS), and repudiation attacks. They pose threats to data integrity, availability, and accountability. **Denial of service (DoS**) attacks prevent legitimate users from accessing resources and services. **Repudiation** is an attack against the accountability of information. It attempts to provide false information by either impersonating someone or denying that an event or a transaction has taken place.

5.2.3 Vulnerabilities

- The paths that provide access to information are often vulnerable to potential attacks.
- Each of the paths may contain various access points, which provide different levels of access to the storage resources.

- It is important to implement adequate security controls at all the access points on an access path.
- Implementing security controls at each access point of every access path is known as defense in depth.
- Attack surface, attack vector, and work factor are the three factors to consider when assessing the extent to which an environment is vulnerable to security threats.
  - An **Attack surface** refers to the various entry points that an attacker can use to launch an attack.
  - An **attack vector** is a step or a series of steps necessary to complete an attack.
  - **Work factor** refers to the amount of time and effort required to exploit an attack vector.

5.3 Storage Security Domains

- To identify the threats that apply to a storage network, access paths to data storage can be categorized into three security domains: application access, management access, and backup, replication, and archive.
- Fig 5.1 depicts the three security domains of a storage system environment.

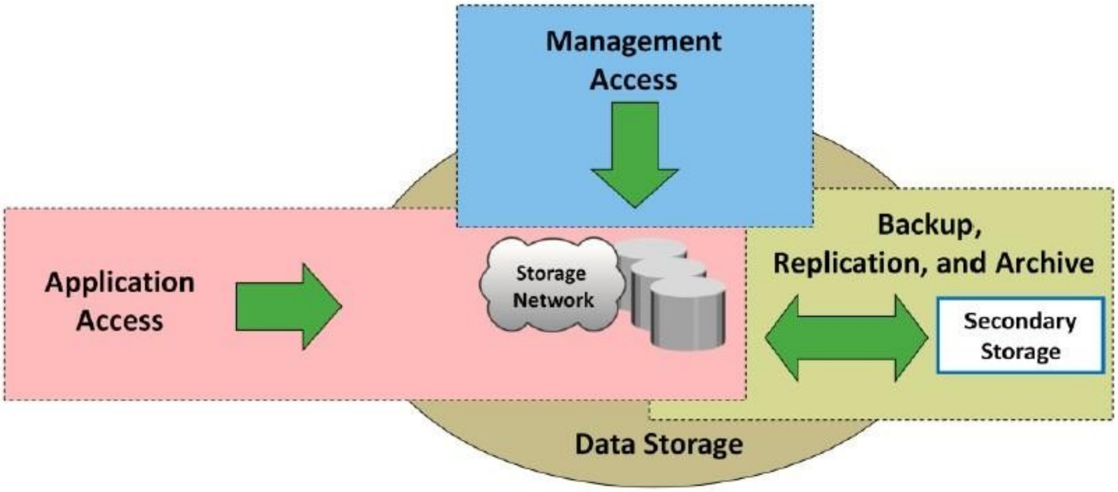


Fig 5.1: Storage security domains

- The first security domain involves application access to the stored data through the storage network.
- The second security domain includes management access to storage and interconnect

devices and to the data residing on those devices. This domain is primarily accessed by storage administrators who configure and manage the environment.

- The third domain consists of backup, replication, and archive access. Along with the access points in this domain, the backup media also needs to be secured.

5.3.1 Securing the Application Access Domain

- The application access domain may include only those applications that access the data through the file system or a database interface.
- An important step to secure the application access domain is to identify the threats in the environment and appropriate controls that should be applied.
- Implementing physical security is also an important consideration to prevent media theft.
- Fig 5.2 shows application access in a storage networking environment.

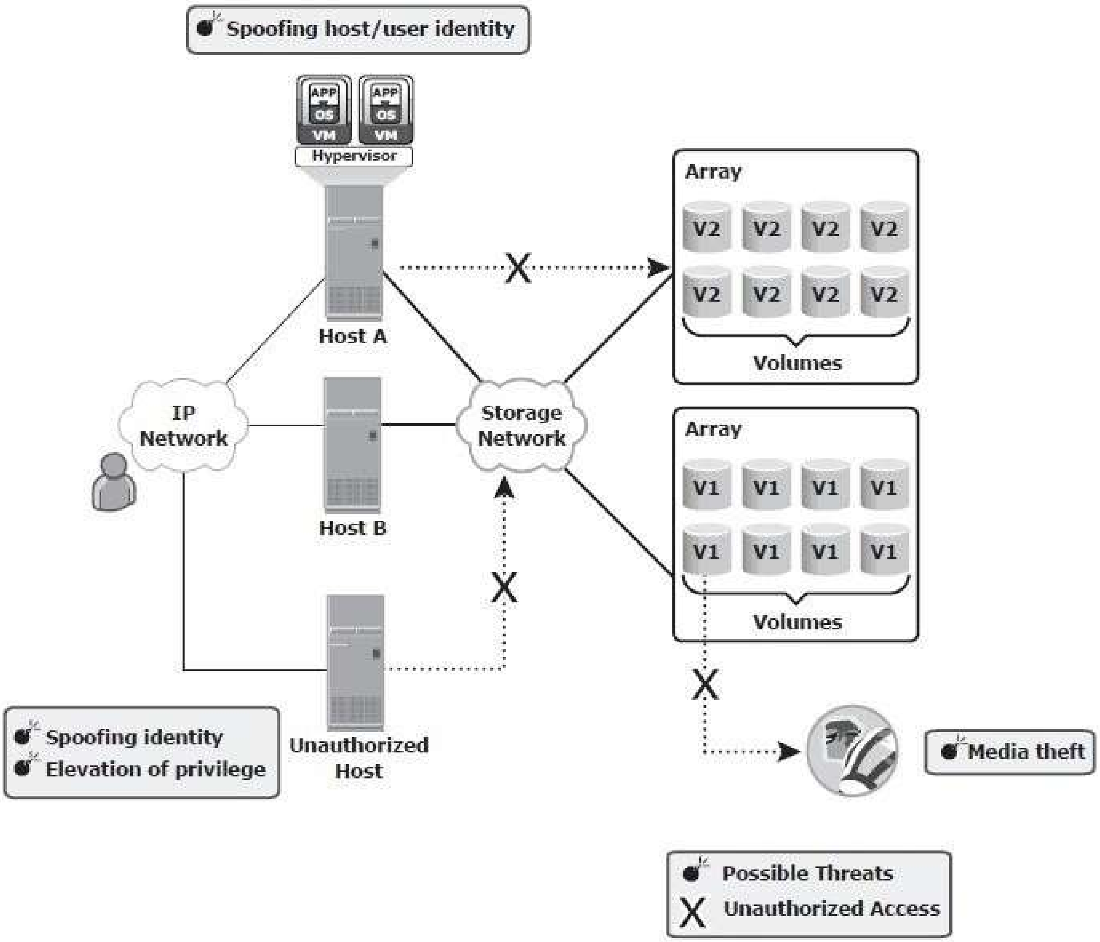


Fig 5.2: Security threats in an application access domain

- Host A can access all V1 volumes; host B can access all V2 volumes. These volumes are classified according to the access level, such as confidential, restricted, and public.
- Some of the possible threats in this scenario could be host A spoofing the identity or elevating to the privileges of host B to gain access to host B's resources. Another threat could be that an unauthorized host gains access to the network; the attacker on this host may try to spoof the identity of another host and tamper with the data, snoop the network, or execute a DoS attack.
- Also any form of media theft could also compromise security. These threats can pose several serious challenges to the network security; therefore, they need to be addressed.

5.3.2 Securing the Management Access Domain

- Management access, whether monitoring, provisioning, or managing storage resources, is associated with every device within the storage network.
- Most management software supports some form of CLI, system management console, or a web-based interface. Implementing appropriate controls for securing storage management applications is important because the damage that can be caused by using these applications can be far more extensive.
- Fig 5.3 depicts a storage networking environment in which production hosts are connected to a SAN fabric and are accessing production storage array A, which is connected to remote storage array B for replication purposes. This configuration has a storage management platform on Host A.
- A possible threat in this environment is an unauthorized host spoofing the user or host identity to manage the storage arrays or network. For example, an unauthorized host may gain management access to remote array B.
- Providing management access through an external network increases the potential for an unauthorized host or switch to connect to that network. In such circumstances, implementing appropriate security measures prevents certain types of remote communication from occurring.
- Using secure communication channels, such as Secure Shell (SSH) or Secure Sockets Layer (SSL)/Transport Layer Security (TLS), provides effective protection against these threats.
- Event log monitoring helps to identify unauthorized access and unauthorized changes to the infrastructure.

- The administrator's identity and role should be secured against any spoofing attempts so that an attacker cannot manipulate the entire storage array and cause intolerable data loss by reformatting storage media or making data resources unavailable.

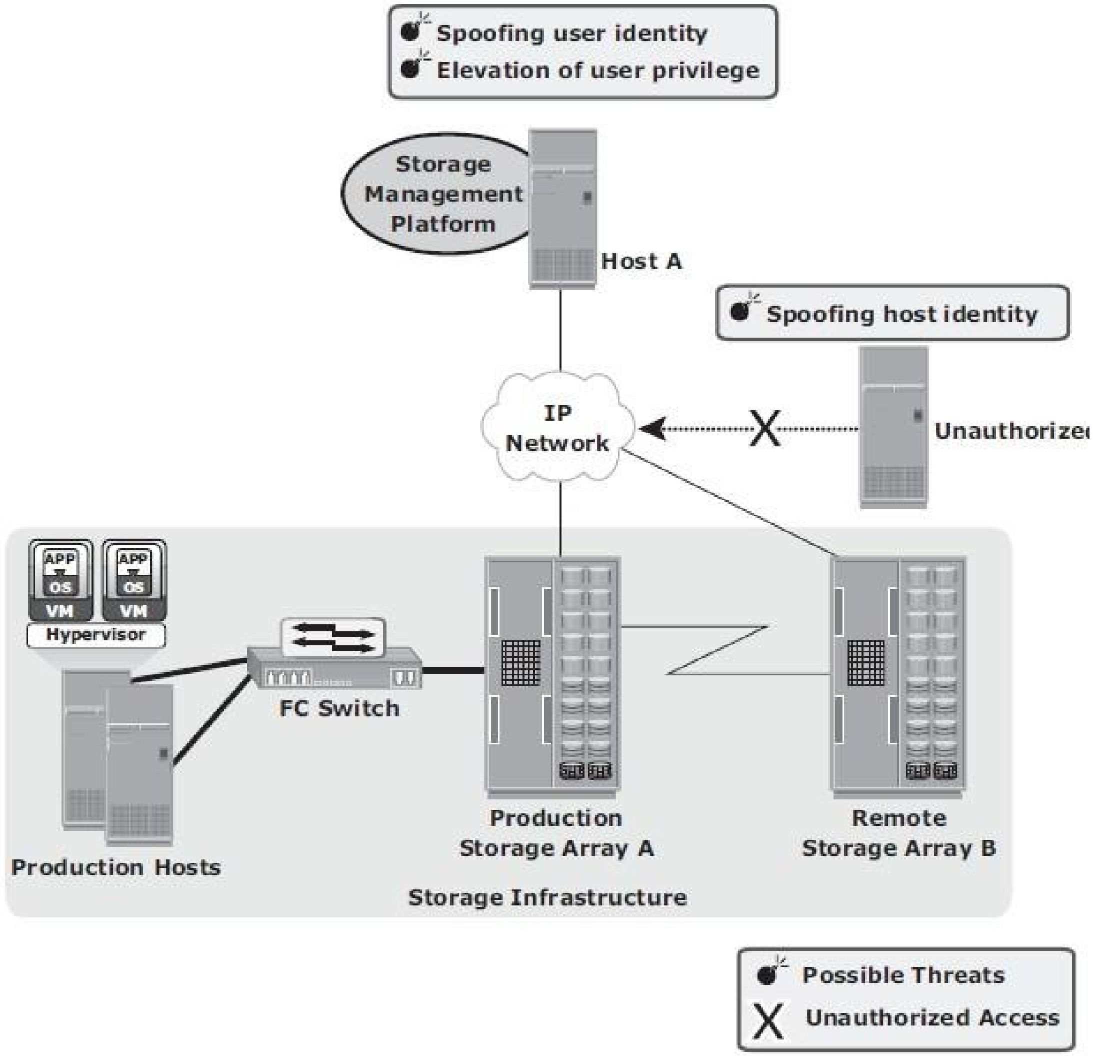


Fig 5.3: Security threats in a management access domain

5.3.3 Securing Backup, Replication and Archive

- Backup, replication, and archive is the third domain that needs to be secured against an attack.
- A backup involves copying the data from a storage array to backup media, such as tapes or disks.
- Securing backup is complex and is based on the backup software that accesses the

storage arrays.

