UNIT - 4

SLO-1 : Storage Security and Management

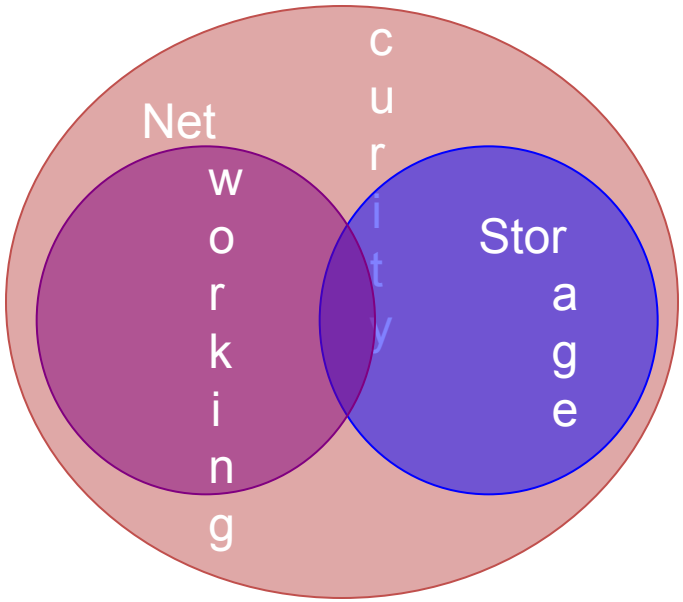
Securing the Storage Infrastructure

- Valuable information, including intellectual property, personal identities, and financial transactions, is routinely processed and stored in storage arrays, which are accessed through the network.
- As a result, storage is now more exposed to various security threats that can potentially damage business-critical data and disrupt critical services.
- It is an intensive and necessary task, essential to managing and protecting vital information

SLO-2 : Information Security Framework

What is Storage Security?

- Application of security principles and practices to storage networking (data storage + networking) technologies
- Focus of storage security: secured access to information
- Storage security begins with building a framework



Storage / Information Security Framework

- The basic information security framework is built to achieve four security goals:
  i. Confidentiality,
  ii. Integrity
  iii. Availability (CIA)
  iv. Accountability
- This framework incorporates all security standards, procedures, and controls, required to mitigate threats in the storage infrastructure environment.

Storage Security Framework Attribute : Confidentiality

- Data confidentiality
  - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
  - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed
- This requires authentication of users who need to access information.
- Data in transit (data transmitted over cables) and data at rest (data residing on a primary storage, backup media, or in the archives) can be encrypted to maintain its confidentiality.
- Requires implementing traffic flow protection measures as part of the security protocol.
- These protection measures generally include hiding source and destination addresses, frequency of data being sent, and amount of data sent

Storage Security Framework Attribute : 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.

Storage Security Framework Attribute : 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 involves that sufficient resources are available to provide a service

Storage Security Framework Attribute : Accountability service

- Accounting for all events and operations that takes place in data center infrastructure that can be audited or traced later
- Helps to uniquely identify the actor that performed an action

Computer Security Terminology

Adversary (threat agent)
An entity that attacks, or is a threat to, a system.

Attack
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Countermeasure
An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Risk
An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Security Policy
A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

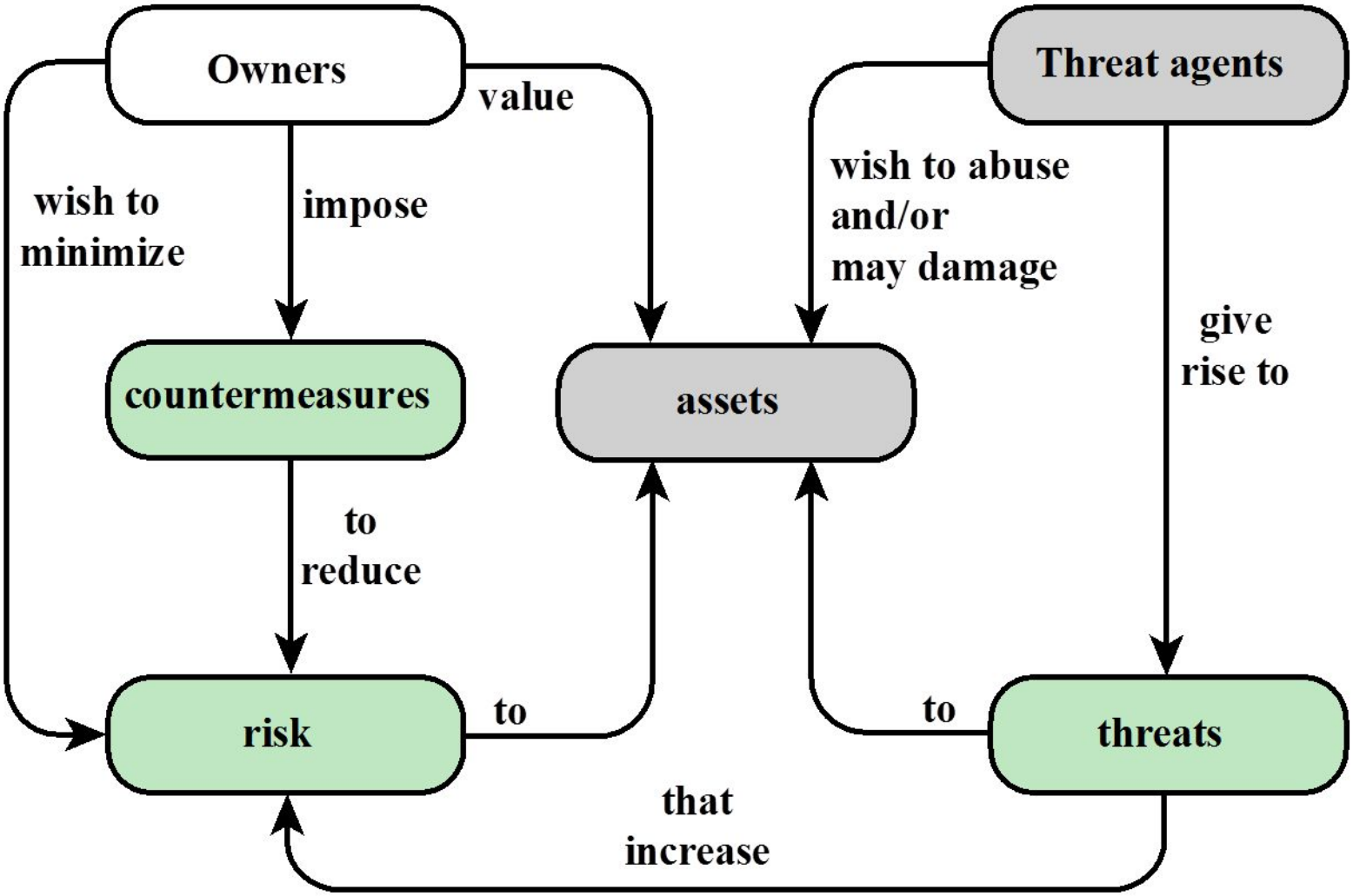
System Resource (Asset)
Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component--hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

Threat
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Vulnerability
A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

SLO : 2
Risk Triad

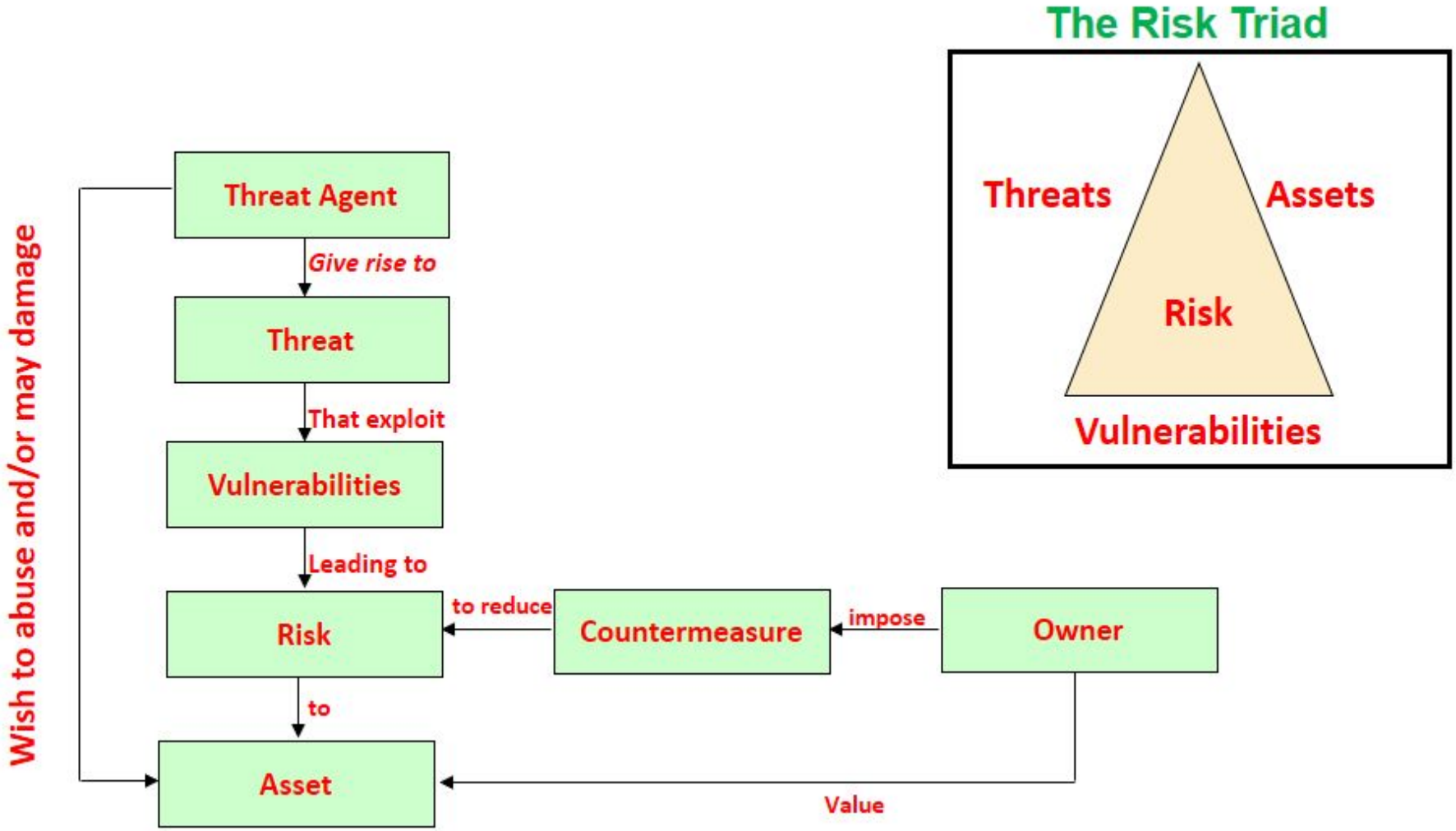
Understanding Security Elements



Risk Triad

- Risk triad defines risk in terms of threats, assets, and vulnerabilities.
- Risk arises when a threat agent (an attacker) uses an existing vulnerability to compromise the security services of an asset,
  - **For example**, if a sensitive document is transmitted without any protection over an insecure channel, an attacker might get unauthorized access to the document and may violate its confidentiality and integrity.
- This may, in turn, result in business loss for the organization.
- In this scenario potential business loss is the risk, which arises because an attacker uses the vulnerability of the unprotected communication to access the document and tamper with it.

Understanding Security elements



Risk Triad...

- To manage risks, organizations primarily focus on vulnerabilities
- Organizations can enforce countermeasures to reduce the possibility of occurrence of attacks and the severity of their impact.
- Risk assessment is the first step to determine the extent of potential threats and risks in an IT infrastructure.
- The process assesses risk and helps to identify appropriate controls to mitigate or eliminate risks.
- Based on the value of assets, risk assessment helps to prioritize investment in and provisioning of security measures.
- To determine the probability of an adverse event occurring, threats to an IT system must be analyzed with the potential vulnerabilities and the existing security controls.

Risk Triad…

- Based on this analysis, a relative value of criticality and sensitivity can be assigned to IT assets and resources.
- For example, a particular IT system component may be assigned a high-criticality value if an attack on this particular component can cause a complete termination of mission-critical services.

The three key elements of the risk triad

1. Assets,
2. Threats
3. Vulnerabilities

Security Elements: Assets

- "Information" – The most important asset
- Other assets
  - Hardware, software, and network infrastructure
- Protecting assets is the primary concern

Security methods have two objectives.

1. Must provide easy access to information assets for authorized users
   - It should also be reliable and stable under disparate environmental conditions and volumes of usage
2. Make it very 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 Elements: Assets

- Security measures should also include,
  - encrypt critical data
  - disable unused services
  - updates to the operating system and other software are installed regularly
  - must provide adequate redundancy in the form of replication and mirroring (ie. to prevent catastrophic data loss if there is an unexpected data compromise)

The effectiveness of a storage security methodology can be measured by two key criteria.

- One, the cost of implementing the system should be a fraction of the value of the protected data.
- Two, it should cost heavily to a potential attacker, in terms of money, effort, and time.

Authenticity & Accountability

Authenticity

- Verifying that users are who they say they are and that each input arriving at the system came from a trusted source

Accountability

- Being able to trace the responsible party/process/entity in case of a security incident or action.

Security Elements: 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

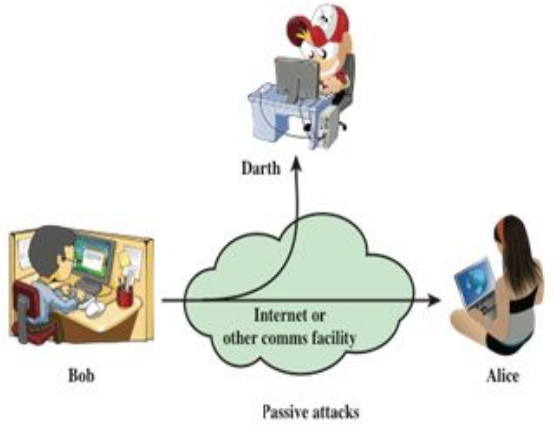
- Attempts to gain unauthorized access into the system
- Threats to confidentiality of information

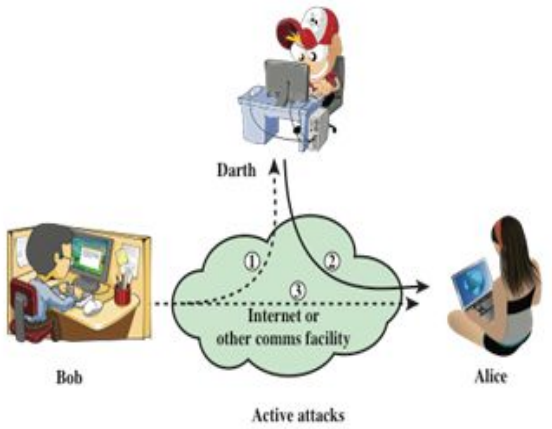
Active attacks includes

i. Data modification,

ii. Denial of Service (DoS),

- Repudiation attacks
- Threats to data integrity, availability and accountability





Attack	Confidentiality	Integrity	Availability	Accountability
Access	√			√
Modification	√	√		√
Denial of Service			√	
Repudiation		√		√

Data modification attack

- Unauthorized user attempts to modify information for malicious purposes.
- A modification attack can target the data at rest or the data in transit
- These attacks pose a threat to data integrity

Denial of Service (DoS)

- Prevent legitimate users from accessing resources and services.
- These attacks generally do not involve access to or modification of information.
- Instead, they pose a threat to data availability
- The intentional flooding of a network or website to prevent legitimate access to authorized users is one example of a DoS attack.

Repudiation

- 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.
- For example, a repudiation attack may involve performing an action and eliminating any evidence that could prove the identity of the user (attacker) who performed that action.
- Repudiation attacks include circumventing(avoiding) the logging of security events or tampering with the security log to conceal(hide) the identity of the attacker.

Security Elements: Vulnerabilities

- Vulnerabilities can occur anywhere in the system
  - An attacker can bypass controls implemented at a single point in the system
  - Implementing security controls at each access point of every access path is known as defense in depth.
  - Requires "defense in depth"
  - Requires "layered approach" - Because there are multiple measures for security at different levels, defense in depth gives additional time to detect and respond to an attack.
  - This can reduce the scope or impact of a security breach.
- Failure anywhere in the system can jeopardize the security of information assets
  - Loss of authentication may jeopardize confidentiality
  - Loss of a device jeopardizes availability

Security Elements: Vulnerabilities (cont.)

