SearchWinComputing.com SearchSQLServer.com SearchExchange.com

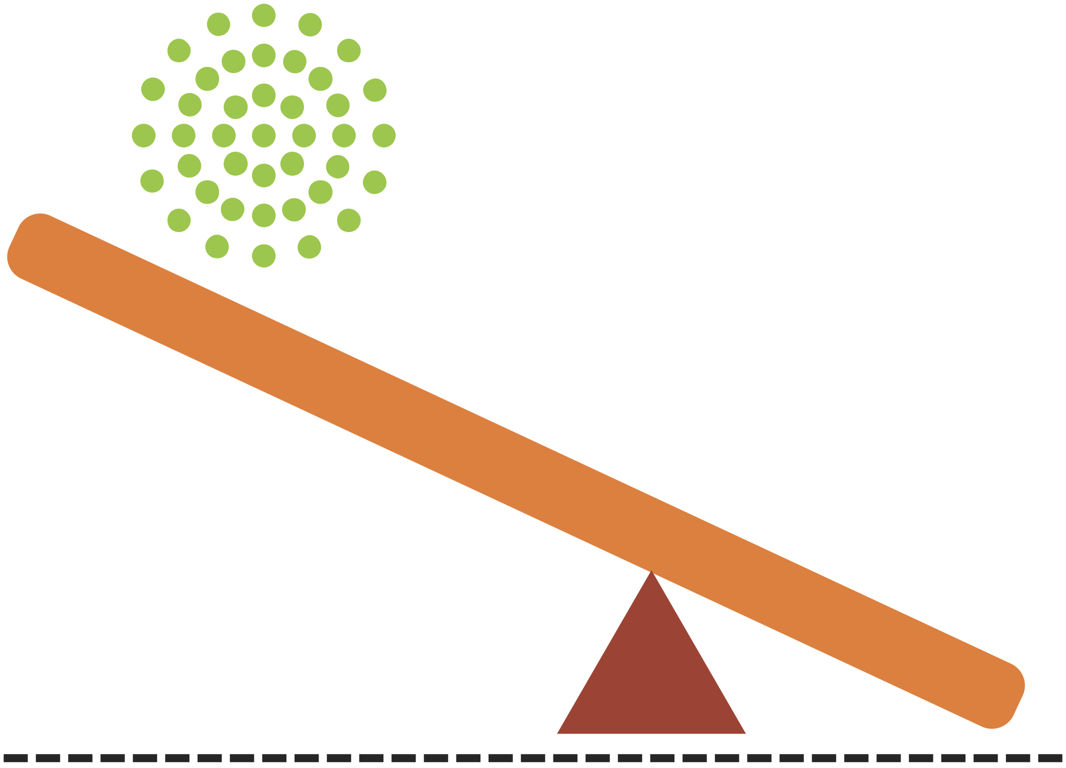
THE WINDOWS MANAGER'S GUIDE TO **iSCSI SANs**

INSIDE:

LEVERAGING SANS WITH WINDOWS SERVERS

SAN RESILIENCY AND DISASTER RECOVERY

UNDERSTANDING THE iSCSI INITIATOR



CHAPTER 1

Leveraging SANs with Windows Servers

Leveraging
iSCSI SANs in Windows Servers

LEVERAGING SANS WITH WINDOWS SERVERS ●
SAN RESILIENCY AND DISASTER RECOVERY ○
UNDERSTANDING THE iSCSI INITIATOR ○

An iSCSI storage area network (SAN) offers several advantages over direct-attached storage (DAS) in a Windows server environment. Get the information every Windows manager needs to gain the most out of an iSCSI storage platform.

BY LAURA E. HUNTER

THERE ARE MANY benefits to using the iSCSI storage platform in a Windows environment. One is eliminating the need for Windows file servers to use direct-attached storage (DAS) in favor of providing direct access to disk space via an iSCSI-based SAN. Intelligent backup solutions available with iSCSI can reduce the amount of data you need to commit to your daily backups while allowing you to restore data in a short time frame.

You can also reduce server-based disk requirements by using the SAN's ability to perform thin provisioning and cloning, particularly in test and/or virtualized environments. Given Microsoft's native support of an iSCSI Initiator, any Windows administrator can leverage the benefits of iSCSI to improve the efficiency of data storage on a Microsoft network.