- ➢ It also depends on the configuration of the storage environments at the primary and secondary sites, especially with remote backup solutions performed directly on a remote tape device or using array-based remote replication.
- ➢ Organizations must ensure that the disaster recovery (DR) site maintains the same level of security for the backed up data.
- ➢ Protecting the backup, replication, and archive infrastructure requires addressing several threats, including spoofing the legitimate identity of a DR site, tampering with data, network snooping, DoS attacks, and media theft. Such threats represent potential violations of integrity, confidentiality, and availability.
- ➢ Fig 5.4 illustrates a generic remote backup design whereby data on a storage array is replicated over a DR network to a secondary storage at the DR site.
- ➢ The physical threat of a backup tape being lost, stolen, or misplaced, especially if the tapes contain highly confi dential information, is another type of threat. Backup-to-tape applications are vulnerable to severe security implications if they do not encrypt data while backing it up.

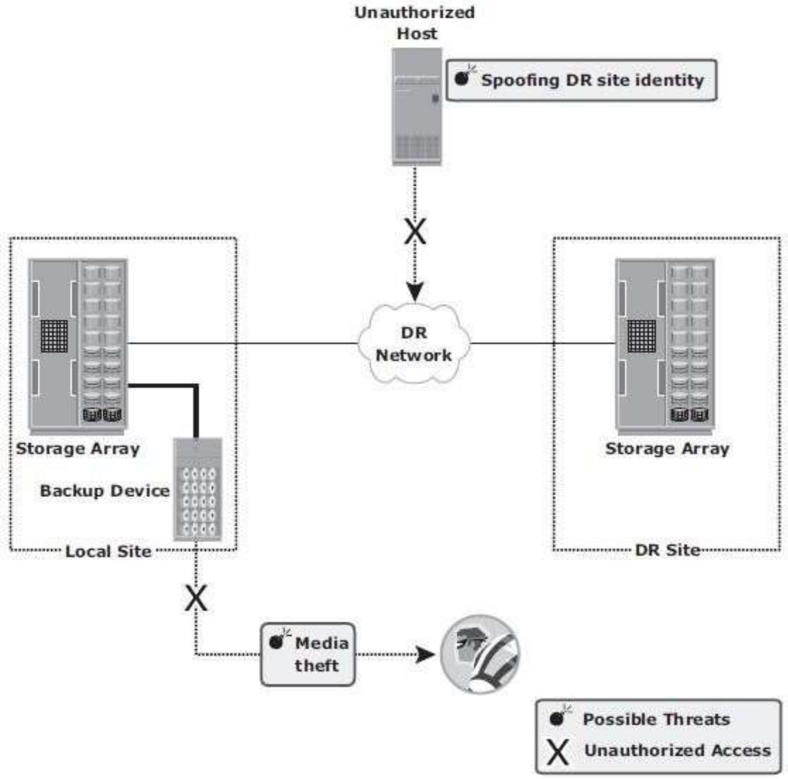


Fig 5.4: Security threats in a backup, replication, and archive environment

5.4 Security solutions for FC-SAN, IP-SAN, NAS Environment

5.4.1 FC-SAN

- Traditional FC SANs have an inherent security advantage over IP-based networks.
- An FC SAN is configured as an isolated private environment with fewer nodes than an IP network.

FC SAN Security Architecture

- Storage networking environments are a potential target for unauthorized access, theft, and misuse because of the vastness and complexity of these environments. Therefore, security strategies are based on the **defense in depth** concept, which recommends multiple integrated layers of security. This ensures that the failure of one security control will not compromise the assets under protection.
- Fig 5.5 illustrates various levels (zones) of a storage networking environment that must be secured and the security measures that can be deployed.

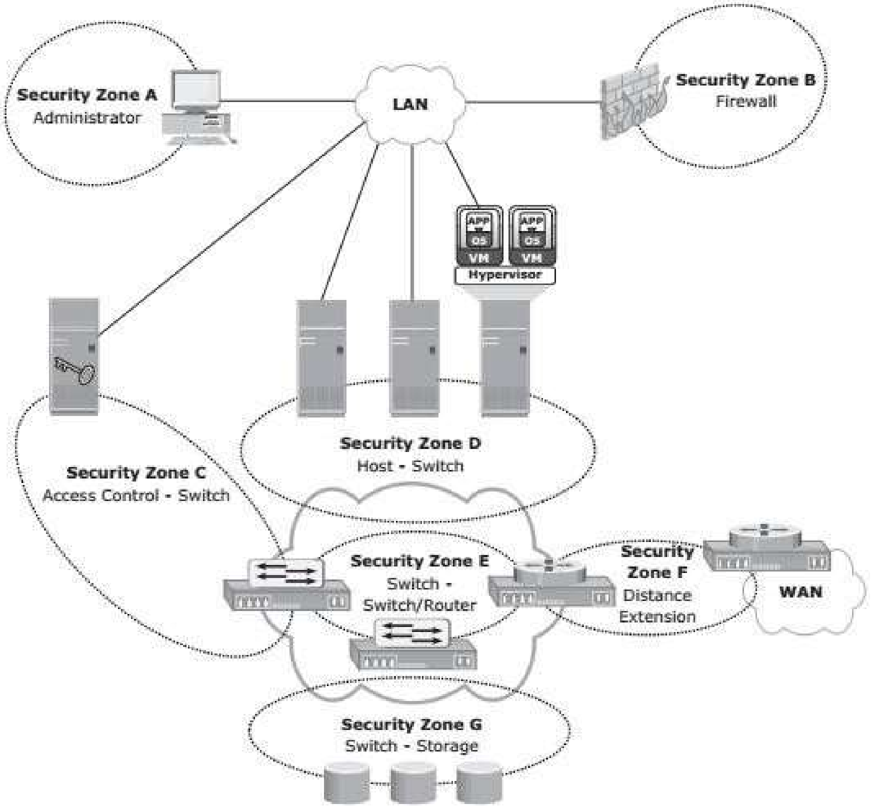
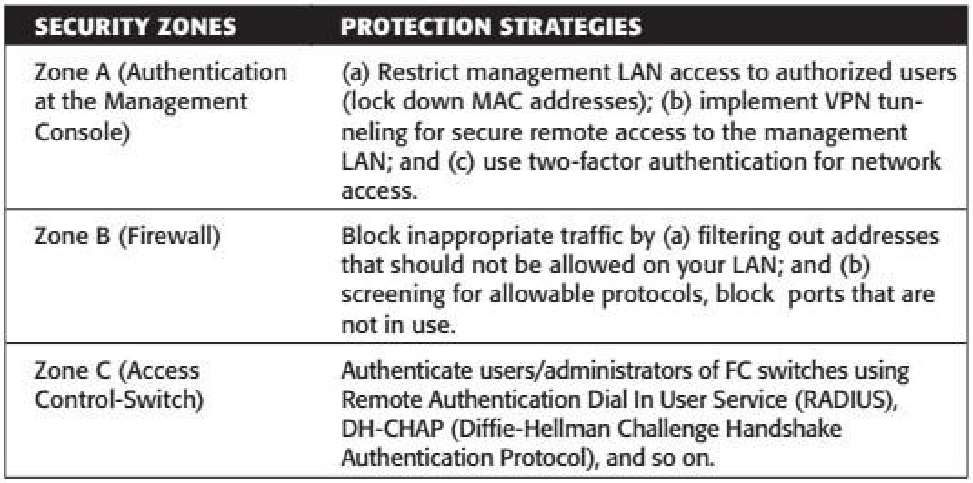


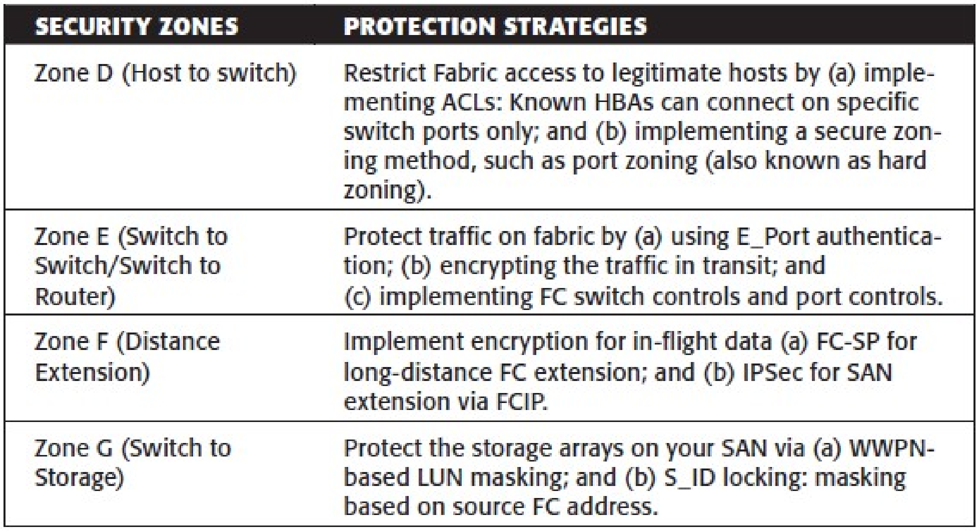
Fig 5.5: FC SAN security architecture

- Table 5.1 provides a comprehensive list of protection strategies that must be implemented in various security zones. Some of the security mechanisms listed in Table 5.1 are not specific to SAN but are commonly used data center techniques. For example, two-factor authentication is implemented widely; in a simple implementation it requires the use of a username/password and an additional security component such as a smart card for authentication.

Table 5.1 : list of protection strategies



SECURITY ZONES	PROTECTION STRATEGIES
Zone A (Authentication at the Management Console)	(a) Restrict management LAN access to authorized users (lock down MAC addresses); (b) implement VPN tunneling for secure remote access to the management LAN; and (c) use two-factor authentication for network access.
Zone B (Firewall)	Block inappropriate traffic by (a) filtering out addresses that should not be allowed on your LAN; and (b) screening for allowable protocols, block ports that are not in use.
Zone C (Access Control-Switch)	Authenticate users/administrators of FC switches using Remote Authentication Dial In User Service (RADIUS), DH-CHAP (Diffie-Hellman Challenge Handshake Authentication Protocol), and so on.



SECURITY ZONES	PROTECTION STRATEGIES
Zone D (Host to switch)	Restrict Fabric access to legitimate hosts by (a) implementing ACLs: Known HBAs can connect on specific switch ports only; and (b) implementing a secure zoning method, such as port zoning (also known as hard zoning).
Zone E (Switch to Switch/Switch to Router)	Protect traffic on fabric by (a) using E_Port authentication; (b) encrypting the traffic in transit; and (c) implementing FC switch controls and port controls.
Zone F (Distance Extension)	Implement encryption for in-flight data (a) FC-SP for long-distance FC extension; and (b) IPSec for SAN extension via FCIP.
Zone G (Switch to Storage)	Protect the storage arrays on your SAN via (a) WWPN-based LUN masking; and (b) S_ID locking: masking based on source FC address.

Basic SAN Security Mechanisms

- LUN masking and zoning, switch-wide and fabric-wide access control, RBAC, and logical partitioning of a fabric (Virtual SAN) are the most commonly used SAN security methods.

LUN Masking and Zoning

- LUN masking and zoning are the basic SAN security mechanisms used to protect against unauthorized access to storage.
- The standard implementations of LUN masking on storage arrays mask the LUNs presented to a frontend storage port based on the WWPNs of the source HBAs.
- A stronger variant of LUN masking may sometimes be offered whereby masking can be done on basis of source FC addresses. It offers a mechanism to lock down the FC address of a given node port to its WWN.
- WWPN zoning is the preferred choice in security-conscious environments.

Securing Switch Ports

- Apart from zoning and LUN masking, additional security mechanisms, such as port binding, port lockdown, port lockout, and persistent port disable, can be implemented on switch ports.
- **Port binding** limits the number of devices that can attach to a particular switch port and allows only the corresponding switch port to connect to a node for fabric access. Port binding mitigates but does not eliminate WWPN spoofing.
- **Port lockdown** and **port lockout** restrict a switch port's type of initialization. Typical variants of port lockout ensure that the switch port cannot function as an E_Port and cannot be used to create an ISL, such as a rogue switch. Some variants ensure that the port role is restricted to only FL_Port, F_Port, E_Port, or a combination of these.
- **Persistent port** disable prevents a switch port from being enabled even after a switch reboot.

Switch-Wide and Fabric-Wide Access Control

- As organizations grow their SANs locally or over longer distances there is a greater need to effectively manage SAN security.
- Network security can be configured on the FC switch by using access control lists (ACLs) and on the fabric by using fabric binding.

