



Application Note:

SAN/iQ Remote Copy Networking Requirements

SAN/iQ Remote Copy provides the capability to take a point in time snapshot of a volume and copy that data to a remote location. This application note provides an overview of best practices for implementing SAN/iQ Remote Copy into your IP networking environment.

Overview

The SAN/iQ Remote Copy technology is built off the SAN/iQ snapshot implementation. When a snapshot is taken, a read-only volume is created, containing only the changed blocks. This read-only snapshot volume is then copied, block for block, to a designated SAN/iQ cluster, which can reside anywhere IP communication is possible. The remote copy is an asynchronous operation which can use existing IP infrastructure. By capturing and copying only changed blocks, SAN/iQ limits the amount of bandwidth required.

Administrators create and schedule SAN/iQ Remote Copy jobs by selecting a specific start time, occurrence interval, and retention policy. Understanding bandwidth limitations and the amount of data to be copied is imperative to creating a successful SAN/iQ Remote Copy implementation and to meeting organizational data protection and recovery mandates. As with all other features, SAN/iQ manages the remote copy operation at the volume level. SAN/iQ allows administrators to select the individual volumes to copy, frequency to perform the operation, and retention policies.

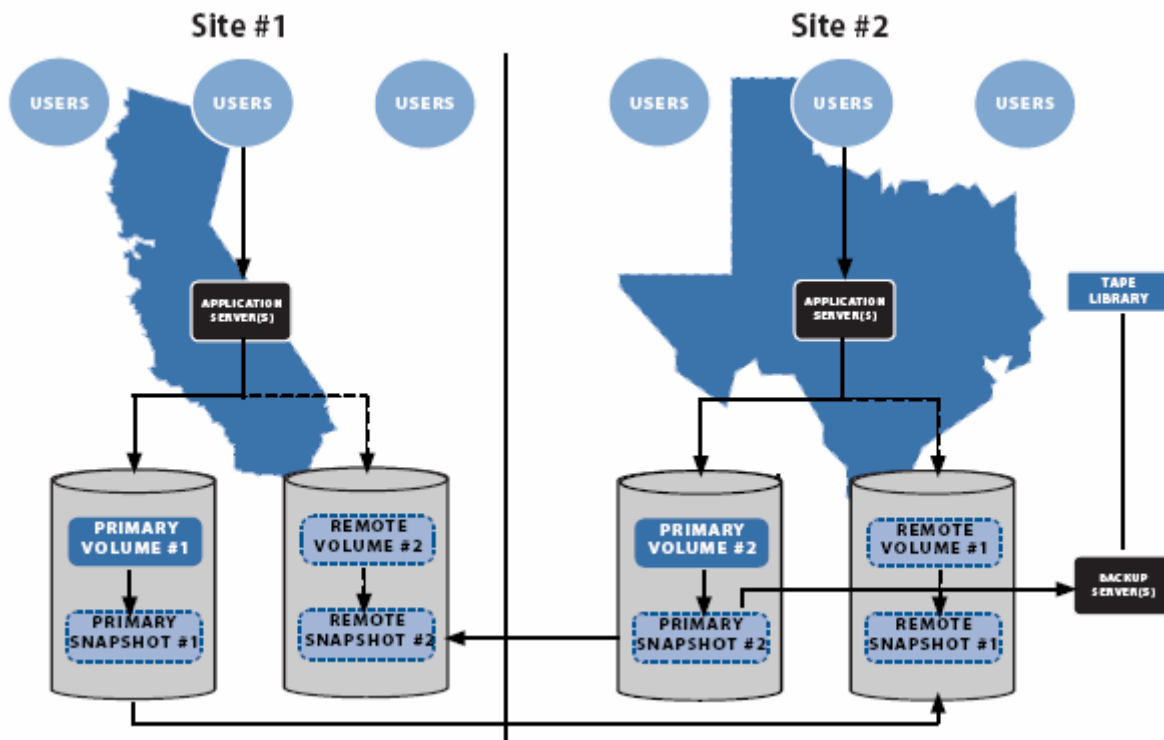


Figure 1. iSCSI SAN Storage Configuration using SAN/iQ Remote Copy



Remote copies can serve many purposes depending on their intended use. Typical uses include disaster recovery at a fail over site, off-site centralized backups, and a “split-mirror” configuration for data migration and content distribution.

Figure 1 shows an example business that has two primary sites of operation. SAN/iQ Remote Copy is being used between the sites as both a means of disaster recovery and for off-site backups. In order to establish a DR site, the primary volume in Site 1 is being remote copied to a remote snapshot in Site 2, and the primary volume in Site 2 is being remote copied to a remote snapshot in Site 1. This creates identical read-only environments in geographically separate locations. Should a disaster take down Site 1, the data that was remote copied to Site 2 is ready to be promoted to a primary, read-write volume and resume activity.