- Understanding Vulnerabilities
  - **Attack surface**
    - Refers to various access points/interfaces that an attacker can use to launch an attack
  - **Attack vectors**
    - Series of steps necessary to launch an attack
  - **Work factor**
    - Amount of time and effort required to exploit an attack vector
- Solution to protect critical assets:
  - Minimize the attack surface
  - Maximize the work factor
  - Manage vulnerabilities
    - Detect and remove the vulnerabilities, or
    - Install countermeasures to lessen the impact

Countermeasures to Vulnerability

- Implement countermeasures (safeguards, or controls) in order to reduce the impact of vulnerabilities
- Controls are technical or non-technical
  - Technical
    - implemented in computer hardware, software, or firmware
  - Non-technical
    - Administrative (policies, standards)
    - Physical (guards, gates)
- Controls provide different functions
  - Preventive
    - (avoid the vulnerabilities from being exploited and prevent an attack or reduce its impact)
  - Corrective
    - (reduce the effect of an attack)
  - Detective
    - (discover attacks and trigger preventive or corrective controls)

SLO-2 : Storage Security Domains

Lesson: Storage Security Domains

Upon completion of this lesson, you will be able to:

- Describe the three security domains
  - **Application**
  - **Management**
  - **Backup, Replication, and Archive**
- List the security threats in each domain
- Describe the controls that can be applied

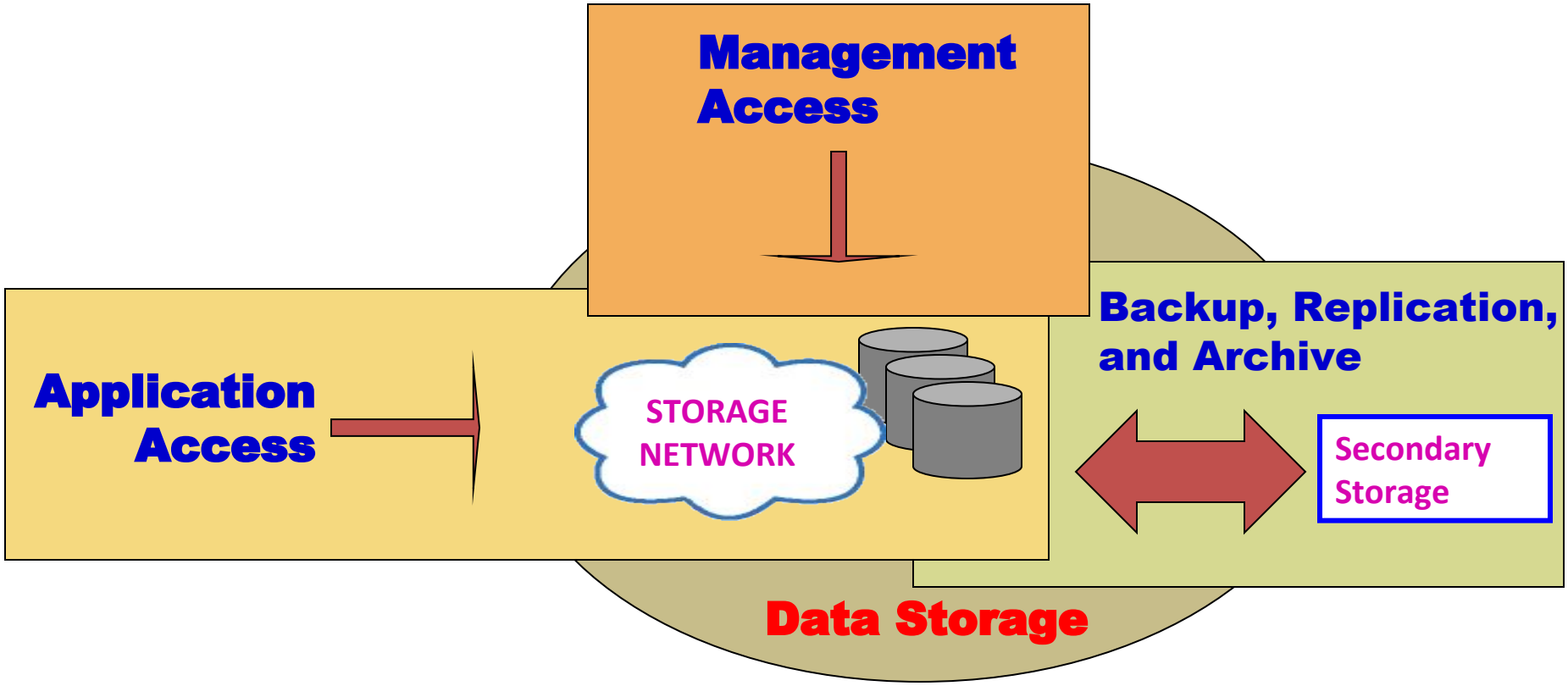
Storage Security Domains...

- Storage devices connected to a network raise the risk level and are more exposed to security threats via networks.
- Increasing use of networking in storage environments, storage devices are becoming highly exposed to security threats from a variety of sources.
- Specific controls must be implemented to secure a storage networking environment.
- This requires a closer look at storage networking security and a clear understanding of the access paths leading to storage resources.
- If each component within the storage network is considered a potential access point, the attack surface of all these access points must be analyzed to identify the associated vulnerabilities.

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:
  i. **Application access**
  ii. **Management access**
  iii. **Backup, Replication, and Archive**
- Figure depicts the three security domains of a storage system environment.

Storage Security Domains



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.
  - 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.

Storage Security Domains…

- To secure the storage networking environment, identify the existing threats within each of the security domains and classify the threats based on the type of security services—
  - availability
  - confidentiality
  - integrity, and
  - accountability
- The next step is to select and implement various controls as countermeasures to the threats.

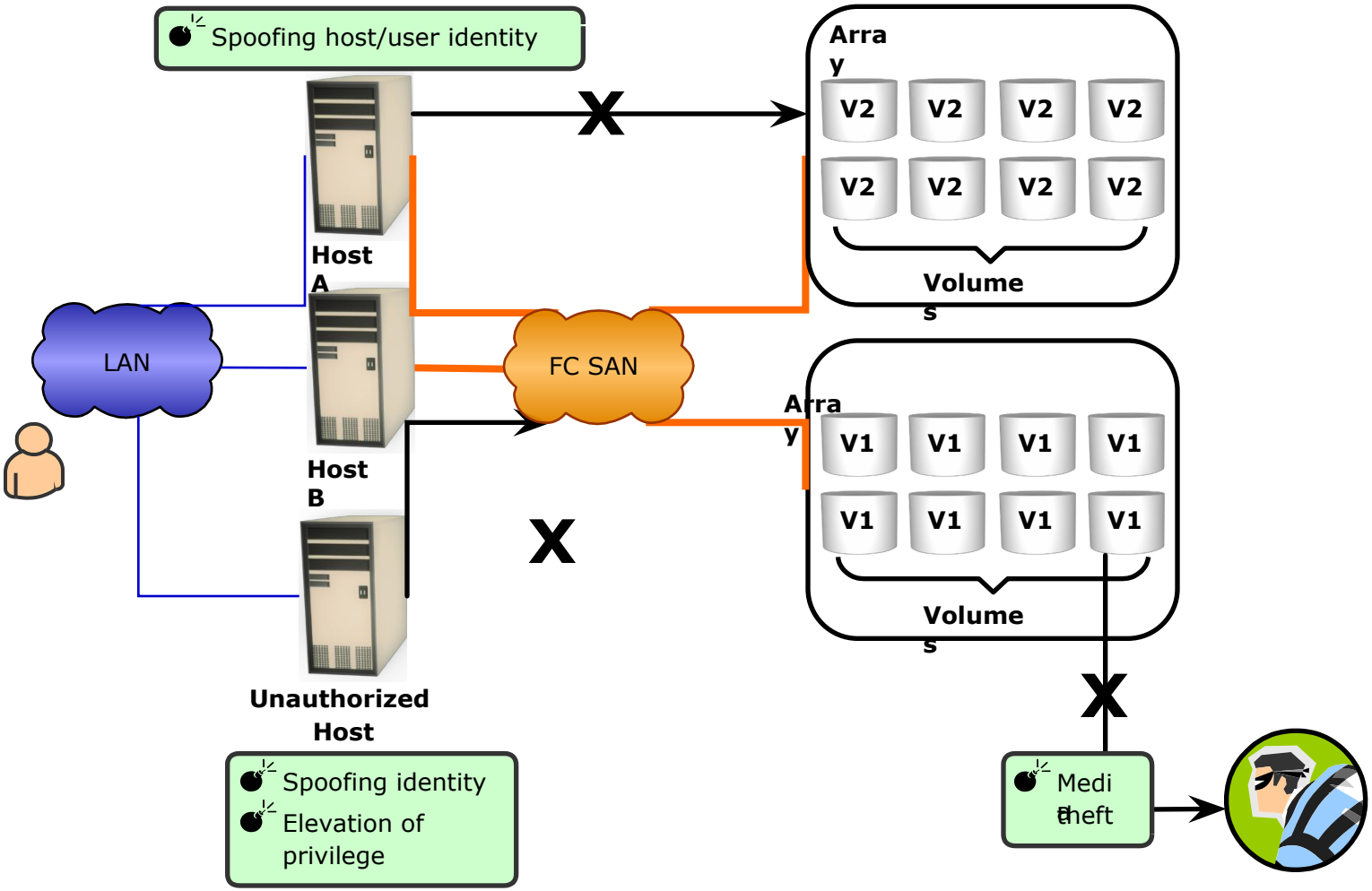
1. Securing the Application Access Domain

- May include only those applications that access the data through the file system or a database interface
- 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

Securing the Application Access Domain…

- Host A can access all V1 volumes; host B can access all V2 volumes.
- Volumes are classified according to the access level, such as ,
  - confidential
  - restricted
  - 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
  - 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.
- Media theft could also compromise security
- These threats can pose several serious challenges to the network security; therefore, they need to be addressed.

Application Access Domain: Threats



Controlling User Access to Data

- Access control services regulate user access to data
- Access control mechanisms used in the application access domain are user and host authentication (technical control) and authorization (administrative control).
- Systems that provide strong authentication and authorization to secure user identities against spoofing.
- NAS devices support the creation of access control lists that regulate user access to specific files.
- After a host has been authenticated, the next step is to specify security controls for the storage resources, such as ports, volumes, or storage pools, that the host is authorized to access.

Controlling User Access to Data

- Zoning is a control mechanism on the switches that segments the network into specific paths to be used for data traffic;
- LUN masking determines which hosts can access which storage devices
- Finally, it is important to ensure that administrative controls,
  - Security policies
  - Standards
  - Regular auditing is required to ensure proper functioning of administrative controls

Protecting the Storage Infrastructure

- Securing the storage infrastructure from unauthorized access involves protecting all the elements of the infrastructure.
- Protecting the network fall into two general categories:
  - Network infrastructure integrity
  - Storage network encryption

- Controls for ensuring the infrastructure integrity include a fabric switch function that ensures fabric integrity.
- This is achieved by preventing a host from being added to the SAN fabric without proper authorization.
- Storage network encryption methods include the use of IPSec for protecting IP-based storage networks, and FC-SP for protecting FC networks
  - FC – SP : Fibre Channel Security Protocol

Protecting the Storage Infrastructure…

- In secure storage environments, root or administrator privileges for a specific device are not granted to every user.
- Instead, role-based access control (RBAC) is deployed to assign necessary privileges to users, enabling them to perform their roles.
- A role may represent a job function
- Finally, physical access to the device console and the cabling of FC switches must be controlled to ensure protection of the storage infrastructure.
- All other established security measures fail if a device is physically accessed by an unauthorized user; this access may render the device unreliable.

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
  - media theft, which compromises data availability and confidentiality
- To protect against these threats,
  - encrypt the data held on the storage media or encrypt the data prior to being transferred to the disk.

Data Encryption

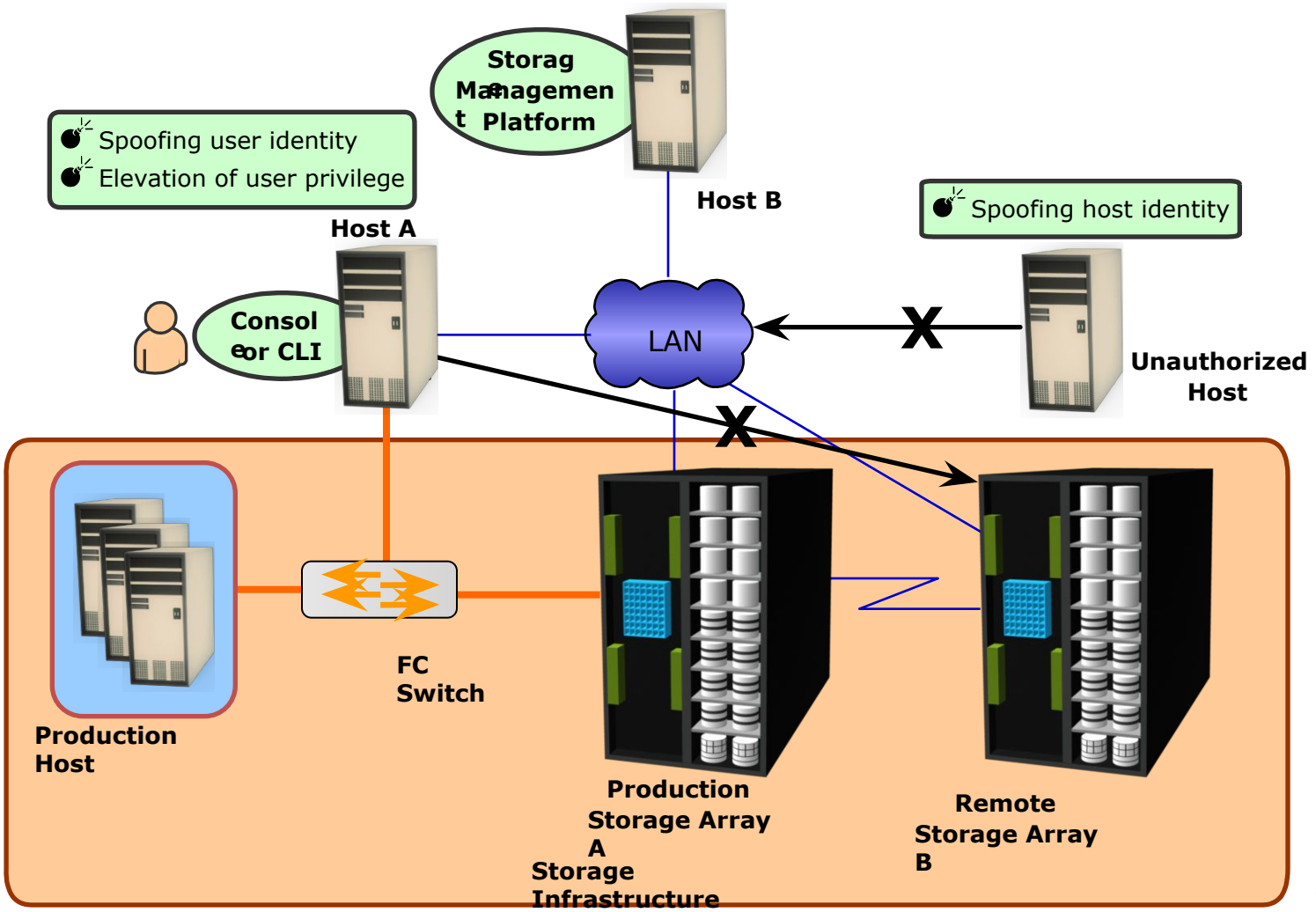
- Data should be encrypted as close to its origin as possible.
- If it is not possible to perform encryption on the host device, an encryption appliance can be used for encrypting data at the point of entry into the storage network.
- Encryption devices can be implemented on the fabric that encrypts data between the host and the storage media.
- These mechanisms can protect both the data at rest on the destination device and data in transit.
- CAS(Content-Addressed Storage), use of MD5 or SHA-256 cryptographic algorithms guarantees data integrity by detecting any change in content bit patterns.

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.

Note : CLI is a **Command Line** program that accepts text input to execute operating system functions.

Management Access Domain: Threats



Securing the Management Access Domain

- 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 also 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.

Securing the Management Access Domain

- 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.
- Event logs should be placed outside the shared storage systems where they can be reviewed if the storage is compromised.

Securing the Management Access Domain

- The storage management platform must be validated for available security controls and ensures that these controls are adequate to secure the overall storage environment.

Controlling Administrative Access

- To storage aims to safeguard against the threats of an attacker spoofing an administrator's identity or elevating privileges to gain administrative access.
- Both of these threats affect the integrity of data and devices.
- To protect against these threats, administrative access regulation and various auditing techniques are used to enforce accountability of users and processes.
- Access control should be enforced for each storage component.
- In some storage environments, it may be necessary to integrate storage devices with third-party authentication directories, such as Lightweight Directory Access Protocol (LDAP) or Active Directory

Controlling Administrative Access

- Security best practices ,
  - no single user should have ultimate control over all aspects of the system
  - number of activities requiring administrative privileges should be minimized
  - Auditing logged events is a critical control measure to track the activities of an administrator
  - access to administrative log files and their content must be protected

Protecting the Management Infrastructure

- Mechanisms to protect the management network infrastructure include
  - encrypting management traffic
  - enforcing management access controls
  - applying IP network security
  - use of IP routers and Ethernet switches to restrict the traffic to certain devices
- Access controls need to be enforced at the storage-array level,
  - to specify which host has management access to which array
  - Some storage devices and switches can restrict management access to particular hosts and limit the commands that can be issued from each host

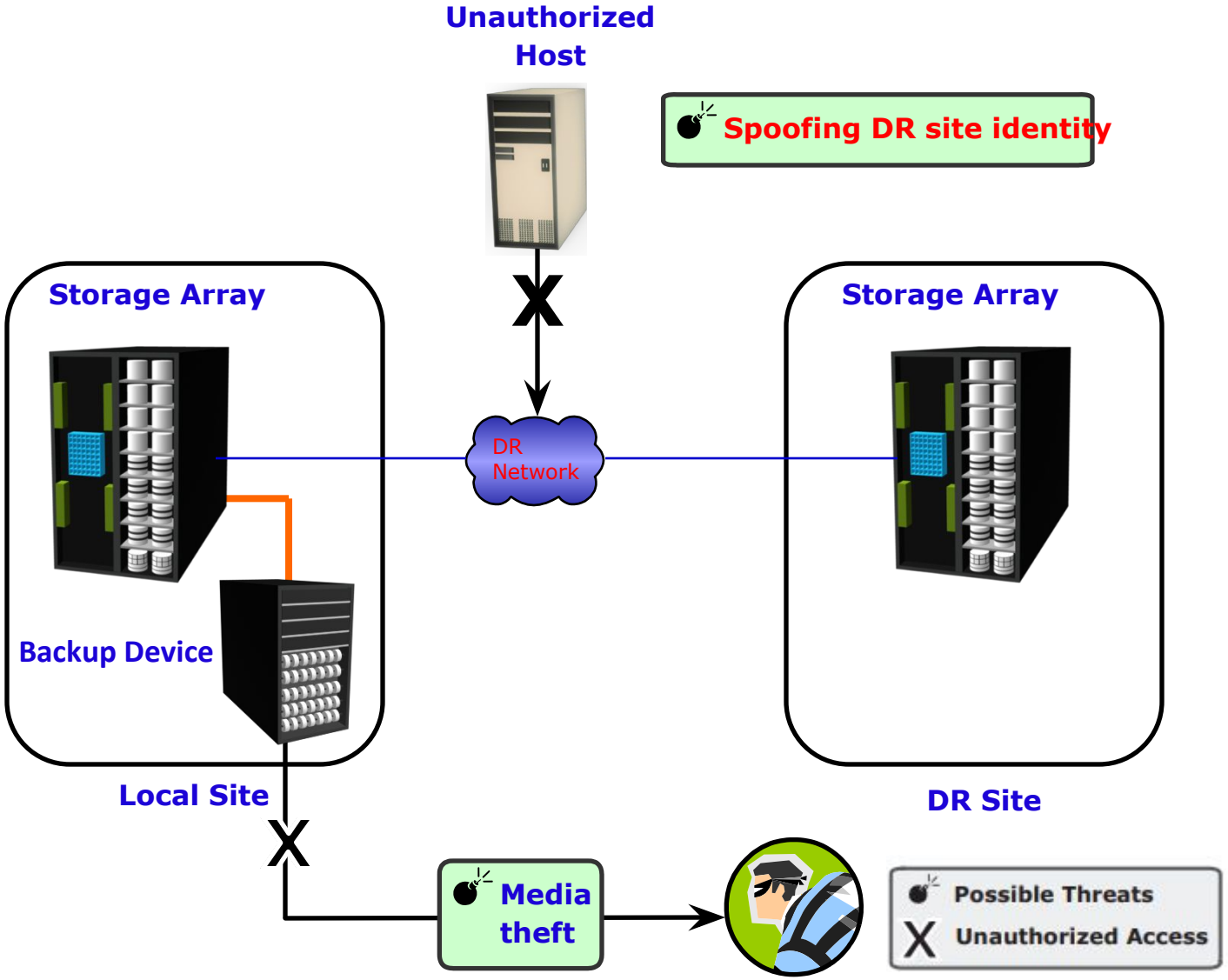
Protecting the Management Infrastructure

- A separate private management network is highly recommended for management traffic
- Unused network services must be disabled on every device within the storage network.
- This decreases the attack surface for that device by minimizing the number of interfaces through which the device can be accessed.
- To summarize, security enforcement must focus on
  - the management communication between devices
  - confidentiality
  - integrity of management data
  - availability of management networks and devices

3. Securing Backup, Replication, and Archive

- It's 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
- 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
  - media theft
- Such threats represent potential violations of integrity, confidentiality, and availability.