- ACLs incorporate the device connection control and switch connection control policies.
- The device connection control policy specifies which HBAs and storage ports can be a part of the fabric, preventing unauthorized devices (identified by WWPNs) from accessing it.
- Similarly, the switch connection control policy specifies which switches are allowed to be part of the fabric, preventing unauthorized switches (identified by WWNs) from joining it.
- Fabric binding prevents an unauthorized switch from joining any existing switch in the fabric.
- It ensures that authorized membership data exists on every switch and that any attempt to connect two switches by using an ISL causes the fabric to segment.
- Role-based access control provides additional security to a SAN by preventing unauthorized management activity on the fabric for management operations.
- It enables the security administrator to assign roles to users that explicitly specify privileges or access rights after logging into the fabric.
- For example, the zoneadmin role is able to modify the zones on the fabric, whereas a basic user may only be able to view fabric-related information, such as port types and logged-in nodes.

Logical Partitioning of a Fabric: Virtual SAN

- VSANs enable the creation of multiple logical SANs over a common physical SAN.
- They provide the capability to build larger consolidated fabrics and still maintain the required security and isolation between them.
- Fig 5.6 depicts logical partitioning in a VSAN.
- The SAN administrator can create distinct VSANs by populating each of them with switch ports. In the example, the switch ports are distributed over two VSANs: 10 and 20 — for the Engineering and HR divisions, respectively. Although they share physical switching gear with other divisions, they can be managed individually as standalone fabrics. Zoning should be done for each VSAN to secure the entire physical SAN. Each managed VSAN can have only one active zone set at a time.

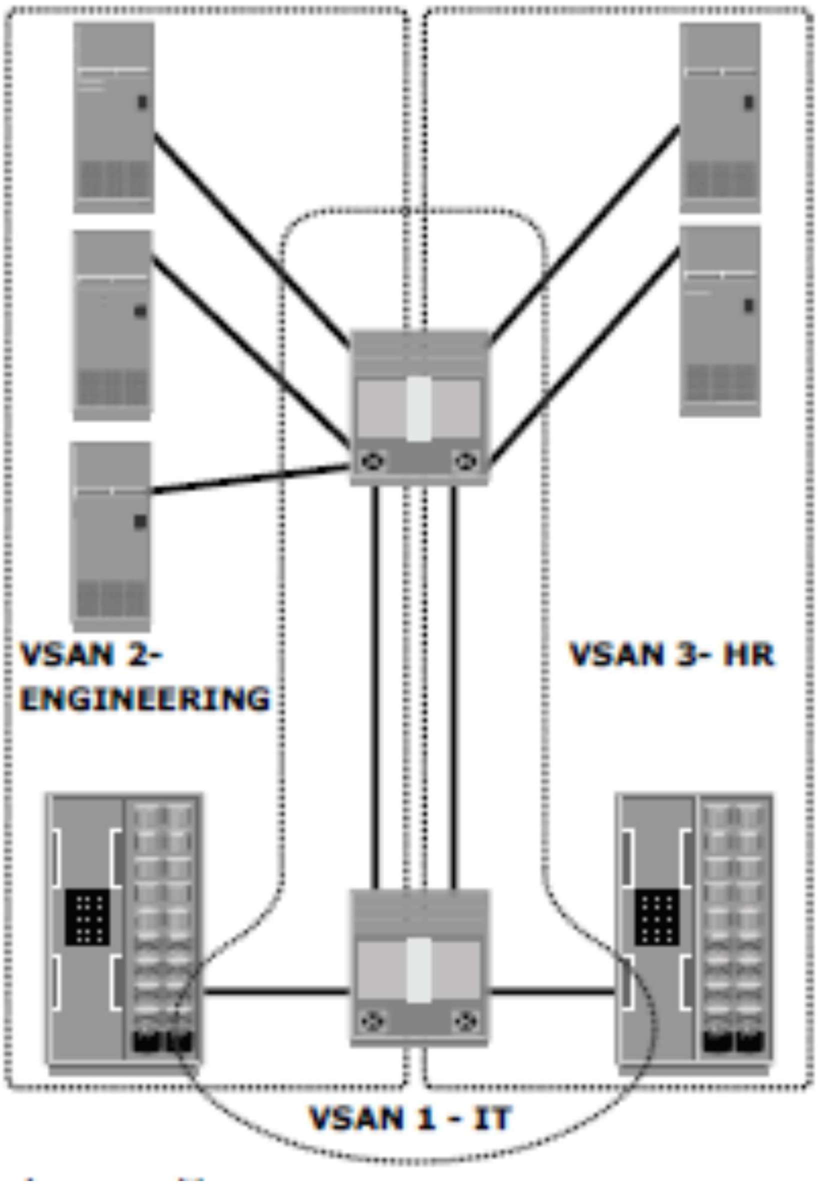


Fig 5.6: Securing SAN with VSAN

5.4.2 NAS

- NAS is open to multiple exploits, including viruses, worms, unauthorized access, snooping, and data tampering.
- Various security mechanisms are implemented in NAS to secure data and the storage networking infrastructure.
- Permissions and ACLs form the first level of protection to NAS resources by restricting accessibility and sharing. These permissions are deployed over and above the default behaviors and attributes associated with files and folders.
- In addition, various other authentication and authorization mechanisms, such as Kerberos and directory services, are implemented to verify the identity of network users and define their privileges. Similarly, firewalls protect the storage infrastructure from unauthorized access and malicious attacks.

NAS File Sharing: Windows ACLs

- Windows supports two types of ACLs:
  - discretionary access control lists (DACLs)
  - system access control lists (SACLs).
- The DACL, commonly referred to as the ACL, that determines access control. The SACL determines what accesses need to be audited if auditing is enabled.
- In addition to these ACLs, Windows also supports the concept of object ownership.
- The owner of an object has hard-coded rights to that object, and these rights do not need to be explicitly granted in the SACL.
- The owner, SACL, and DACL are all statically held as attributes of each object. Windows also offers the functionality to inherit permissions, which allows the child objects existing within a parent object to automatically inherit the ACLs of the parent object.
- ACLs are also applied to directory objects known as security identifiers (SIDs). These

are automatically generated by a Windows server or domain when a user or group is created, and they are abstracted from the user.

- In this way, though a user may identify his login ID as "User1," it is simply a textual representation of the true SID, which is used by the underlying operating system.
- Internal processes in Windows refer to an account's SID rather than the account's username or group name while granting access to an object. ACLs are set by using the standard Windows Explorer GUI but can also be configured with CLI commands or other third-party tools.

NAS File Sharing: UNIX Permissions

- For the UNIX operating system, a user is an abstraction that denotes a logical entity for assignment of ownership and operation privileges for the system.
- A user can be either a person or a system operation.
- A UNIX system is only aware of the privileges of the user to perform specific operations on the system and identifies each user by a user ID (UID) and a username, regardless of whether it is a person, a system operation, or a device.
- In UNIX, users can be organized into one or more groups. The concept of group serves the purpose to assign sets of privileges for a given resource and sharing them among many users that need them.
- For example, a group of people working on one project may need the same permissions for a set of files.
- UNIX permissions specify the operations that can be performed by any ownership relation with respect to a file. These permissions specify what the owner can do, what the owner group can do, and what everyone else can do with the file.
- For any given ownership relation, three bits are used to specify access permissions. The first bit denotes read (r) access, the second bit denotes write (w) access, and the third bit denotes execute (x) access.
- Because UNIX defines three ownership relations (Owner, Group, and All), a triplet (defining the access permission) is required for each ownership relationship, resulting in nine bits. Each bit can be either set or clear. When displayed, a set bit is marked by its corresponding operation letter (r, w, or x), a clear bit is denoted by a dash (-), and all are put in a row, such as rwxr-xr-x. In this example, the owner can do anything with the file, but group owners and the rest of the world can read or execute only.

When displayed, a character denoting the mode of the file may precede this nine-bit pattern. For example, if the file is a directory, it is denoted as “d”; and if it is a link, it is denoted as “l.”

NAS File Sharing: Authentication and Authorization

- In a file-sharing environment, NAS devices use standard file-sharing protocols, NFS and CIFS.
- Therefore, authentication and authorization are implemented and supported on NAS devices in the same way as in a UNIX or Windows file sharing environment.
- Authentication requires verifying the identity of a network user and therefore involves a login credential lookup on a Network Information System (NIS) server in a UNIX environment.Similarly, a Windows client is authenticated by a Windows domain controller that houses the Active Directory.
- The Active Directory uses LDAP to access information about network objects in the directory and Kerberos for network security. NAS devices use the same authentication techniques to validate network user credentials.
- Fig 5.7 depicts the authentication process in a NAS environment.
- Authorization defines user privileges in a network. The authorization techniques for UNIX users and Windows users are quite different. UNIX files use mode bits to define access rights granted to owners, groups, and other users, whereas Windows uses an ACL to allow or deny specific rights to a particular user for a particular file.

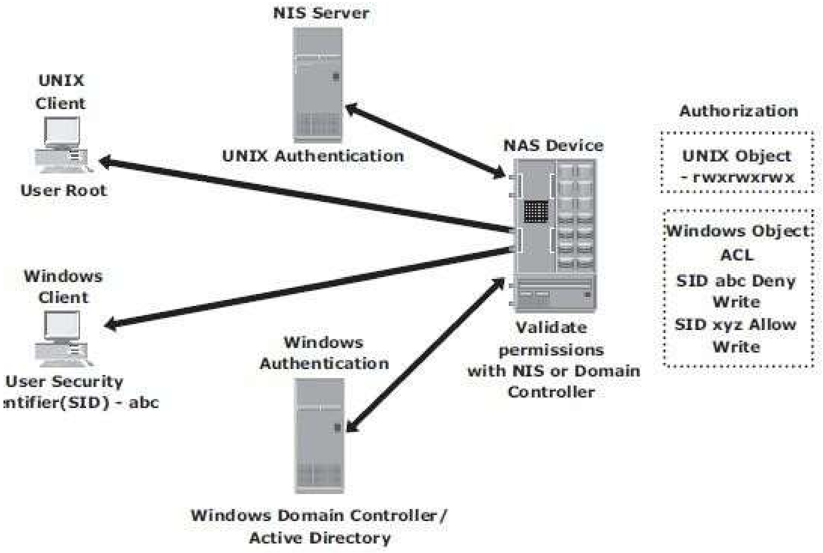

NIS Server
UNIX Client
User Root
UNIX Authentication
NAS Device
Authorization
UNIX Object - rwxrwxrwx
Windows Object ACL SID abc Deny Write SID xyz Allow Write
Windows Client
User Security ntifier(SID) - abc
Windows Authentication
Validate permissions with NIS or Domain Controller
Windows Domain Controller / Active Directory

Fig 5.7 Securing user access in a NAS environment

Kerberos

- Kerberos is a network authentication protocol, which is designed to provide strong authentication for client/server applications by using secret-key cryptography.
- It uses cryptography so that a client and server can prove their identity to each other across an insecure network connection.
- In Kerberos, authentications occur between clients and servers.
- The client gets a ticket for a service and the server decrypts this ticket by using its secret key.
- Any entity, user, or host that gets a service ticket for a Kerberos service is called a **Kerberos client.**
- The term **Kerberos server** generally refers to the Key Distribution Center (KDC).
- The KDC implements the Authentication Service (AS) and the Ticket Granting Service (TGS).
- The KDC has a copy of every password associated with every principal, so it is absolutely vital that the KDC remain secure.
- In Kerberos, users and servers for which a secret key is stored in the KDC database are known as *principals*.
- In a NAS environment, Kerberos is primarily used when authenticating against a Microsoft Active Directory domain, although it can be used to execute security functions in UNIX environments.

The Kerberos authentication process shown in Fig 5.8 includes the following steps:

1. The user logs on to the workstation in the Active Directory domain (or forest) using an ID and a password. The client computer sends a request to the AS running on the KDC for a Kerberos ticket. The KDC verifies the user’s login information from Active Directory.

2. The KDC responds with an encrypted Ticket Granting Ticket (TGT) and an encrypted session key. TGT has a limited validity period. TGT can be decrypted only by the KDC, and the client can decrypt only the session key.

3. When the client requests a service from a server, it sends a request, consisting of the previously generated TGT, encrypted with the sessionkey and the resource information to the

KDC.

4. The KDC checks the permissions in Active Directory and ensures that the user is authorized to use that service.

5. The KDC returns a service ticket to the client. This service ticket contains fields addressed to the client and to the server hosting the service.

6. The client then sends the service ticket to the server that houses the required resources.

7. The server, in this case the NAS device, decrypts the server portion of the ticket and stores the information in a key tab file. As long as the client's Kerberos ticket is valid, this authorization process does not need to be repeated. The server automatically allows the client to access the appropriate resources.

8. A client-server session is now established. The server returns a session ID to the client, which tracks the client activity, such as file locking, as long as the session is active.