Additionally, a tape backup is being created for both volumes at site 2 by mounting up the snapshots to a separate backup server. With this scenario, not only are there redundant copies of data and means to a quick and simple recovery, but there is also no need to configure another backup environment at Site 1.

IP Networking Requirements

SAN/iQ Remote Copy from one cluster to another cluster may occur on a single IP subnet as well as across routed environments. In the routed environment, the two IP subnets must have IP routes to each target network without Network Address Translation (NAT) or Port Forwarding. Private WAN connections using point-to-point protocols can be used or a VPN tunnel must be setup between two networks that are separated by the public internet. The VPN tunnel effectively acts as one hop on a router and will allow the use of private IP space on each side.

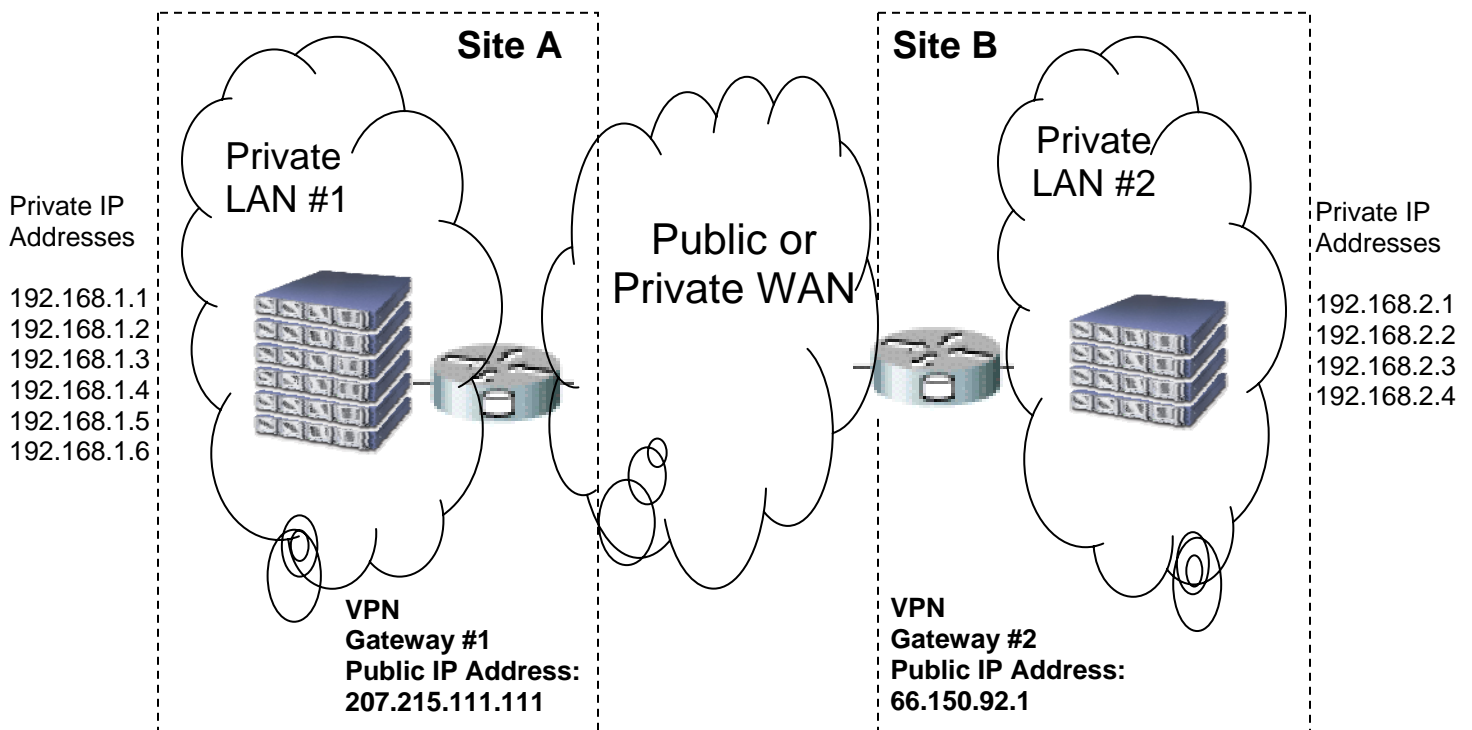


Figure 2. Example IP Network configuration for SAN/iQ Remote Copy using VPN gateways to route TCP and UDP traffic between the two private networks.



