UNIT-4

Storage Security And Management

Information Security Framework

- Accountability
- Confidentiality
- Integrity
- Availability

Risk Triad

- Risk triad defines the risk in terms of threats, assets, and vulnerabilities.
- Risk arises when a threat agent (an attacker) seeks to access assets by exploiting an existing vulnerability.

Three key elements of the risk triad.

- Assets
- Threats
- Vulnerability

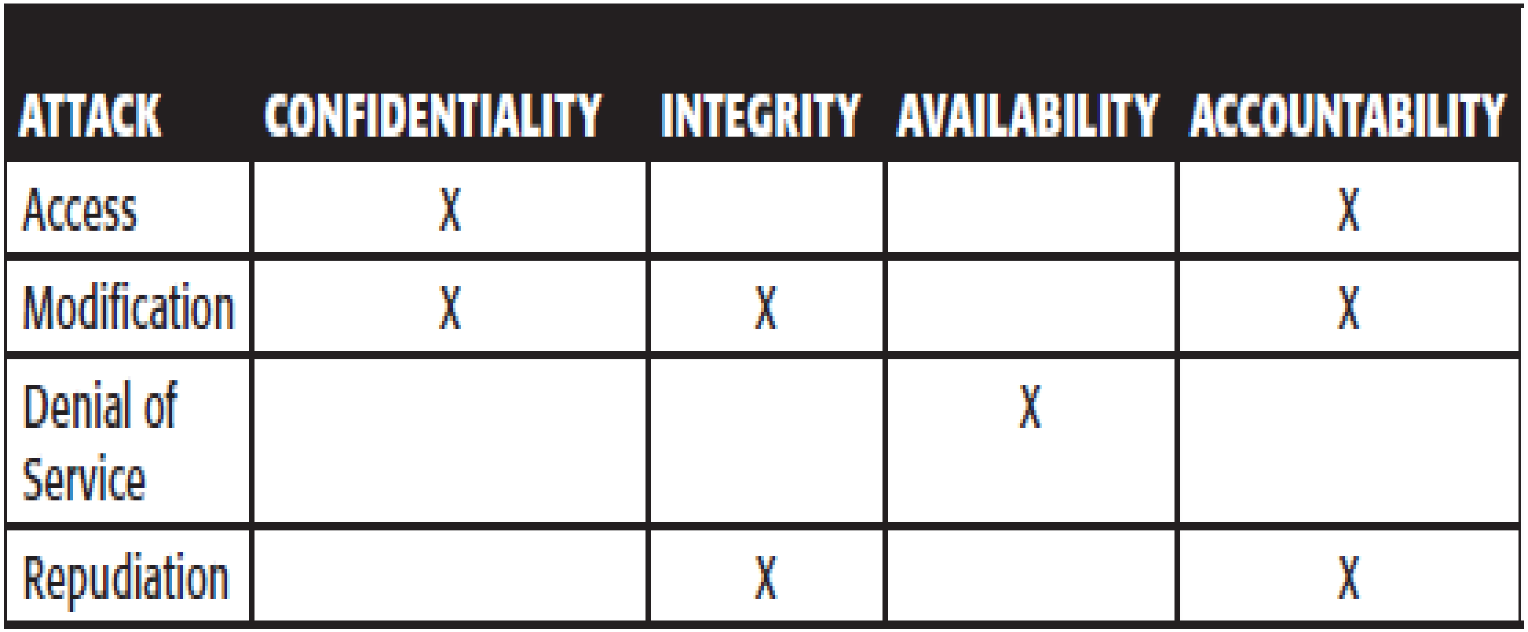
Assets

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

Threats

- Threats are the potential attacks that can be carried out on an IT infrastructure.
- These attacks can be classified as active or passive.
- ***Passive* attacks** are attempts to gain unauthorized access into the system.
- **Active attacks** include data modification, Denial of Service (DoS), and repudiation attacks

Security Services for Various Types of Attacks



ATTACK	CONFIDENTIALITY	INTEGRITY	AVAILABILITY	ACCOUNTABILITY
Access	X			X
Modification	X	X		X
Denial of Service			X	
Repudiation		X		X

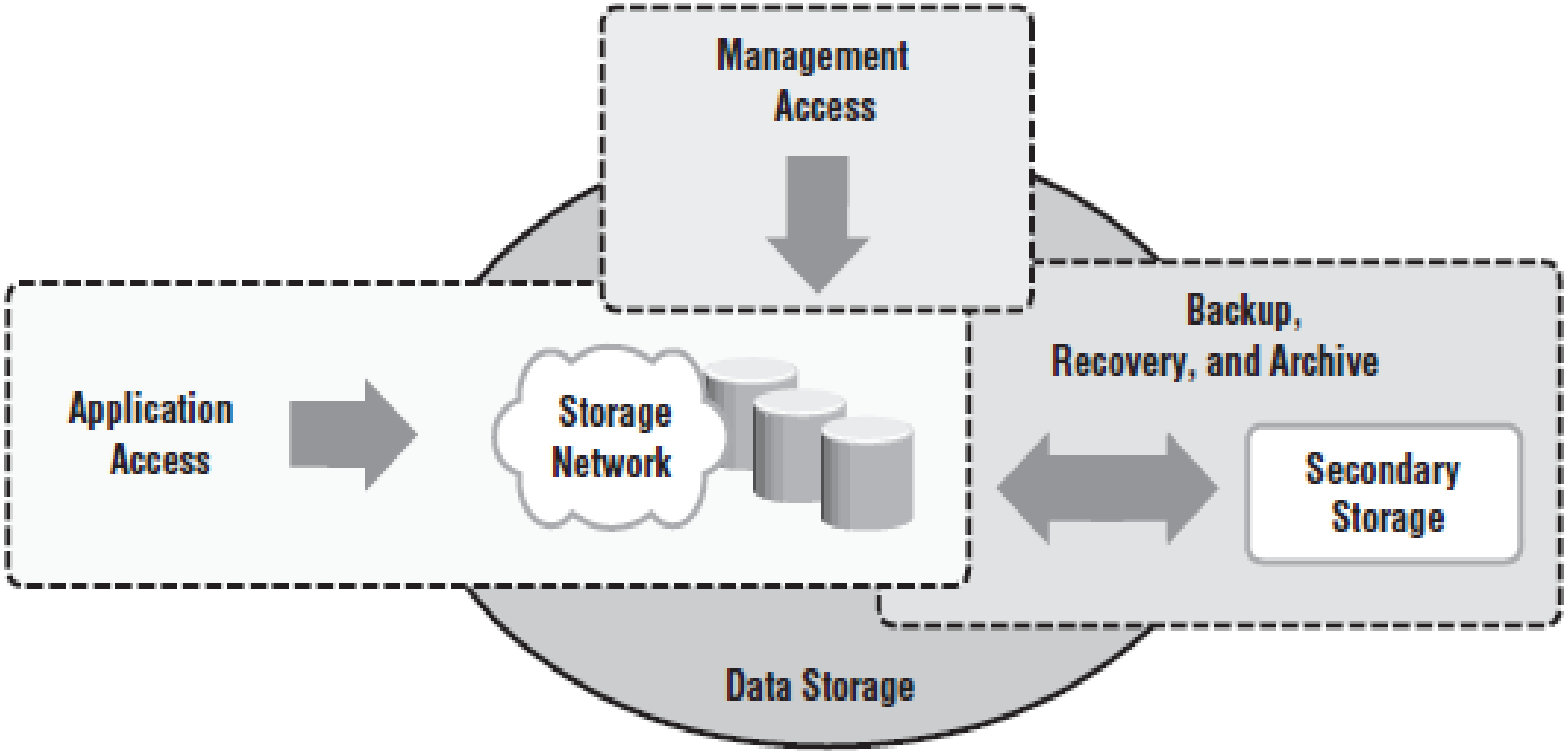
Vulnerability

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

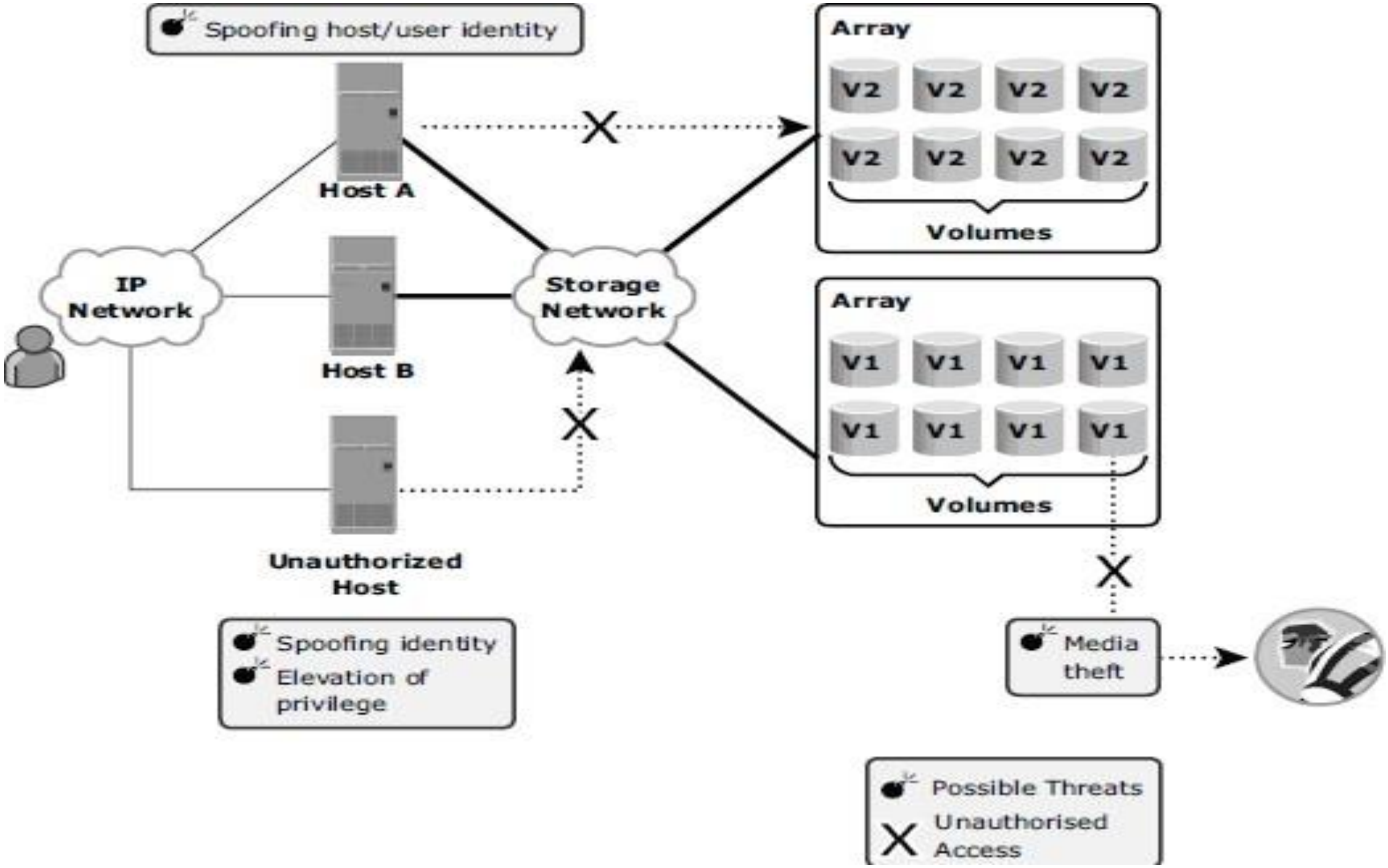
Storage Security Domains

- Storage devices that are not connected to a storage network are less vulnerable because they are not exposed to security threats via networks.
- In order 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 *BURA (backup, recovery, and archive)*.