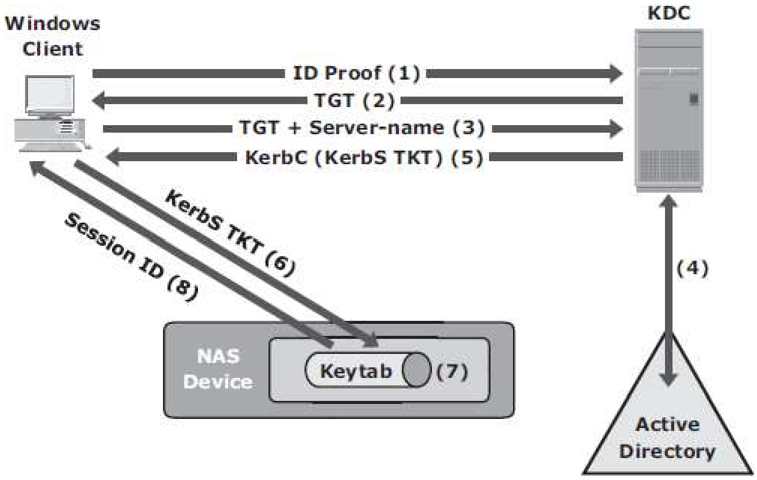


Fig 5.8 Kerberos authorization

Network-Layer Firewalls

- ➢ Because NAS devices utilize the IP protocol stack, they are vulnerable to various attacks initiated through the public IP network.
- ➢ Network layer firewalls are implemented in NAS environments to protect the NAS

devices from these security threats. These network-layer firewalls can examine network packets and compare them to a set of confi ed security rules. Packets that are not authorized by a security rule are dropped and not allowed to continue to the destination.

- Rules can be established based on a source address (network or host), a destination address (network or host), a port, or a combination of those factors (source IP, destination IP, and port number). The effectiveness of a firewall depends on how robust and extensive the security rules are.
- Fig 5.9 depicts a typical firewall implementation.

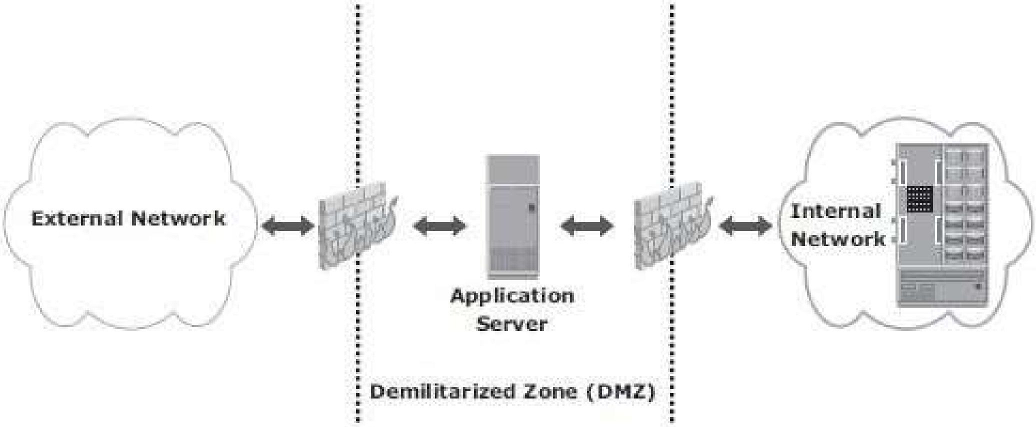


Fig 5.9: Securing a NAS environment with a network-layer firewall

- A demilitarized zone (DMZ) is commonly used in networking environments. A DMZ provides a means to secure internal assets while allowing Internet-based access to various resources. In a DMZ environment, servers that need to be accessed through the Internet are placed between two sets of firewalls.
- Application-specific ports, such as HTTP or FTP, are allowed through the firewall to the DMZ servers. No Internet-based traffic is allowed to penetrate the second set of firewalls and gain access to the internal network. The servers in the DMZ may or may not be allowed to communicate with internal resources.
- In such a setup, the server in the DMZ is an Internet-facing web application accessing data stored on a NAS device, which may be located on the internal private network. A secure design would serve only data to internal and external applications through the DMZ.

5.4.3 IP SAN

- The *Challenge-Handshake Authentication Protocol* (CHAP) is a basic authentication mechanism that has been widely adopted by network devices an hosts.
- CHAP provides a method for initiators and targets to authenticate each other by utilizing a secret code or password. CHAP secrets are usually random secrets of 12 to 128 characters.
- The secret is never exchanged directly over the communication channel; rather, a one-way hash function converts it into a hash value, which is then exchanged. A hash function, using the MD5 algorithm, transforms data in such a way that the result is unique and cannot be changed back to its original form. Fig 5.10 depicts the CHAP authentication process.

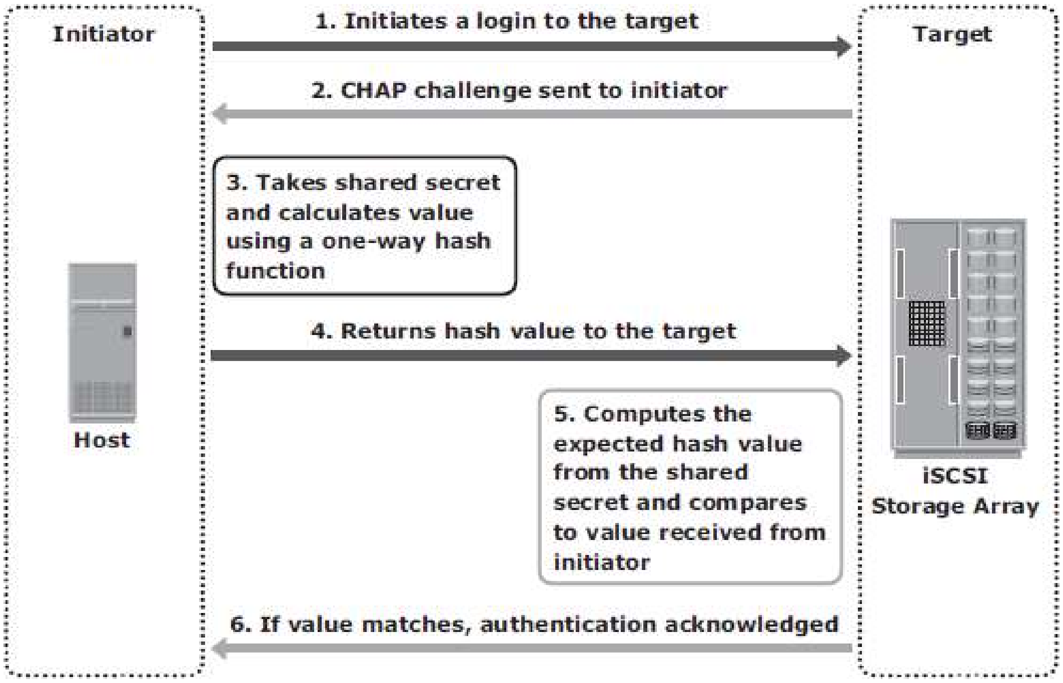

Initiator
1. Initiates a login to the target
Target
2. CHAP challenge sent to initiator
3. Takes shared secret and calculates value using a one-way hash function
4. Returns hash value to the target
Host
5. Computes the expected hash value from the shared secret and compares to value received from initiator
iSCSI Storage Array
6. If value matches, authentication acknowledged

Fig 5.10 : Securing IPSAN with CHAP authentication

- If the initiator requires reverse CHAP authentication, the initiator authenticates the target by using the same procedure.
- The CHAP secret must be configured on the initiator and the target. A CHAP entry, composed of the name of a node and the secret associated with the node, is maintained by the target and the initiator.

- The same steps are executed in a two-way CHAP authentication scenario. After these steps are completed, the initiator authenticates the target. If both authentication steps succeed, then data access is allowed.
- CHAP is often used because it is a fairly simple protocol to implement and can be implemented across a number of disparate systems.
- *iSNS discovery domains* function in the same way as FC zones. Discovery domains provide functional groupings of devices in an IP-SAN.
- For devices to communicate with one another, they must be configured in the same discovery domain.
- State change notifications (SCNs) inform the iSNS server when devices are added to or removed from a discovery domain. Fig 5.11 depicts the discovery domains in iSNS.

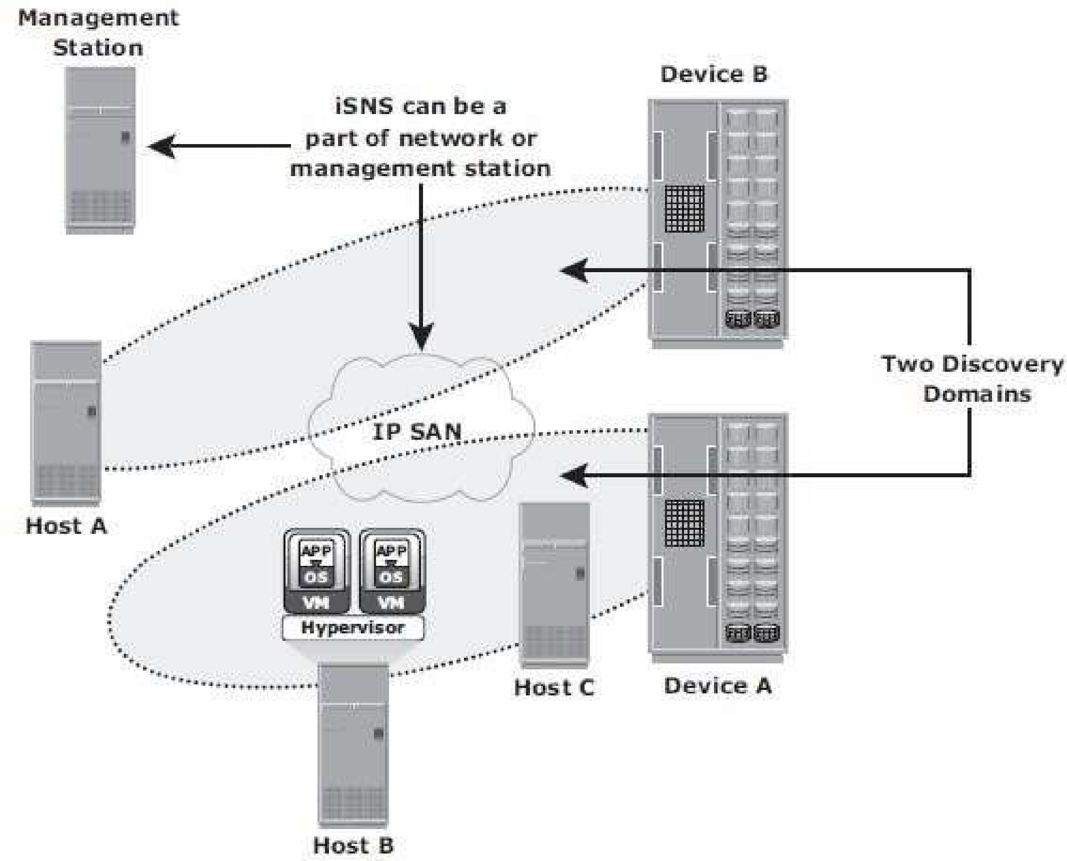


Fig 5.11 : Securing IPSAN with iSNS discovery domains

5.5 Securing Storage Infrastructure in Virtualizedand Cloud Environments

5.5.1 Security Concerns

- Organizations are rapidly adopting virtualization and cloud computing, however they have some security concerns.
- The key security concerns are multitenancy, velocity of attack, information assurance, and data privacy.
- **Multitenancy**, by virtue of virtualization, enables multiple independent tenants to be serviced using the same set of storage resources.
- **Velocity-of-attack** refers to a situation in which any existing security threat in the cloud spreads more rapidly and has a larger impact than that in the traditional data center environments.
- **Information assurance** for users ensures confidentiality, integrity, and availability of data in the cloud.
- Also the cloud user needs assurance that all the users operating on the cloud are genuine and access the data only with legitimate rights and scope.
- Data privacy is also a major concern in a virtualized and cloud environment. A CSP needs to ensure that Personally Identifiable Information (PII) about its clients is legally protected from any unauthorized disclosure.

5.5.2 Security Measures

- Security measures can be implemented at the compute, network, and storage levels.

Security at the Compute Level

- Securing a compute infrastructure includes enforcing the security of the physical server, hypervisor, VM, and guest OS (OS running within a virtual machine).
- Physical server security involves implementing user authentication and authorization mechanisms. These mechanisms identify users and provide access privileges on the server.
- To minimize the attack surface on the server, unused hardware components, such as NICs, USB ports, or drives, should be removed or disabled.
- A hypervisor is a single point of security failure for all the VMs running on it. Rootkits and malware installed on a hypervisor make detection difficult for the antivirus software installed on the guest OS. To protect against attacks, security-

critical hypervisor updates should be installed regularly.