Protecting the Management Infrastructure



Securing Backup, Replication, and Archive

- Figure 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.
- In a remote backup solution where the storage components are separated by a network, the threats at the transmission layer need to be countered.
- Otherwise, an attacker can spoof the identity of the backup server and request the host to send its data.
- The unauthorized host claiming to be the backup server may lead to a remote backup being performed to an unauthorized and unknown site.
- In addition, attackers can use the DR network connection to
  - tamper with data
  - snoop the network
  - create a DoS attack against the storage devices

Securing Backup, Replication, and Archiv

- The physical threat of a backup tape being
  - lost
  - stolen, or misplaced
- Especially if the tapes contain highly confidential 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.

SLO : 1
Security Implementations in Storage Networking

Security Implementations in Storage Networking

- The basic security implementations,
  - **FC SAN**
  - **IP-SAN environments**
  - **NAS**

FC SAN

- Traditional FC SANs enjoy 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.
- Consequently, FC SANs impose fewer security threats.
- However, scenario has changed with storage consolidation and larger SAN design that span multiple sites across the enterprise

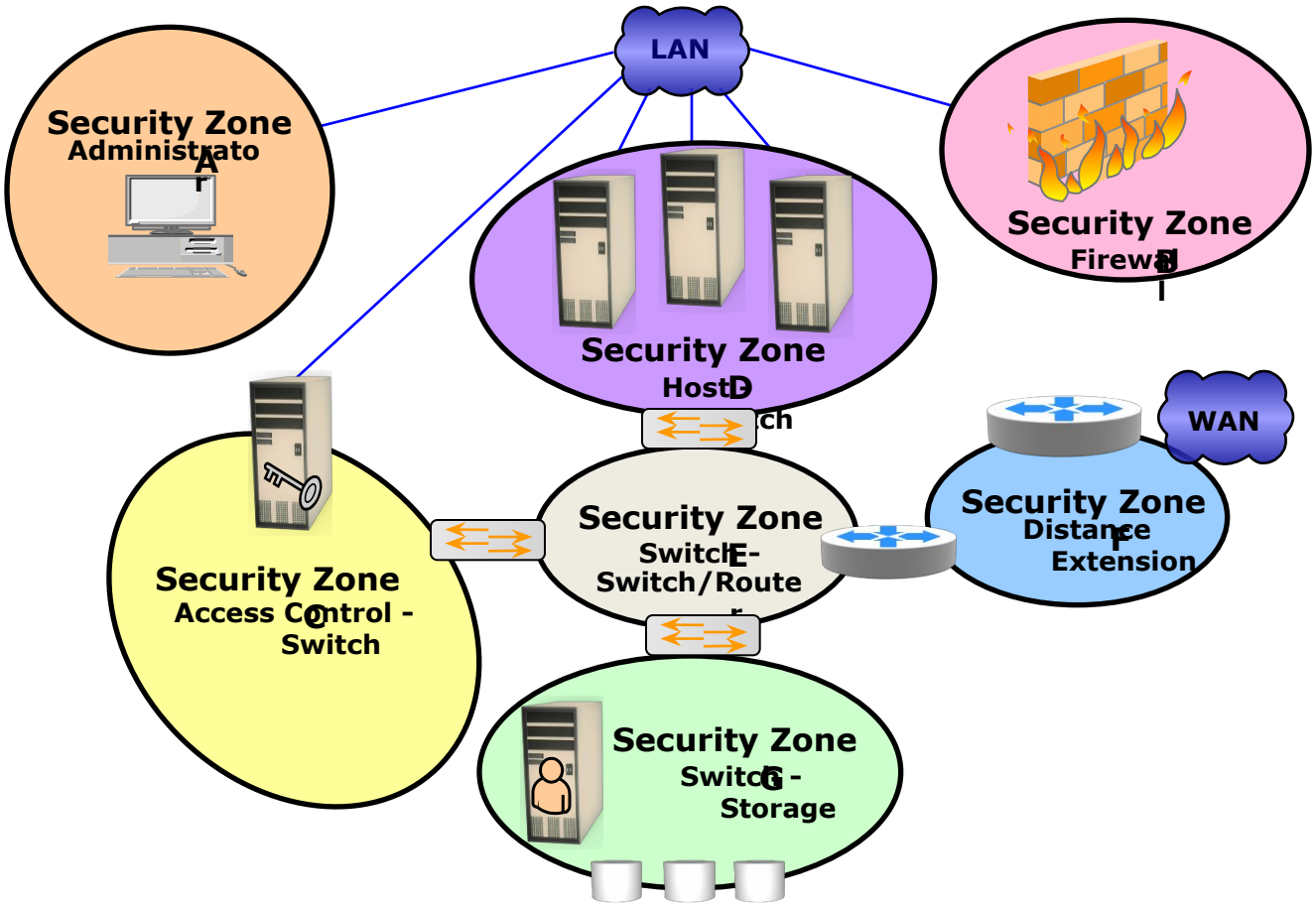
FC SAN

- FC-SP (Fibre Channel Security Protocol)
  - Align(support) security mechanisms and algorithms between IP and FC interconnects
- This standards describe guidelines for:
  - Authenticating FC entities
  - Setting up session keys
  - Negotiating parameters required to ensure frame-by-frame integrity and confidentiality

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.
- So, security strategies are based on the *defense in depth* concept-multiple integrated layers of security.
- Ensures that the failure of one security control will not compromise the assets under protection.

SAN Security Architecture – "defense-in-depth"



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

Two-factor authentication

- Table provides a comprehensive list of protection strategies that must be implemented in various security zones.
- Some of the security mechanisms listed in Table 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
  - an additional security component such as a smart card for authentication

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) (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) (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.
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	Protect the storage arrays on your SAN via (a) WWPNbased LUN masking; and (b) S_ID locking: masking based on source FC address.

Basic SAN Security Mechanisms

Most commonly used SAN security methods,

1. **LUN masking and zoning**
2. **Securing switch ports**
3. **Switch-wide and fabric-wide access control**
   - **RBAC (Role based access control)**
4. **Logical partitioning of a fabric (Virtual SAN)**

1. LUN Masking and Zoning

- LUN masking on storage arrays mask the LUNs presented to a frontend storage port based on the WWPNs of the source HBAs.
- Also can be done on the basis of source FC addresses.
- Offers a mechanism to lock down the FC address of a given node port to its WWN.
- World Wide Name — A vendor-supplied, 64-bit globally unique identifier number assigned to nodes and ports in a fabric.)
- *WWPN zoning is the preferred choice* in security-conscious environments.

2. Securing Switch Ports

Can be implemented using following methods,

a) **Port binding**

b) **Port lock down & Port lockout**

c) **Persistent port disable**

2. Security on FC Switch Ports

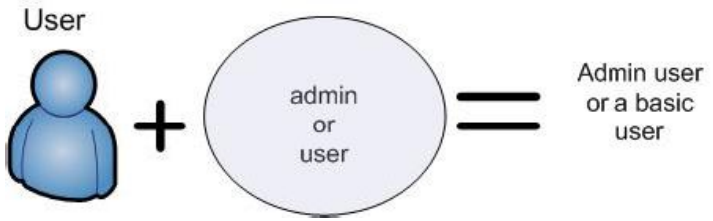
- Port Binding
  - Limits devices that can attach to a particular switch port
  - A node must be connected to its corresponding switch port for fabric access
    - Mitigates – but does not eliminate - WWPN spoofing
- Port Lockdown, Port Lockout
  - Restricts the type of initialization of a switch port
  - Typical variants include:
    - Port cannot function as an E-Port; cannot be used for ISL, e.g. to a rogue switch
    - Port role is restricted to just FL-Port, F-Port, E-Port, or some combination
- Persistent Port Disable
  - Prevents a switch port from being enabled, even after a switch reboot

3. 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.

3. Switch-wide and Fabric-wide Access Control...

- Access Control Lists (ACLs)
  - Typically implemented policies may include
    - Device Connection Control
      - Prevents unauthorized devices (identified by WWPN) from accessing the fabric
    - Switch Connection Control
      - Prevents unauthorized switches (identified by WWN) from joining the fabric
- Fabric Binding
  - Prevents unauthorized switch from joining any existing switch in the fabric
- RBAC
  - Specifies which user can have access to which device in a fabric

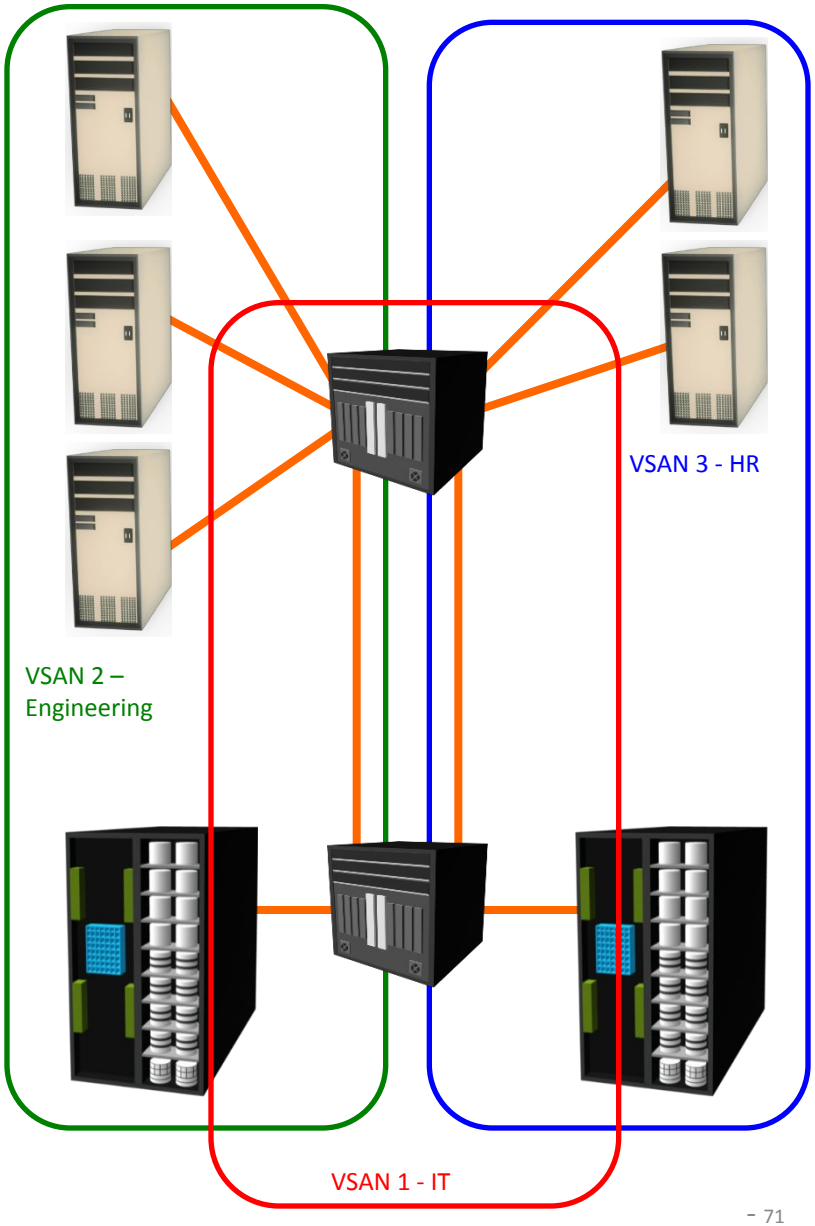


3. Switch-Wide and Fabric-Wide Access Control..

- It ensures that authorized membership data exists on every switch and any attempt to connect any switch in the fabric by using an ISL causes the fabric to segment.
- Role-based access control provides additional security to a SAN by preventing unauthorized 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 zone admin role can modify the zones on the fabric, whereas a basic user may view only fabric related information, such as port types and logged-in nodes.

4. Logical Partitioning of a Fabric: VSAN

- Dividing a physical topology into separate logical fabrics
  - Administrator allocates switch ports to different VSANs
  - A switch port (and the HBA or storage port connected to it) can be in only one VSAN at a time
  - Each VSAN has its own distinct active zone set and zones
- Fabric Events (e.g. RSCNs – (Registered state change notification)) in one VSAN are not propagated to the others
- Role-based management
  - can be on a per-VSAN basis



IP SAN

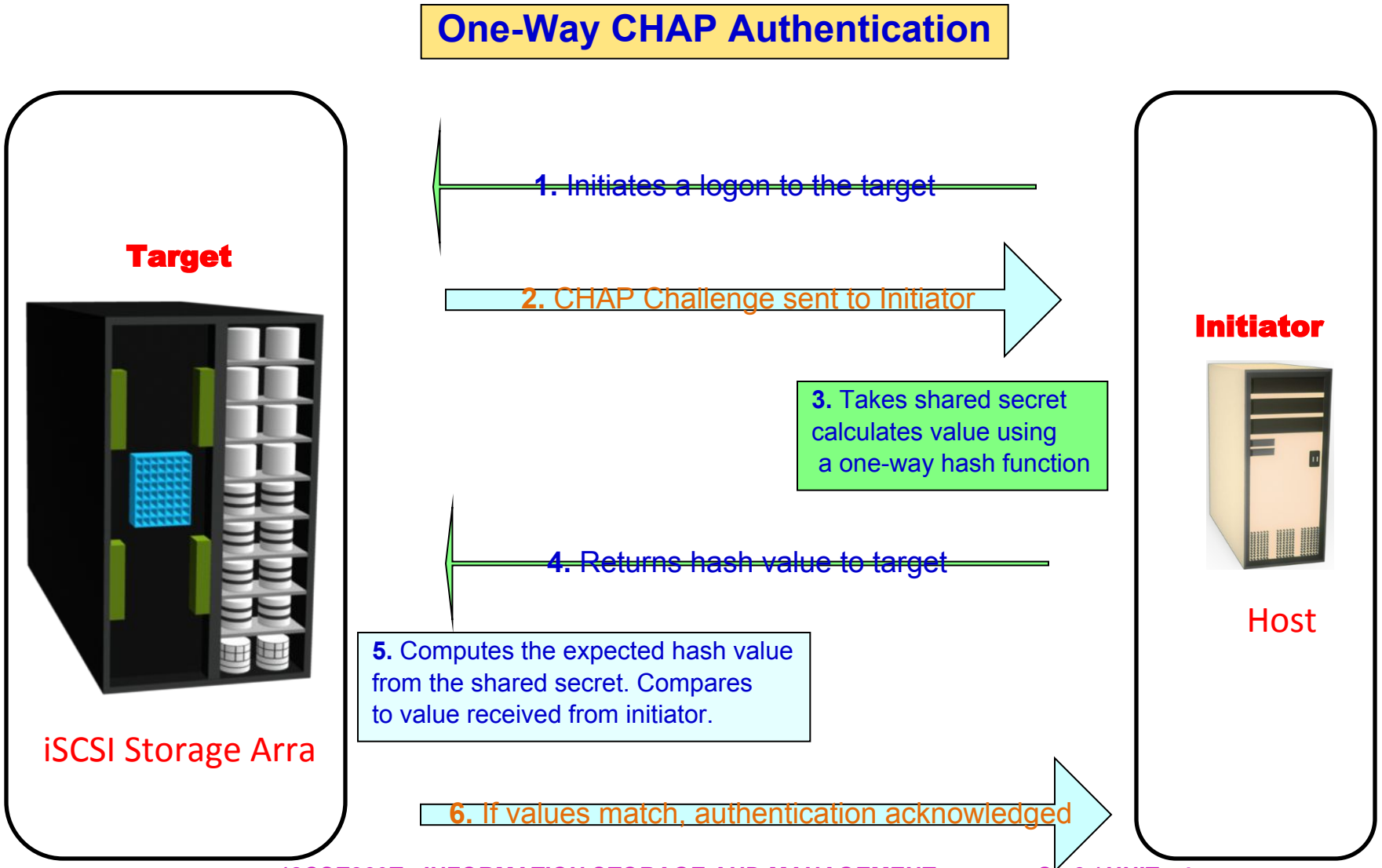
Securing Implementation in IP SAN

- Challenge-Handshake Authentication Protocol (CHAP)
  - Basic Authentication Mechanism
  - Authenticates a user to a network resource
  - 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
  - Implemented as:
    - **One way**
      - Authentication password configured on only one side of the connection
    - **Two way**
      - Authentication password configured on both sides of the connection, requiring both nodes to validate the connection e.g. mutual authentication

Securing Implementation in IP SAN

- 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.

