Configuring iSCSI for High Availability

Creating a single connection to iSCSI storage makes that storage available. However, it does not make that storage highly available. If iSCSI loses the connection, the server loses access to its storage. Therefore, most iSCSI storage connections are made redundant through one of two high availability technologies: Multiple Connected Session (MCS) and Multipath input/output (I/O) (MPIO).

Although similar in results they achieve, these two technologies use different approaches to achieve high availability for iSCSI storage connections.

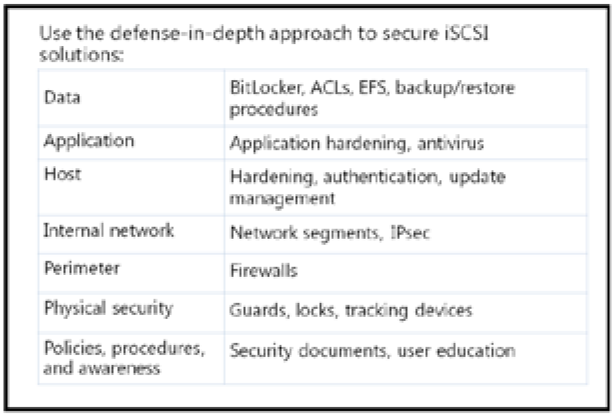
MCS is a feature of the iSCSI protocol that:

- Enables multiple TCP/IP connections from the initiator to the target for the same iSCSI session.
- Supports automatic failover. If a failure occurs, all outstanding iSCSI commands are reassigned to another connection automatically.
- Requires explicit support by iSCSI SAN devices, although the Windows Server 2012 iSCSI target server role supports it.

MPIO provides redundancy differently:

- If you have multiple network interface cards (NICs) in your iSCSI initiator and iSCSI target server, you can use MPIO to provide failover redundancy during network outages.
- MPIO requires a device-specific module (DSM) if you want to connect to a third-party SAN device that is connected to the iSCSI initiator. The Windows operating system includes a default MPIO DSM that is installed as the MPIO feature within Server Manager.
- MPIO is widely supported. Many SANs can use the default DSM without any additional software, while others require a specialized DSM from the manufacturer.
- MPIO is more complex to configure, and is not as fully automated during failover as MCS.

iSCSI Security Options



Use the defense-in-depth approach to secure iSCSI solutions:

Data	BitLocker, ACLs, EFS, backup/restore procedures
Application	Application hardening, antivirus
Host	Hardening, authentication, update management
Internal network	Network segments, IPsec
Perimeter	Firewalls
Physical security	Guards, locks, tracking devices
Policies, procedures, and awareness	Security documents, user education

Because iSCSI is a protocol that provides access to storage devices over a TCP/IP network, it is crucial that you secure your iSCSI solution to protect it from malicious users or attacks. You can mitigate risks to your iSCSI solution by providing security at various infrastructure layers. The term *defense-in-depth* is often used to describe the use of multiple security technologies at different points throughout your organization.

Defense-in-depth security strategy includes:

- Policies, procedures, and awareness. As a security best practice, security policy measures need to operate within the context of organizational policies. For example, consider enforcing a strong user password policy throughout the organization, but having an even stronger administrator password policy for accessing iSCSI storage devices and computers that have iSCSI management software installed.
- Physical security. If any unauthorized person can gain physical access to iSCSI storage devices or a computer on your network, then most other security measures are not useful. You must ensure that iSCSI storage devices, the computers that manage them, and the servers to which they are connected are physically secure, and that access is granted to authorized personnel only.
- Perimeter. Perimeter networks mark the boundary between public and private networks. Providing firewalls and reverse proxy servers in the perimeter network enables you to provide more secure corporate services across the public network, and prevent possible attacks on the iSCSI storage devices from the Internet.

- Networks. Once you connect iSCSI storage devices to a network, they are susceptible to a number of threats. These threats include eavesdropping, spoofing, denial of service, and replay attacks. You should use authentication such as CHAP to protect communication between iSCSI initiators and iSCSI targets. You might also consider implementing Internet Protocol security (IPsec) for encrypting the traffic between iSCSI initiators and iSCSI targets. Isolating iSCSI traffic to its own virtual LAN (VLAN) also strengthens security by not allowing malicious users that are connected on corporate VLAN network to attack iSCSI storage devices that are connected to a different VLAN. You should also protect network equipment (such as routers and switches) that is used by iSCSI storage devices, from unauthorized access.
- Host. The next layer of defense is the protection layer for the host computers that are connected to iSCSI storage devices. You must maintain secure computers by using the latest security updates. You should consistently use the Windows Update feature in Windows operating systems to keep your operating system up-to-date. You also have to configure security policies such as password complexity, configure the host firewall, and install antivirus software.
- Applications. Applications are only as secure as their latest security update. For applications that run on your servers but do not integrate in Windows Update, you should regularly check for security updates issued by the application vendor. You should also update the iSCSI management software according to vendor recommendations and best practices.
- Data. This is the final layer of security. To help protect your network, ensure that you are using file user permissions properly. Do this by using Windows BitLocker® Drive Encryption, using Access Control Lists (ACLs), implementing the encryption of confidential data with Encrypting File System (EFS), and performing regular backups of data.