## Module-5

9 a. What are the different rules tried for information security? Explain in detail FCSAN based security implementation. **(08 Marks)**

b. List and explain different storage infrastructure management activities in detail. **(08 Marks)**

**OR**

10 a. Explain different storage management activities. **(08 Marks)**

b. What is ILM? List and explain various benefits of ILM. **(08 Marks)**

* * * * *

9A)



## 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.

### 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.

9B)

# 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.

## 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.

**10B)**

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

## Module-5

| | | | |
|---|---|---|---|
| 9 | a. | Explain FC SAN security architecture with neat diagram. | **(08 Marks)** |
| | b. | Explain the concept of Kerberos with neat diagram. | **(08 Marks)** |

**OR**

| | | | |
|---|---|---|---|
| 10 | a. | Explain the storage management activities in detail. | **(08 Marks)** |
| | b. | Explain Information Lifecycle Management (ILM) in detail with challenges. | **(08 Marks)** |

### 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.

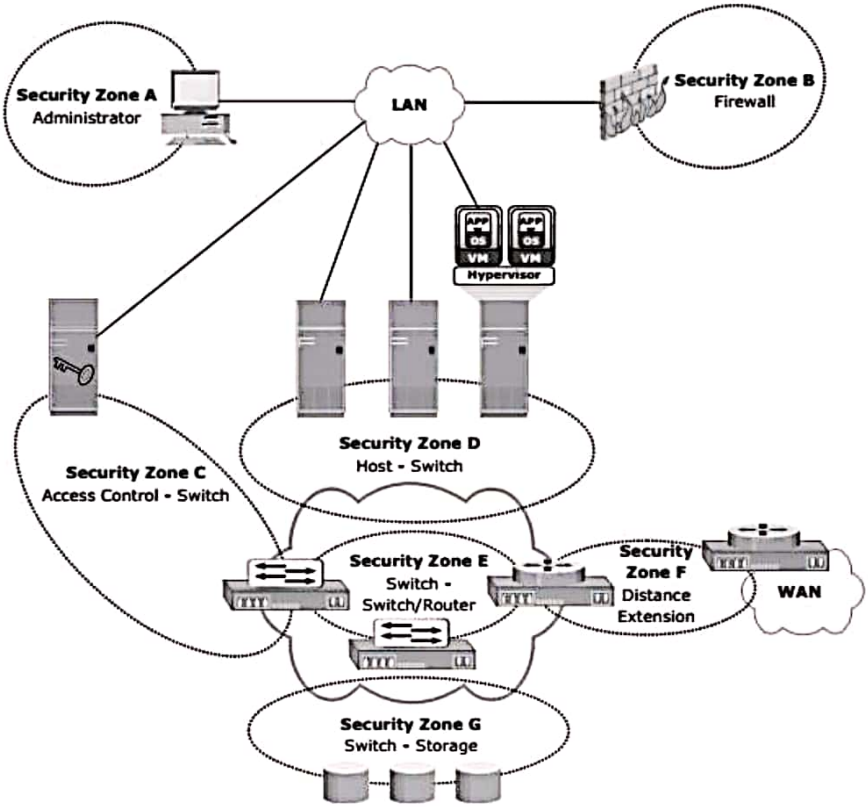


Fig 5.5: FC SAN security architecture

| 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. |

**9B)**

**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*.

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.

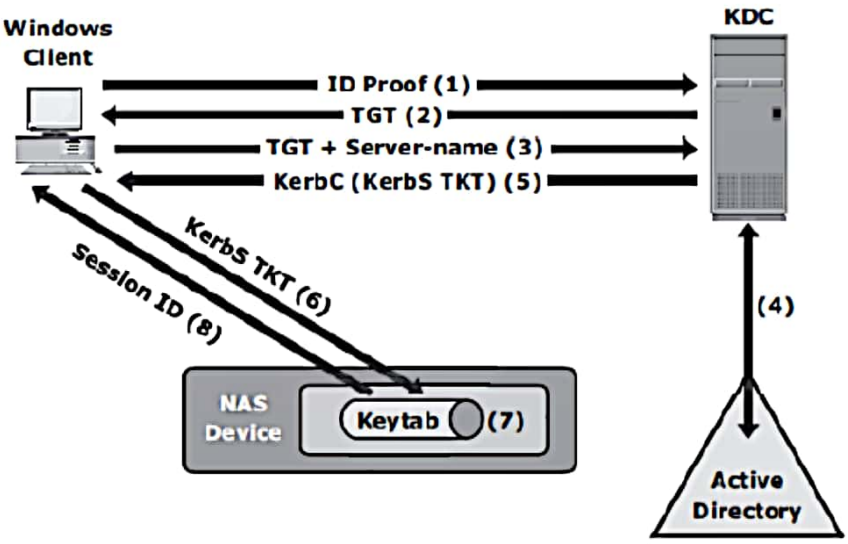


Fig 5.8 Kerberos authorization

**10A)**

## 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.

## Module-5

9 a. Explain the different types of security threats. **(06 Marks)**

b. Discuss security solutions for FC – SAN and IP-SAN. **(10 Marks)**

**OR**

10 a. Explain the various information infrastructure components in classic and virtual Environments. **(08 Marks)**

b. Write a short notes on the following :

i) Information Life Cycle Management (ILM). ii) Storage Tiering. **(08 Marks)**

* * * * *

9A)

