Enterprise Storage Network Management

Lou Przystas

EMC Corporation

171 South Street
Hopkinton, MA 01748
(508) 435-1000

Przystas_Lou@EMC.com

Managing the Enterprise Storage Network
Storage network growth requires scaleable storage management tools

As larger Enterprise Storage Networks (ESN) are being deployed faster than anyone could have anticipated, it is important to implement the proper management tools. The cost of managing the storage, and the storage network, is much greater than simply the cost of acquiring hardware and software.

In an ESN environment, storage resources are truly shared, and can be reallocated as needed to meet changing business needs. This environment allows *any-to-any* connectivity, providing the most-flexible storage infrastructure.

The ESN must be managed for access control and contention for the common resources. To successfully implement a shared switched fabric environment, administrators need tools that can help with managing the storage network. Access control is required for security of the data, and partitioning is necessary to meet service-level agreements.

LUN masking at the storage device provides centralized access control of the data volumes. The control is placed in the storage array, as close to the data as possible. If a particular host requests data to which it does not have access, the request is denied. This is particularly important when adding new Windows NT® servers to the ESN. Partitioning of the Fibre Channel switches through *zoning* reduces risk and allows each server to have its own virtual ESN. The combination of access control and zoning provides the solution for such various aspects as:

- **Data Integrity** — As more and more systems are introduced to the ESN, the danger of encroaching into each other's storage area increases, and invites potential data corruption and information loss.

- **Security** — While increasing connectivity is desired, it should not be accomplished without the ability to enforce information accessibility per the security policies of individual businesses.

Most businesses today rely on vast amounts of information, management of which must adhere to the security policies of those businesses. Utilizing the proper tools allows storage and storage network administrators to easily enforce these policies.

Access Control for the ESN is built on top of two foundation elements:

1. **The Storage Subsystem Access Control Policy** is provided by the storage subsystem to define and enforces access control policy nearest to where the information is being managed.

2. **The Storage Network Access Control Policy** that defines and manages the connectivity access controls.

Other more abstract and granular level of access control capabilities can then be added.
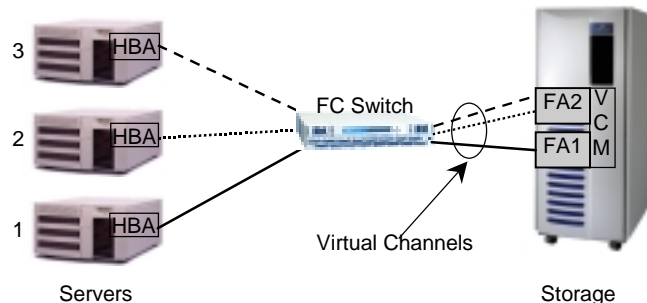
Storage Subsystem Access Control Policy
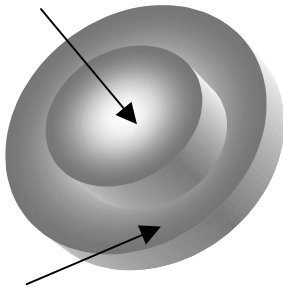
Storage Network Access Control Policy

The storage subsystem access control policy

In a storage network where point-to-point cabling keeps each host's storage volumes separate from those of other hosts, each host detects only the volumes to which it is directly connected. In ESN environments in where multiple hosts are connected to a single Storage port, a problem arises when all hosts have the potential to see and use the same storage volumes.

In a typical Fibre Channel topology, each host is connected to the Fibre Channel hub or switch through one or more Host Bus Adapter (HBA) ports. Each Storage port is connected to the Fibre Channel hub or switch through one or more Fibre Channel Adapter (FA) ports, each FA port providing access to a given set of volumes. Each port in the Fibre Channel topology (HBA and FA) is uniquely identified by its World Wide Name (WWN). VCM is the volume configuration management software that controls access to logical volumes. Unlike host-based access control mechanisms that are error prone (since each host must be trusted not to conflict with others), the storage based access control mechanism avoids such conflicts by single centralized monitoring. Using volume configuration management software, you can define a *virtual channel* connecting each host with its storage volumes, even though there may be many hosts sharing the same storage fibre port. The figure illustrates access control applied to three hosts in a multi-initiator environment.