Three security domains of data storage



1.Securing the Application Access Domain



- ***Controlling User Access to Data***
  - Access control services regulate user access to data.
- These services mitigate the threats of spoofing host identity and elevating host privileges. Both of these threats affect data integrity and confidentiality
- Different storage networking technologies, such as iSCSI, FC, and IP-based storage, use various authentication mechanisms, such as Challenge-Handshake Authentication Protocol (CHAP), Fibre Channel Security Protocol (FC-SP), and IPSec, respectively, to authenticate host access.

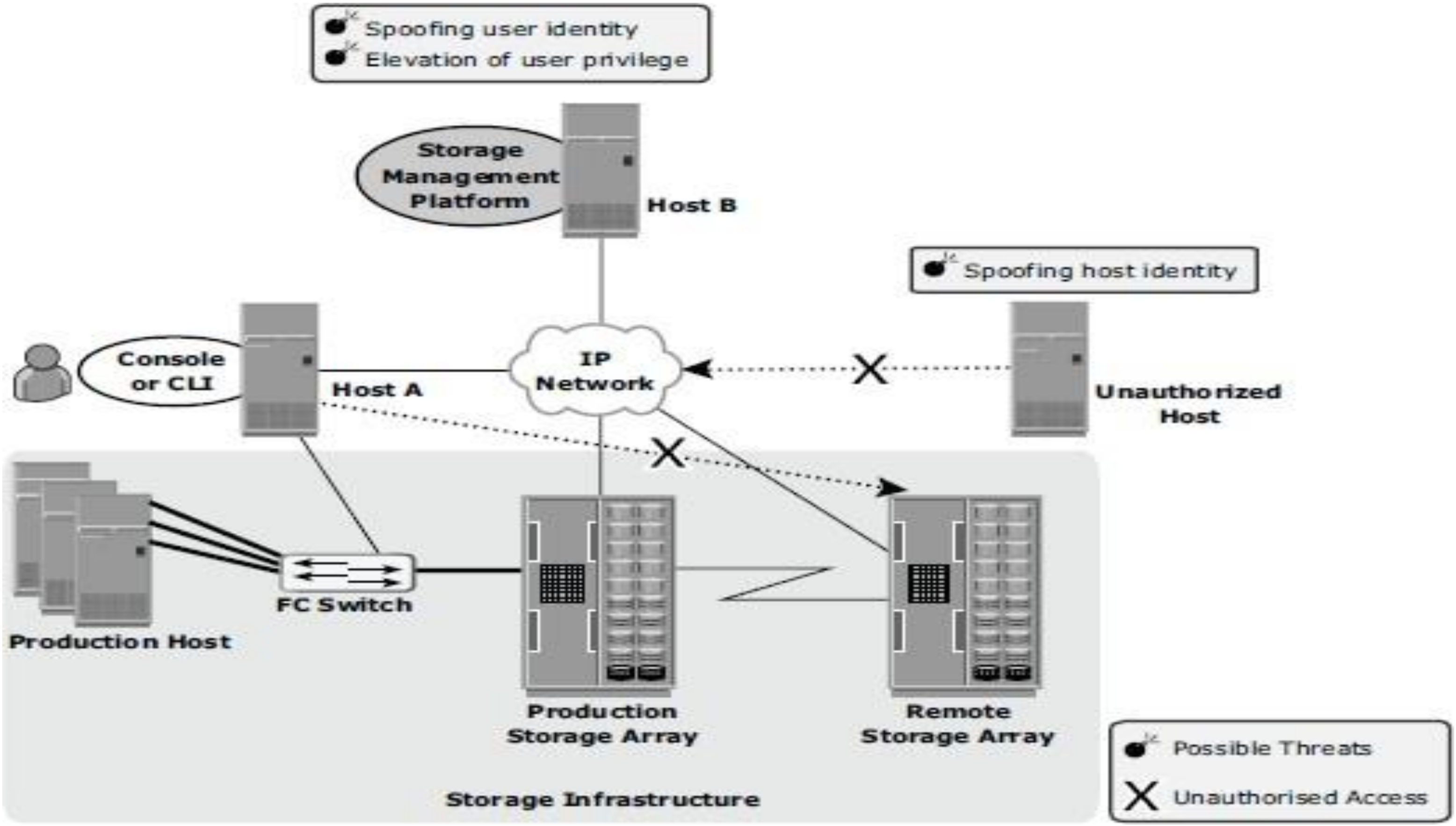
Protecting the Storage Infrastructure

- Securing the storage infrastructure from unauthorized access involves protecting all the elements of the infrastructure
- The security controls for protecting the network fall into two general categories: *connectivity infrastructure integrity* and *storage network encryption*

Data Encryption

The most important aspect of securing data is protecting data held inside the storage arrays. Threats at this level include tampering with data, which violates data integrity, and media theft, which compromises data availability and confidentiality

2.Securing the Management Access Domain

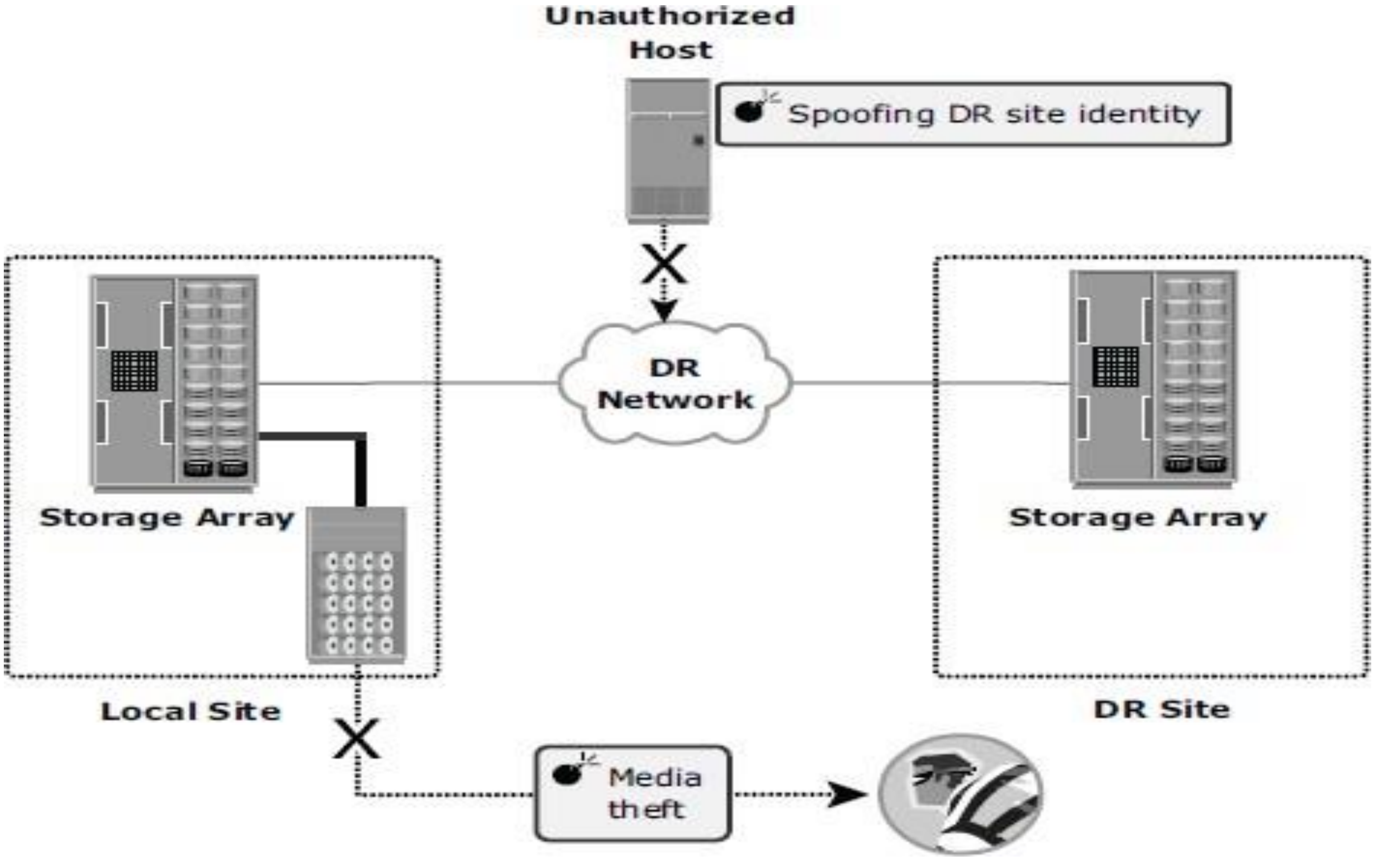


Controlling Administrative Access

- Controlling administrative access to storage aims to safeguard against the threats of an attacker spoofing an administrator’s identity or elevating another user’s identity and privileges to gain administrative access.
- Both of these threats affect the integrity of data and devices.

- ***Protecting the Management Infrastructure***
  - Protecting the management network infrastructure is also necessary.
  - Controls to protect the management network infrastructure include encrypting management traffic, enforcing management access controls, and applying IP network security best practices.

3.Securing Backup, Recovery, and Archive (BURA)



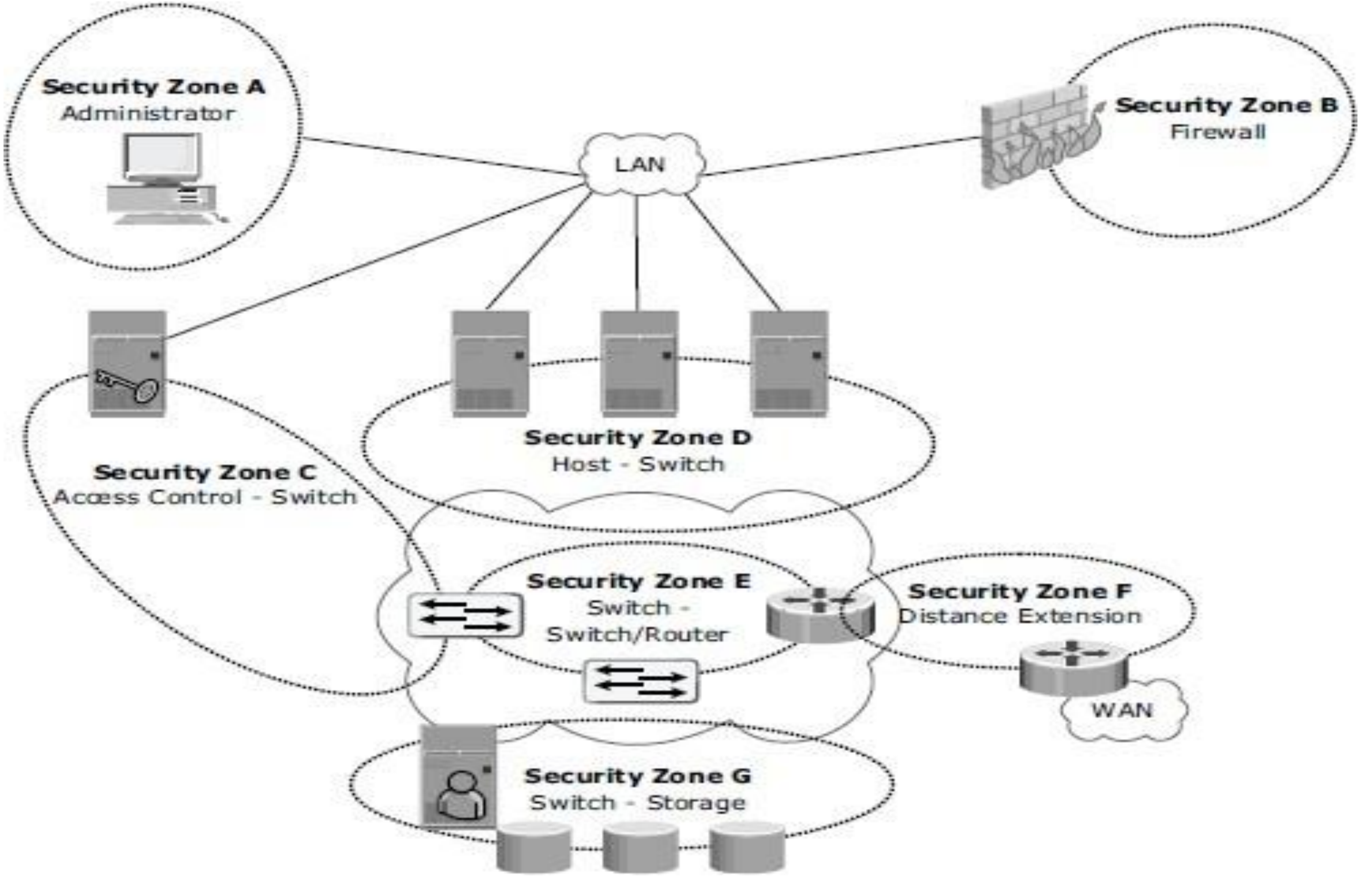
Security Implementations in Storage Networking

- Basic security implementations in
- SAN
- NAS
- IP-SAN environments.