What can an iSCSI SAN do for Windows administrators that an array of disks directly attached to the server cannot?

The first major benefit of an iSCSI

LEVERAGING SANS WITH WINDOWS SERVERS

SAN RESILIENCY AND DISASTER RECOVERY

UNDERSTANDING THE iSCSI INITIATOR

SAN is improved utilization of your total storage capacity. It seems hard to believe, but the typical utilization of DAS is less than 30% and can be significantly less than that in some cases. If you have 100 GB of storage attached to a server, you can assume that 70 GB of it will be unused.

Why is disk utilization on a DAS solution so low? Because disks small enough to host only the Windows operating system no longer exist, administrators are forced to allocate significantly more space on the system drive than the operating system actually requires.

Consider a typical file server with a pair of 72 GB disks configured in a RAID 1 array. Out of 144 GB of raw space, 72 GB are actually usable by Windows due to RAID 1 mirroring. A Windows OS needs no more than 10 GB of space, but most admins are reluctant to do anything else with the 62 GB of usable disk space on the system drive for fear that they'll compromise server performance. This leads to a massive 134 GB of "wasted" disk space just to install Windows.

Let's extend the example to include a separate data partition on the same server. Assume the server has an external array of 14 disks, each with 144 GB capacity. Within 2 TB of raw disk space, we typically need to take away 144 GB (one disk) for RAID 5 parity and another 144 GB to configure a hot spare. This leaves us with 1.7 TB of available storage out of 2 TB total.

Add this to the 134 GB of wasted space on the system drive, and in a single server, we're wasting nearly half a terabyte of disk space. For a company with multiple file servers, the amount of wasted space can increase exponentially. This situation can get even worse. There are many proponents of RAID 10 because it's a good way to deliver two-disk failure resilience and good read/write performance. The problem is that your original 14-disk array immediately shrinks to 7 disks, unless the array is configured with a hot spare.

Once you place your storage onto an iSCSI SAN, you can allocate your disk space more efficiently by using the SAN's thin provisioning feature. With thin provisioning, an application is presented with a virtual volume of arbitrary size, but only allocates physical capacity to it as data is actually written. Thin provisioning increases storage utilization to the 50 to 70% range; and now vendors are promising utilization figures as high as 97%.

Most storage platforms let you over-allocate your storage, meaning you can present more gigabytes to the network than you actually have on disk. Consider a project manager who insists he needs 10 GB of space on a file server, although you're sure he'll really need only 1 to 2 GB. With thin provisioning, you can "fool" the project manager into thinking he has the full 10 GB available. In reality,

LEVERAGING SANS WITH WINDOWS SERVERS

SAN RESILIENCY AND DISASTER RECOVERY

UNDERSTANDING THE iSCSI INITIATOR

he's only taking up the actual amount of space his files are using.

With thin provisioning, you can monitor the project manager's disk utilization and add to it only when you need to. This is a useful feature because most major storage platforms allow you to extend an existing disk array without having to take it down or use a large amount of resources in the rebuilding process. This spreads the cost of disk purchases over time, turning disk space procurement into a just-in-time process.

The same principle applies to LUN provisioning. Windows Servers have not previously handled resizing drive letters (disk volumes) on the fly. Even with Windows Server 2008, there are only some circumstances in which this can be achieved. In such cases, growing—not shrinking—is possible.

By contrast, with an iSCSI SAN, you allocate the number of LUNs that you require and make them as big as you see fit. Should the unforeseen happen to invalidate your initial sizing decisions, use the vendor's management software to increase the size of the drive letter on the fly.

iSCSI SANs can also boost performance. Users can access data much faster when it is spread across multiple disk spindles. Storing a file on an array with only a few disks will lead to much slower read and write operations than if the same file were stored on an array spanning many disks. In addition, file access performance will be improved if those disks have a smaller capacity.

BACKUP AND RESTORE

Protecting the data on a file server requires regular full backups, followed by daily incremental or differential backups. The same applies for other application servers. This can mean a vast amount of backup information being transferred to tape, either via disk over the network or directly to an attached tape drive. To save time and preserve tape capacity, you're likely to conduct only one backup once per day.