- The hypervisor management system must also be protected.
- VM isolation and hardening are some of the common security mechanisms to effectively safeguard a VM from an attack. VM isolation helps to prevent a compromised guest OS from impacting other guest OSs. VM isolation is implemented at the hypervisor level.
- Hardening is a process to change the default configuration to achieve greater security.
- Apart from the measures to secure a hypervisor and VMs, virtualized andncloud environments also require further measures on the guest OS and application levels.

Security at the Network Level

- The key security measures that minimize vulnerabilities at the network layer are firewall, intrusion detection, demilitarized zone (DMZ), and encryption of data-in-flight.
- A firewall protects networks from unauthorized access while permitting only legitimate communications. In a virtualized and cloud environment, a firewall can also protect hypervisors and VMs.
- Intrusion Detection (ID) is the process to detect events that can compromise the confidentiality, integrity, or availability of a resource.

Security at the Storage Level

- Major threats to storage systems in virtualized and cloud environments arise due to compromises at compute, network, and physical security levels. This is because access to storage systems is through compute and network infrastructure. Therefore, adequate security measures should be in place at the compute and network levels to ensure storage security.
- Common security mechanisms that protect storage include the following:
    - Access control methods to regulate which users and processes access the data on the storage systems
    - Zoning and LUN masking
    - Encryption of data-at-rest (on the storage system) and data-in-transit. Data encryption should also include encrypting backups and storing encryption keys separately from the data.
    - Data shredding that removes the traces of the deleted data

5.6 Monitoring the Storage Infrastructure

- Monitoring is one of the most important aspects that forms the basis for managing storage infrastructure resources. Monitoring provides the performance and accessibility status of various components. Monitoring also helps to analyze the utilization and consumption of various storage infrastructure resources.

5.6.1 Monitoring Parameters

- Storage infrastructure components should be monitored for accessibility, capacity, performance, and security.
- **Accessibility** refers to the availability of a component to perform its desired operation during a specified time period.
- **Capacity** refers to the amount of storage infrastructure resources available.
- **Performance** monitoring evaluates how efficiently different storage infrastructure components are performing and helps to identify bottlenecks.
- **Security** monitoring helps to track unauthorized configuration changes to storage infrastructure resources.

5.6.2 Components Monitored

- The components within the storage environment that should be monitored are:
  - Hosts,
  - networks, and
  - storage
- The components are monitored for below parameters:
  - accessibility,
  - capacity,
  - performance, and
  - security.
- These components can be physical or virtualized.

Hosts:

- **The accessibility** of a host depends on the availability status of the hardware components and the software processes running on it.
- For example, a host’s NIC (hardware) failure might cause inaccessibility of the host to its user.

- Server clustering is a mechanism that provides high availability if a server failure occurs.
- ***Capacity monitoring of the file system utilization*** is important to ensure that sufficient capacity is available to the applications, otherwise this disrupts application availability.
- Administrator can extend (manually or automatically) the file system's space proactively to prevent application outage.
- Use of virtual provisioning technology enables efficient management of storage capacity requirements but is highly dependent on capacity monitoring.
- ***Performance monitoring of the host*** mainly involves a status check on the utilization of various server resources, such as *CPU* and *memory*.
- High utilization leads to *degraded performance and slower response time*.
- Actions taken by administrators to correct the problem are, *upgrading or adding more processors and shifting the workload to different servers*.
- In a virtualized environment, *additional CPU and memory* may be allocated to VMs dynamically from the pool, if available, to meet performance requirements.
- ***Security monitoring*** on servers involves tracking of login failures and execution of unauthorized applications or software processes.
- Proactive measures against unauthorized access to the servers are based on the threat identified.
- For example, an administrator can block user access if multiple login failures are logged.

Storage Network

- **Storage networks** need to be monitored to ensure uninterrupted communication between the server and the storage array.
- **Accessibility:** Uninterrupted access to data depends on the accessibility of both the physical and logical components.
- The physical components include **switches, ports, and cables**.
- The logical components include constructs, such as **zones**.
- Any failure in the physical or logical components causes **data unavailability**.
- **Capacity monitoring** in a storage network involves monitoring the number of available ports in the fabric, the utilization of the interswitch links, or individual ports,

and each interconnect device in the fabric.

- **Performance monitoring** of the storage network enables assessing individual component performance and helps to identify network bottlenecks.
- For IP networks, monitoring the performance includes monitoring network latency, packet loss, bandwidth utilization for I/O, network errors, packet retransmission rates, and collisions.
- **Security monitoring** of storage network provides information about any unauthorized change to the configuration of the fabric.
- Login failures and unauthorized access to switches for performing administrative changes should be logged and monitored continuously.

Storage

- **The accessibility** of the storage array should be monitored for its hardware components and various processes.
- Storage arrays are configured with redundant hardware components, and therefore individual component failure does not affect their accessibility.
- Failure of any process in the storage array might disrupt or compromise business operations. Example: failure of a replication task affects disaster recovery capabilities.
- Some storage arrays provide the capability to send messages to the vendor’s support center if hardware or process failures occur, referred to as a call home.
- **Capacity monitoring** of a storage array enables the administrator to respond to storage needs preemptively based on capacity utilization and consumption trends.
- Information about unconfigured and unallocated storage space enables the administrator to decide whether a new server can be allocated storage capacity from the storage array.
- **Performance monitoring** of a storage array involves using a number of performance metrics, such as utilization rates of the various storage array components, I/O response time, and cache utilization.
- A storage array is usually a shared resource, which may be exposed to security threats. **Monitoring security** helps to track unauthorized configuration of the storage array and ensures that only authorized users are allowed to access it.

5.6.3 Monitoring Examples

Accessibility Monitoring

- Failure of any component might affect the accessibility of one or more components due to their interconnections and dependencies.
- Consider an implementation in a storage infrastructure with three servers: H1, H2, and H3. All the servers are configured with two HBAs, each connected to the production storage array through two switches, SW1 and SW2, as shown in Fig 5.12.
- All the servers share two storage ports on the storage array and multipathing software is installed on all the servers.
- If one of the switches (SW1) fails, the multipathing software initiates a path failover, and all the servers continue to access data through the other switch, SW2.
- Due to the absence of a redundant switch, a second switch failure could result in inaccessibility of the array.
- Monitoring for accessibility enables detecting the switch failure and helps an administrator to take corrective action before another failure occurs.
- In most cases, the administrator receives symptom alerts for a failing component and can initiate actions before the component fails.

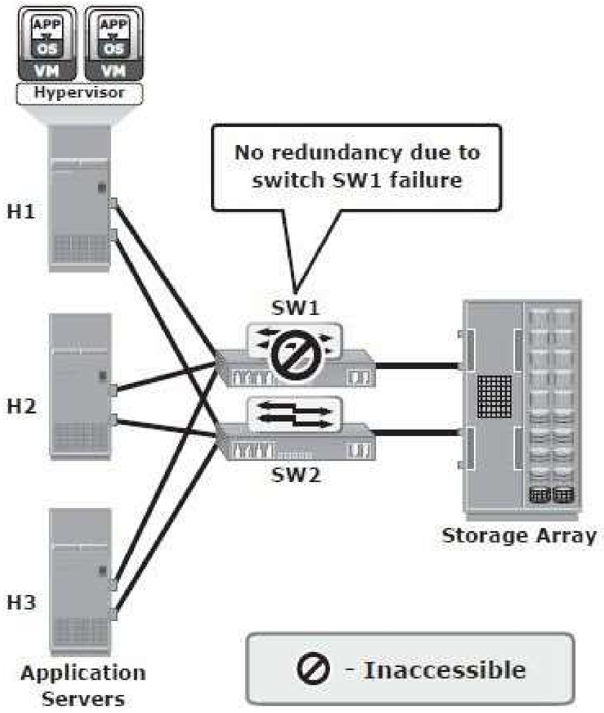


Fig 5.12: Switch failure in a storage infrastructure

Capacity Monitoring

- In the scenario shown in Fig 5.13, servers H1, H2, and H3 are connected to the production array through two switches, SW1 and SW2. Each of the servers is allocated storage on the storage array.
- When a new server is deployed in this configuration, the applications on the new server need to be given storage capacity from the production storage array.
- Monitoring the available capacity on the array helps to decide whether the array can provide the required storage to the new server.
- Also, monitoring the available number of ports on SW1 and SW2 helps to decide whether the new server can be connected to the switches.

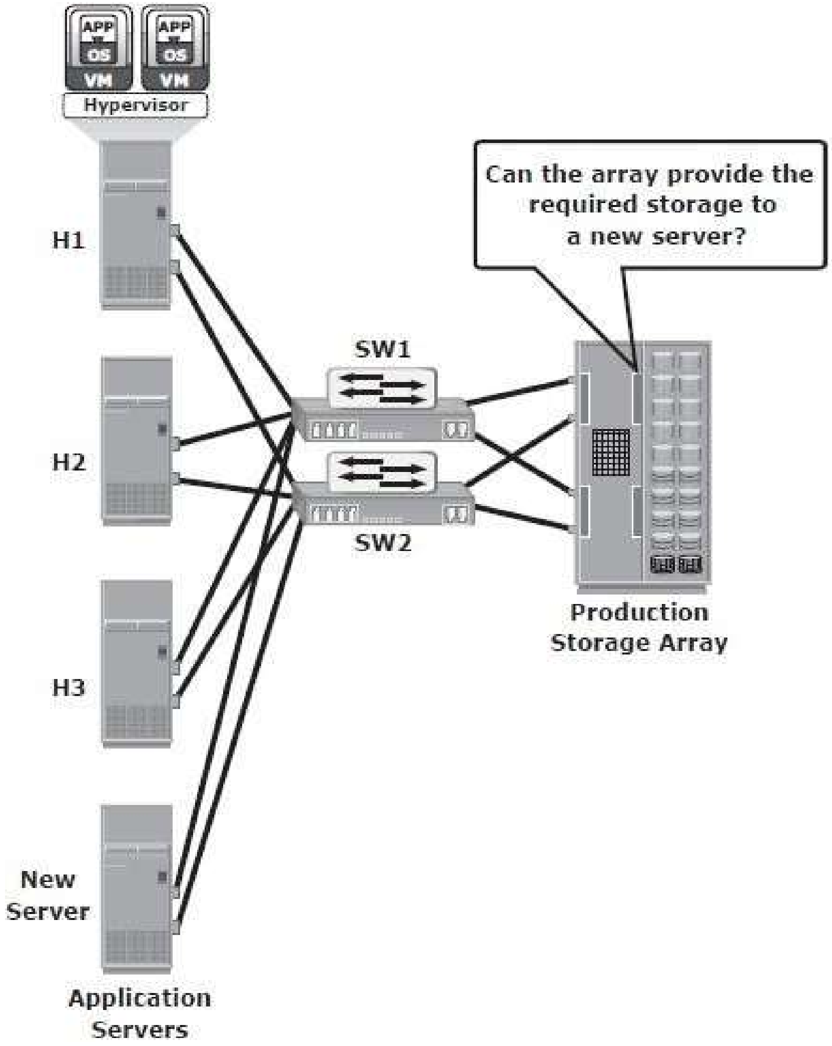


Fig 5.13: Monitoring storage array capacity

- The following example illustrates the importance of monitoring the file system capacity on file servers. Fig 5.14 (a) illustrates the environment of a file system when full and that results in application outage when no capacity monitoring is implemented.
- Monitoring can be configured to issue a message when thresholds are reached on the file system capacity. For example, when the file system reaches 66 percent of its capacity, a warning message is issued, and a critical message is issued when the file system reaches 80 percent of its capacity (Fig 5.14 [b]). This enables the administrator to take action to extend the file system before it runs out of capacity. Proactively monitoring the file system can prevent application outages caused due to lack of file system space.

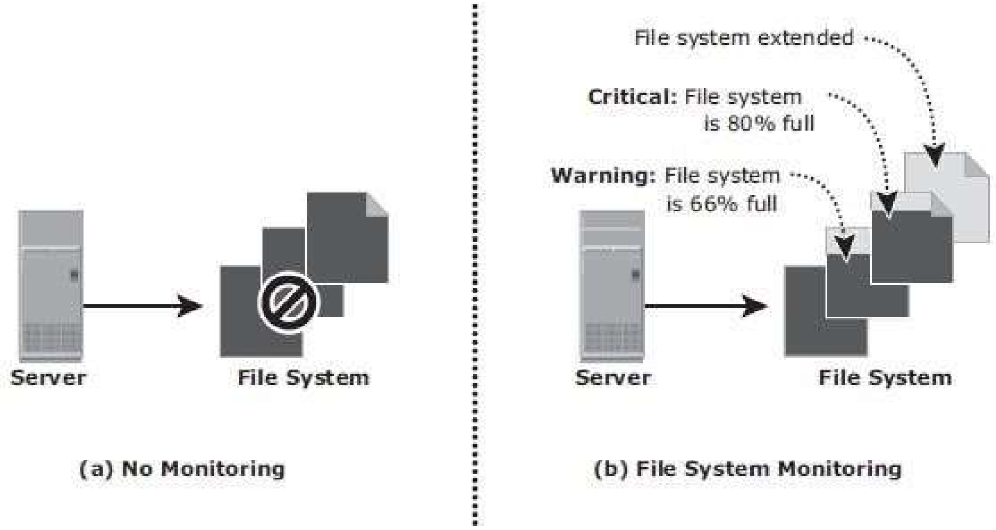

File system extended
Critical: File system is 80% full
Warning: File system is 66% full
Server
File System
Server
File System
(a) No Monitoring
(b) File System Monitoring

Fig 5.14: Monitoring server file system space

Performance Monitoring

- The example shown in Fig 5.15 illustrates the importance of monitoring performance on storage arrays.
- In this example, servers H1, H2, and H3 (with two HBAs each) are connected to the storage array through switch SW1 and SW2. The three servers share the same storage ports on the storage array to access LUNs.
- A new server running an application with a high work load must be deployed to share the same storage port as H1, H2, and H3.
- Monitoring array port utilization ensures that the new server does not adversely affect

the performance of the other servers.