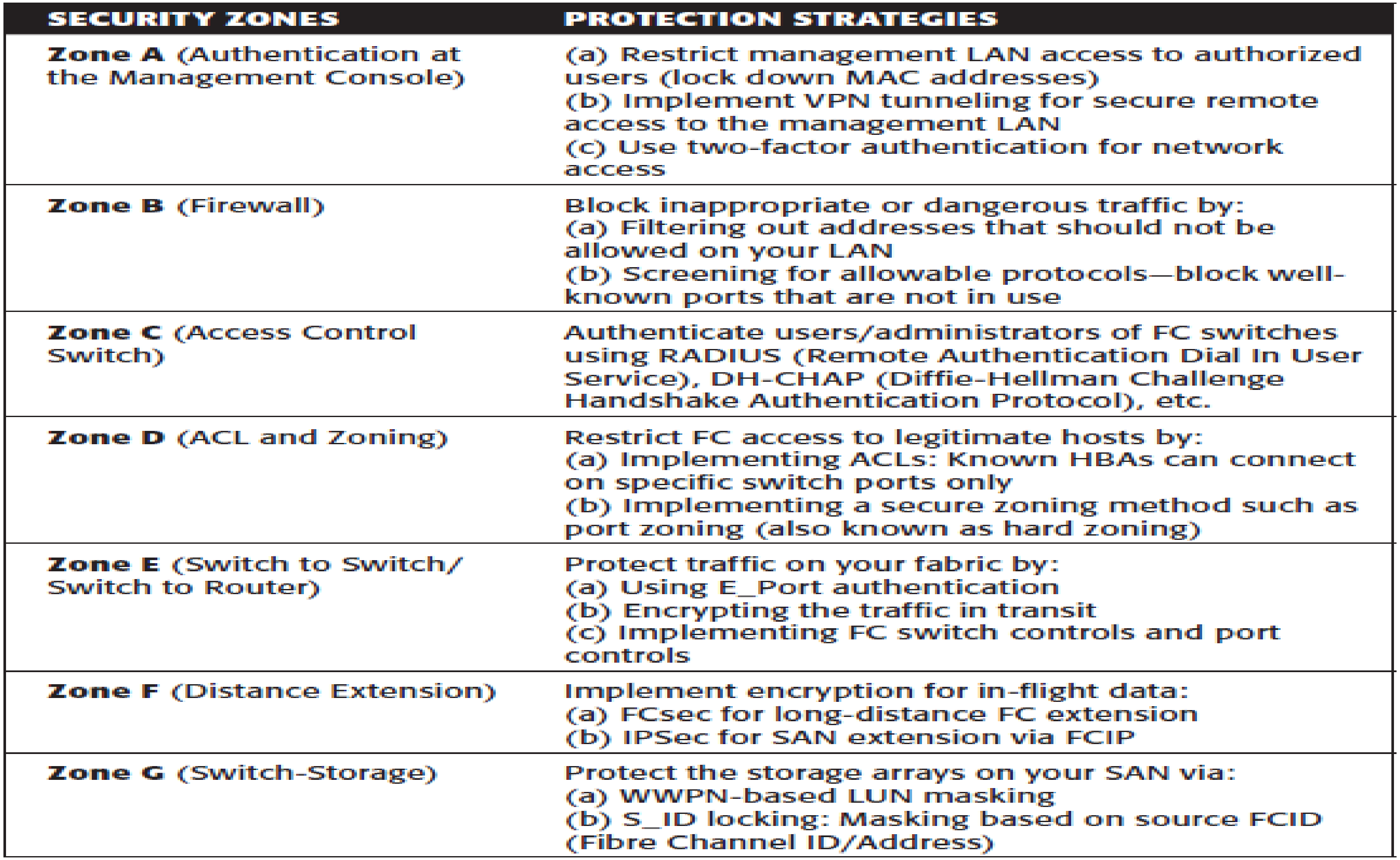
SAN

- An FC SAN is configured as an isolated private environment with fewer nodes than an IP network
- The current version of the FC-SP standard is referred to as FC-SP-1.

SAN Security Architecture



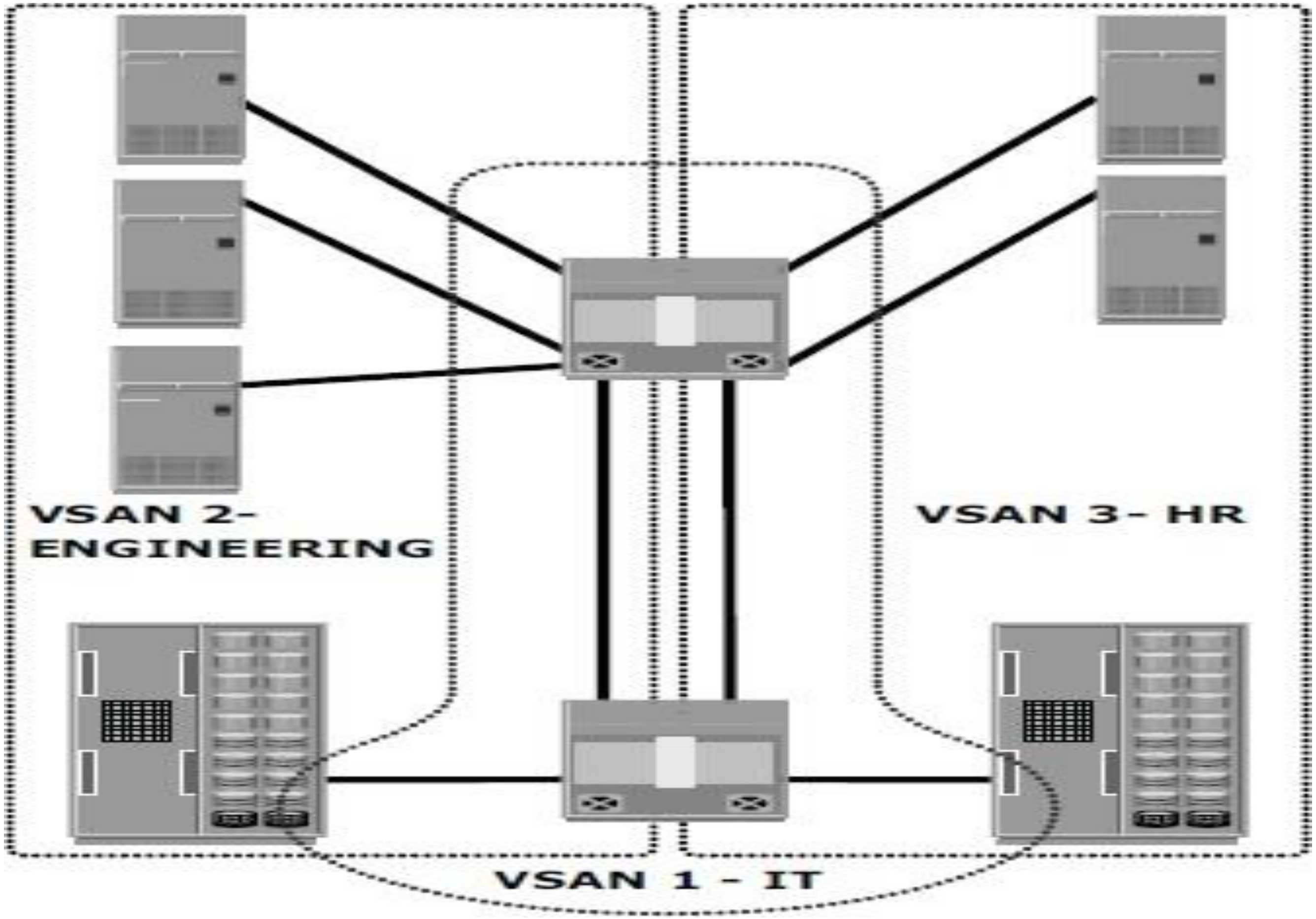
Security Zones and Protection Strategies



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 (c) Use two-factor authentication for network access
Zone B (Firewall)	Block inappropriate or dangerous traffic by: (a) Filtering out addresses that should not be allowed on your LAN (b) Screening for allowable protocols—block well-known ports that are not in use
Zone C (Access Control Switch)	Authenticate users/administrators of FC switches using RADIUS (Remote Authentication Dial In User Service), DH-CHAP (Diffie-Hellman Challenge Handshake Authentication Protocol), etc.
Zone D (ACL and Zoning)	Restrict FC access to legitimate hosts by: (a) Implementing ACLs: Known HBAs can connect on specific switch ports only (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 your fabric by: (a) Using E_Port authentication (b) Encrypting the traffic in transit (c) Implementing FC switch controls and port controls
Zone F (Distance Extension)	Implement encryption for in-flight data: (a) FCsec for long-distance FC extension (b) IPSec for SAN extension via FCIP
Zone G (Switch-Storage)	Protect the storage arrays on your SAN via: (a) WWPN-based LUN masking (b) S_ID locking: Masking based on source FCID (Fibre Channel ID/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.


VSAN 2-
ENGINEERING
VSAN 3- HR
VSAN 1 - IT

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.

