



## **Shared Storage Security – It Is a Reality**

**Jeffrey S. Bardin, CTO**

**Treadstone 71**

The concept of virtual or shared storage is a relatively new concept for corporate information technology professionals. The typical mainstream corporate data center is structured around storage dedicated to specific business centers within the corporation, or storage leveraged across the enterprise. Discussion of virtual or shared storage usually reveals considerable concern within the IT community about issues such as data security, sharing logical space on a physical device, and disk performance.

Adoption of the virtual or shared storage technology requires a significant paradigm shift in the current corporate thinking. Data storage to date has been customer centric, one customer per storage device. Virtual or shared storage alters that model enabling multiple customers to share the same physical device.

### Defining virtual storage

Virtual storage is the presentation of a single storage image to host servers utilizing an array of network-connected disk storage devices. The storage image can be hosted on disk technologies from a single vendor or from multiple vendors, and the network can be IP- or fiber-based. The virtual storage environment provides a common storage management interface that has the capability to span multiple storage technologies. It supports routine management tasks, reconfiguration of storage, and data backup and recovery with a single suite of tools. It also helps storage asset allocation and utilization, and adds to the flexibility of cost-effectively accommodating dynamic, high-growth storage environments. Internet data centers (IDC) providing virtual storage services can more efficiently manage storage administration leading to lower overall price per gigabyte.

Software can provide solutions that centralize storage management, simplify administration, provide centralized security features, and reduce long-term operating costs. This is also key for the IDC and its ability to consolidate heterogeneous servers and storage in an integrated SAN environment.

Data security is probably the greatest concern to the IT community in a shared or virtual storage environment. Historically, corporate data sharing adjacent space on a physical disk to another's data has been deemed unacceptable (although this practice is accepted in mainframe environments). In an environment where packets from multiple customers routinely transit wide area (WAN) and local area (LAN) networks, current thinking views shared storage as a security risk.

Is it a security risk?

In a properly engineered and executed environment, shared storage is not a security risk for the same reason that packets transported across an IP network are not intrinsically at risk. The architecture of an IP network directs packets across the network to its intended destination by unique IP addresses. The addresses uniquely identify routes and servers eligible to transport and read the data. Storage area networks (SAN) provide security for data by means of a similar addressing schema. SANs associate hosts eligible to read and/or write data with disk resources by means of switch zoning and logical unit number (LUN) masking. The zoning of switches and hubs allows only specific ports on the switch or hub to see other pre-defined ports on the switch or hub. Zoning limits server access to data to only those devices physically connected to storage devices on specified ports.

LUN masking associates the world wide node name (WWNN) - unique to a server's host bus adapter (HBA) and the logical equivalent to a network interface card's MAC Address - with a LUN, a defined disk partition on a storage device. A LUN can be made up of an individual disk, a portion of a disk, or multiple portions of disks as defined by disk management software. This technology "masks" storage on a device from other servers on the network, effectively making the disk available only to the designated server. In fact, authorized users can't cross between the storage pools created using the above techniques. If there is a security breach, it is contained within the specific portion of the SAN.

Sharing logical space

For discussion purposes, a storage device may exist with a mirrored 73-gigabyte physical disk. This disk can be presented to the host as a 73-gigabyte disk, or it can be apportioned into multiple logical disks and presented to multiple hosts. If the disk is presented as a whole disk, there exists a single LUN assigned to the device. You can map that LUN to a specific host using the hosts HBA WWNN, fibre switch WWPN, and storage WWNN with specified LUN. This allows the host HBA, via a specified port, exclusive access to the LUN on the disk array. The physical disk can be carved into multiple 9-gigabyte logical devices and presented to different hosts using the same hard zoning techniques as above. This allows the storage administrator to assign either a whole or partial disk to a single or multiple hosts. Since the WWNN and WWPN are unique identifiers, other hosts cannot access the data or see the physical device.

Some switch vendors are providing the ability to enforce zoning all the way to the LUN level within the switch, building zoning capabilities right into the switch hardware, where it can be enforced at wire speed. These vendors also often provide for password encryption, creating what amounts to a trusted switch similar to an IP trusted host. In such a SAN, security policy could be changed only at the trusted switch. The organization could also encrypt traffic at the switch.

These techniques also are critical for IDCs intending to use a SAN to meet the different storage needs of multiple customers. IDCs need to be able to break the SAN into

manageable, independent sections so each customer has what amounts to its own SAN - at a fraction of the cost of purchasing and building one (not including the time, cost, and effort needed to train or hire staff to manage this environment). An IDC needs to use LUN masking and zoning to segregate the SAN into virtual SANs for each customer.

#### Disk performance and security in a shared environment

Disk performance in a shared storage environment is similar to disk performance in an enterprise storage environment with multiple internal customers accessing the device. Performance is dependent on the administration of resources within the storage device. It is incumbent upon the storage administrator to monitor performance of the storage device, and balance resource requirements across all available disk devices.

Where do the security breaches usually come from against SANs? Gartner Report indicates that 74 percent of security breaches are internal. Keep in mind that an effective breach of a SAN requires someone with the ability to write sophisticated driver-level code. This level of skill is normally beyond the capabilities of the typical corporate employee, whether in the IT group or not. Since SANs in IDCs are well behind firewalls, the implementation of physical security practices within the data center and throughout the organization - in combination with hardware and software security measures - need be standardized within the selected IDC.

IDCs also need to check the backgrounds of operational personnel, and institute security policies and procedures ensuring that only authorized, highly trained and trusted staff have access to the servers and components residing on the SAN. But then again, this is true of all operational staff. Well-defined and constantly scrutinized security practices at the IDC - and on the SAN-connected systems along with LUN masking and switch-based zoning - can do much to significantly minimize security threats.

Jeffrey S. Bardin, CTO  
Treadstone 71  
[jbardin@treadstone71.com](mailto:jbardin@treadstone71.com)