However, iSCSI SANs provide a more efficient means of backing up and restoring data. These SANs have a software feature called snapshots—

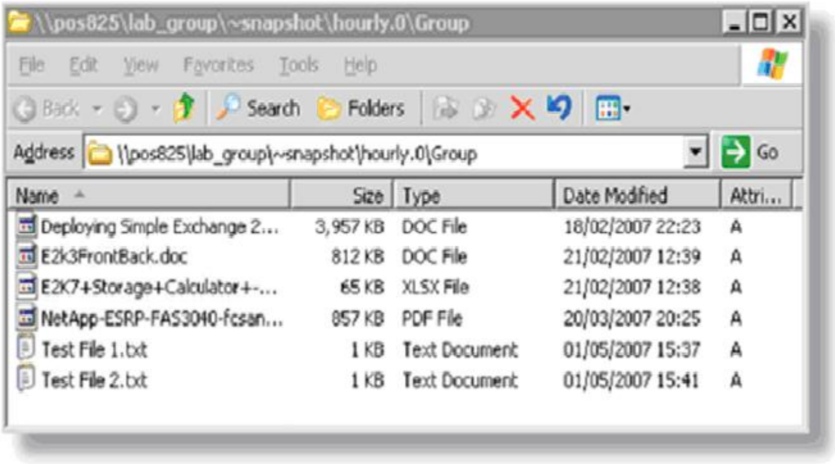
WHAT IS... A Snapshot?

A STORAGE SNAPSHOT is a set of reference markers, or pointers, to data stored on a disk drive, on a tap or in a SAN. A snapshot is similar to a detailed table of contents, but a computer treats it as a complete data backup. Snapshots streamline access to stored data and can speed up the process of data recovery. —WHATIS.COM

LEVERAGING SANS WITH WINDOWS SERVERS

SAN RESILIENCY AND DISASTER RECOVERY

UNDERSTANDING THE iSCSI INITIATOR



\\pos825\lab_group\~snapshot\hourly.0\Group

Name	Size	Type	Date Modified	Attri...
Deploying Simple Exchange 2...	3,957 KB	DOC File	18/02/2007 22:23	A
E2k3FrontBack.doc	812 KB	DOC File	21/02/2007 12:39	A
E2K7+Storage+Calculator+-...	65 KB	XLSX File	21/02/2007 12:38	A
NetApp-ESRP-FAS3040-fcsan...	857 KB	PDF File	20/03/2007 20:25	A
Test File 1.txt	1 KB	Text Document	01/05/2007 15:37	A
Test File 2.txt	1 KB	Text Document	01/05/2007 15:41	A

FIGURE 1: *Snapshot of a hidden directory.*

the ability to take a “photograph” of all the disk blocks in use on a drive array. When you perform a subsequent backup, a second photograph is taken and the two are compared to capture the differences between them. Once this comparison has been made, only those disk blocks that have changed are backed up, which sets up two benefits:

1 **IT REDUCES THE AMOUNT OF SPACE THAT THE BACKUPS CONSUME.** The first backup you perform will be a complete copy of everything on the disk, but subsequent backups will just take up a fraction of the total space on disk, since only the changes that occurred between snapshots are actually backed up.

If a 10 MB file is edited and saved, only disk blocks that changed will be marked for backup. Rather than sending the entire 10 MB to tape that night, perhaps only a few kilobytes of data will actually be copied onto the backup tape. The rest of the file didn’t change, so it doesn’t need to go to tape again (since those unchanged blocks are already stored on the initial backup).

Not only does this save a significant amount of space, but the increased speed of these snapshot backups allows you to perform more frequent backups. This, in turn, can reduce the amount of potential downtime in case of an outage. The snapshot feature allows you to perform many backups throughout the day and store them onto disk while taking up a minimal amount of additional space.

2 **IT ACCESSES PREVIOUS VERSIONS OF BACKED-UP FILES.** This feature is also available on Windows Server 2003 and later, even without the use of a SAN. Figure 1 shows a hidden directory (snapshot), which, when opened, contains an exact directory structure as the one that is visible. Opening those folders presents you

LEVERAGING SANS WITH WINDOWS SERVERS

SAN RESILIENCY AND DISASTER RECOVERY

UNDERSTANDING THE iSCSI INITIATOR

with what might look like exact copies of the files in the production folders, including sizes. In reality, these are not full copies of the files, but merely the blocks on the disk of the file before it was changed.