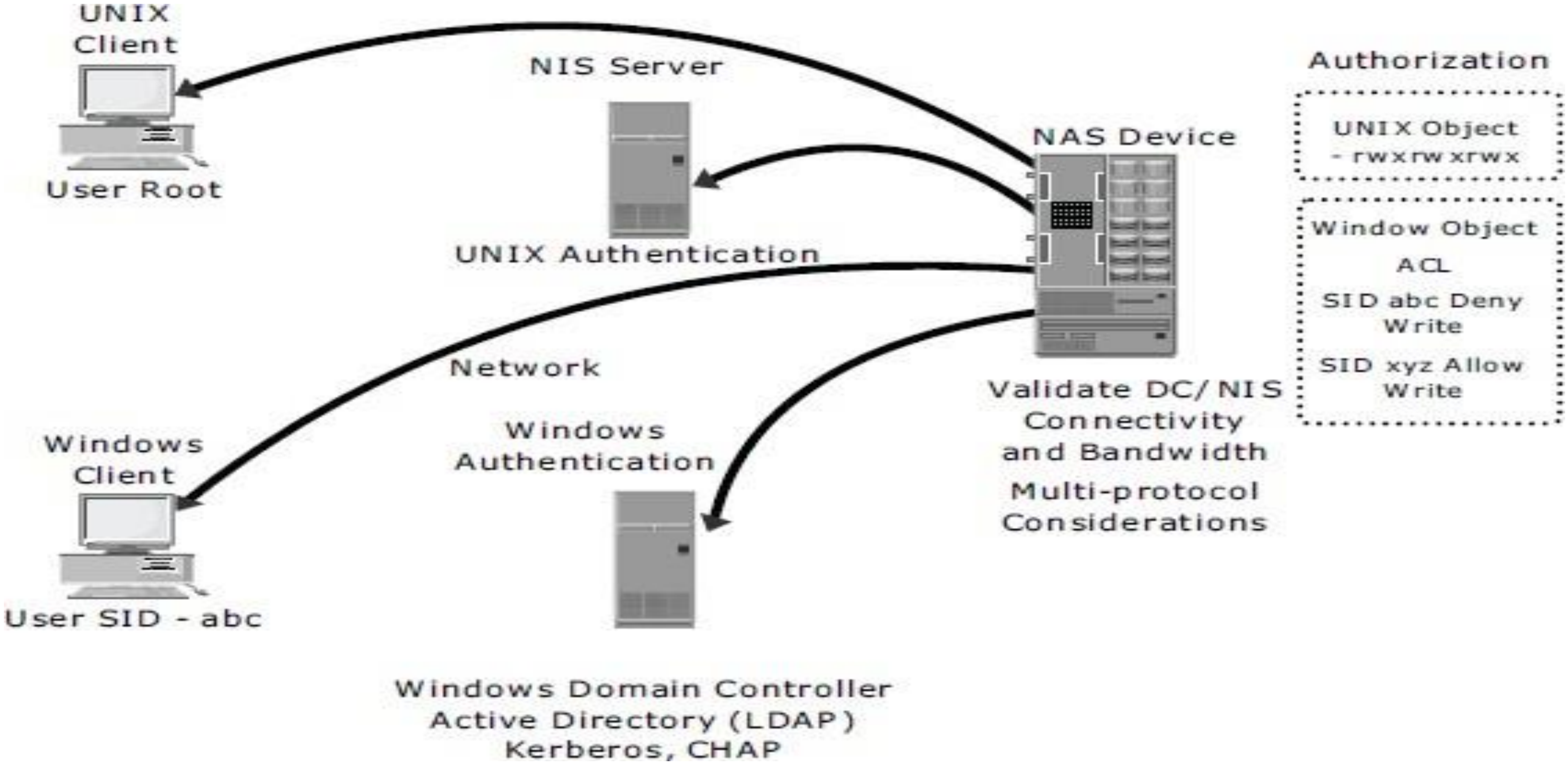
NAS File Sharing: Windows ACLs

- Windows supports two types of ACLs: *discretionary access control lists (DACLs)* and *system access control lists (SACLs)*.

NAS File Sharing: UNIX Permissions

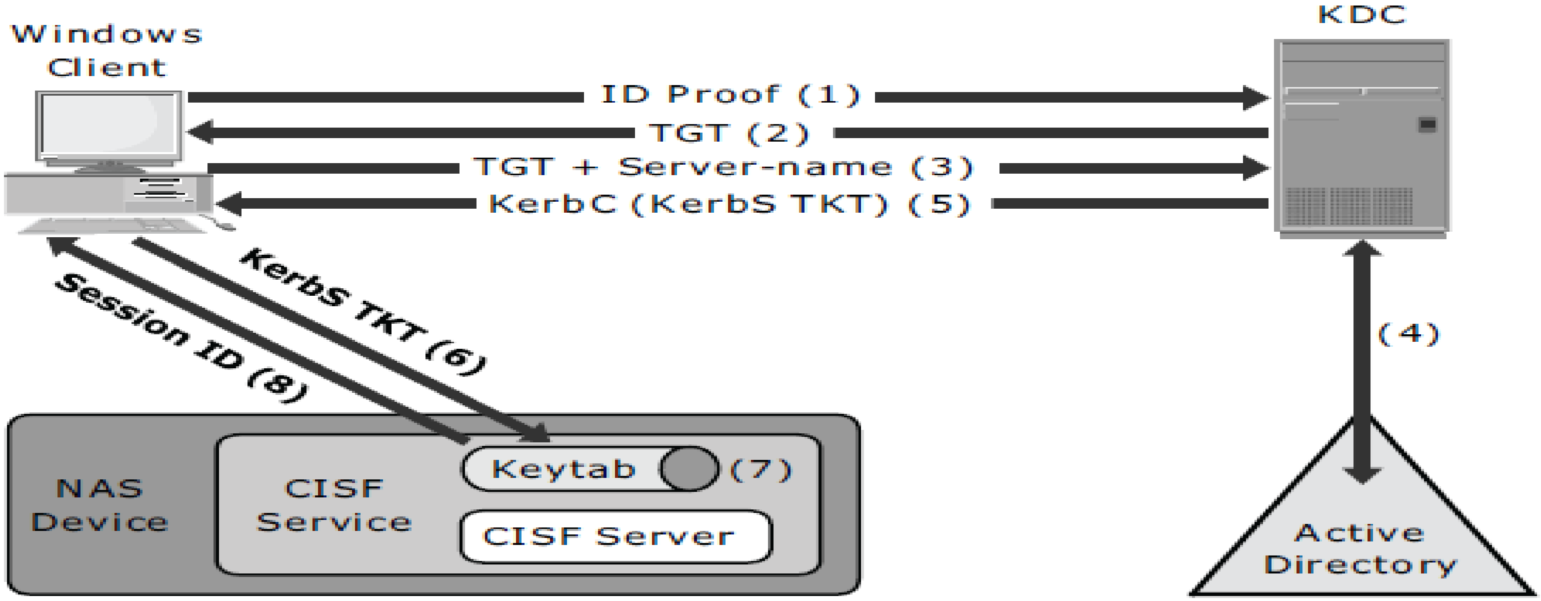
- For the UNIX operating system, a *user* is an abstraction that denotes a logical entity for assignment of ownership and operation privileges for the system.
- A user can be either a person or a system operation

- ***Authentication and Authorization***

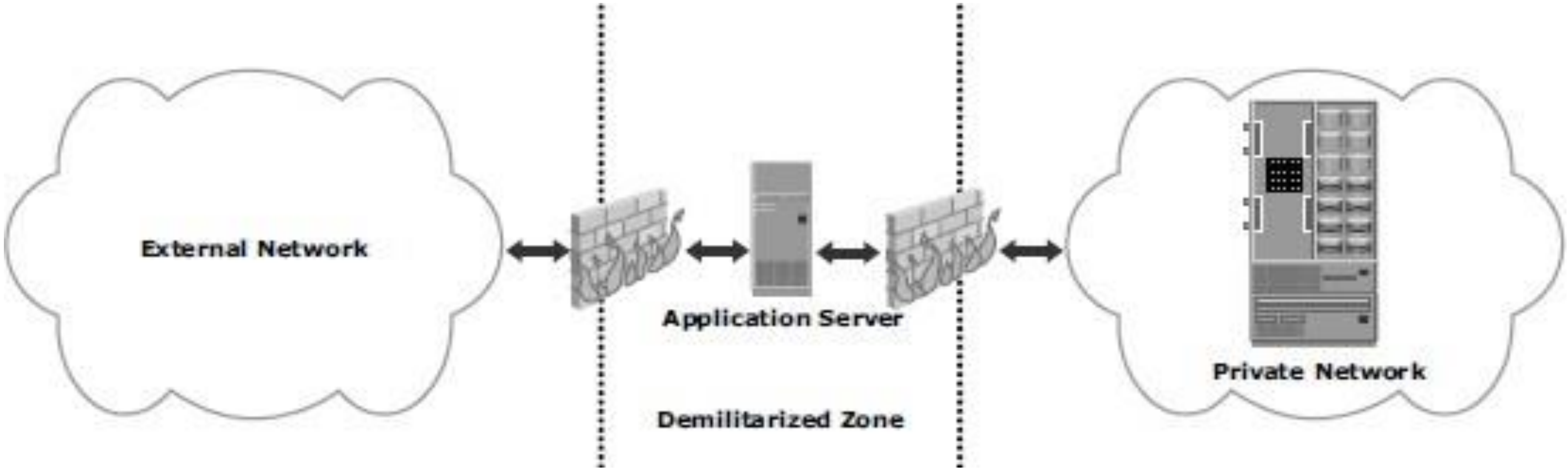


Kerberos

- Kerberos is a network authentication protocol.
- It is designed to provide strong authentication for client/server applications by using secret-key cryptography.



- ***Network-Layer Firewalls***
  - Network layer firewalls are implemented in NAS environments to protect the NAS devices from these security threats.
  - These network-layer firewalls are capable of examining network packets and comparing them to a set of configured security rules.

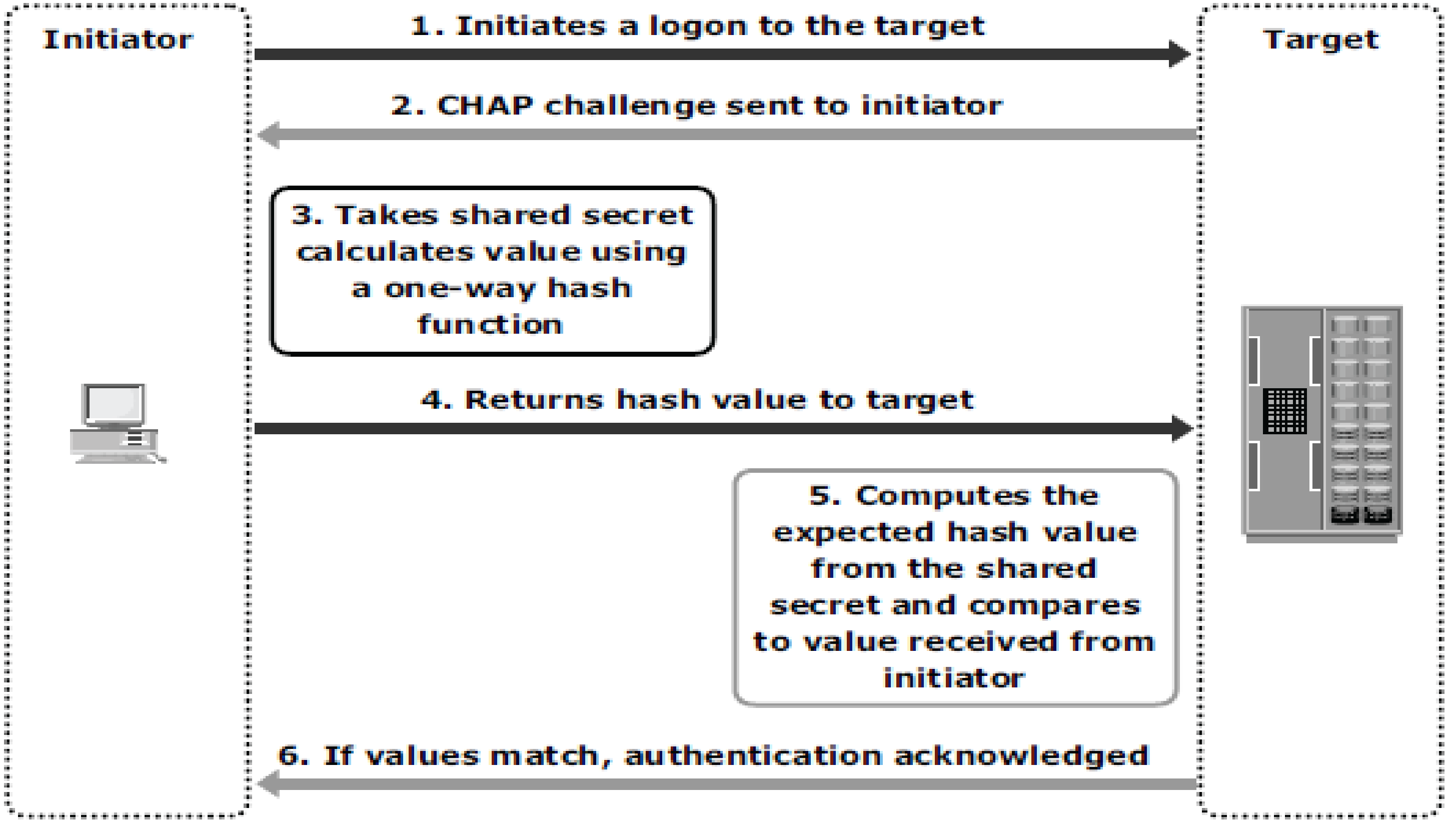


IP SAN

- – This section describes some of the basic security mechanisms of IP SAN environments.
- – The *Challenge-Handshake Authentication Protocol (CHAP)* is a basic authentication mechanism that has been widely adopted by network devices and hosts.