- In this example, utilization of the shared storage port is shown by the solid and dotted lines in the graph.
- If the port utilization prior to deploying the new server is close to 100 percent, then deploying the new server is not recommended because it might impact the performance of the other servers. However, if the utilization of the port prior to deploying the new server is closer to the dotted line, then there is room to add a new server.

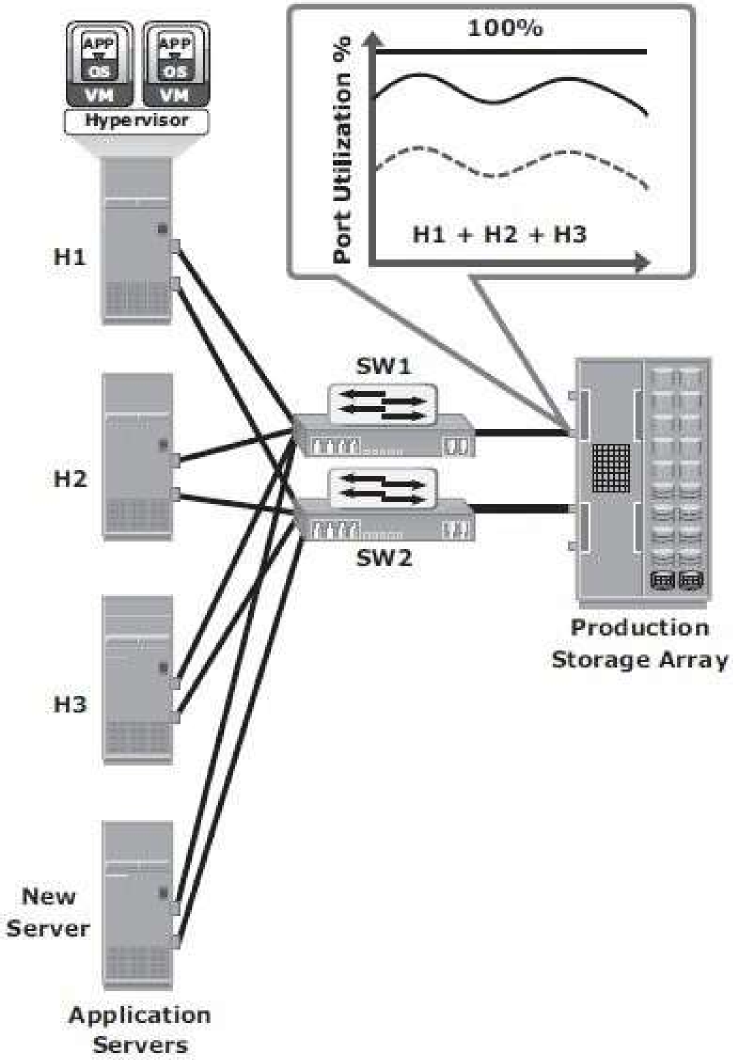


Fig 5.15: Monitoring array port utilization

Security Monitoring

- The example shown in Fig 5.16 illustrates the importance of monitoring security in a storage array.
- In this example, the storage array is shared between two workgroups, WG1 and WG2. The data of WG1 should not be accessible to WG2 and vice versa. A user from WG1 might try to make a local replica of the data that belongs to WG2.
- If this action is not monitored or recorded, it is difficult to track such a violation of information security. If this action is monitored, a warning message can be sent to prompt a corrective action or at least enable discovery as part of regular auditing operations.
- An example of host security monitoring is tracking of login attempts at the host. The login is authorized if the login ID and password entered are correct; or the login attempt fails. These login failures might be accidental (mistyping) or a deliberate attempt to access a server. Many servers usually allow a fixed number of successive login failures, prohibiting any additional attempts after these login failures.
- In a monitored environment, the login information is recorded in a system log file, and three successive login failures trigger a message, warning of a possible security threat.

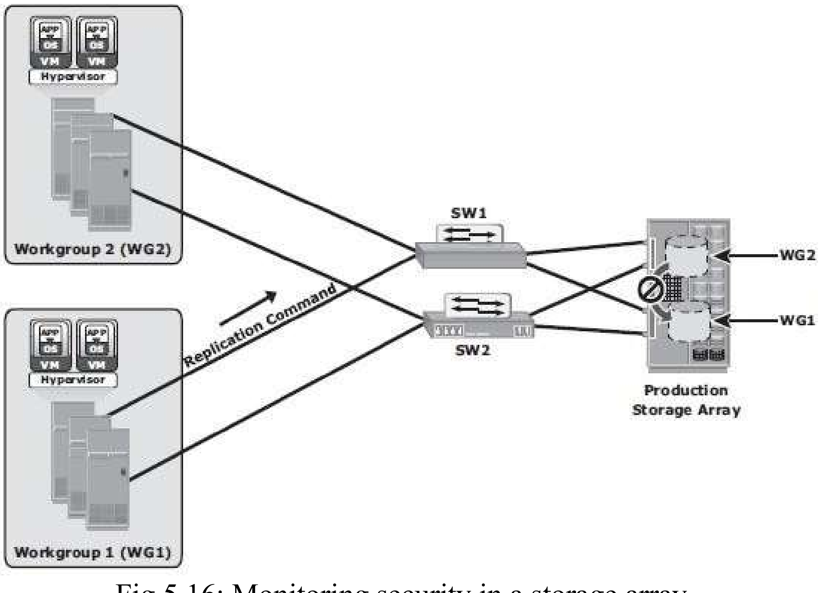


Fig 5.16: Monitoring security in a storage array

5.6.4 Alerts

- Alerting of events is an integral part of monitoring. Alerting keeps administrators informed about the status of various components and processes — for example, conditions such as failure of power, disks, memory, or switches, which can impact the availability of services and require immediate administrative attention. Other conditions, such as a file system reaching a capacity threshold are considered warning signs and may also require administrative attention.
- Monitoring tools enable administrators to assign different severity levels based on the impact of the alerted condition.
- Whenever a condition with a particular severity level occurs, an alert is sent to the administrator, a script is triggered, or an incident ticket is opened to initiate a corrective action.
- Alert classifications can range from information alerts to fatal alerts.
- **Information alerts** provide useful information but do not require any intervention by the administrator.
- **Warning alerts** require administrative attention so that the alerted condition is contained and does not affect accessibility.
- **Fatal alerts** require immediate attention because the condition might affect overall performance, security, or availability.
- Continuous monitoring, with automated alerting, enables administrators to respond to failures quickly and proactively. Alerting provides information that helps administrators prioritize their response to events.

5.7 Storage Infrastructure Management Activities

- The key storage infrastructure management activities performed in a data center can be broadly categorized into:
  - availability management,
  - capacity management,
  - performance management,
  - security management, and
  - reporting.

5.7.1 Availability Management

- Availability management requires establishing a proper guideline based on defined **service levels** to ensure availability.
- *Availability management* involves all availability-related issues for components or services to ensure that service levels are met.
- In availability management, the key activity is to provision **redundancy** at all levels, including components, data, or even sites.
- Eg: When a server is deployed to support critical business function, it requires high availability by deploying two or more HBAs, multipathing software, and server clustering.
- The server must be connected to the storage array using at least two independent fabrics and switches that have built-in redundancy.
- In addition, the storage arrays should have built-in redundancy for various components and should support local and remote replication.

5.7.2 Capacity Management

- The goal of **capacity management** is to ensure adequate *availability* of resources based on their service level requirements.
- Capacity management also involves *optimization* of capacity based on the cost and future needs.
- Capacity management provides *capacity analysis* that compares allocated storage to forecasted storage on a regular basis.
- It also provides *trend analysis* based on the rate of consumption, which must be rationalized against storage acquisition and deployment timetables.
- **Storage provisioning** is an example of capacity management which involves activities, such as creating RAID sets and LUNs, and allocating them to the host.
- **Enforcing capacity quotas** for users is another example of capacity management. Provisioning a fixed amount of user quotas restricts users from exceeding the allocated capacity.
- *Data deduplication and compression*, have reduced the amount of data to be backed up and thereby reduced the amount of storage capacity to be managed.

5.7.3 Performance Management

- **Performance management** ensures the optimal operational efficiency of all components.
- Performance analysis helps to identify the performance of storage infrastructure components and provides information on whether a component meets expected performance levels.
- Several performance management activities need to be performed when deploying a new application or server in the existing storage infrastructure.
- For example, to optimize the expected performance levels, *fine-tuning* is required for activities on the server, such as the volume configuration, database design or application layout, configuration of multiple HBAs, and intelligent multipathing software.
- The performance management tasks on a SAN include designing and implementing *sufficient ISLs* in a multiswitch fabric with adequate bandwidth to support the required performance levels.
- The storage array configuration tasks include selecting the appropriate RAID type, LUN layout, front-end ports, back-end ports, and cache configuration, when considering the end-to-end performance.

5.7.4 Security Management

- The key objective of the *security management* activity is to ensure **confidentiality**, **integrity**, and **availability** of information in both virtualized and nonvirtualized environments.
- Security management *prevents unauthorized* access and configuration of storage infrastructure components.
- For example, while deploying an application or a server, the security management tasks include *managing the user accounts and access policies* that authorize users to perform role-based activities.
- The security management tasks in a SAN environment include configuration of zoning to restrict an unauthorized HBA from accessing specific storage array ports.
- The security management task on a storage array includes LUN masking that restricts a host’s access to intended LUNs only.

5.7.5 Reporting

- **Reporting** on a storage infrastructure involves keeping track and gathering information from various components and processes.
- This information is compiled to generate reports for **trend analysis, capacity planning, chargeback,** and **performance**.
- *Capacity planning reports* contain current and historic information about the utilization of storage, file systems, database tablespace, ports, and so on.
- *Configuration and asset management reports* include details about device allocation, local or remote replicas, and fabric configuration. It also lists all the equipment, with details of their purchase date, lease status, and maintenance records.
- *Chargeback reports* contain information about the allocation or utilization of storage infrastructure components by various departments or user groups.
- *Performance reports* provide details about the performance of various storage infrastructure components.

5.7.6 Storage Infrastructure Management in a Virtualized Environment

- Storage virtualization has enabled dynamic migration of data and extension of storage volumes. Due to dynamic extension, storage volumes can be expanded nondisruptively to meet both capacity and performance requirements.
- Since virtualization breaks the bond between the storage volumes presented to the host and its physical storage, data can be migrated both within and across data centers without any downtime. This has made the administrator’s tasks *easier* while reconfiguring the physical environment.
- ***Virtual storage provisioning*** is another tool that has changed the infrastructure management cost and complexity scenario.
- In conventional provisioning, storage capacity is provisioned upfront in anticipation of future growth. This results in overutilization or underutilization issues.
- Use of virtual provisioning can address this challenge and make capacity management less challenging. In virtual provisioning, storage is allocated from the shared pool to hosts on-demand. This improves the storage capacity utilization, and thereby reduces capacity management complexities.
- Virtualization has also contributed to network management efficiency. VSANs and VLANs made the administrator’s job easier by isolating different networks logically

using management tools rather than physically separating them.

- Disparate virtual networks can be created on a single physical network, and reconfiguration of nodes can be done quickly without any physical changes.
- It has also addressed some of the security issues that might exist in a conventional environment.
- On the host side, compute virtualization has made host deployment, reconfiguration, and migration easier than physical environment.
- Compute, application, and memory virtualization have not only improved provisioning, but also contributed to the high availability of resources.