### 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.

9B)

### 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.

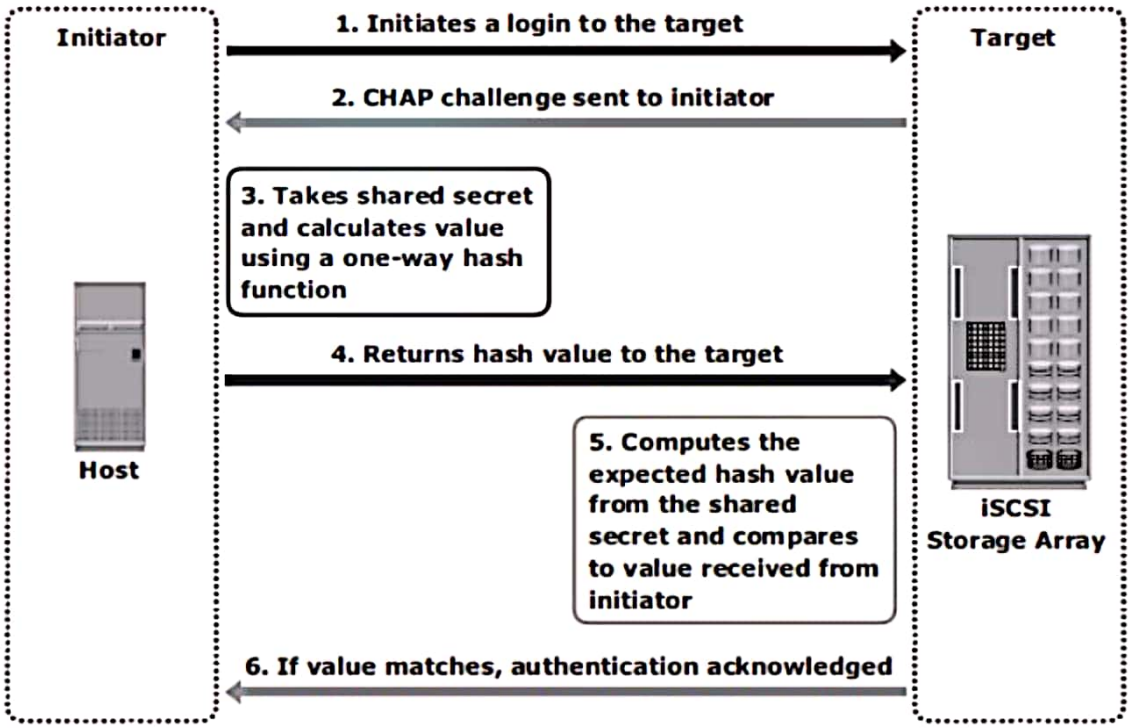


Fig 5.10 : Securing IPSAN with CHAP authentication

- 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 confi gured 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.

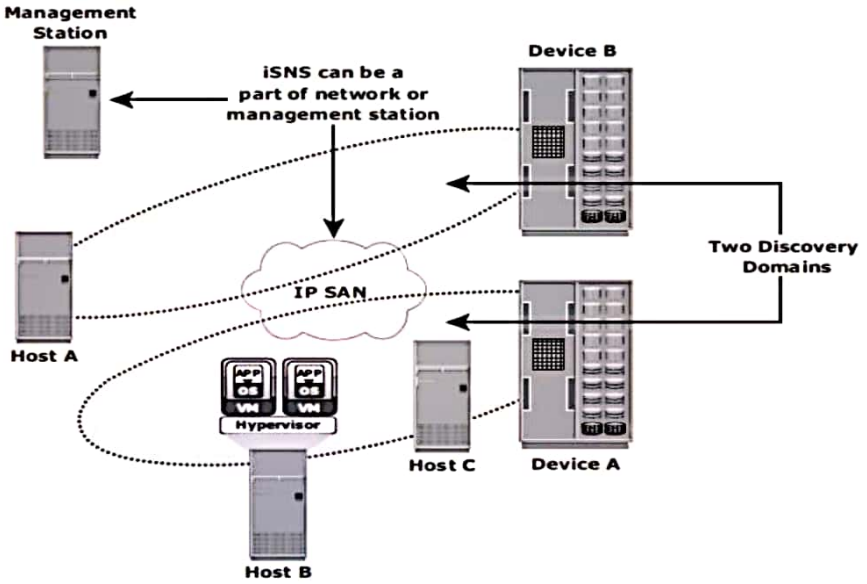


Fig 5.11 : Securing IPSAN with iSNS discovery domains

10A) UNAVAILABLE

10B)