- 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.

Securing IPSAN with CHAP authentication



Initiator

Target

1. Initiates a logon to the target

2. CHAP challenge sent to initiator

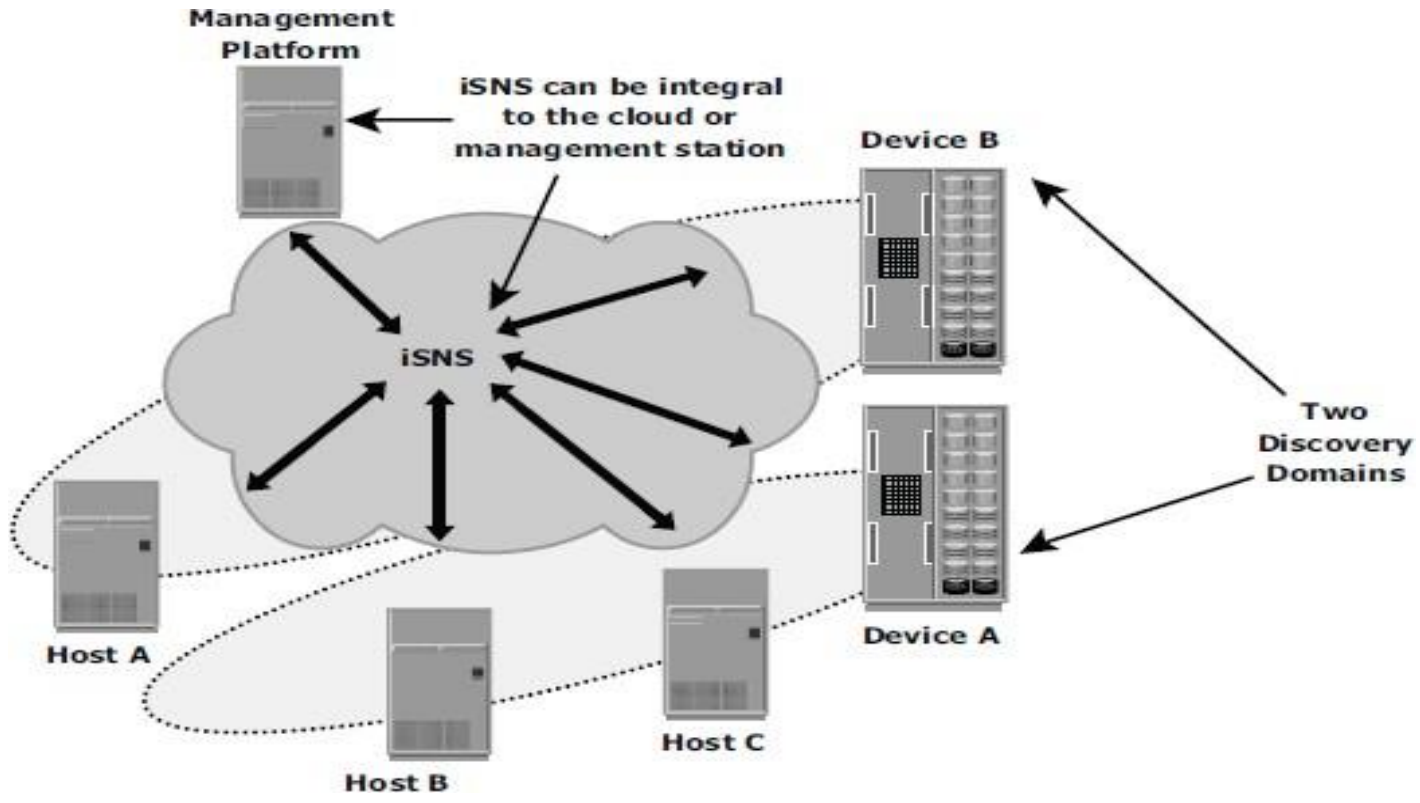
3. Takes shared secret calculates value using a one-way hash function

4. Returns hash value to target

5. Computes the expected hash value from the shared secret and compares to value received from initiator

6. If values match, authentication acknowledged

Securing IPSAN with iSNS discovery domains



Securing Storage Infrastructure in Virtualized and Cloud Environments

Security Concerns

- These key security concerns are multitenancy, velocity of attack, information assurance, and data privacy.

Security Measures

->Security at the Compute Level

->Security at the Network Level

->Security at the Storage Level

RSA and VMware Security Products

- RSA, the security division of EMC, is the premier provider of security, risk, and compliance solutions, helping organizations to solve their most complex and sensitive security challenges. VMware offers secure and robust virtualization solutions for virtualized and cloud environments

- RSA SecureID
- RSA Identity and Access Management
- RSA Data Protection Manager
- VMware vShield

RSA Data Protection Manager

- ApplicationEncryption and Tokenization
- Enterprise Key Management.

VMware vShield

vShieldApp

vShieldEdge

vShield Endpoint.

Monitoring the Storage Infrastructure

- Monitoring helps to analyze the status and utilization of various storage infrastructure components.
- Monitoring supports capacity planning, trend analysis, and root cause/impact analysis.

1.Parameters Monitored

- Storage infrastructure components should be monitored for accessibility, capacity, performance, and security.
- *Accessibility* refers to the availability of a component to perform a desired operation.
- *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.

2.Components Monitored

- Hosts, networks, and storage are components within the storage environment that should be monitored for accessibility, capacity, performance, and security.

Hosts

- Mission-critical application hosts should be monitored continuously.
- The accessibility of a host depends on the status of the hardware components and software processes running on it.

Storage Network

The storage network needs to be monitored to ensure proper communication between the server and the storage array.

The physical components of a storage network include elements such as switches, ports, cables, GBICs, and power supplies.

Monitoring the performance of a storage network is useful in assessing individual component performance and helps to identify network bottlenecks.