STORAGE MULTITENANCY

- Multiple tenants sharing the same resources provided by a single landlord (resource provider) is called **multitenancy**.
- Two common examples of multitenancy are:
  - multiple virtual machines sharing the same server hardware through the use of a hypervisor running on the server,
  - multiple user applications using the same storage platform.
- **Security** and **service level assurance** are a key concerns in any multitenant storage environment.
- *Secure multitenancy* means that no tenant can access another tenant's data.
- Below are the four pillars of multitenancy:
  - **Secure separation:** This enables data path separation across various tenants in a multitenant environment. This pillar can be divided into four basic requirements: separation of data at rest, address space separation, authentication and name service separation, and separation of data access.
  - **Service assurance:** Consistent and reliable service levels are integral to storage multitenancy. Service assurance plays an important role in providing service levels that can be unique to each tenant.
  - **Availability:** High availability ensures a resilient architecture that provides fault tolerance and redundancy. This is even more critical when storage infrastructure is shared by multiple tenants, because the impact of any outage is magnified.

- **Management:** This includes provisions that allow a landlord to manage basic infrastructure while delegating management responsibilities to tenants for the resources that they interact with day to day. This concept is known as balancing the provider (landlord) in-control with the tenant in-control capabilities.

5.7.7 Storage Management Examples

Example 1: Storage Allocation to a New Server/Host

- Consider the deployment of a new RDBMS server to the existing **nonvirtualized storage infrastructure environment**.
- Below are the storage management activities, performed by the administrator:
  1. Install and configure the HBAs and device drivers on the server before it is physically connected to the SAN. Multipathing software can also be installed on the server.
  2. Connect storage array ports to the SAN and perform zoning on the SAN switches to allow the new server access to the storage array ports via its HBAs.
  3. Ensure redundant paths between the server and the storage array by connecting the HBAs of the new server to different switches and zoning with different array ports.
  4. Configure LUNs on the array and assign these LUNs to the storage array front-end ports. LUN masking configuration is performed on the storage array, which restricts access to LUNs by a specific server.
  5. The server then discovers the LUNs assigned to it by either a bus rescan process or sometimes through a server reboot, depending upon the operating system installed.
  6. A volume manager may be used to configure the logical volumes and file systems on the host. The number of logical volumes or file systems to be created depends on how a database or an application is expected to use the storage.
  7. Install database or an application on the logical volumes or file systems that were created.
  8. The last step is to make the database or application capable of using the new file system space.

- Fig 5.17 illustrates the activities performed on a server, a SAN, and a storage array for the allocation of storage to a new server.

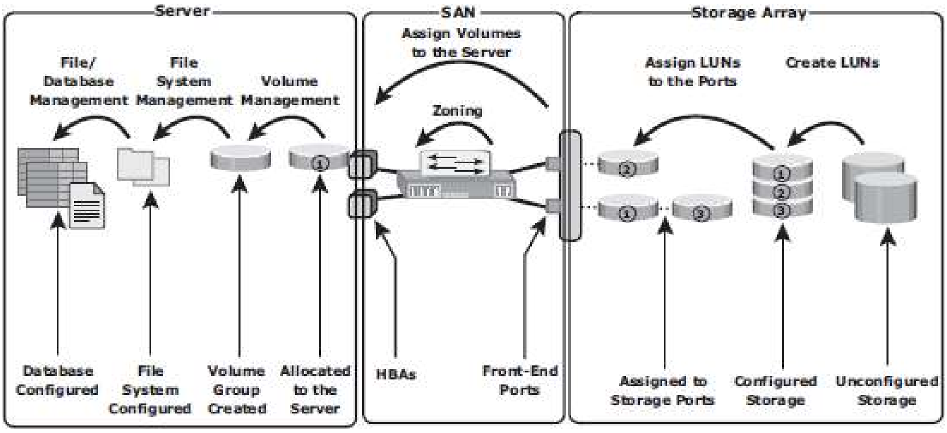


Fig 5.17: Storage allocation tasks

- Below are the various administrative tasks performed in a **virtualized environment** to provision storage to a VM that runs an RDBMS.

1. Similar to nonvirtualized environment, a physical connection must be established between the physical server, which hosts the VMs, and the storage array through the SAN.
2. At the SAN level, a VSAN can be configured to transfer data between the physical server and the storage array. This isolates storage traffic from any other traffic in the SAN. Zoning can be configured within the VSAN.
3. At the storage side, administrators need to create thin LUNs from the shared storage pool and assign these thin LUNs to the storage array front-end ports. LUN masking needs to be carried out on the storage array.
4. At the physical server side, the hypervisor discovers the assigned LUNs. The hypervisor creates a logical volume and file system to store and manage VM files.
5. Administrator creates a VM and installs the OS and RDBMS on the VM. During this, the hypervisor creates a virtual disk file and other VM files in the hypervisor file system. The virtual disk file appears to the VM as a SCSI disk and is used to store the RDBMS data. Alternatively, the hypervisor enables virtual provisioning to create a thin virtual disk and assigns it to the VM.
6. Hypervisors usually have native multipathing capabilities. Optionally, a third-party multipathing software may be installed on the hypervisor.

Example 2: File System Space Management

- To prevent a file system from running out of space, administrators need to perform tasks to offload data from the existing file system.
- This includes deleting unwanted files or archiving data that is not accessed for a long time.
- Alternatively, an administrator can *extend the file system* to increase its size and avoid an application outage.
- The dynamic extension of file systems or a logical volume depends on the operating system or the logical volume manager (LVM) in use.
- Fig 5.18 shows the steps and considerations for the extension of file systems in the flow chart.

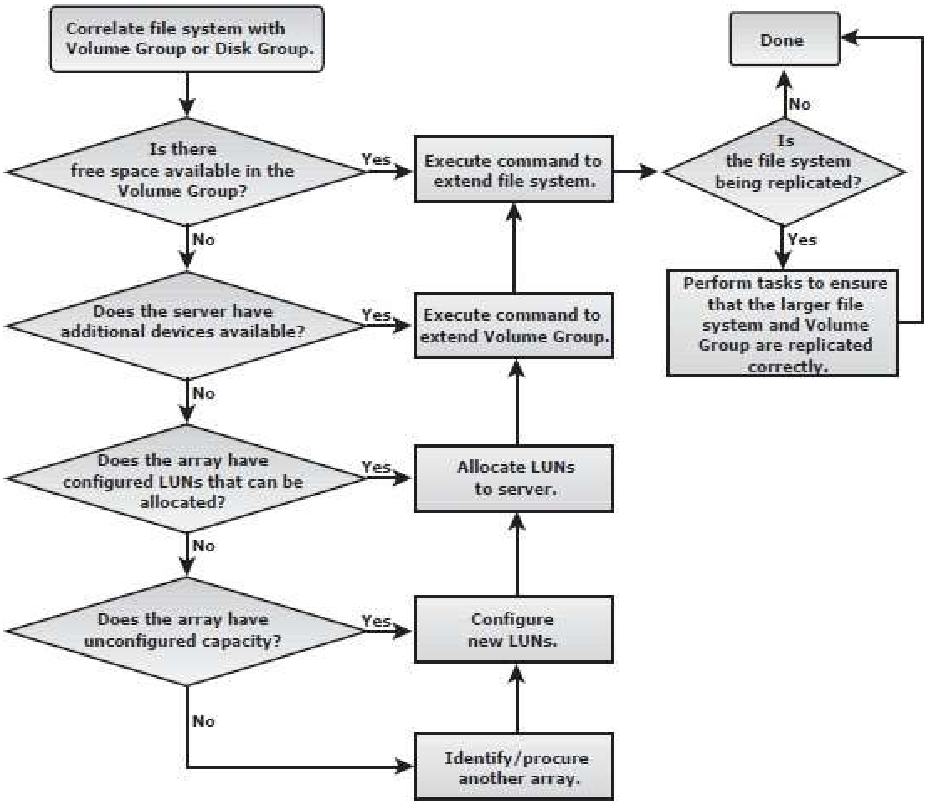

Correlate file system with Volume Group or Disk Group.
Is there free space available in the Volume Group?
Yes
No
Execute command to extend file system.
Is the file system being replicated?
No
Yes
Done
Perform tasks to ensure that the larger file system and Volume Group are replicated correctly.
Does the server have additional devices available?
Yes
No
Execute command to extend Volume Group.
Does the array have configured LUNs that can be allocated?
Yes
No
Allocate LUNs to server.
Does the array have unconfigured capacity?
Yes
No
Configure new LUNs.
Identify/procure another array.

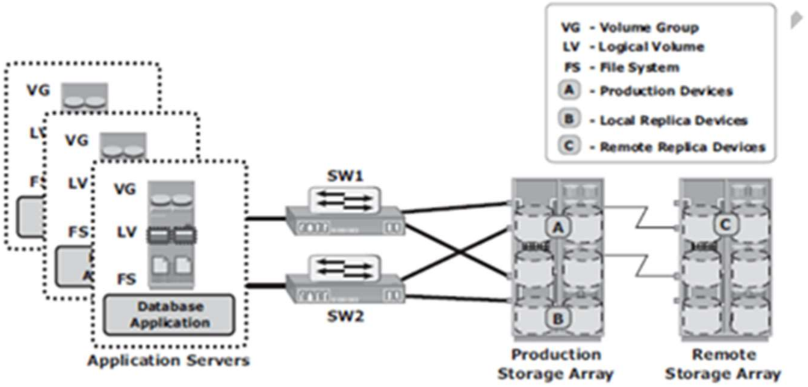
Fig 5.18: Extending a file system

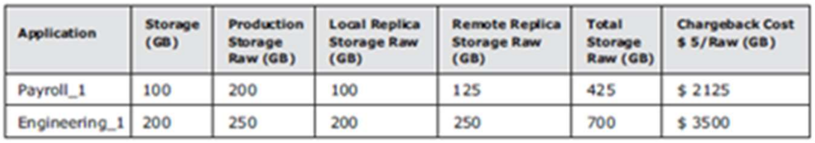
Example 3: Chargeback Report

- This example explores the storage infrastructure management tasks necessary to create a **chargeback report**.
- Fig 5.19 shows a configuration deployed in a storage infrastructure. Three servers with two HBAs each connect to a storage array via two switches, SW1 and SW2.
- Array replication technology is used to create local and remote replicas. The production device is represented as A, the local replica device as B, and the remote replica device as C.
- Individual departmental applications run on each of the servers.
- A report documenting the exact amount of storage resources used by each application is created using a *chargeback analysis* for each department.
- If the unit for billing is based on the amount of *raw storage* (usable capacity plus protection provided) configured for an application used by a department, the exact amount of raw space configured must be reported for each application.
- Fig 5.19 shows a sample report for two applications, *Payroll_1* and *Engineering_1*.
- The first step to determine chargeback costs is to correlate the application with the exact amount of raw storage configured for that application.
- Fig 5.20 shows the storage space used for Payroll_1 application identified based on file systems to logical volumes to volume groups and to the LUNs on the array.
- When the applications are replicated, the storage space used for local replication and remote replication is also identified.
- In the example shown, Payroll_1 is using *Source Vol 1* and *Vol 2* (in the production array). The replication volumes are *Local Replica Vol 1* and *Vol 2* (in the production array) and *Remote Replica Vol 1* and *Vol 2* (in the remote array).
- Based on this example, consider that Source Vol 1 and Vol 2 are each 50 GB in size, the storage allocated to the application is 100 GB (50 + 50). The **allocated storage** for replication is 100 GB for local replication and 100 GB for remote replication.
- The **raw storage** configured for the application is determined from the allocated storage based on the RAID protection that is used.
- If the Payroll_1 application's production volumes are RAID 1-protected, the raw space used is 200 GB.
- Assume the local replicas are on unprotected volumes, and the remote replicas are protected with a RAID 5 configuration, then 100 GB of raw space is used by the local

replica and 125 GB by the remote replica.

- ➢ Therefore, the total raw capacity used by the Payroll_1 application is 425 GB. The total cost of storage provisioned for Payroll_1 application will be $2,125 (assume cost per GB of storage is $5).
- ➢ This exercise must be repeated for each application in the enterprise (eg: Engineering_1, etc) to generate the chargeback report.
- ➢ Chargeback reports can be extended to include a pre-established cost ofother





Application	Storage (GB)	Production Storage Raw (GB)	Local Replica Storage Raw (GB)	Remote Replica Storage Raw (GB)	Total Storage Raw (GB)	Chargeback Cost $ 5/Raw (GB)
Payroll_1	100	200	100	125	425	$ 2125
Engineering_1	200	250	200	250	700	$ 3500

Fig 5.19: Configuration and Chargeback report

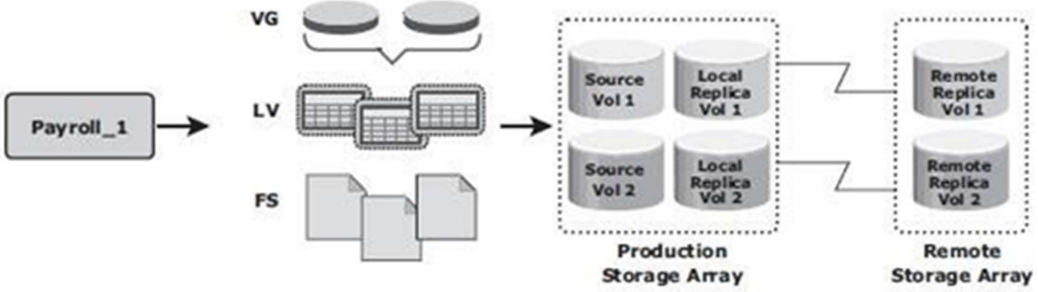


Fig 5.20: Correlation of capacity configured for an application

5.8 Storage Infrastructure Management Challenges

- The main challenge in monitoring and managing today's complex storage infrastructure is due to the heterogeneity of storage arrays, networks, servers, databases, and applications in the environment.
- Eg: heterogeneous storage arrays vary in their capacity, performance, protection, and architectures. Each of the components in a data center typically comes with vendor-specific tools for management.
- An environment with multiple tools makes understanding the overall status of the environment challenging because the tools may not be interoperable.
- Ideally, management tools should correlate information from all components in one place. Such tools provide an end-to-end view of the environment, and a quicker root cause analysis for faster resolution to alerts.