SAN/iQ solutions use both TCP and UDP protocols to communicate between the storage modules and to the clients initiating volumes. The amount of connections to each storage module dictates the quantity of UDP ports used. UDP protocol uses port ranges and must not be restricted. TCP ports 13838, 13840, 13841, and 13843 are used by the management console to manage SAN/iQ Remote Copy tasks.

Figure 2 shows how two private LANs can connect using VPN devices over the public internet. Each storage module uses the inside interface of the VPN device as its default gateway. The VPN device encapsulates and encrypts storage module traffic across the public WAN connection allowing the storage modules to communicate with remote peers. The management console must be able to communicate with all of the Private IP Addresses.

Best Practices

- Use a Dial-Up VPN Client on a remote host running the management console to manage SAN/iQ Remote Copy tasks. Tasks may also be managed from either Private LAN.
- Use Private Line Point-To-Point or VPN connections for your SAN/iQ Remote Copy implementations.
- If using existing VPN solutions, dedicate an interface on each end of the VPN for storage traffic.

Scheduling Bandwidth Usage

The size and frequency of the remote copy snapshots are the two main factors affecting the amount of bandwidth needed for an implementation. You can determine the sizes of your snapshots by using the management console and following these steps:

- Setup a local snapshot schedule with the frequency you plan to use, and let this run for a couple days.
- Highlight the Cluster in the management console and click on the "Disk Usage" tab in the tab pane.
- Monitor the sizes of the snapshots, and use this size to calculate the amount of bandwidth required.

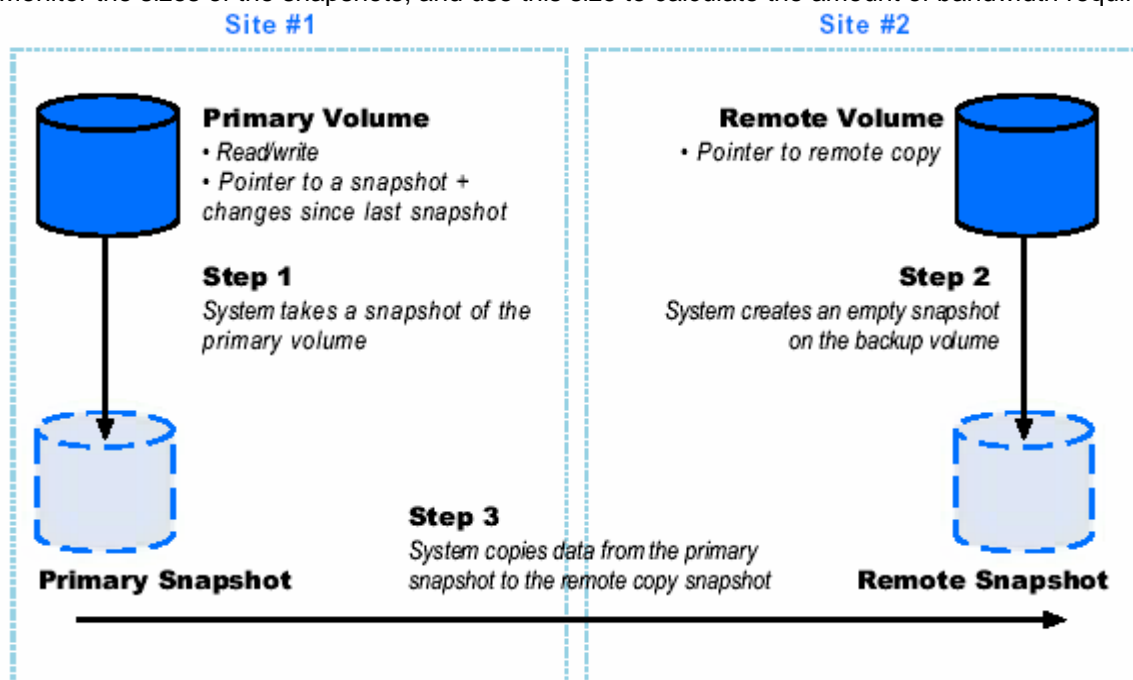


Figure 3. Remote Snapshot Creation. Only changes recorded in the primary site snapshots are copied to the remote site after the initial copy.



Once the amount of change in your volumes over time is characterized, it is time to determine if the amount of bandwidth you have available is adequate to keep up with the frequency.

Figure 3 depicts the creation of a remote volume. Understanding the sizes of the snapshots that are created and transferred is the key to having a successful remote copy implementation.