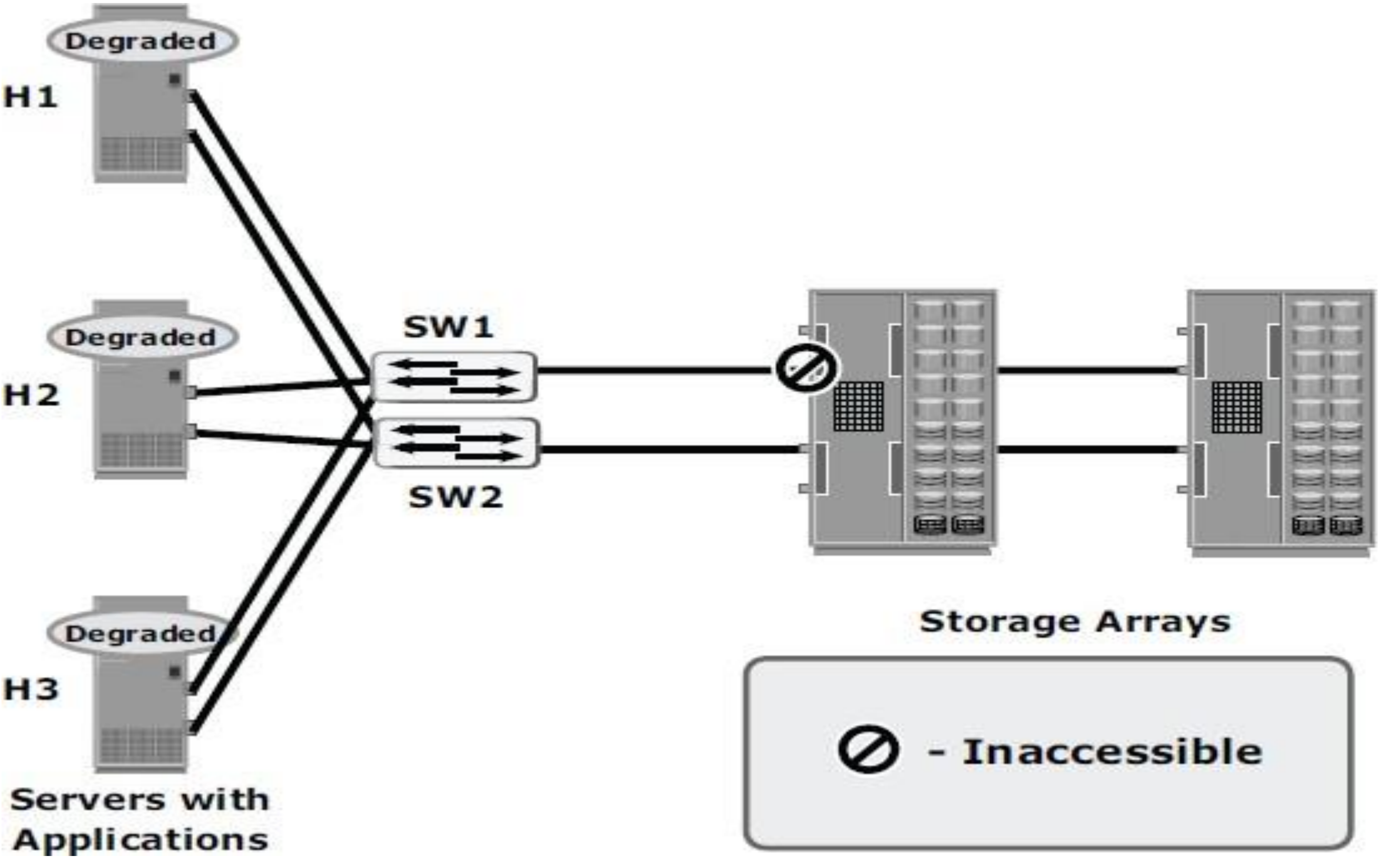
Storage

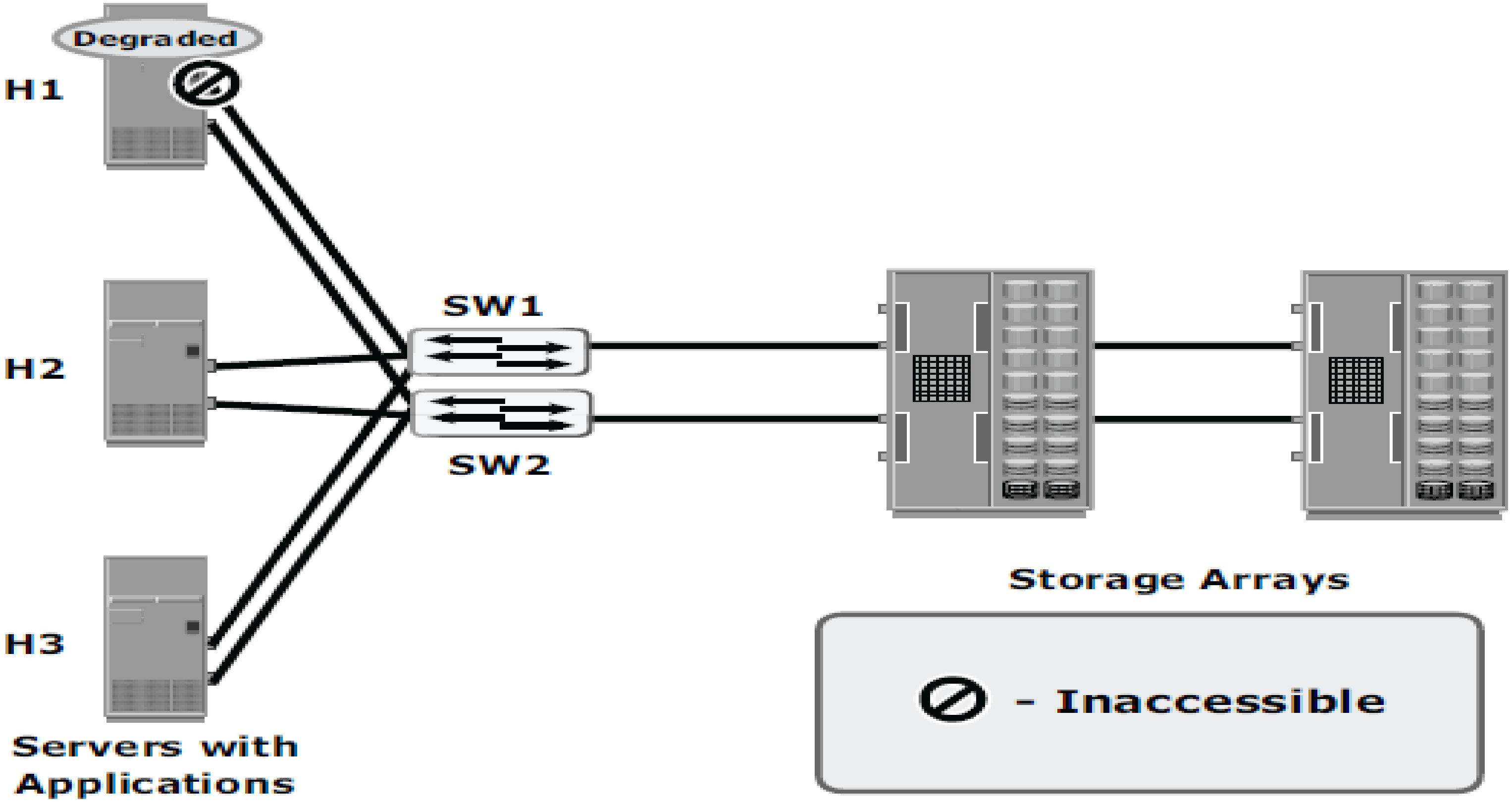
- The accessibility of the storage array should be monitored for its hardware components and various processes
- A storage array can be monitored by a number of performance metrics, such as utilization rates of the various storage array components, I/O response time, and cache utilization

3.Monitoring Examples

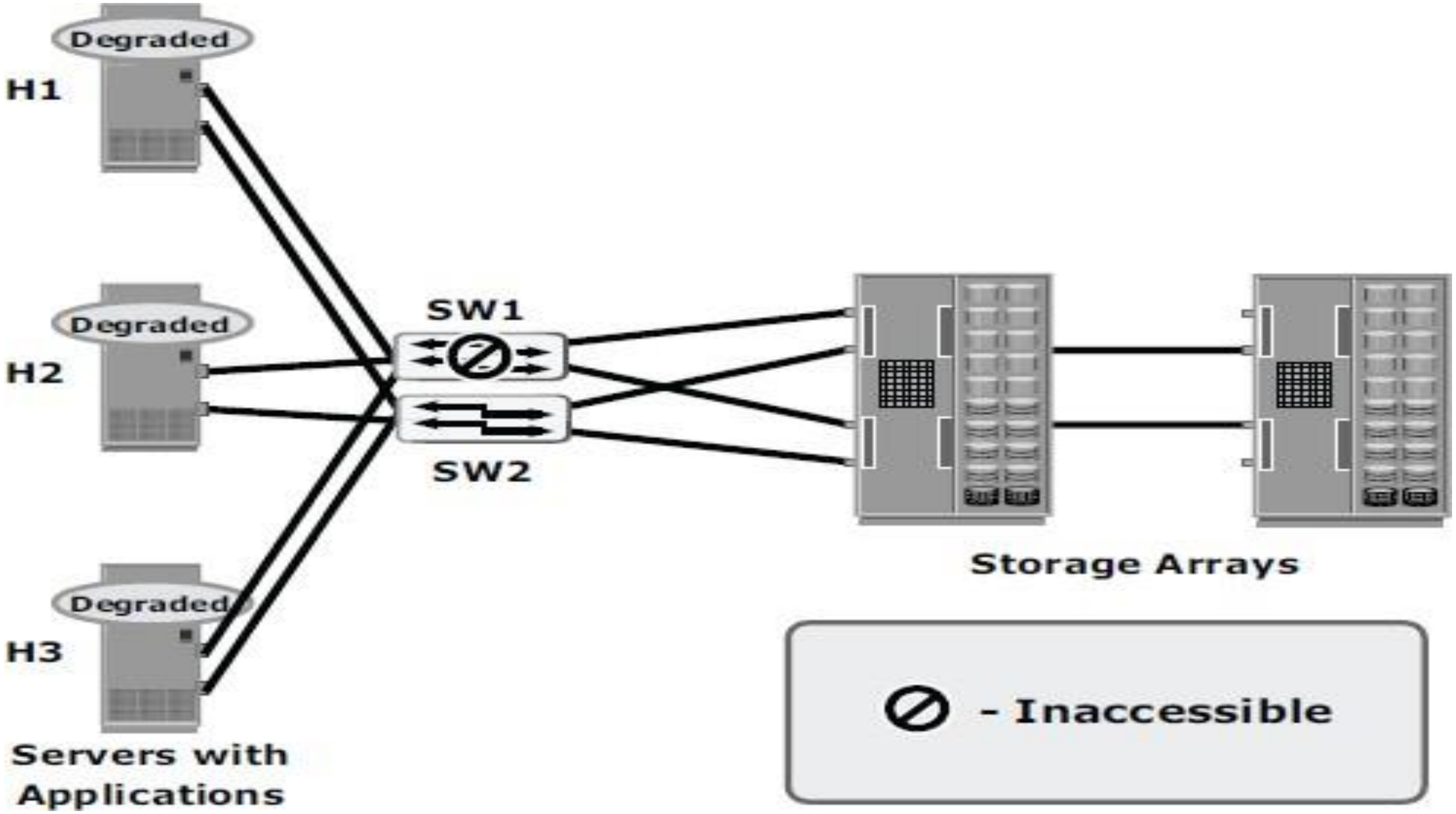
- A storage infrastructure requires implementation of an end-to-end solution to actively monitor all the parameters of its critical components.
- Early detection and instant alerts ensure the protection of critical assets.

Accessibility Monitoring

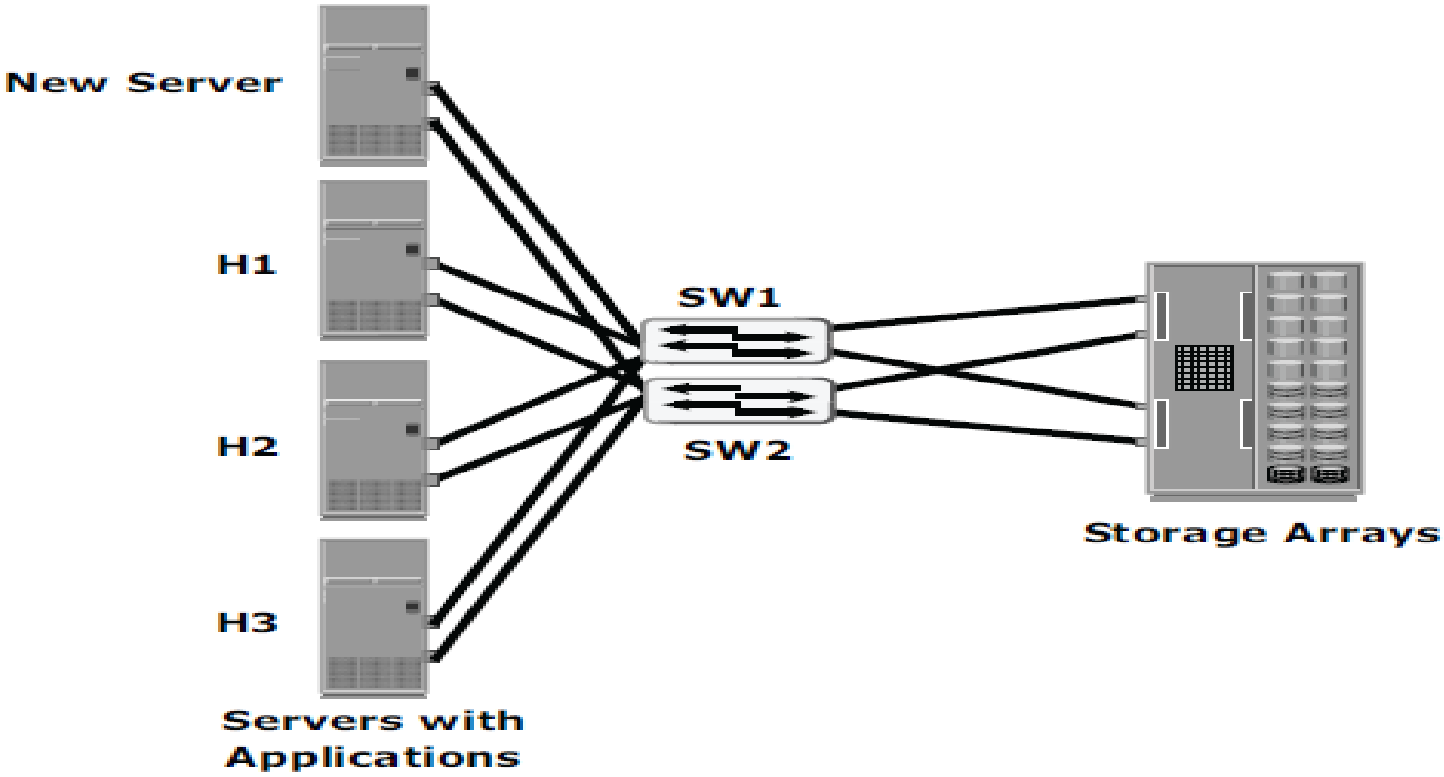



Degraded
H1
H2
H3
SW1
SW2
Storage Arrays
Servers with Applications
⊘ - Inaccessible