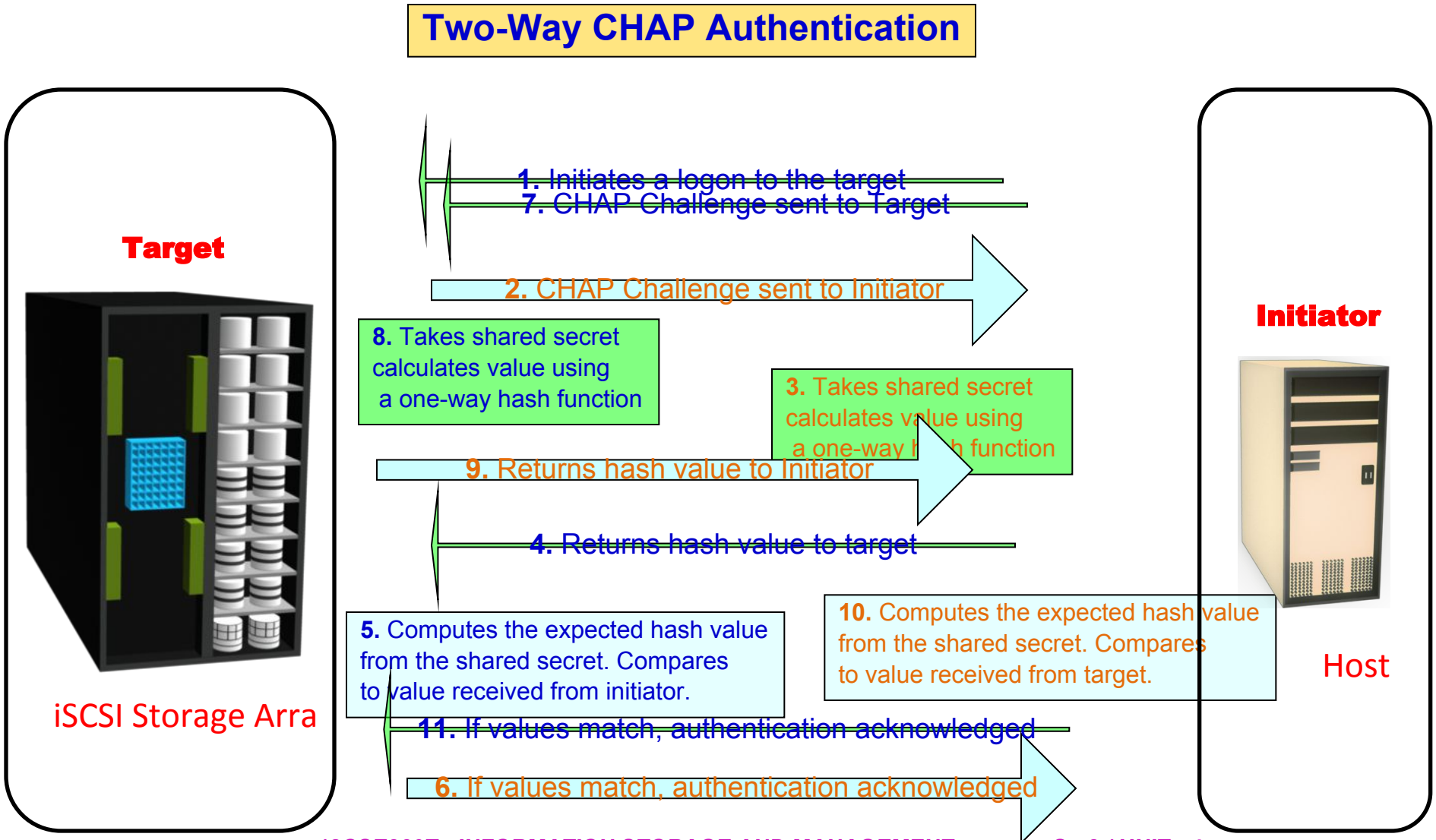
Securing IPSAN with CHAP authentication



Two-way 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.

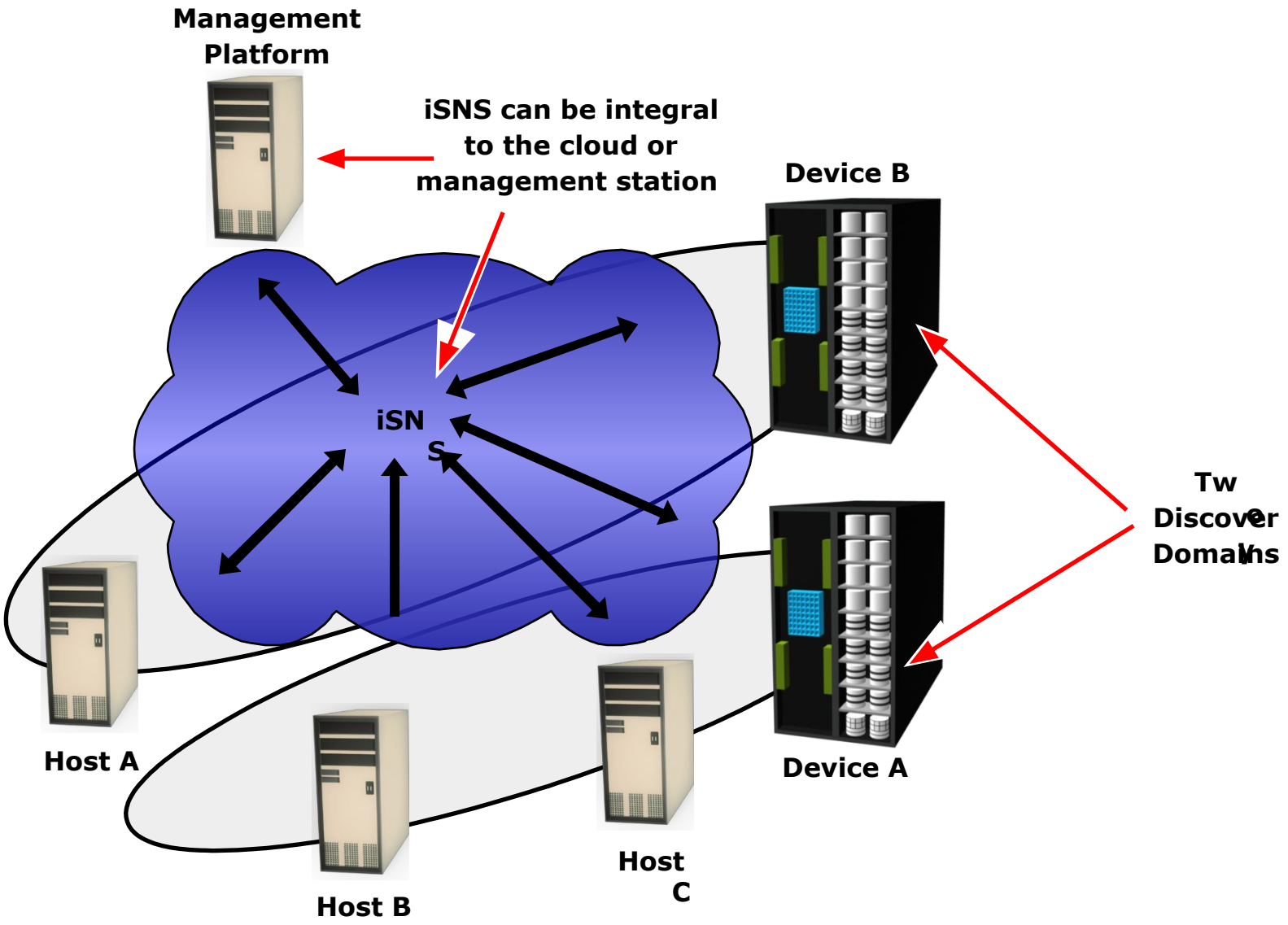
Two-Way CHAP Authentication



iSNS discovery domains function

- iSNS(**Internet Storage Name Service**) 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.

Securing IPSAN with iSNS discovery domains



NAS

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.
- Authentication and authorization mechanisms
  - Kerberos and Directory services
    - Identity verification
  - Firewalls
    - Protection from unauthorized access and malicious attacks

NAS File Sharing: Windows ACLs

- Types of ACLs
  - Discretionary access control lists (DACL)
    - Commonly referred to as ACL
    - Used to determine access control
  - System access control lists (SACL)
    - Determines what accesses need to be audited if auditing is enabled
- Object Ownership
  - Object owner has hard-coded rights to that object
    - Rights do not have to be explicitly granted in the SACL
  - Child objects within a parent object automatically inherit the ACLs
- SIDs
  - ACLs applied to directory objects
    - User ID/Login ID is a textual representation of true SIDs
  - Automatically created when a user or group is created

NAS File Sharing: UNIX Permissions

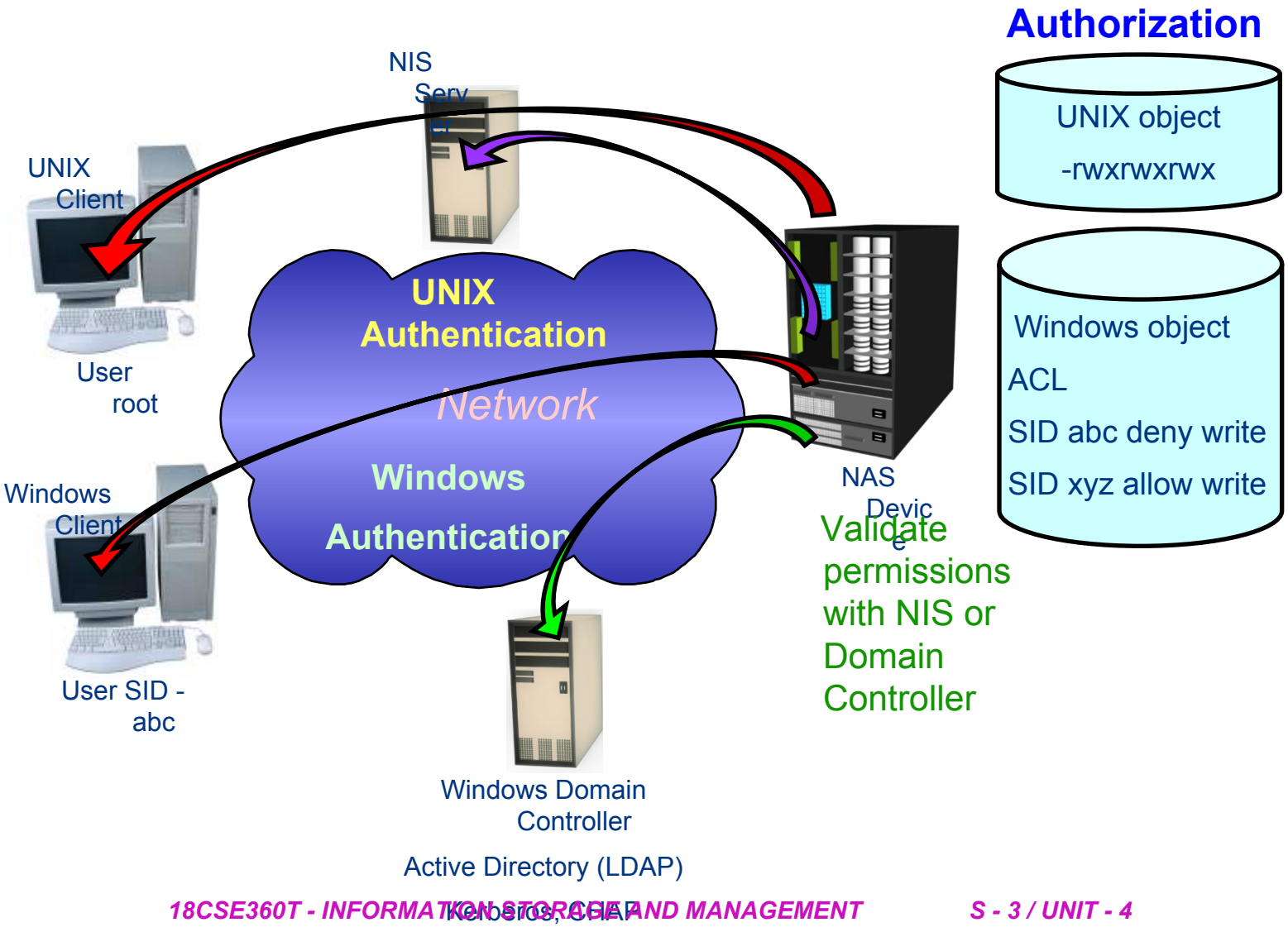
- User
  - A logical entity for assignment of ownership and operation privileges
  - Can be either a person or a system operation
  - Can be organized into one or more groups
- Permissions tell UNIX what can be done with that file and by whom
- Common Permissions
  - Read/Write/Execute
- Every file and directory (folder) has three access permissions:
  - rights for the file owner
  - rights for the group you belong to
  - rights for all others in the faculty
- File or Directory permission looks:
  - # rwx rwx rwx (Owner, Group, Others)
  - # : d for directory, - for file

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.
- 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.

Securing user access in a NAS environment

- Windows and UNIX Considerations



Kerberos

- A network authentication protocol
  - provide strong authentication for client/server applications by using secret-key cryptography
  - A client can prove its identity to a server (and vice versa) 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).

Kerberos

- 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

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. (This step is not explicitly shown in Figure)

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 session key and the resource information to the KDC.

The Kerberos authentication process

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

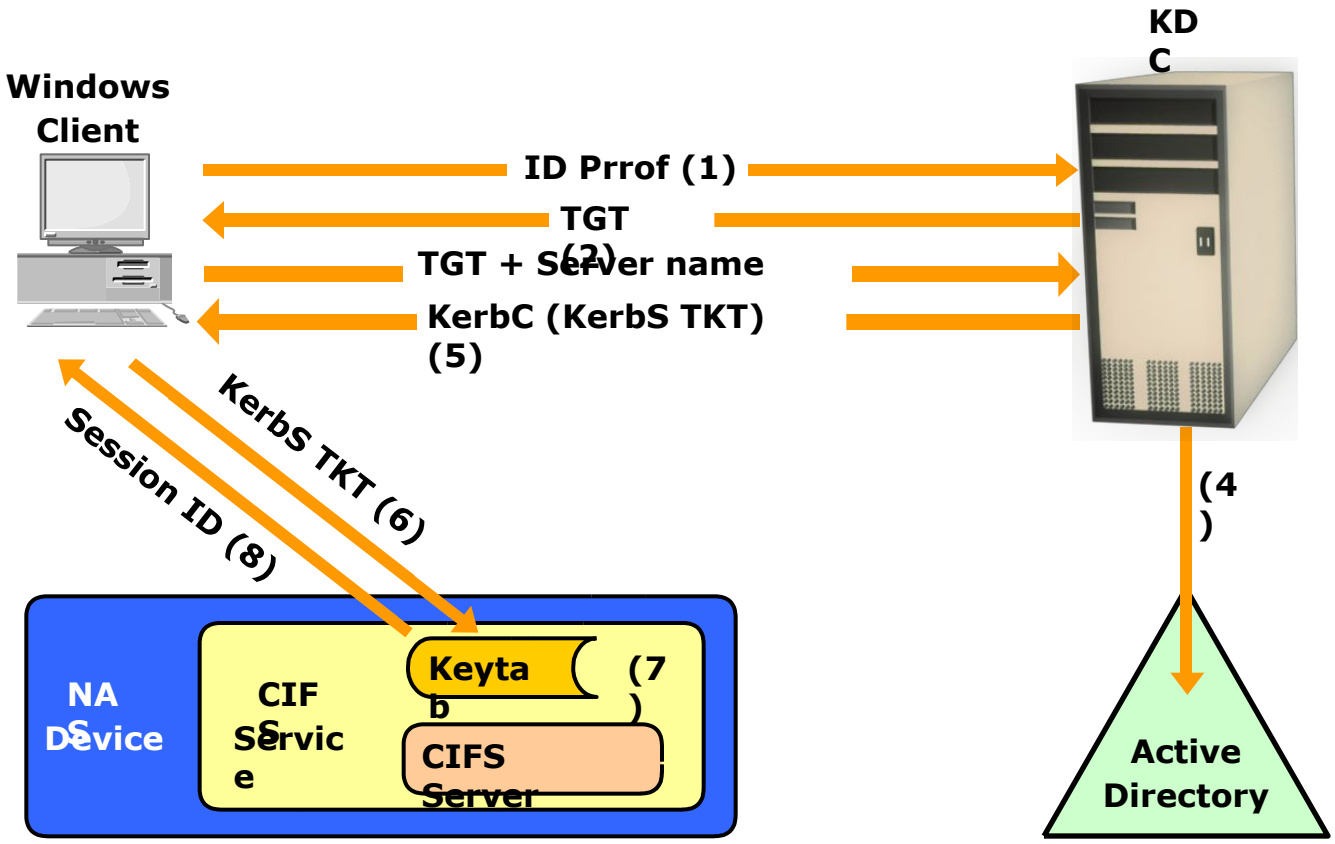
5. The KDC returns a service ticket to the client. This service ticket contains fields addressed to the client and to the server hosting the service.

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 keytab 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.