When a host attempts to access a storage volume on the storage subsystem, the host HBA's WWN, as supplied during login to the Fabric or Arbitrated Loop, is passed to the storage FA port. The storage subsystem records the connection, stores the WWN in a login history

table, and builds a filter listing the volumes available to that WWN through that FA port. The HBA port then sends I/O requests directed at particular volumes to the FA port. Each request includes the identity of the requesting HBA (from which its WWN can be determined) and the identity of the requested volume, with its FA and Logical Unit Number (LUN). The volume configuration management software that runs on the storage subsystem processes each I/O request to verify that the HBA is allowed to access that volume. Any request for a volume that an HBA does not have access to, returns an error to the host.

## Zoning provides access control of the Enterprise Storage Network

Zoning is a technique used to partition a switched Fibre Channel environment. Zones are used to create and manage subsets of logical devices (host bus adapters and storage devices). Devices in the same zone can communicate with one another but not with devices that are not members of that zone. Zoning is often used to restrict access to shared storage network resources, in order to provide higher levels of access control, performance, and availability.

Most Fibre Channel switches provide management utilities that allow zoning of the specific switches. Switch zoning and other fabric control is typically managed in a vendor-specific manner. Each switch stores its own configuration data. Local switch management is adequate when the ESN contains only one or two switches; however, when more switches are added, some kind of centralized management software becomes necessary.
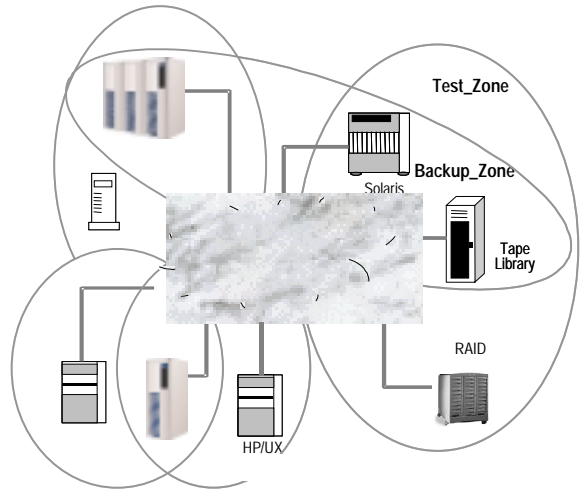
Zoning with LUN Masking – An Example

Consider the example shown in the figure below. Each host has two HBA ports, and there are two switches, each connected to a Storage FA port. Each FA can access devices 0 through 20 on the storage subsystem. In an unmanaged environment, each HBA could access all of the volumes on the storage subsystem, but the administrator chooses to use zoning and LUN masking together to control each HBA's access to the Storage devices.
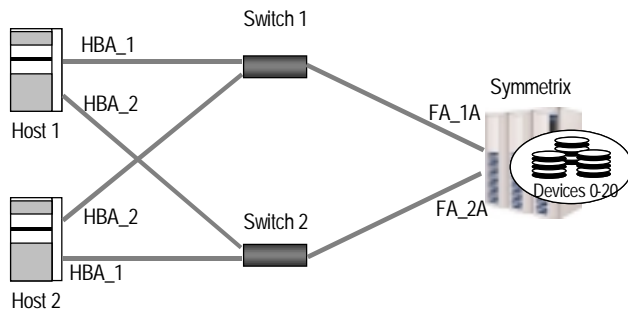
First, the administrator uses Zoning to create a set of single-HBA zones. These zones dictate which HBA on the host side can talk to which FA on the Storage side. In this example, the user created four zones, each of which contains two members consisting of an HBA and a Fibre Adapter (FA). There are 2 zone Sets with one switch in each.

After configuring the paths, the user can set up the Storage system using LUN masking to restrict HBA access to specific logical volumes. In this case, although both FA ports can access devices 0 through 20, the administrator restricts the devices seen by the HBAs on Host1 to devices 1 through 10 and the devices seen by the HBA on Host2 to devices 11 through 20.

Summary

These are the basic functions that are required to provide access control in an Enterprise Storage Network. The proper tools can greatly reduce the labor required to manage the storage infrastructure.

As Enterprise Storage Networks grow larger, it is imperative that good management practices are implemented.

These are key best practices for managing an enterprise storage network:

- Centralize the administration
- Utilize tools that can manage a multi-vendor ESN/SAN environment.
- Provide access control to constantly growing volumes of information. Access control is most effective at the storage level, where the data resides.
- Utilize centralized zoning tools to provide access control of the storage network.
- Deploy interoperability-tested Fibre Channel hardware and software components.
- Utilize hardware and software that comply with industry standards.