Capacity Monitoring

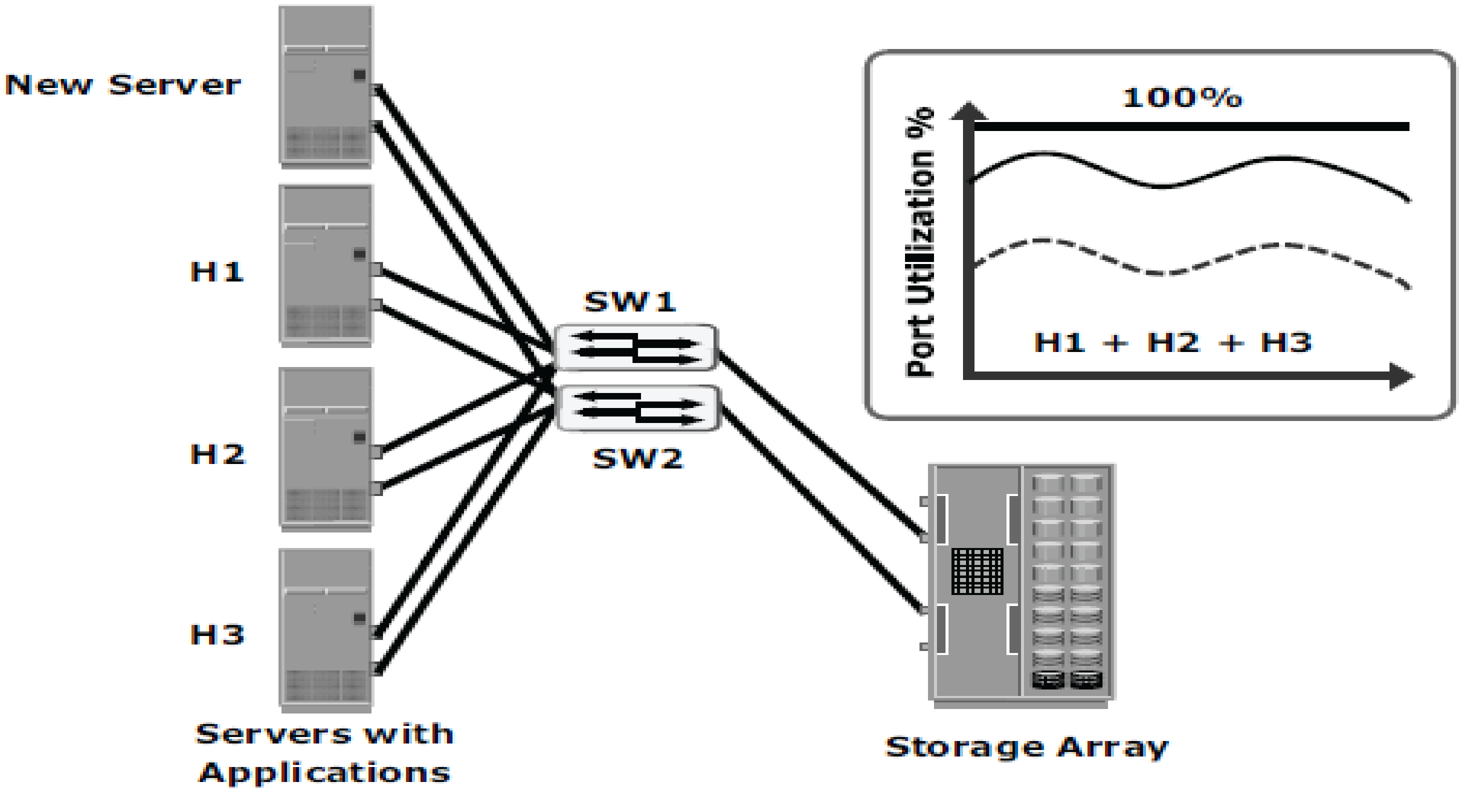


- Monitoring storage array capacity

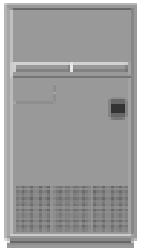


Performance Monitoring

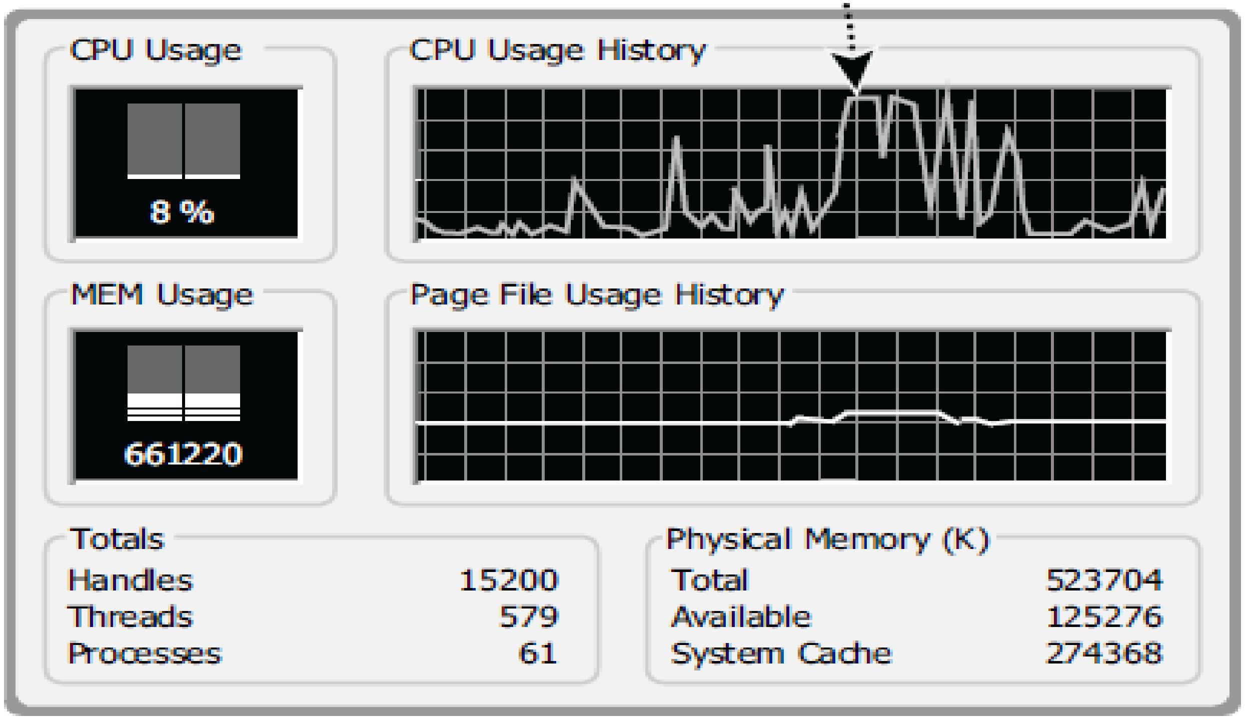
- Monitoring array port utilization



- Monitoring the performance of servers



Critical: CPU usage above 90% for the last 90 minutes



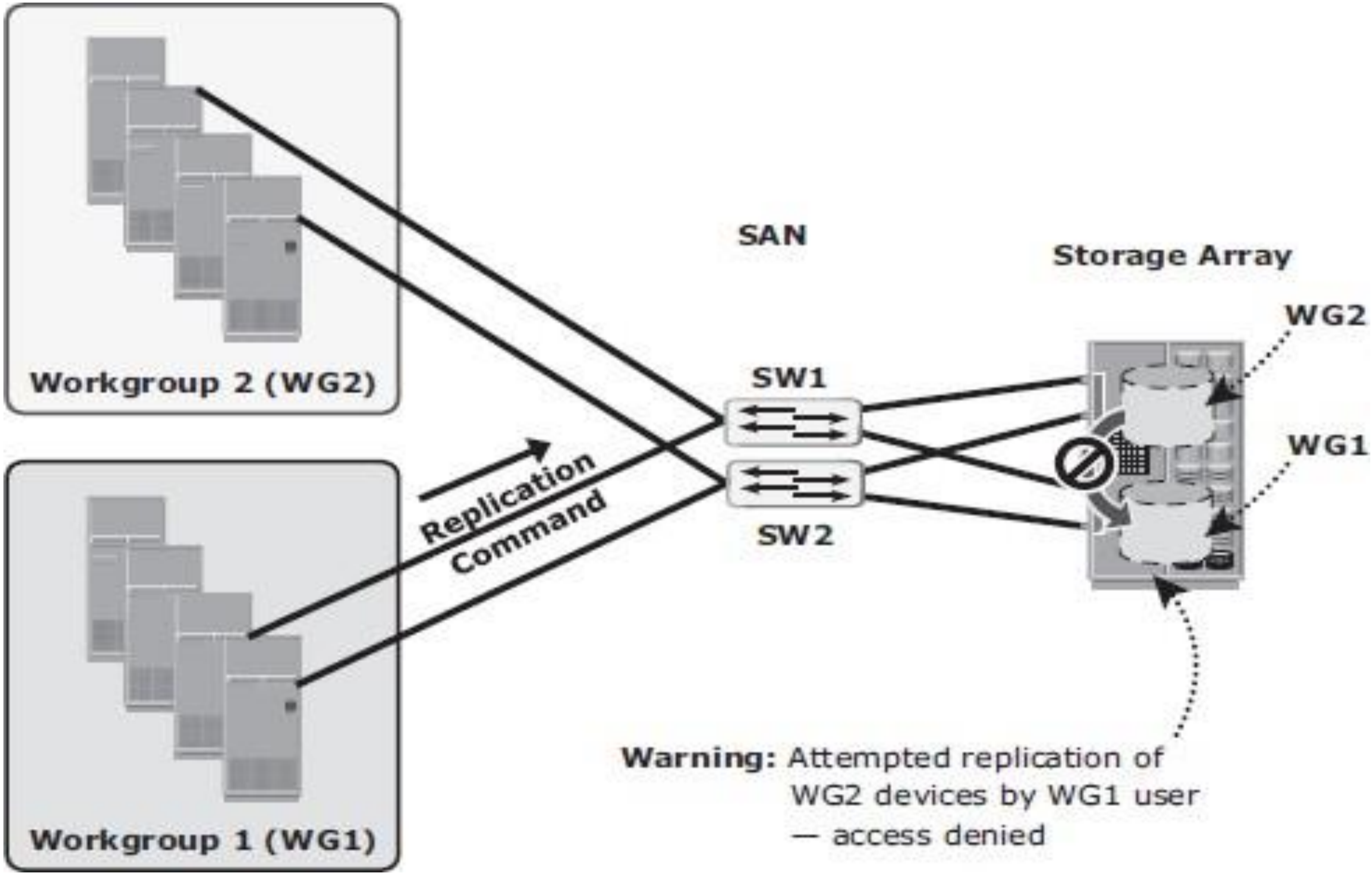
CPU Usage: 8 %

MEM Usage: 661220

Totals	
Handles	15200
Threads	579
Processes	61

Physical Memory (K)	
Total	523704
Available	125276
System Cache	274368

Security Monitoring.



4.Alerts

- Alerting of events is an integral part of monitoring.
- There are conditions observed by monitoring, such as failure of power, disks, memory, or switches, which may impact the availability of services that requires immediate administrative attention.
- ***Information alerts*** provide useful information that does 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 may affect overall performance or availability.