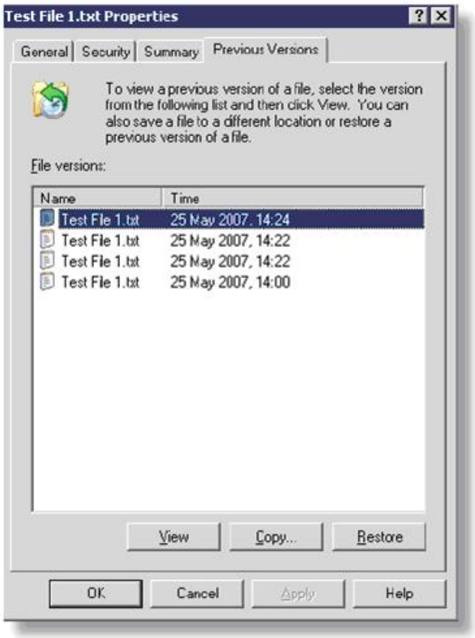
To restore a file from a previous version, you have two choices:

1 **RIGHT-CLICK** on a file stored on an iSCSI SAN with snapshots enabled as shown in Figure 2, and you'll see versions of the file that are available for recovery. You can either select to restore the file to its original location or copy it to another location on disk.

2 A more complex method requires the administrator to **UNHIDE** the ~snapshot folder. Contents of the ~snapshot directory are read-only and cannot be edited, but you can copy items to another location on the disk via drag-and-drop. Once an item has been moved out of the ~snapshot structure, it becomes writable again and you can be place it anywhere you want.

Everything shown here applies not only to files stored on the iSCSI SAN, but also to files in Exchange, SQL Server, Oracle or any other application that stores data on the SAN. All major storage vendors have their own backup and restore solutions for the Microsoft suite of products, and they all work much the same.

FIGURE 2:
Files stored on an iSCSI SAN.



To view a previous version of a file, select the version from the following list and then click View. You can also save a file to a different location or restore a previous version of a file.

File versions:

Name	Time
Test File 1.txt	25 May 2007, 14:24
Test File 1.txt	25 May 2007, 14:22
Test File 1.txt	25 May 2007, 14:22
Test File 1.txt	25 May 2007, 14:00

TRICKS YOU CAN PLAY

In addition to snapshot benefits and thin provisioning, iSCSI SANs allow you to play some other interesting "tricks" with the way you manage data. For instance, in development and test environments, using an iSCSI SAN, you can clone the volume that holds your production data and make it available to the testing team. That way, they can test a new version of their code against an exact replica of the live environment—completely risk-free.

The advantage here is that the clone you give to the testers takes up practically no disk space. How is this possible? The cloned volume uses the same information that is on the production volume and only the deltas