5.9 Information Lifecycle Management

- In both traditional data center and virtualized environments, managing information can be expensive if not managed appropriately.
- Along with the tools, an effective management strategy is also required to manage information efficiently.
- This strategy should address the following key challenges that exist in today's data centers:
  - **Exploding digital universe:** The rate of information growth is increasing exponentially. Creating copies of data to ensure high availability and repurposing has contributed to the multifold increase of information growth.
  - **Increasing dependency on information:** The strategic use of information plays an important role in determining the success of a business and provides competitive advantages in the marketplace.
  - **Changing value of information:** Information that is valuable today might become less important tomorrow. The value of information often changes over time.
- Framing a strategy to meet these challenges involves understanding the value of information over its life cycle.
- When information is first created, it often has the highest value and is accessed

frequently. As the information ages, it is accessed less frequently and is of less value to the organization. Understanding the value of information helps to deploy the appropriate infrastructure according to the changing value of information.

- For example, in a sales order application, the value of the information (customer data) changes from the time the order is placed until the time that the warranty becomes void (see Fig 5.21).
- The value of the information is highest when a company receives a new sales order and processes it to deliver the product. After the order fulfillment, the customer data does not need to be available for real-time access.
- The company can transfer this data to less expensive secondary storage with lower performance until a warranty claim or another event triggers its need.
- After the warranty becomes void, the company can dispose of the information.

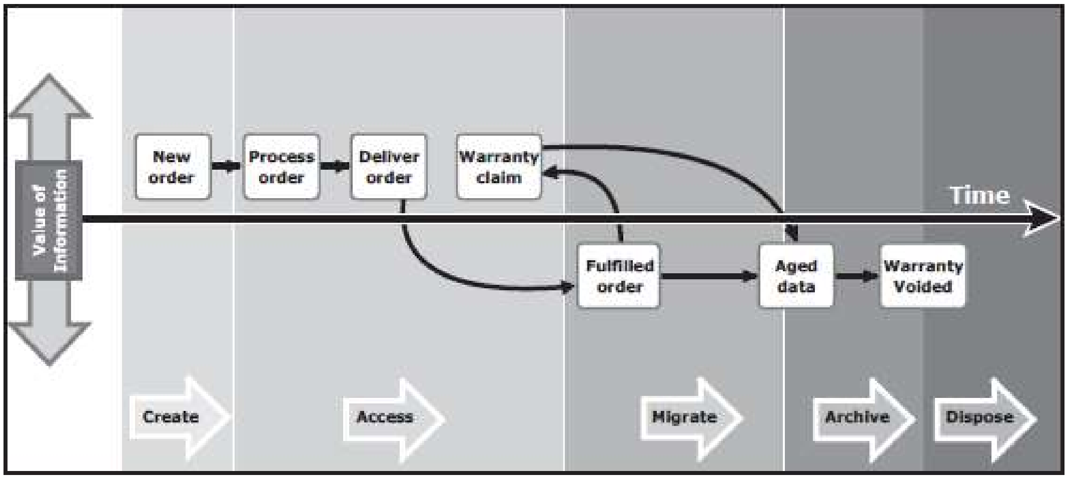


Fig 5.21 Changing value of sales order information

- **Information Lifecycle Management (ILM)** is a proactive strategy that enables an IT organization to effectively manage information throughout its life cycle based on predefined business policies.
- From data creation to data deletion, ILM aligns the business requirements and processes with service levels in an automated fashion. This allows an IT organization to optimize the storage infrastructure for maximum return on investment.
- Implementing an ILM strategy has the following key benefits that directly address the challenges of information management:
  - **Lower Total Cost of Ownership (TCO):** By aligning the infrastructure and management costs with information value. As a result, resources are not wasted,

and complexity is not introduced by managing low-value data at the expense of high-value data.

- o **Simplified management:** By integrating process steps and interfaces with individual tools and by increasing automation
- o **Maintaining compliance**: By knowing what data needs to be protected for what length of time
- o **Optimized utilization**: By deploying storage tiering

5.10 Storage Tiering

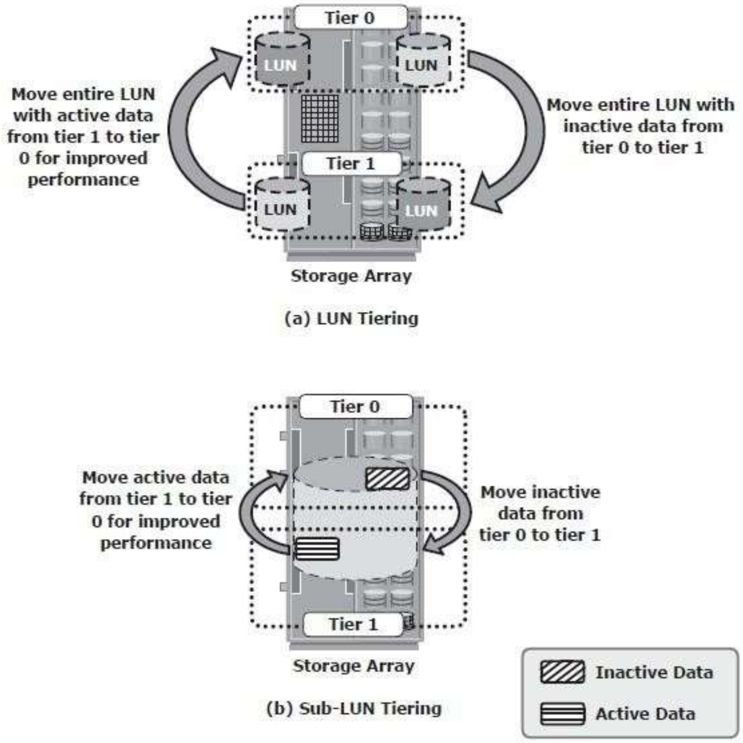
- ➢ Storage tiering is a technique of establishing a hierarchy of different storage types (tiers). This enables storing the right data to the right tier, based on service level requirements, at a minimal cost.
- ➢ Each tier has different levels of protection, performance, and cost. For example, high performance solidstate drives (SSDs) or FC drives can be configured as tier 1 storage to keep frequently accessed data, and low cost SATA drives as tier 2 storage to keep the less frequently accessed data.
- ➢ Keeping frequently used data in SSD or FC improves application performance. Moving less-frequently accessed data to SATA can free up storage capacity in high performance drives and reduce the cost of storage. This movement of data happens based on defined tiering policies.
- ➢ The tiering policy might be based on parameters, such as file type, size, frequency of access, and so on. For example, if a policy states “Move the files that are not accessed for the last 30 days to the lower tier,” then all the files matching this condition are moved to the lower tier.
- ➢ Storage tiering can be implemented as **a manual or an automated process.**
- ➢ Manual storage tiering is the traditional method where the storage administrator monitors the storage workloads periodically and moves the data between the tiers. Manual storage tiering is complex and time-consuming.
- ➢ Automated storage tiering automates the storage tiering process, in which data movement between the tiers is performed nondisruptively. In automated storage tiering, the application workload is proactively monitored; the active data is automatically moved to a higher performance tier and the inactive data to a higher

capacity, lower performance tier.

- Data movements between various tiers can happen within (**intra-array**) or between (**inter-array**) storage arrays.

5.10.1 Intra-Array Storage Tiering

- The process of storage tiering within a storage array is called intra-array storage tiering.
- It enables the efficient use of SSD, FC, and SATA drives within an array and provides performance and cost optimization.
- The goal is to keep the SSDs busy by storing the most frequently accessed data on them, while moving out the less frequently accessed data to the SATA drives.
- Data movements executed between tiers can be performed at the LUN level or at the sub-LUN level.
- The performance can be further improved by implementing tiered cache.
- **LUN tiering, sub-LUN tiering,** and **cache tiering** are explained next.
- Traditionally, storage tiering is operated at the LUN level that moves an entire LUN from one tier of storage to another (see Fig 5.22 [a]).
- This movement includes both active and inactive data in that LUN.
- This method does not give effective cost and performance benefits.
- Today, storage tiering can be implemented at the sub-LUN level (see Fig 5.22 [b]).
- In sub-LUN level tiering, a LUN is broken down into smaller segments and tiered at that level. Movement of data with much finer granularity, for example 8 MB, greatly enhances the value proposition of automated storage tiering.
- Tiering at the sub-LUN level effectively moves active data to faster drives and less active data to slower drives.


Tier 0
LUN
LUN
Move entire LUN with active data from tier 1 to tier 0 for improved performance
Move entire LUN with inactive data from tier 0 to tier 1
Tier 1
LUN
LUN
Storage Array
Tier 0
Move active data from tier 1 to tier 0 for improved performance
Move inactive data from tier 0 to tier 1
Tier 1
Storage Array
▨ Inactive Data
☰ Active Data

(a) LUN Tiering

(b) Sub-LUN Tiering

Fig 5.22: Implementation of intra-array storage tiering

15.10.2 Inter-Array Storage Tiering

- The process of storage tiering between storage arrays is called inter-array storage tiering. Inter-array storage tiering automates the identification of active or inactive data to relocate them to different performance or capacity tiers between the arrays.
- Figure 5.23 illustrates an example of a two-tiered storage environment. This environment optimizes the primary storage for performance and the secondary storage for capacity and cost.
- The policy engine, which can be software or hardware where policies are configured, facilitates moving inactive or infrequently accessed data from the primary to the secondary storage.
- Some prevalent reasons to tier data across arrays is archival or to meet compliance requirements.
- As an example, the policy engine might be configured to relocate all the files in the primary storage that have not been accessed in one month and archive those files to the secondary storage.
- For each archived file, the policy engine creates a small space-saving stub file in the primary storage that points to the data on the secondary storage.

- When a user tries to access the file at its original location on the primary storage, the user is transparently provided with the actual file from the secondary storage.

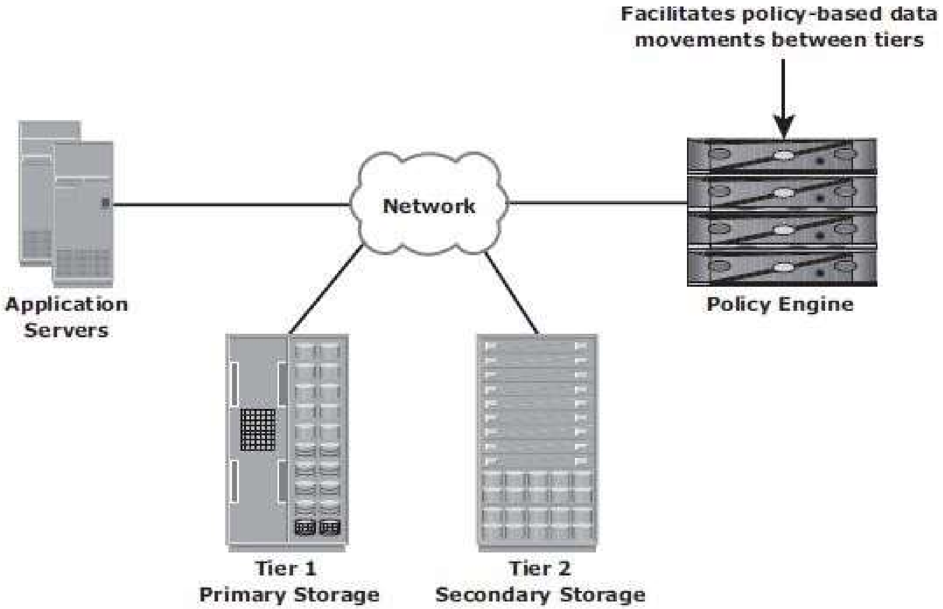


Fig 5.23: Implementation of intra-array storage tiering