Kerberos authorization



CIFS - Common Internet File System

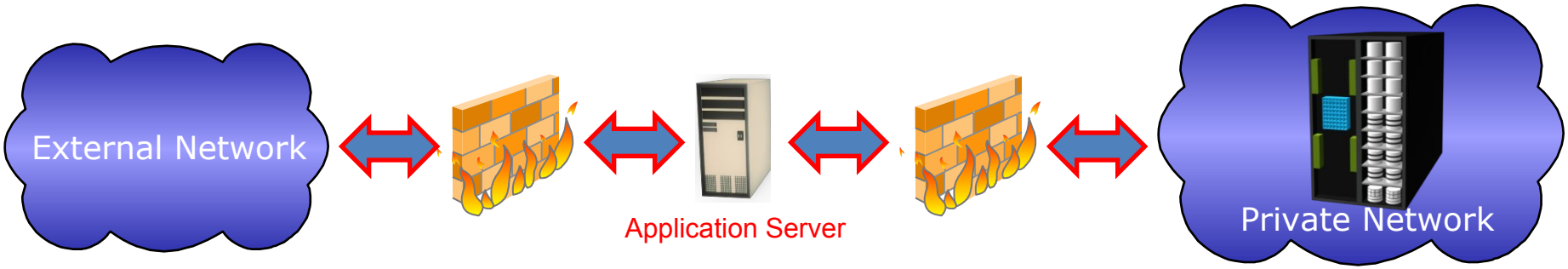
Network-Layer Firewalls

- 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 configured 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).

Network-Layer Firewalls...

- 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.
- However, no Internet-based traffic is allowed to penetrate the second set of firewalls and gain access to the internal network.

Network Layer Firewalls



Demilitarized Zone (DMZ)

SLO : 1
Securing Storage Infrastructure in Virtualized and Cloud Environments

Securing Storage Infrastructure in Virtualized and Cloud Environments

- These environments have additional threats due to multitenancy and lack of control over the cloud resources
- Virtualization-specific security concerns are common for all cloud models
- In public clouds, there are additional security concerns, which demand specific countermeasures
  - Clients have less control to enforce security measures in public clouds
  - Difficult for cloud service provider(CSP) to meet the security needs of all the clients

Security Concerns

- Multitenancy
  - Enables multiple independent tenants to be serviced using the same set of storage resources
    - Co-location of multiple VMs in a single server and sharing the same resources increase the attack surface
- Velocity of attack
  - Any existing security threat in the cloud spreads more rapidly and has larger impact than that in the traditional data center
- Information assurance and data privacy

Security Measures

- Securing compute
  - Securing physical server, VMs, and hypervisor
- Securing network
  - Virtual firewall
    - Provides packet filtering and monitoring of the VM-to-VM traffic
  - DMZ and data encryption
- Securing storage
  - Access control and data encryption
  - Use separate LUNs for VM configuration files and VM data
  - Segregate VM traffic from management traffic

SLO : 1 & 2
RSA and VMware Security Products

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.
- Provides a brief introduction to RSA SecureID, RSA Identity and Access Management, RSA Data Protection Manager, and VMware vShield.

RSA SecureID

- RSA SecurID two-factor authentication provides an added layer of security to ensure that only valid users have access to systems and data.
  - RSA SecurID is based on something a user knows (a password or PIN)
  - something a user has (an authenticator device).
- It provides a much more reliable level of user authentication than reusable passwords.
- It generates a new one-time password code every 60 seconds.
- To access their resources, users combine their secret Personal Identification Number (PIN) with the token code that appears on their SecurID authenticator display at that given time.
- The result is a unique, one-time password to assure a user's identity

RSA Identity and Access Management

- The RSA Identity and Access Management product provides,
  - identity, security, and access-controls management for physical, virtual, and
  - cloud-based environments through access management.
- It enables trusted identities to freely and securely interact with systems and access.
- The RSA Identity and Access Management family has two products:
  - RSA Access Manager
  - RSA Federated Identity Manager
- RSA Access Manager enables organizations to centrally manage authentication and authorization policies for a large number of users, online web portals, and application resources.
- Access Manager provides seamless user access with Single Sign-On (SSO) and preserves identity context for greater security.

RSA Data Protection Manager

- The RSA Data Protection Manager family is composed of two products:
  1. Application Encryption and Tokenization
  2. Enterprise Key Management
- Application Encryption and Tokenization with RSA Data Protection Manager helps to prevent data loss.
  - It works at the point of creation, ensuring that the data stays encrypted as it is transmitted and stored.
- Enterprise key management is an easy-to-use management tool for encrypting keys at the database, file server, and storage layers.
  1. It also helps to ensure that information is properly secured and fully accessible when needed at any point in its life cycle.

VMware vShield

- The VMware vShield family includes three products:
  1. vShield App
  2. vShield Edge
  3. vShield Endpoint
- VMware vShield App is a hypervisor-based application-aware firewall solution.
  - VMware vShield App observes network activity between virtual machines to define and refine firewall policies and secure business processes through detailed reporting of application traffic
- VMware vShield Edge provides comprehensive perimeter network security for a virtualized environment.
  - It provides many services including firewall, VPN, and Dynamic Host Configuration Protocol (DHCP) services.

VMware vShield

- VMware vShield Endpoint consists of a hardened special security VM with a third party antivirus software.
- VMware vShield Endpoint streamlines and accelerates antivirus and antimalware deployment because antivirus engine and signature files are updated only within the special security VM.
- VMware vShield Endpoint improves VM performance by offloading file scanning and other tasks from VMs to the security VM.
- It also satisfies audit requirements with detailed logging of antivirus and antimalware activities

SLO – 1 :
Monitoring the Storage Infrastructure

Storage Infrastructure Management

- Managing storage infrastructure is key to ensures continuity of business
- Establishing management processes and implementing appropriate tools is essential to meeting service levels proactively
- Management activities include availability, capacity, performance, and security management
- Monitoring is the most important aspects that forms basis for storage management
- Continuous monitoring enables availability and scalability by taking proactive measures

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. It also enables administrators to perform essential management activities.
- Monitoring also helps to analyze the utilization and consumption of various storage infrastructure resources.
- This analysis facilitates capacity planning, forecasting, and optimal use of these resources.
- Storage infrastructure environment parameters such as heating and power supplies are also monitored.

SLO – 2 :
Monitoring Parameters

Monitoring Parameters

- Storage infrastructure components should be monitored for accessibility, capacity, performance, and security

Accessibility

- To identify failure of any component that may lead to service unavailability or degraded performance

Capacity

- To ensure availability of adequate amount of resources and prevent service unavailability or degraded performance

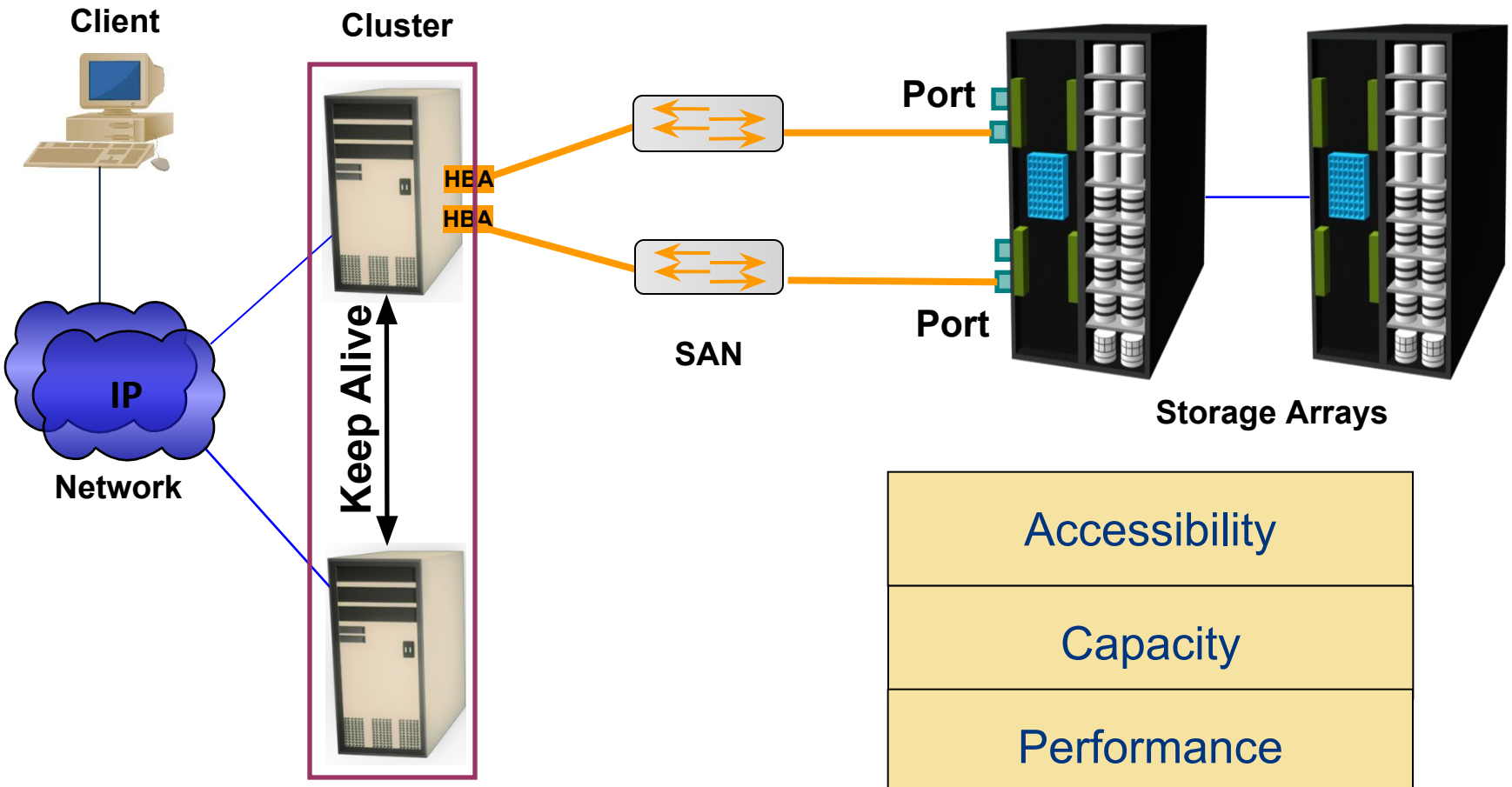
Performance

- To evaluate efficiency and utilization of components and identify bottlenecks

Security

- To ensure confidentiality, integrity, and availability of storage infrastructure

Monitoring Storage Infrastructure



- Accessibility
- Capacity
- Performance
- Security

Accessibility

- Accessibility refers to the availability of a component to perform its desired operation during a specified time period.
- Monitoring the accessibility of hardware components (for example, a port, an HBA, or a disk drive) or software component (for example, a database) involves checking their availability status by reviewing the alerts generated from the system.
- Failure of a component might cause an outage that affects application availability, or it might cause performance degradation even though accessibility is not compromised.
- Continuously monitoring for expected accessibility of each component and reporting any deviation helps the administrator to identify failing components and plan corrective action to maintain SLA(service-level agreement) requirements.

Capacity

- Capacity refers to the amount of storage infrastructure resources available.
- Inadequate capacity leads to degraded performance or even application/service unavailability.
- Capacity monitoring ensures uninterrupted data availability and scalability by avoidance outages before they occur.
- For example, if 90 percent of the ports are utilized in a particular SAN fabric, this could indicate that a new switch might be required if more arrays and servers need to be installed on the same fabric.
- Capacity monitoring usually help to understand future resource requirements and provide an estimation on the time line to deploy them.

Performance

- Performance monitoring evaluates how efficiently different storage infrastructure components are performing and helps to identify bottlenecks.
- Performance monitoring measures and analyzes behavior in terms of response time or the ability to perform at a certain predefined level.
- It also deals with the utilization of resources, which affects the way resources behave and respond.
- Performance measurement is a complex task that involves assessing various components on several interrelated parameters.
- The number of I/Os performed by a disk, application response time, network utilization, and server-CPU utilization are examples of performance parameters that are monitored.

Security

- Monitoring a storage infrastructure for security helps to track and prevent unauthorized access, whether accidental or malicious.
- Security monitoring helps to track unauthorized configuration changes to storage infrastructure resources.
- Security monitoring also detects unavailability of information to authorized users due to a security breach.
- Physical security of a storage infrastructure can also be continuously monitored using badge readers, biometric scans, or video cameras.

SLO – 1 :
1. Components Monitored
2. Monitoring Examples

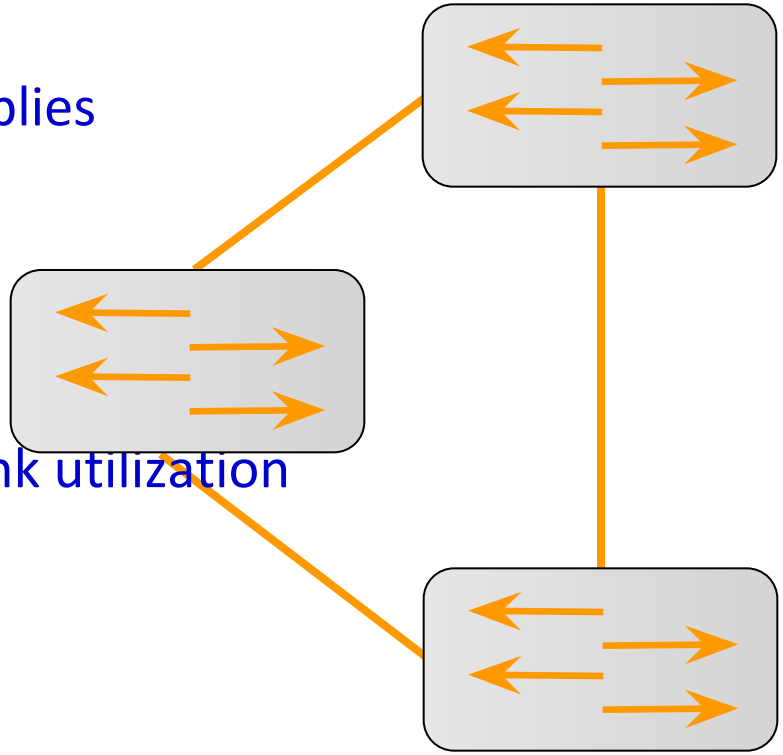
1. Components Monitored

Monitoring Hosts

- Accessibility
  - Hardware components: HBA, NIC, graphic card, internal disk – (failure might cause inaccessibility)
  - Status of various processes/applications
- Capacity
  - File system utilization
  - Database: Table space/log space utilization
  - User quota
- Performance
  - CPU and memory utilization
  - Transaction response times
- Security
  - Login and authorization
  - Physical security (Data center access)

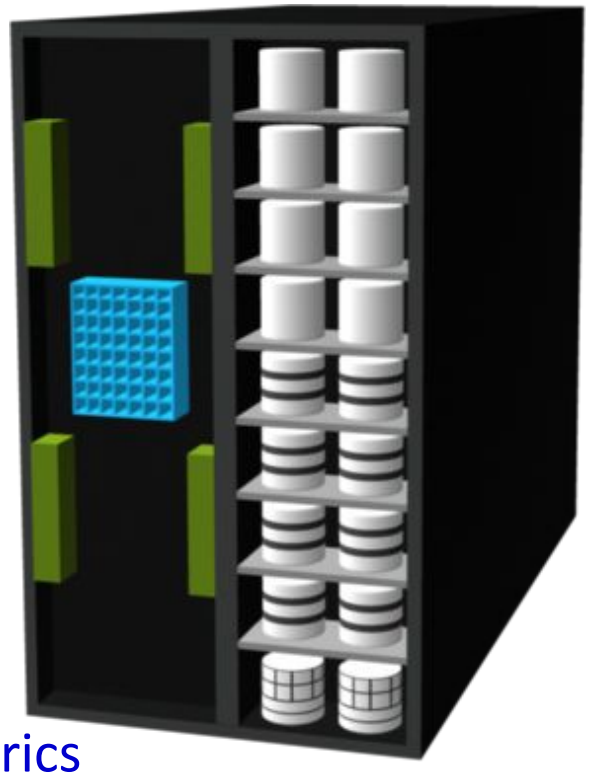
Monitoring the SAN

- Accessibility
  - Fabric errors, zoning errors, GBIC (Gigabit Interface Converter) failure
  - Device status/attribute Change
  - Processor cards, fans, power supplies
- Capacity
  - ISL(Inter-Switch Link) and port utilization
- Performance
  - Connectivity ports
    - Link failures, Loss of signal, Link utilization
  - Connectivity devices
    - Port statistics
- Security
  - Zoning and LUN Masking
  - Administrative Tasks and physical security
    - Authorized Access, Strict Passwords



Monitoring Storage Arrays

- Accessibility
  - All Hardware components
  - Array Operating Environment
    - RAID processes
    - Environmental Sensors
    - Replication processes
- Capacity
  - Configured/un-configured capacity
  - Allocated/unallocated storage
  - Fan-in/fan-out ratios
- Performance
  - FE and BE utilization/throughput
  - I/O profile, response time, cache metrics
- Security
  - Physical and administrative security



Storage Array

2. Monitoring Examples

Monitoring Examples

- A storage infrastructure requires implementation of an end-to-end solution to actively monitor all the parameters of its components.
- Early detection and preemptive alerting ensure uninterrupted services from critical assets.
- In addition, the monitoring tool should analyze the impact of a failure and deduce the root cause of symptoms