LEVERAGING SANS WITH WINDOWS SERVERS

SAN RESILIENCY AND DISASTER RECOVERY

UNDERSTANDING THE iSCSI INITIATOR

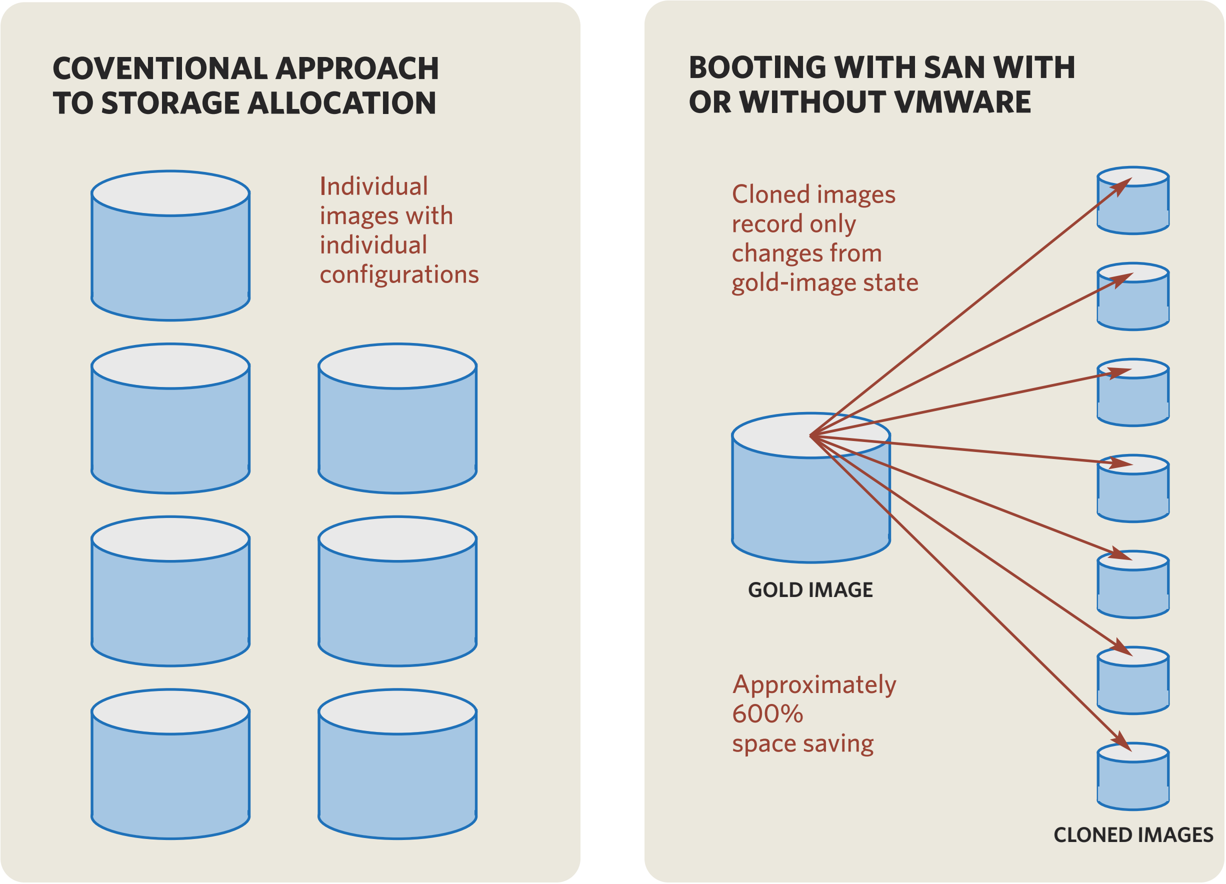
(any changes made to the data in the testing environment) are written to the volume holding the clone.

Rather than the testing team taking up 100% of the space in use by production, they only take up the amount of space used by their deltas, which can be as low as 5% to 10% of the total volume.

This holds equally true if you extend this cloning idea to your server operating systems, particularly in a virtualized environment. Here's how it works in a VMware or Microsoft Virtual Server environment: Create a gold-standard image of a server operating system, and then make multiple clones of that image to support any number of virtualized servers, as shown in Figure 3. This lets you reduce the acquisition cost of each server by at least two disks. (You now may be able to buy a different model of server, since you no longer need internal disks.)

Even if you choose not to use virtualization in your server deployments, you can still benefit from the gold-

FIGURE 3: *Cloning in a virtualized enviroment.*


COVENTIONAL APPROACH TO STORAGE ALLOCATION
Individual images with individual configurations
BOOTING WITH SAN WITH OR WITHOUT VMWARE
Cloned images record only changes from gold-image state
GOLD IMAGE
Approximately 600% space saving
CLONED IMAGES

LEVERAGING SANS WITH WINDOWS SERVERS

SAN RESILIENCY AND DISASTER RECOVERY

UNDERSTANDING THE iSCSI INITIATOR

standard image approach. The only difference is that you can't employ the single set of drivers used within a virtualization platform, so the cloned images become somewhat larger than they would be when using virtualization software.

SAN RESILIENCY AND DISASTER RECOVERY

We all know about using server clusters to provide fault-tolerance for critical applications. However, it's more difficult to achieve data resiliency with clustering, since cross-site clustering is expensive.

An application such as Clustered Continuous Replication (CCR) in Exchange 2007 and log shipping in SQL Server can achieve data resiliency from one server to another. But this functionality can be complex to implement, and depending on the version of Windows used, may require collaboration with the network teams. Such an approach to cross-site clustering is also extremely bandwidth-hungry relative to what is strictly necessary to create data resiliency.

A better approach may be to allow the iSCSI SAN to do the replication for you. Because replication occurs at the block level, you're more confident that the data is valid because of the large amount of error-checking that occurs on the SAN.