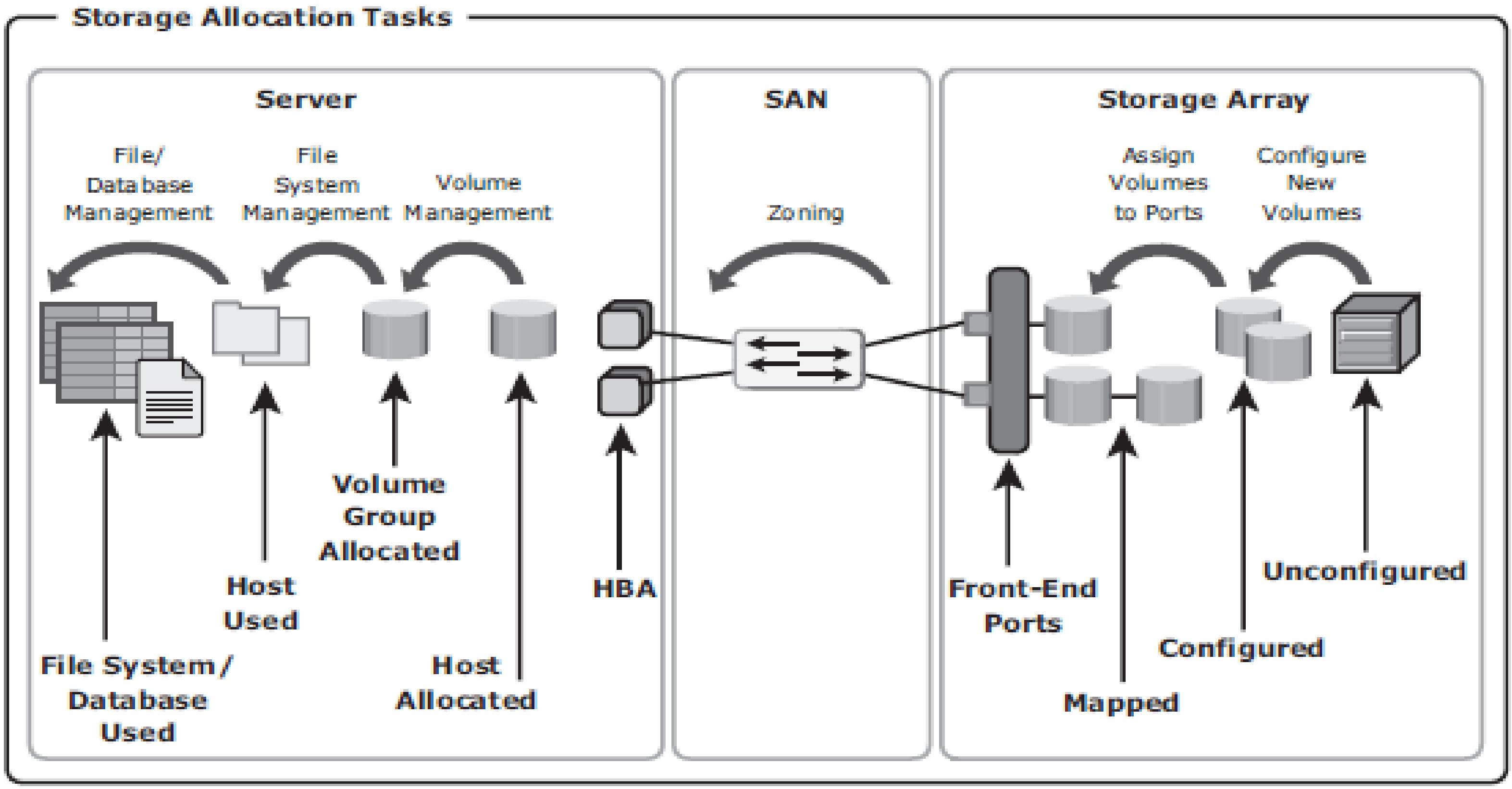
Storage Infrastructure Management Activities

- Availability management
- Capacity management
- Performance management
- Security management
- Reporting.

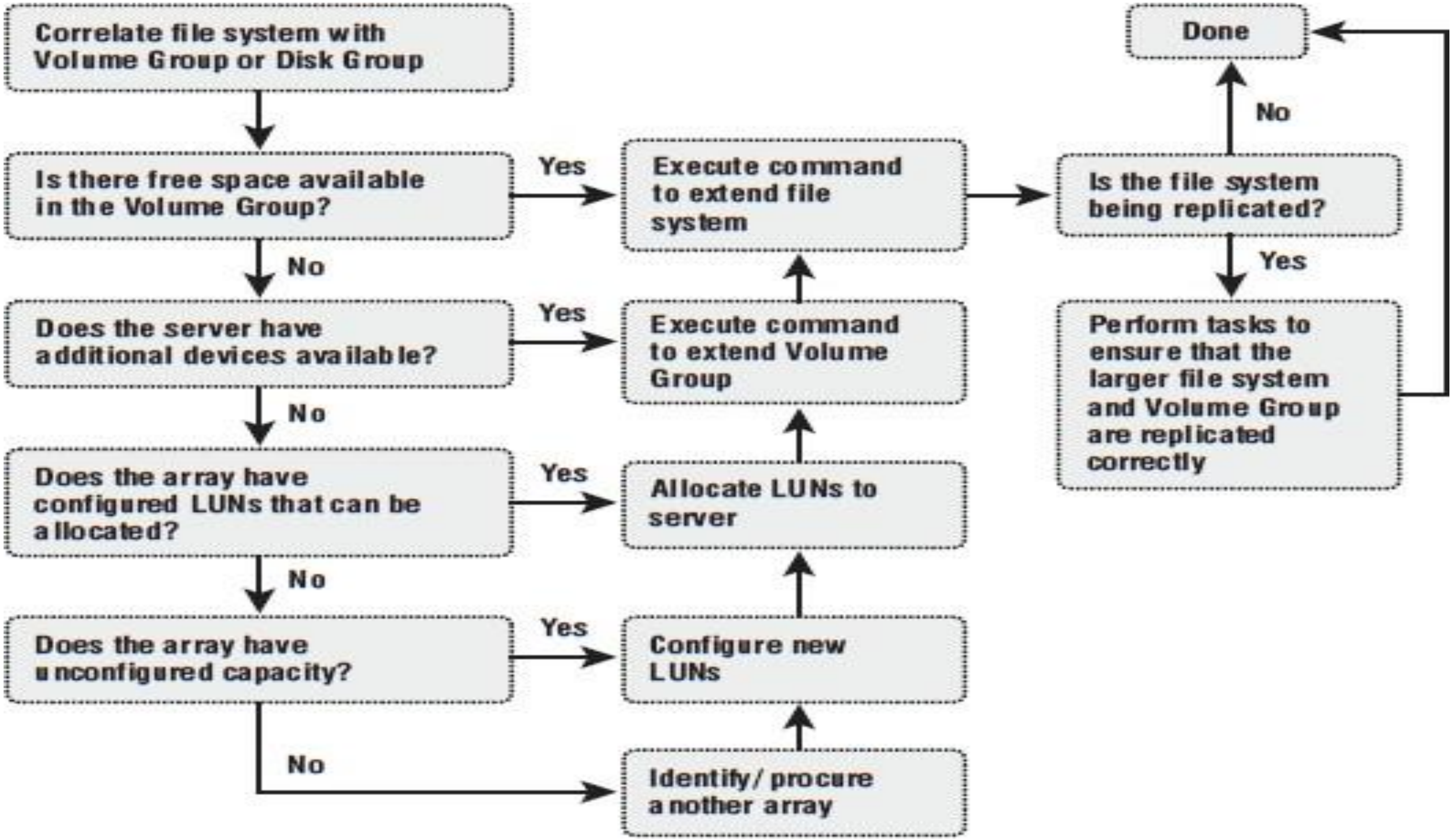
Storage Management Examples

- ***Example : Storage Allocation to a New Server/Host***
  - Consider a deployment of the new RDBMS server to the existing non- virtualized SAN environment.
  - As a part of storage array management activities, the administrator needs to configure new volumes on the array and assign those volumes to the array front-end ports.

- Storage allocation tasks



- ***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 and offloading files to backup media that have not been accessed for a long time.



Correlate file system with Volume Group or Disk Group

Is there free space available in the Volume Group?

Yes

Execute command to extend file system

Is the file system being replicated?

No

Done

Yes

Perform tasks to ensure that the larger file system and Volume Group are replicated correctly

No

Does the server have additional devices available?

Yes

Execute command to extend Volume Group

No

Does the array have configured LUNs that can be allocated?

Yes

Allocate LUNs to server

No

Does the array have unconfigured capacity?

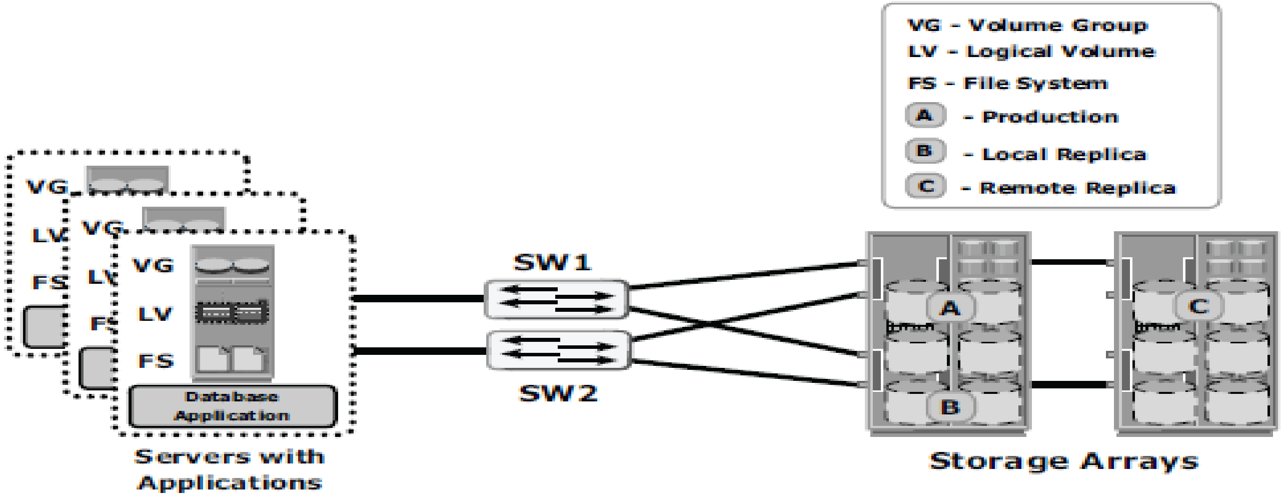
Yes

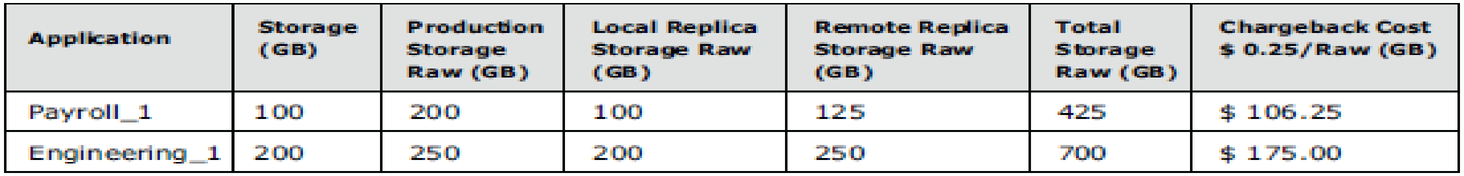
Configure new LUNs

No

Identify/ procure another array

- ***Example 3: Chargeback Report***





Application	Storage (GB)	Production Storage Raw (GB)	Local Replica Storage Raw (GB)	Remote Replica Storage Raw (GB)	Total Storage Raw (GB)	Chargeback Cost $ 0.25/Raw (GB)
Payroll_1	100	200	100	125	425	$ 106.25
Engineering_1	200	250	200	250	700	$ 175.00

Storage Infrastructure Management Challenges

- Monitoring and managing today’s complex storage infrastructure environment has become very challenging due to the number and variety of storage arrays, networks, servers, databases, and applications.
- There is a variety of storage devices varying in capacity, performance, and protection methodologies.
- Storage infrastructures deploy both SAN and IP networks and servers with different operating systems such as UNIX, LINUX, Windows, or mainframe.