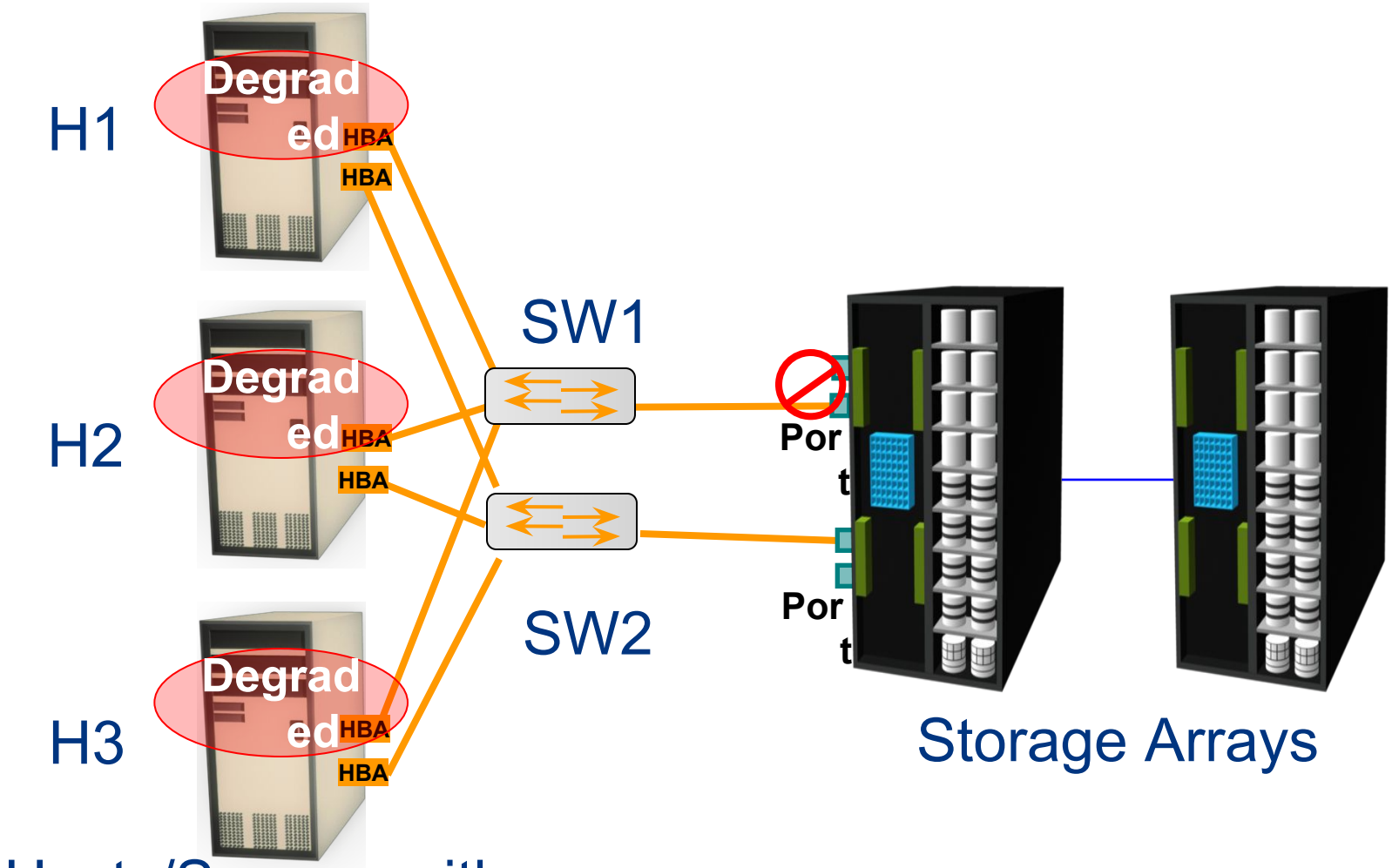
Accessibility Monitoring

- 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
- All the servers share two storage ports on the storage array and multipathing software is installed on all the servers.

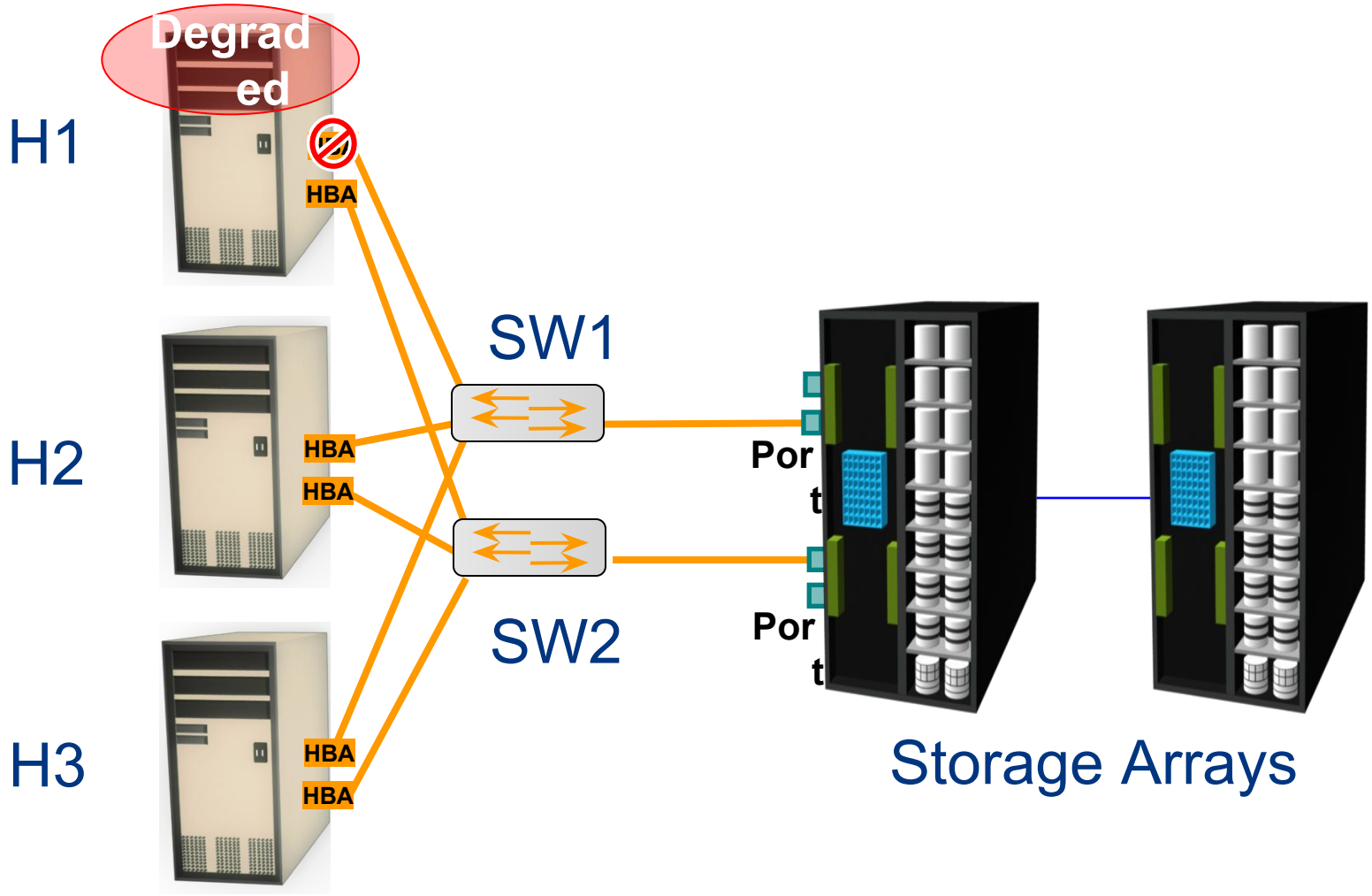
Accessibility Monitoring

- 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.
- However, 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.

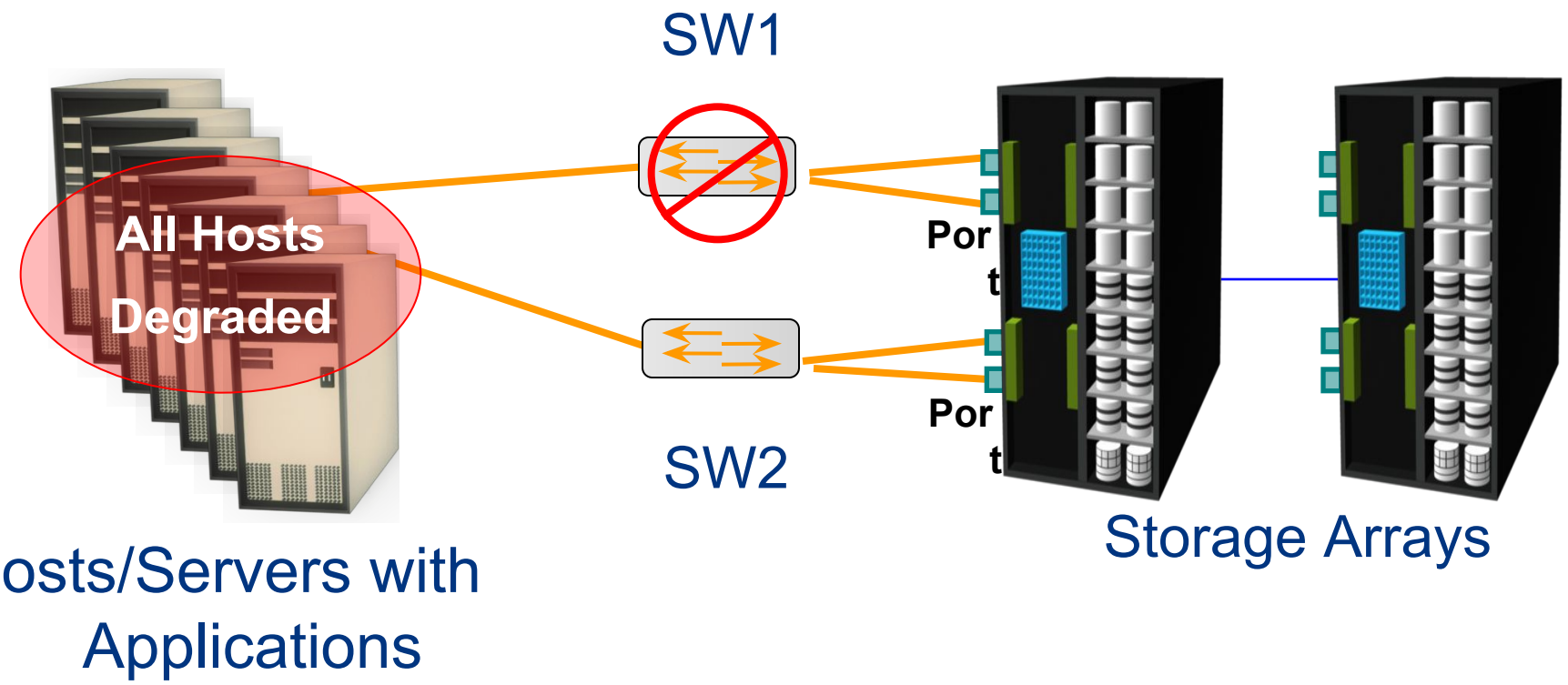
Accessibility Monitoring Example: Array Port Failure



Accessibility Monitoring Example: HBA Failure



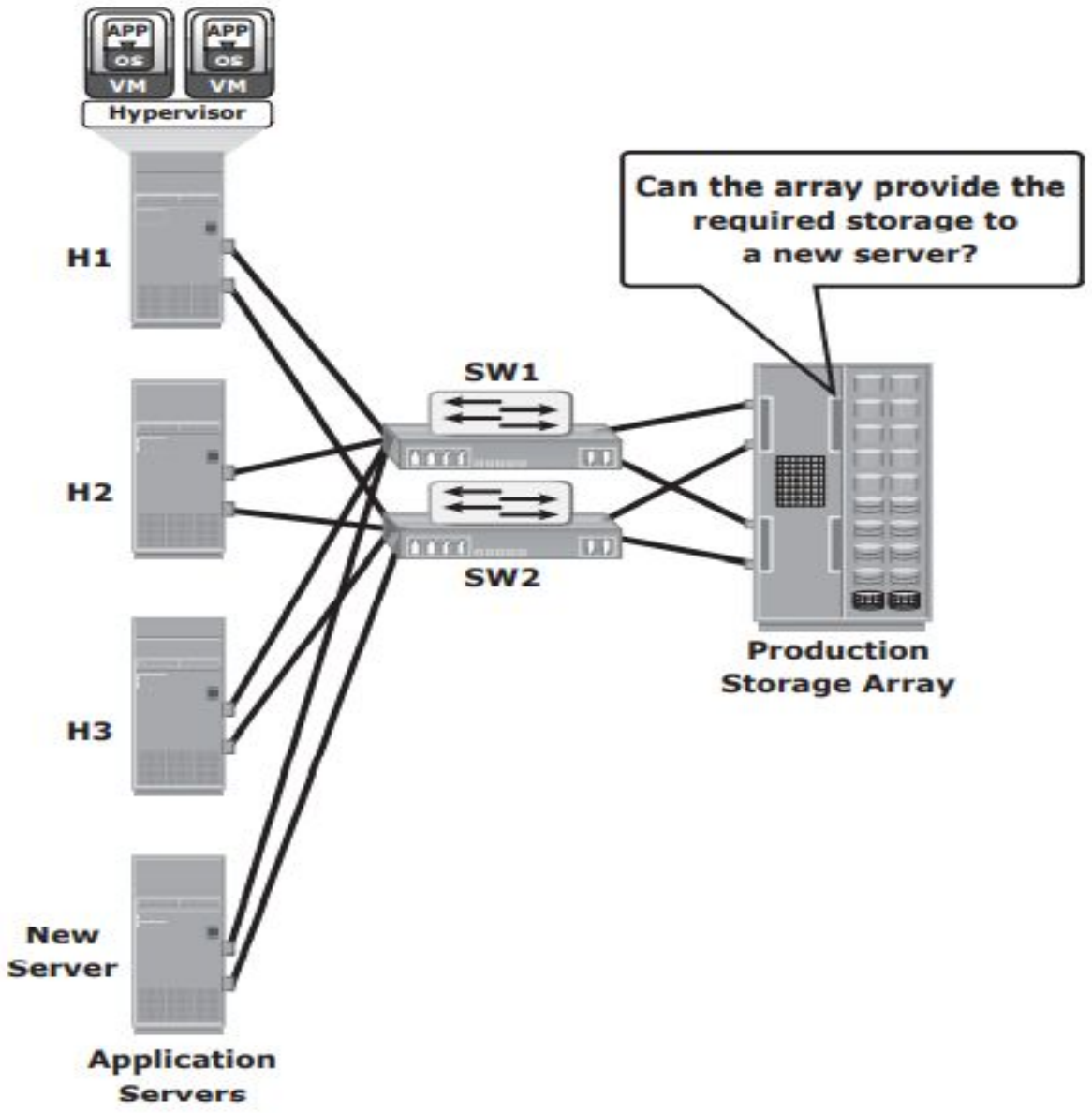
Accessibility Monitoring Example: Switch Failure



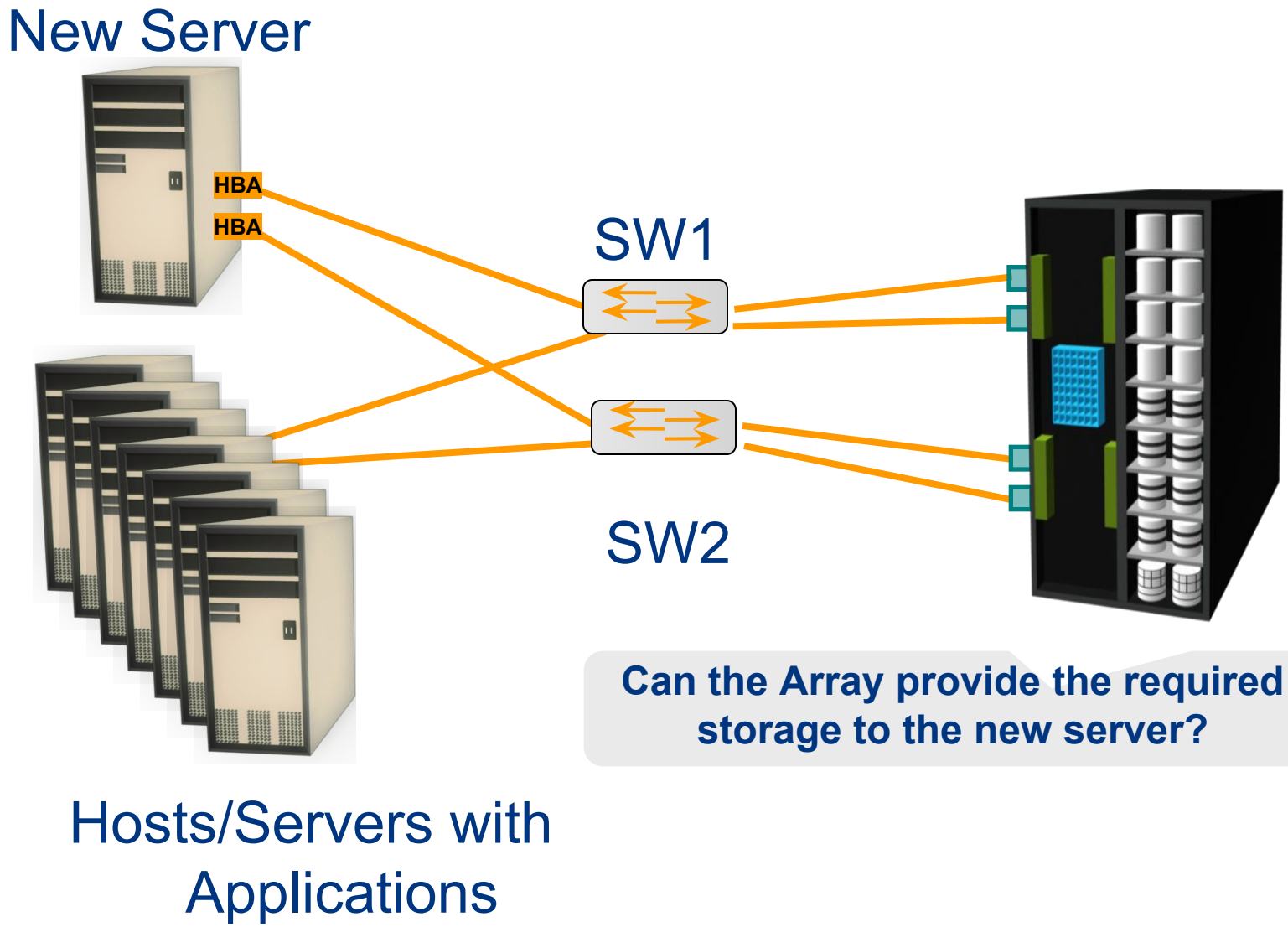
Capacity Monitoring

- 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 (configurable and unallocated) on the array helps to proactively 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.