An iSCSI SAN can also change your disaster recovery options. Rather than securing data on backup tapes and shipping the tapes off to a disaster recovery location, the information on your SAN is replicated, in near real time, to an off-site location. Should a catastrophe strike, just power up the servers in the standby location, then run some scripts to turn the volume that the replicated data resides on into a writable copy. Just like that, you're up and running again.

Once you're ready to go back to providing service on the production SAN, you can initiate replication in the other direction, and then make the cutover at a time that's convenient to your business. If you initiated the failover to the standby site due to a failure unrelated to the SAN itself, you only need to replicate the blocks that were changed on the replica. Again, the migration back from disaster recovery to production can now be achieved in a short time frame (again, the benefit of data snapshots at work).

There's one more benefit to using iSCSI SAN replication for disaster recovery: You don't have to use the same type of disk hardware in production as in the disaster recovery site. You can deploy Fibre Channel on your production network and SATA in your disaster recovery site to reduce costs—but only if your business realizes that the performance of storage at the disaster recovery site will be a bit lower than that on the main SAN due to the use of lower-speed SATA disks in that site. ■

Understanding the iSCSI Initiator

LEVERAGING SANS WITH WINDOWS SERVERS
○
SAN RESILIENCY AND DISASTER RECOVERY
○
UNDERSTANDING THE iSCSI INITIATOR
●

The iSCSI Initiator is natively installed on Windows Vista and Windows Server 2008–demonstrating Microsoft's support of the software. Installing the iSCSI Initiator on other flavors of Windows enables you to link your computer to a remote target. Here's how.

BY BRIEN M. POSEY

WITH WINDOWS VISTA and Windows Server 2008, Microsoft increased its emphasis on storage area networks (SANs). One of the ways the company did this was by including an iSCSI Initiator with both operating systems.

In an iSCSI environment, storage devices are referred to as targets. A target can be a disk, tape drive or any other SCSI-based storage device. A computer connects to a remote target using the iSCSI Initiator.

To access the iSCSI Initiator:
1 open the Control Panel and click on the System and Maintenance link, followed by the Administrative Tools and the iSCSI Initiator links.

When doing this for the first time, Windows will display a warning message that informs you that the iSCSI service isn't running and asks if you want to start it. If you choose to start the iSCSI service, it will launch automatically each subsequent time that Windows is started.

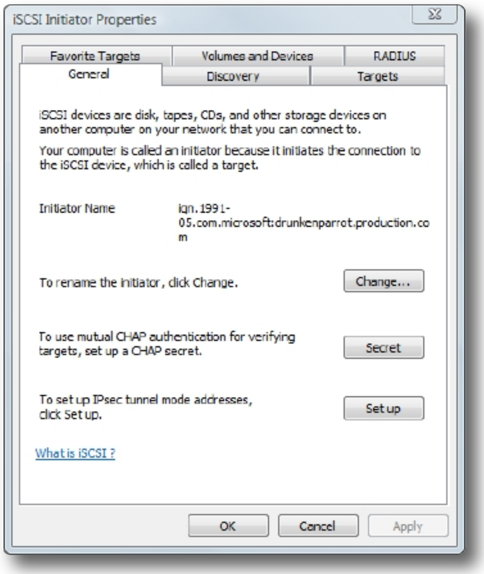
LEVERAGING SANS WITH WINDOWS SERVERS

SAN RESILIENCY AND DISASTER RECOVERY

UNDERSTANDING THE iSCSI INITIATOR

2 Next, you should see a prompt asking if you want to unblock the Windows firewall ports associated with the iSCSI Initiator. Answer **YES**, or Windows will generate an error message when you attempt to connect to a target.

3 Windows then opens the iSCSI Initiator (Figure 1). The properties sheet's **GENERAL TAB** is selected by default. The first option on this tab allows you to change the Initiator's name. Each iSCSI Initiator must be assigned a name, but you can usually use the default name. iSCSI uses three different naming conventions; the Windows implementation uses a naming convention known as IQN, or iSCSI Qualifying Name.



iSCSI devices are disk, tapes, CDs, and other storage devices on another computer on your network that you can connect to.

Your computer is called an initiator because it initiates the connection to the iSCSI device, which is called a target.