Estimate Time to Copy

Link speeds are commonly listed in mbits/sec or kbits/sec on lower bandwidth connections. First convert the size of the volume to Bytes. Multiplying the GigaBytes by 1024 to get MegaBytes. Multiply MegaBytes again by 1024 to get to KiloBytes, and again, multiply by 1024 to get Bytes. Multiply the Bytes by 8 to yield the amount of bits. Divide the number of bits by 1000 to yield kbits or again by 1000 to yield mbits. Finally, divide your result by the link speed to get the number of seconds to complete the copy. Convert to the correct order of magnitude, kbits or mbits, before dividing by the corresponding units per second of link speed. After determining the amount of time per each remote copy task, a schedule can be developed by verifying that the actual times fit your proposed schedules.

GigaBytes (GB)	MegaBytes (MB)	KiloBytes (KB)	Bytes	bits	Kilobits	Megabits	Seconds to Copy	Hours to Copy
GB X 1024 = MB	MB X 1024 = KB	KB X 1024 = Bytes	Bytes X 8 = bits	bits / 1000 = kbits	kbits / 1000 = mbits	mbits / link speed = seconds to copy	Seconds to copy / 60 = minutes to copy	Minutes to copy / 60 = hours to copy

Verify Time to Copy

Once you have created a remote copy operation, verify your estimated calculations by selecting the remote copy snapshot, and under the remote snapshot tab looking at the remote copy details.

Remote IP Copy Details

Source Info Primary Mgmt Group: Site2 Primary Snapshot: v2-rsss_Pri.1 Remote Mgmt Group: Site2 Remote Snapshot: v2-rsss_Rmt.1	Time Start Time: 11/30/2005 04:06:52 PM MST Elapsed Time: 15s Est. Time Remaining: 45s Completion Time: N/A
Status Manual Scheduled: Scheduled State: Copying % Complete: 16.5%	Data Data Copied: 27.25 MB Data Remaining: 167.75 MB Current Rate: 14,882 Kb/sec Avg Rate: 14,882 Kb/sec

OK



Utilize Bandwidth Resources

Most commercial internet access connections have symmetric bandwidth both upstream and downstream. Typically, a site will use one stream more than another. Employing Quality of Service technologies can be used to limit the amount of bandwidth your remote copy tasks have available to them. Understanding your link utilization is important when planning your implementation. A table below estimates the time it takes to duplicate 10GB of data to a remote site for particular link speed or bandwidth allocation.

Tune Bandwidth Usage

SAN/iQ Remote Copy is a pull technology and initiates jobs from the remote side of the task. The remote management group should be configured to use only the amount of bandwidth that has been allocated. Use the management console to edit the remote side by Right-Clicking on the Management Group and selecting "Edit Management Group". Use the suggested values in the table below for specifying the Copy Bandwidth setting for use with your link speed.

Link Speed	Remote IP Copy Bandwidth	Estimated Time to copy 10GB
384 kbits/sec	46 KB/sec	62 Hours
768 kbits/sec	93 KB/sec	31 Hours
1.05 mbits/sec	128 KB/sec	23 Hours
1.27 mbits/sec	155 KB/sec	19 Hours
1.54 mbits/sec	188 KB/sec	15 Hours
2.0 mbits/sec	244 KB/sec	12 Hours
3.0 mbits/sec	366 KB/sec	8 Hours
10.0 mbits/sec	1220 KB/sec	2.5 Hours
25.0 mbits/sec	3052 KB/sec	1 Hour
500 mbits/sec	61035 KB/sec	3 minutes
830 mbits/sec	101376 KB/sec	2 minutes

Best Practices

- Limit scheduling of SAN/iQ Remote Copy to three concurrent tasks.
- Ensure that your remote snapshots can complete the copy prior to the next scheduled snapshot.
- Initiate your first remote copy on a schedule with members of your remote cluster at the primary site prior to installing at the remote location. Differential changes only will be copied once you have re-addressed the storage modules and connected to them simultaneously with the management console.
- SAN/iQ Remote Copy can be tuned for high bandwidth, high latency connections (< 250ms). Contact support for detailed information.



Additional References

- SAN/iQ Remote Copy bandwidth tool – used to determine the bandwidth requirements for a specific volume of data and a specific timeframe.
https://www.lefthandnetworks.com/member_area/dl_file.php?fid=213&action=display
- Support Note – SAN/iQ Remote Copy in an Exchange Environment – how to deploy remote copy in an Exchange environment, providing best practices, creating schedules and controlling bandwidth usage.
https://www.lefthandnetworks.com/member_area/dl_file.php?fid=359&action=display

The Information in this article applies to

- SAN/iQ 6.3 and above
- OS independent