## 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.**
- 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

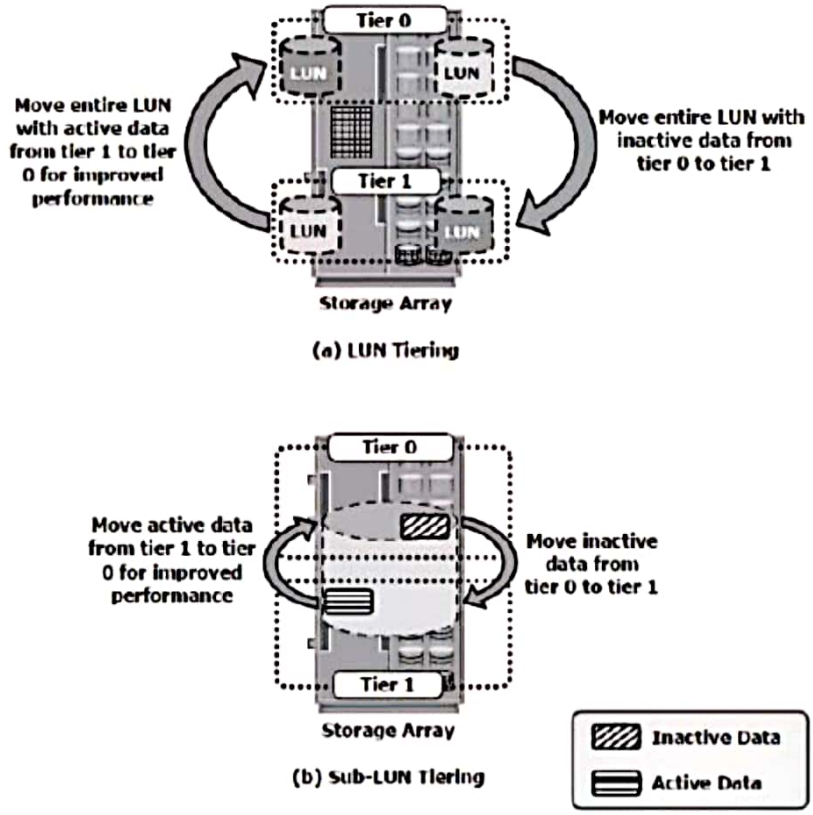


Fig 5.22: Implementation of intra-array storage tiering

## 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.

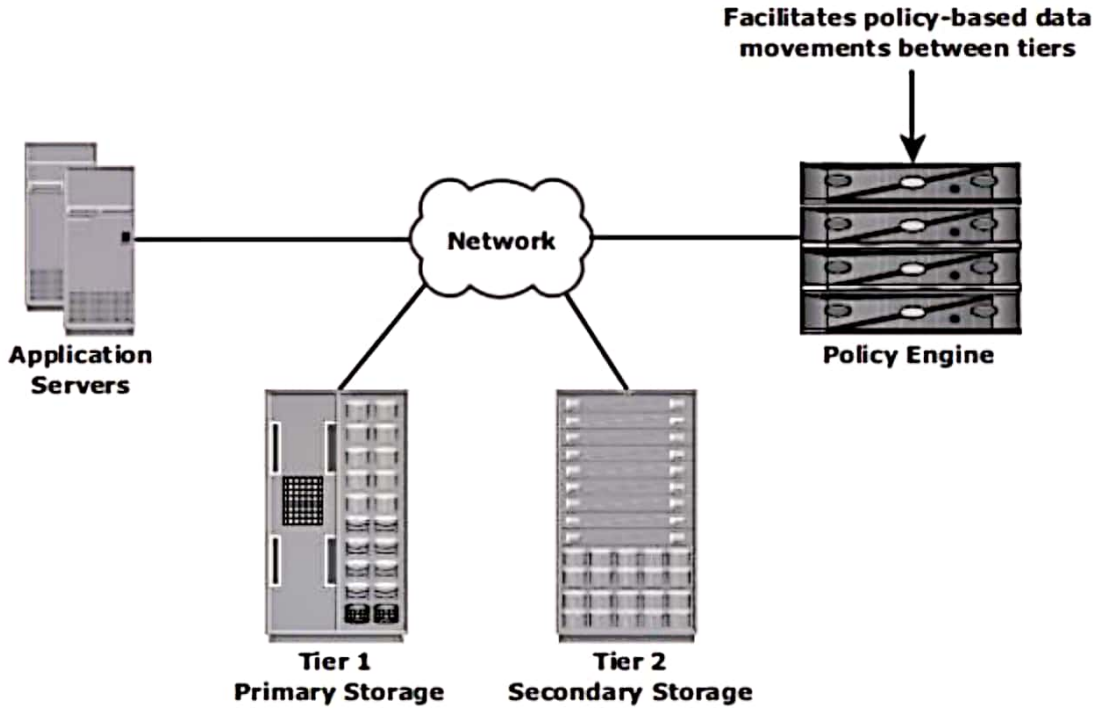


Fig 5.23: Implementation of intra-array storage tiering