Initiator Name iqn.1991-05.com.microsoft:drunkenparrot.production.com

To rename the initiator, click Change.

To use mutual CHAP authentication for verifying targets, set up a CHAP secret.

To set up IPsec tunnel mode addresses, click Set up.

FIGURE 1: *iSCSI Initiator*

The General tab contains a couple of other options. One option lets you specify a CHAP secret, in case you want to use mutual CHAP authentication for verifying targets. Another

WHAT IS... CHAP?

Challenge handshake authentication protocol, or CHAP, is a procedure used to connect to a system. It's considered more secure than the Password Authentication Procedure (PAP). Here's how CHAP works:

1. After a link is made, the server sends a challenge message to the connection requestor. The requestor responds with a value obtained using a one-way hash function.
2. The server compares the response to its calculation of the expected hash value.
3. If values match, authentication is acknowledged; if not, the connection is terminated.

The server can request that the connected party send a new challenge message at any time. CHAP identifiers are changed frequently; the server can request authentication at any time. **—WHATIS.COM**

LEVERAGING SANS WITH WINDOWS SERVERS

SAN RESILIENCY AND DISASTER RECOVERY

UNDERSTANDING THE iSCSI INITIATOR

option gives you the ability to set up IPsec tunnel mode addresses or IPsec encryption.

THE DISCOVERY TAB

The Discovery tab gives you two options for performing iSCSI discovery. One is the ability to manually specify a static list of target portals using the iscsicli. When you do, the iSCSI Initiator will perform an iSCSI discovery login, followed by a Send Targets operation that allows the iSCSI Initiator to acquire a list of available targets.

The other option on this tab provides a list of iSNS servers. iSNS servers give clients a list of iSCSI targets. The idea is that the server is configured with the list of targets so that each client doesn't have to be manually configured with anything but a reference to the iSNS server. If a change needs to be made later, it can be applied to the iSNS server and the clients will be notified of the change automatically.

ADDITIONAL TABS

TARGETS TAB gives you a list of all targets that have been detected. You can then select a target and click the **LOG ON** button to attach to it.

The **FAVORITES TAB** lists your favorite targets. A target is considered a favorite if you have logged into it.

Typically, when you attach to a target, you must associate that target with some sort of volume mount point (usually a drive letter).

The **VOLUMES AND DEVICES TAB** allows you to associate a volume mount point with a target.

Allowing clients to attach to targets without any authentication presents a major security risk. Typically, authentication is performed by a RADIUS Server or an Internet Authentication Server (IAS, Microsoft's own version of RADIUS). The **RADIUS TAB** lets you inform the iSCSI Initiator which RADIUS server you want to use for authentication. You have the option of listing multiple RADIUS servers, which will be used in the order that they're listed. ■

Allowing clients to attach to targets without any authentication creates a major security risk.

Click here to read this full article with figures.

LEVERAGING SANS WITH WINDOWS SERVERS

SAN RESILIENCY AND DISASTER RECOVERY

UNDERSTANDING THE iSCSI INITIATOR

ABOUT THE AUTHORS:

Laura E. Hunter, *CISSP, MCSE: Security, MCDBA, Microsoft MVP, is employed as an Active Directory architect. She is a five-time recipient of the prestigious Microsoft "Most Valuable Professional" award in the area of Directory Services. She is the author of* Active Directory Field Guide, *published by Apress.com, and* Active Directory Cookbook, Second Edition *published by O'Reilly.*

Brien M. Posey, *MCSE, has received Microsoft's Most Valuable Professional Award four times for his work with Windows Server, IIS and Exchange Server. He has served as CIO for a nationwide chain of hospitals and healthcare facilities, and was once a network administrator for Fort Knox. You can visit his personal website at www.brienposey.com.*

SearchWinComputing.com

The Windows Manager's Guide to iSCSI SANs is part of the Windows Manager's Guide series.

Marilyn Cohodas
Editorial Director
mcohodas@techtarget.com

Michelle Boisvert
Editor
mboisvert@techtarget.com

Martha Moore
Copy Editor
mmoore@techtarget.com

Linda Koury
Art Director of Digital Content
lkoury@techtarget.com

Jonathan Brown
Publisher
jebrown@techtarget.com

Matt Salamone
Senior Director of Sales
msalamone@techtarget.com