Monitoring storage array capacity



Capacity Monitoring Example: Storage Array

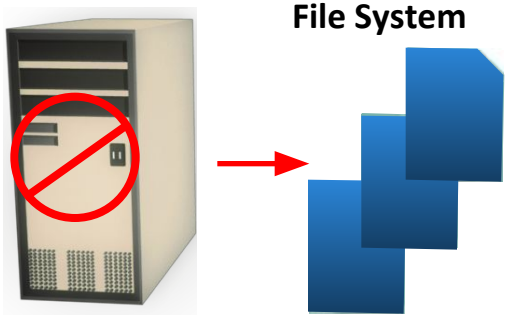


Monitoring server file system space

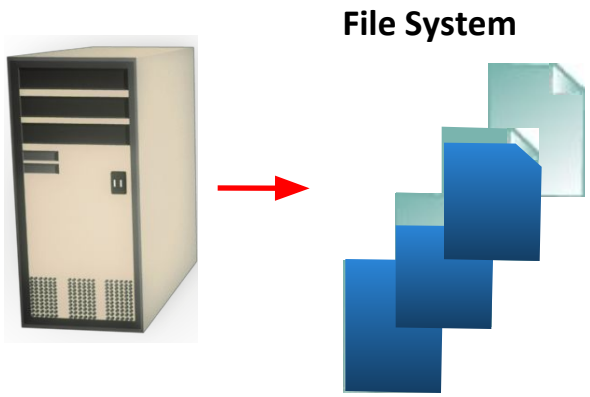
- Figure illustrates the environment of a file system when full and that results in application outage when no capacity monitoring is implemented.
- Monitoring can be configured to issue a message when thresholds are reached on the file system capacity.
- For example, when the file system reaches 66 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
- 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 lac of file system space

Capacity Monitoring Example: File System Space

No Monitoring



FS Monitoring



Extend FS

Warning: FS is 66% Full

Critical: FS is 80% Full

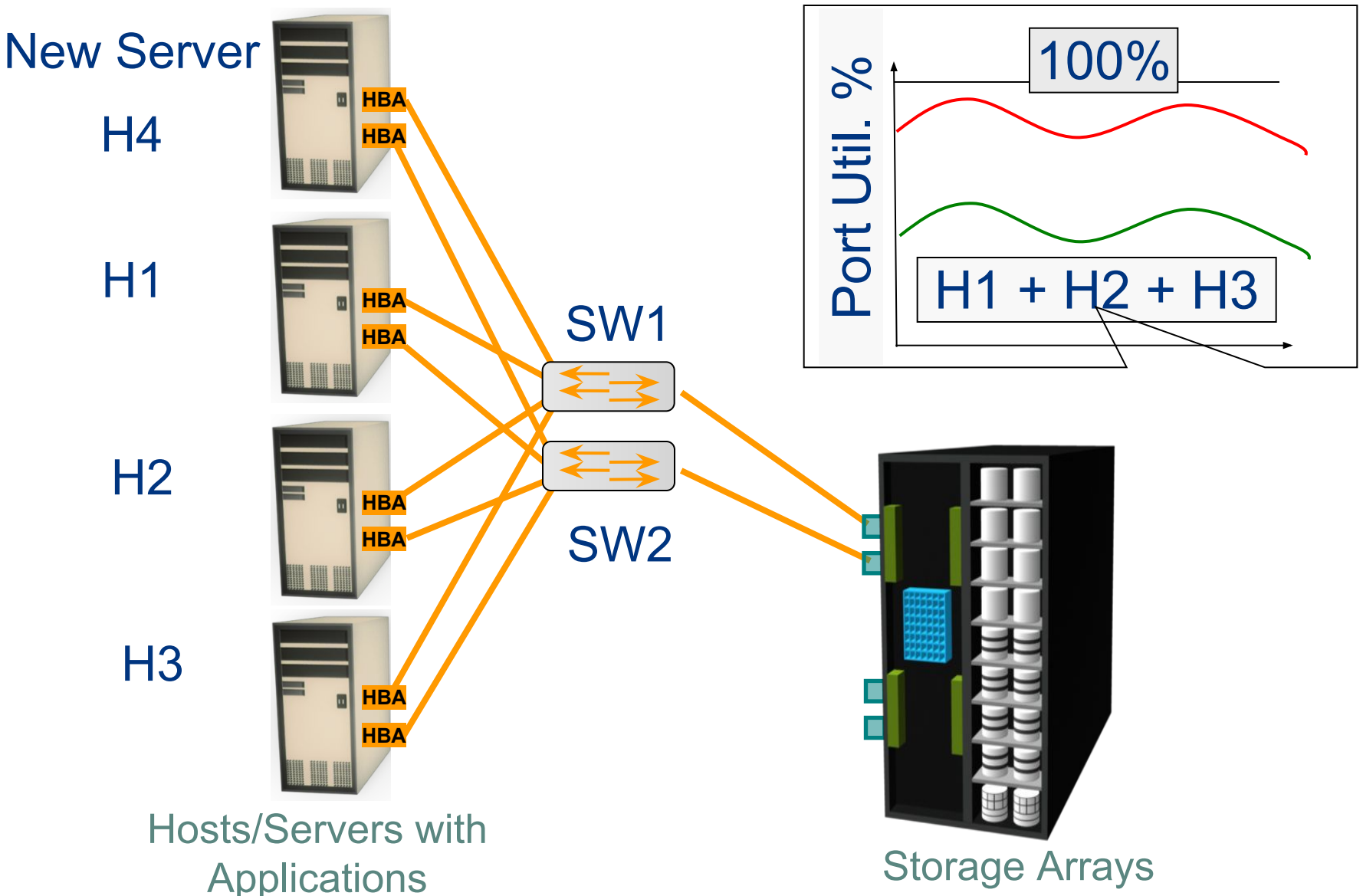
Performance Monitoring

- 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.

Performance Monitoring

- 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(red) and dotted lines(green) 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(green), then there is room to add a new server.

Performance Monitoring Example: Array Port Utilization

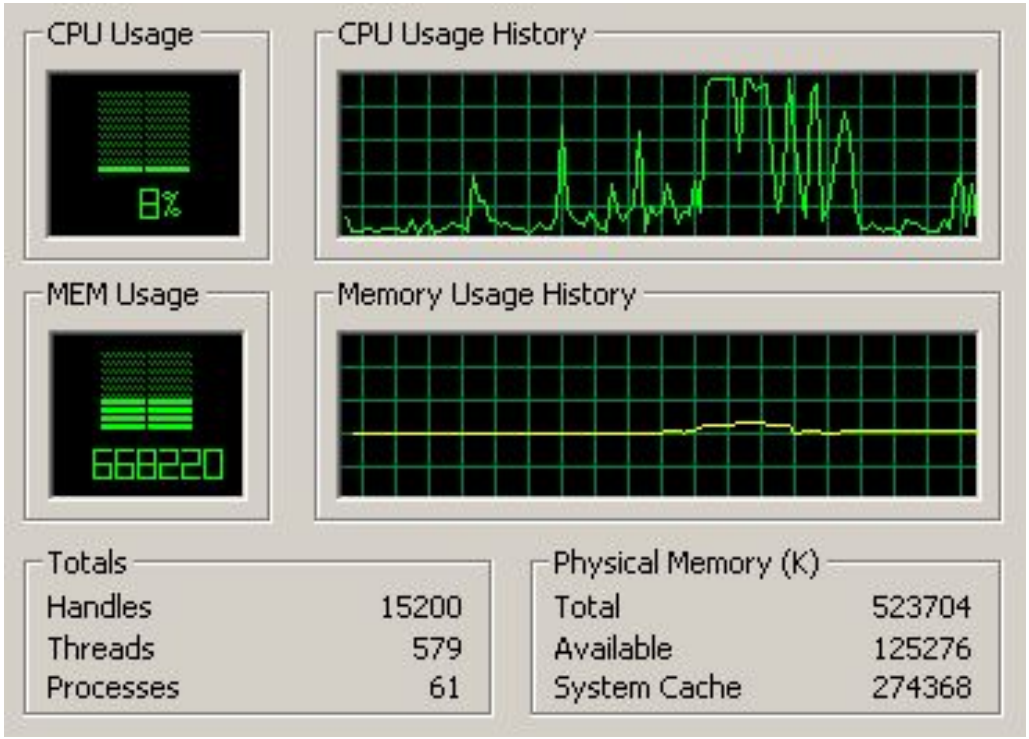


Performance Monitoring

- Most servers offer tools that enable monitoring of server CPU usage.
- For example, Windows Task Manager displays CPU and memory usage, as shown in Figure
- However, these tools are inefficient at monitoring hundreds of servers running in a data-center environment.
- A data-center environment requires intelligent performance monitoring tools that are capable of monitoring many servers simultaneously.

Performance Monitoring Example: Servers CPU Utilization

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



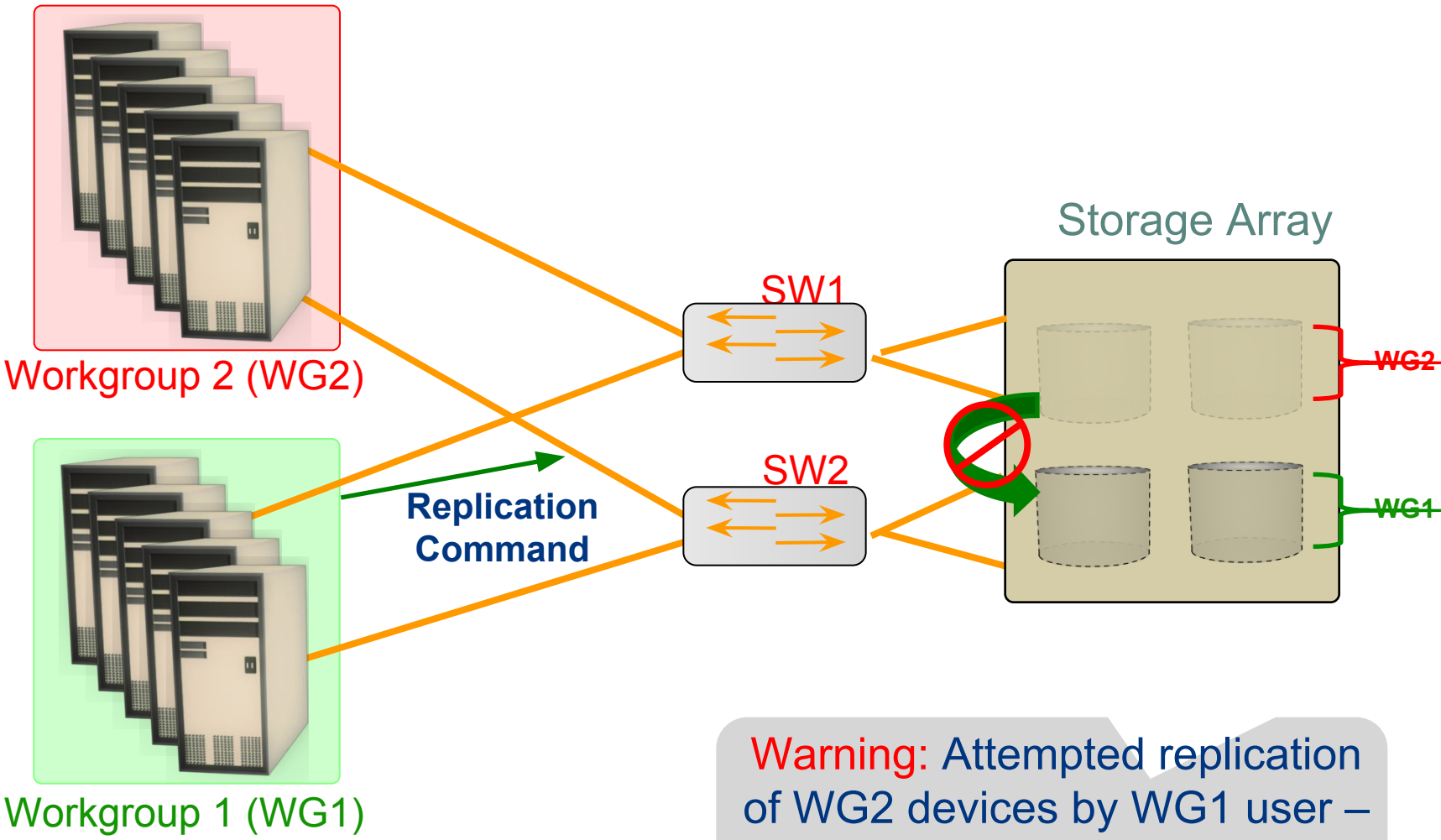
Security Monitoring

- 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.
- Conversely, 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.

Security Monitoring

- 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.

Security Monitoring Example: Storage Array

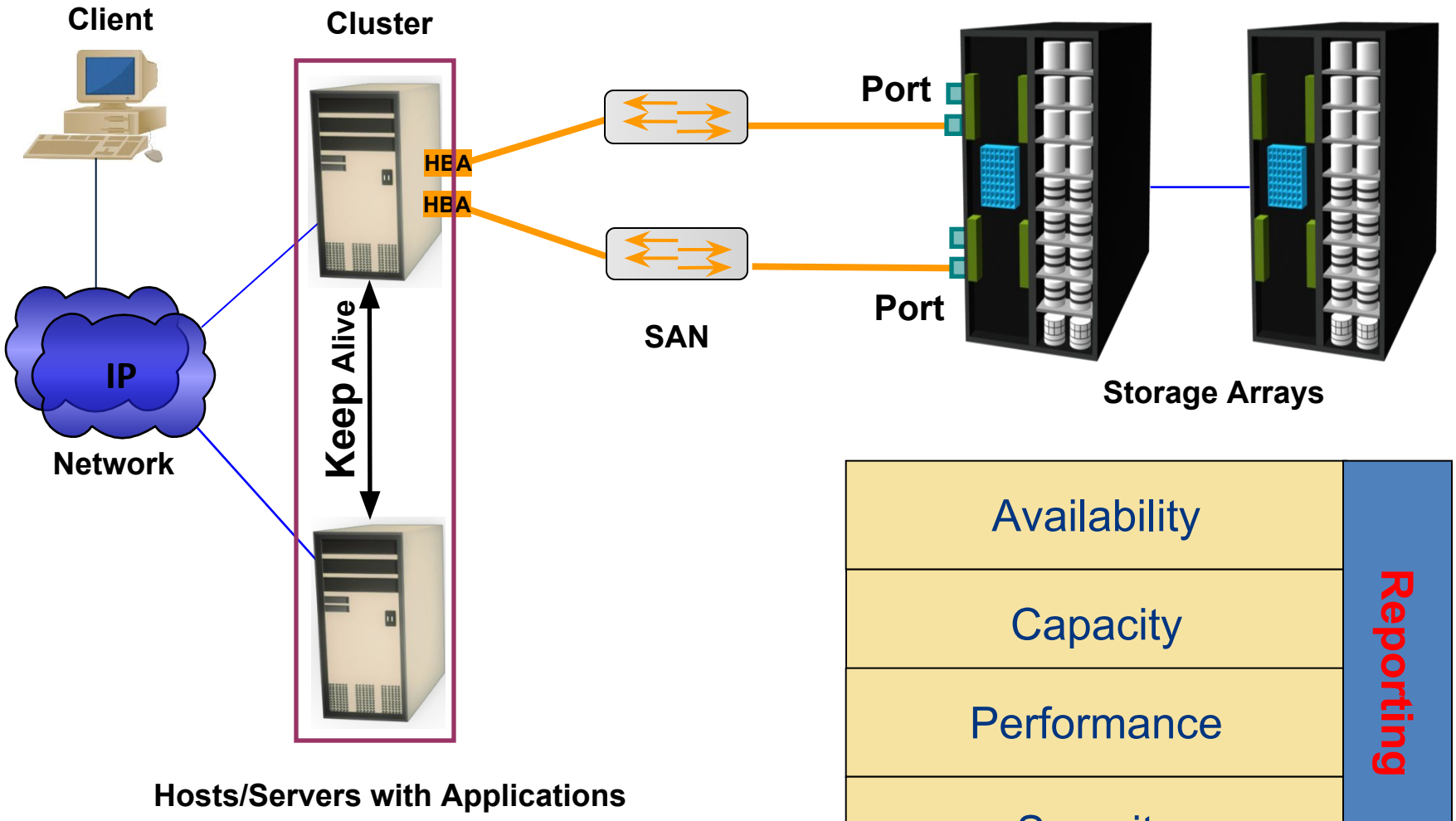


SLO-2 :
Storage Infrastructure Management Activities

Storage Infrastructure Management Activities

- All the management tasks in a storage infrastructure can be broadly categorized into,
  - availability management
  - capacity management
  - performance management
  - security management
  - reporting
- The major storage infrastructure components that should be managed are
  - Servers, databases and applications
  - Network ((SAN) and IP Networks (switches, routers, bridges))
  - Storage Arrays

Storage Infrastructure Management Activities



Availability Management

- Establishing guidelines for all configurations based on service levels
- A key activity in availability management is to provision redundancy at all levels, including components, data, or even sites.
- To ensure high availability by:
  - Eliminating single points of failure deploy/configure
    - Two or more HBAs
    - Multipathing software
    - RAID protection
    - Redundant Fabrics
  - Configuring data backup and replication
  - Deploying virtualized environment

Capacity Management

- The goal of capacity management is to Ensures adequate availability of resources based on their service level requirements
- Capacity management also involves optimization of capacity based on the cost and future needs
- Compares allocated storage to forecasted storage on a regular basis
- It involves activities, such as creating RAID sets and LUNs, and allocating them to the host.
- Provisioning a fixed amount of user quotas restricts users from exceeding the allocated capacity
- Technologies, such as 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.

Performance Management

- Ensures the optimal operational efficiency of all components
- Performance analysis is an important activity that helps to identify the performance of storage infrastructure components.
  - This analysis provides information on whether a component meets expected performance levels.
- Every component must be validated for adequate performance capabilities as defined by the service levels
- Performance analysis
  - Identify bottlenecks
  - Fine tuning for performance enhancement
- Key activities
  - Host: Volume management, database/application layout
  - SAN: Designing sufficient ISLs with adequate bandwidth
  - 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

Security Management

- Key objective of the security management activity is to ensure confidentiality, integrity, and availability of information in both virtualized and nonvirtualized environments
- Prevent unauthorized activities or access
- Key activities
  - Server:
    - Creation of user logins, user privileges, access policies that authorize users to perform role-based activities
  - SAN:
    - Configuration of zoning to restrict unauthorized HBA's
  - Storage Array:
    - LUN masking prevents data corruption on the storage array by restricting host access to a defined set of logical devices

Reporting

- Reporting on a storage infrastructure involves keeping track and gathering information from various components/processes
- This information is compiled to generate reports for trend analysis, capacity planning, chargeback, performance, and to illustrate basic configuration of storage infrastructure components
- Capacity – 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
- 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.

SLO – 1:
1. Storage Infrastructure Management Challenges
2. Storage Management Examples

1. Storage Infrastructure Management Challenges

Storage Infrastructure Management Challenges

- Monitoring and managing today's complex storage infrastructure is challenging.
- This is due to the heterogeneity of storage arrays, networks, servers, databases, and applications in the environment.
- For example, heterogeneous(vendor-specific) storage arrays vary in their capacity, performance, protection, and architectures.
- 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.

2. Storage Management Examples

Storage Management Examples

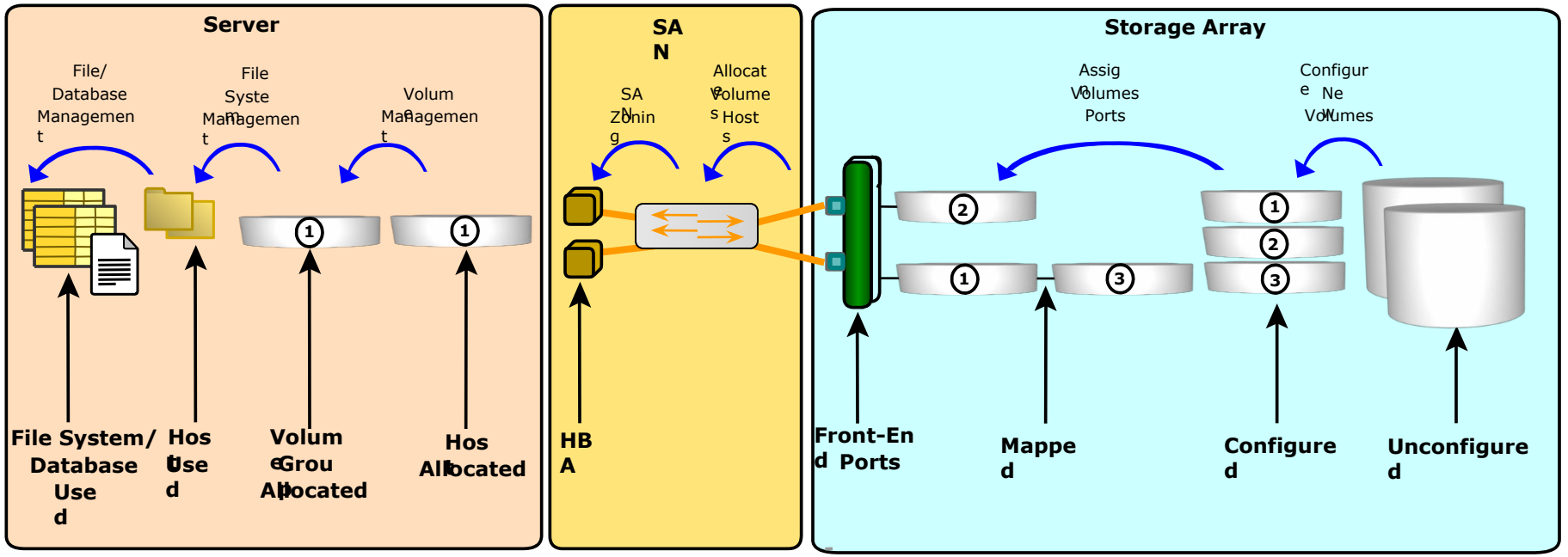
1. Storage Allocation to a New Server/Host
2. File System Space Management
3. Chargeback Report

SLO – 2:
Storage Allocation to a New Server/Host

Example 1: Storage Allocation to a New Server/Host

- Consider the deployment of a new RDBMS server to the existing **nonvirtualized** storage infrastructure.
- First, the administrator needs to install and configure the HBAs and device drivers on the server before it is physically connected to the SAN.
- Optionally, multipathing software can be installed on the server, which might require additional configuration.
- Further, storage array ports should be connected to the SAN.

Managing Example: Storage Allocation to Server/Host



Storage Allocation Tasks

Storage Allocation to Server/Host…

- As the next step, the administrator needs to perform zoning on the SAN switches to allow the new server access to the storage array ports via its HBAs.
- To ensure redundant paths between the server and the storage array, the HBAs of the new server should be connected to different switches and zoned with different array ports.
- Further, the administrator needs to configure LUNs on the array and assign these LUNs to the storage array front-end ports.
- In addition, LUN masking configuration is performed on the storage array, which restricts access to LUNs by a specific server.

Storage Allocation to Server/Host…

- The server then discovers the LUNs assigned to it by either a bus rescan process or sometimes through a server reboot
- 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.
- The administrator's task also includes installation of a database or an application on the logical volumes or file systems that were created.
- The last step is to make the database or application capable of using the new file system space.
- Figure illustrates the activities performed on a server, a SAN, and a storage array for the allocation of storage to a new server.

Storage Allocation to Server/Host...

- In a **virtualized environment**, provisioning storage to a VM that runs an RDBMS requires different administrative tasks.
- Similar to a nonvirtualized environment, a physical connection must be established between the physical server, which hosts the VMs, and the storage array through the SAN.
- At the SAN level, a VSAN can be configured to transfer data between the physical server and the storage array.
- The VSAN isolates this storage traffic from any other traffic in the SAN.
- Further, the administrator can configure zoning within the VSAN.
- 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.
- Similar to a physical environment, LUN masking needs to be carried out on the storage array

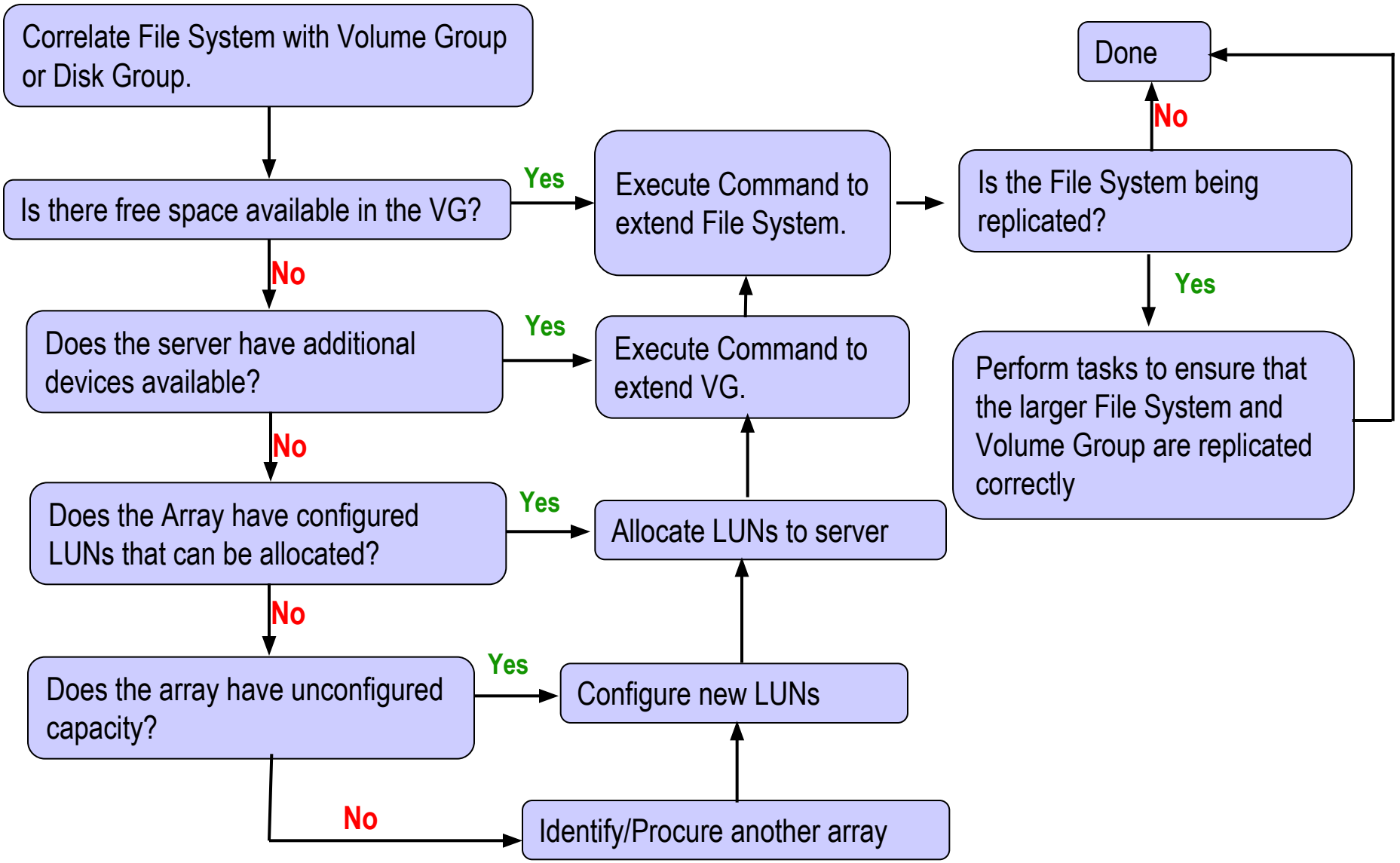
Storage Allocation to Server/Host…

- 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.
- Then, the administrator creates a VM and installs the OS and RDBMS on the VM.
- While creating the VM, the hypervisor creates a virtual disk file and other VM files in the hypervisor file system.
- Alternatively, the hypervisor enables virtual provisioning to create a thin virtual disk and assigns it to the VM.
- 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.

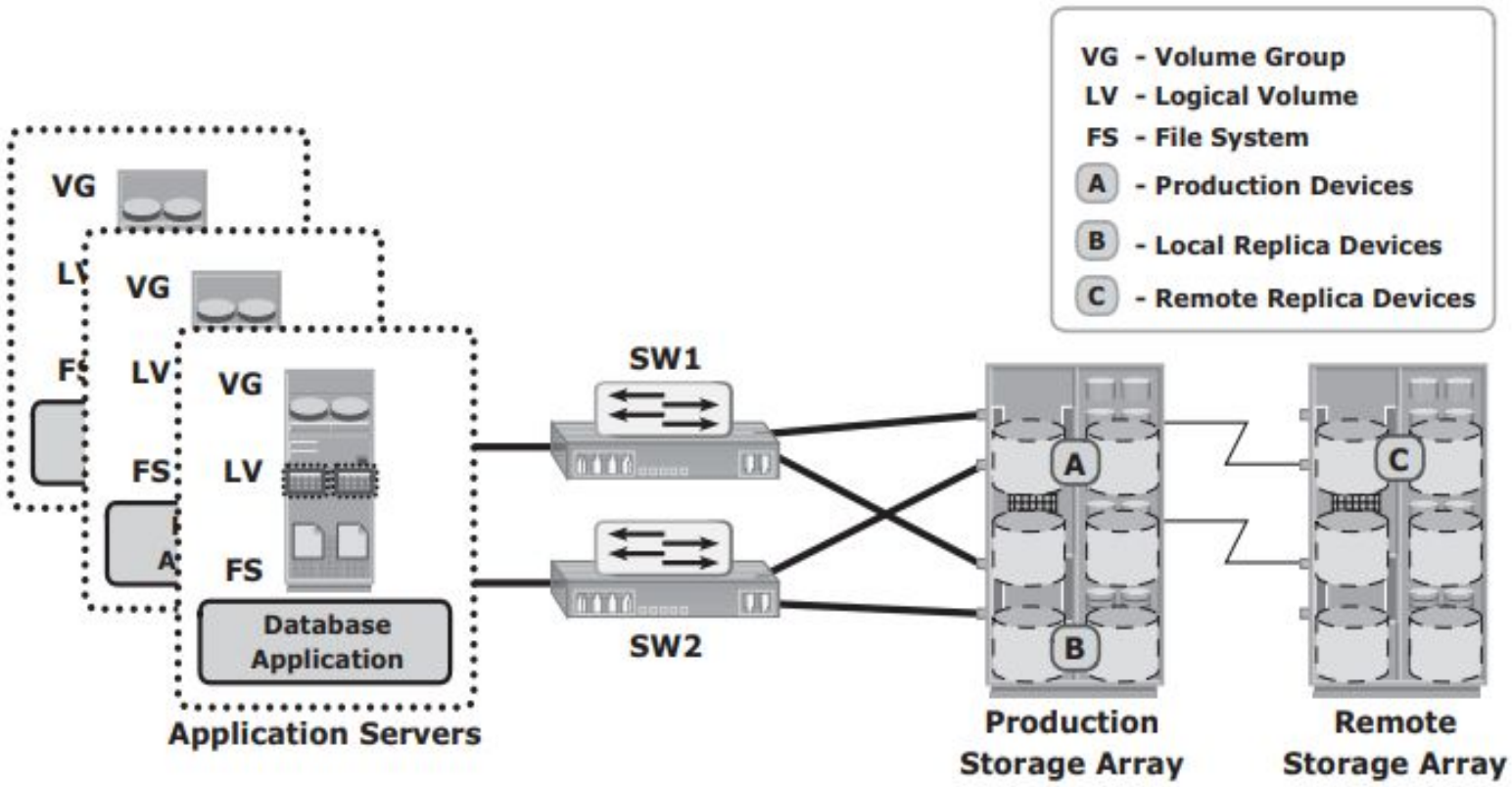
Managing Example: Configuring File System Space



Example 3: Chargeback Report

- Figure 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.
- Individual departmental applications run on each of the servers.
- 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.

Managing Example: 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 $ 5/Raw (GB)
Payroll_1	100	200	100	125	425	$ 2125
Engineering_1	200	250	200	250	700	$ 3500

Chargeback Report…

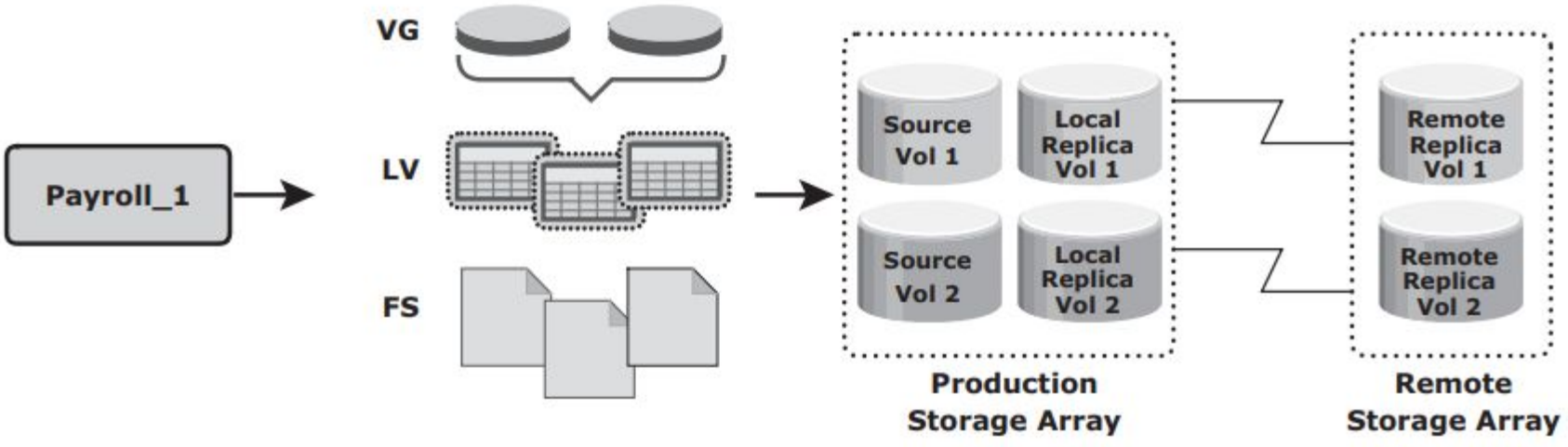
- A report documenting the exact amount of storage resources used by each application is created using a chargeback analysis for each department.
- If the unit for billing is based on the amount of raw storage (usable capacity plus protection provided) configured for an application used by a department, the exact amount of raw space configured must be reported for each application.
- The report shows the information for two applications, Payroll_1 and Engineering_1.

Chargeback Report…

- The first step to determine chargeback costs is to correlate the application with the exact amount of raw storage configured for that application.
- The Payroll_1 application storage space is traced from 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.

Correlation of capacity configured for an application

- In the example shown, the application 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)



Chargeback Report…

- The amount of storage allocated to the application can be easily computed after the array devices are identified.
- Compute the chargeback amount based of price/raw GB of storage

Example:

- Allocated Storage (2 Source Vols) = 2*50GB = 100 GB
- For Local Replica = 100 GB
- For Remote Replica = 100 GB
- Production Volume Raw capacity (RAID 1) = 200 (100 *2) GB
- Local Replica Raw Capacity (un-protected) = 100 GB
- Remote Replica Raw capacity (RAID 5) = 125 GB (4+1 RAID 5)
- Total Raw capacity used by the applications = 425 GB
- Chargeback cost = 425 * $5 = $ 2,125

(The total cost of storage provisioned for Payroll_1 application will be $2,125 (assume cost per GB of storage is $5))

Chargeback Report...

- This exercise must be repeated for each application in the enterprise to generate the chargeback report.
- Chargeback reports can be extended to include a pre-established cost of other resources, such as the number of switch ports, HBAs, and array ports in the configuration.
- Chargeback reports are used by data center administrators to ensure that storage consumers are well aware of the costs of the services that they have requested

Reference

- **Somasundaram, Gnanasundaram, Alok Shrivastava (2012), *Information Storage and Management* -** *Storing, Managing, and Protecting Digital Information in Classic, Virtualized, and Cloud Environments*, **2nd Edition, EMC Corporation**