Managing Backup SAN’s

Strategies For Troubleshooting
VERITAS NetBackup™ SAN’s With
VERITAS SANPoint Control™ 3.6

Prepared by: John Blumenthal
Technical Product Manager
Storage Management Products
VERITAS Software
November 2003
Introduction ............................................................................................................................................................3
The Emergence of the Backup SAN........................................................................................................................................................................3
Best Practice: A Backup Lifecycle ......................................................................................................................................................7
  Design ........................................................................................................................................................................8
  Configuration and Testing .............................................................................................................................................8
  Production Implementation ..........................................................................................................................................8
  Re-configuration ..................................................................................................................................................8
  Chargeback .......................................................................................................................................................9
  Service Level Agreement .........................................................................................................................................9
Backup SAN Configurations ....................................................................................................................................................9
Common Backup SAN Problems .................................................................................................................................................9
  Troubleshooting Approaches with SANPoint Control 3.6 .................................................................................................12
  Use Case 1: NetBackup can no longer access drives/robots .....................................................................................12
  Use Case 2: NetBackup device discovery cannot see a robot/drive ........................................................................12
  Use Case 3: Intermittent drive failure ........................................................................................................................................13
Troubleshooting Examples .....................................................................................................................................................13
Techniques for Troubleshooting VERITAS NetBackup using VERITAS SANPoint Control 3.6........................................................................14
  Launching SANPoint Control ..........................................................................................................................................14
  Connectivity/device check ...........................................................................................................................................14
  Log Correlation .....................................................................................................................................................14
  SAN Traceroute ..................................................................................................................................................15
  Configuration management .........................................................................................................................................15
Future considerations for Backup SANs .........................................................................................................................................15
  Mixed Fabrics ..........................................................................................................................................................15
  VSANs ....................................................................................................................................................................15
  Server-free ..............................................................................................................................................................16
  Security ..................................................................................................................................................................16
  Disk-to-disk ..........................................................................................................................................................16
  Backup and Restore Optimization ........................................................................................................................................16
Summary ........................................................................................................................................................................16
**Introduction**

This paper describes tips and techniques for troubleshooting VERITAS NetBackup\textsuperscript{TM} implementations in storage area network (SAN) environments using VERITAS SANPoint Control\textsuperscript{TM} 3.6. A backup lifecycle approach is suggested along with backup system patterns, both enabled by SANPoint Control 3.6. Some familiarity with NetBackup is assumed but not required as the use of SANPoint Control 3.6 on backup SAN’s can be useful with other backup applications.

**The Emergence of the Backup SAN**

Backup was among the first applications implemented on Fibre-Channel-based storage area networks (SAN’s) in a logical and swift evolution from traditional, direct-attached configurations. This evolution is by no means complete. Enterprises continue to leverage commodity storage and network technology to meet the unremitting growth of data and unchanging rules of business and backup: resources must be shared to maximize utility and backup windows must be minimized or eliminated. NetBackup and SAN’s, managed in combination by SANPoint Control 3.6, introduce new economic and technical capabilities to the mix.

Direct-attached, LAN-based backup emerged in the 1990s as the primary approach to backup. Clients (i.e. servers with DAS) backed up across the LAN at the direction of a master server to a backup server, which controlled tape devices.

*Diagram 1: the first use of a SAN for backup applications allowed shared storage over a dedicated, high-capacity direct connection. Backup traffic remained on the IP LAN: backup data paths are indicated by dotted lines.*
Very quickly the network became the bottleneck as both data and clients proliferated. A new topology using increased networking bandwidth and switching was adopted to keep pace: LAN-free back-up had arrived. Administrators began installing hi-speed NIC's in servers with large amounts of DAS and used a separate network segregated from the production network as a new backup path.

Diagram 2: Network offloading achieved through the use of a segregated IP LAN from the client network. A dedicated and direct FC SAN enabled the sharing of backup devices: backup data paths are indicated by dotted lines.
IP routing and switching on the backup LAN provided the necessary sharing of resources but this, too, began to bog down as data growth rates mushroomed and backup windows shrunk. At this point, leading administrators began to experiment with SAN’s to avoid further segmentation of the network by using an I/O optimized protocol on a higher bandwidth pipe. By the end of the 1990s LAN-free implementations were commonly found using FC-based SAN’s in major enterprises.

Diagram 3: Advanced backup on a SAN sharing both primary and backup data paths; backup I/O is confined to the FC SAN in a first step to fabric-based backup.
State of the art enterprise backup is represented in the above diagram. However, this is not to say the evolution is complete since LAN-free – even using SAN’s – does not fundamentally change the relationship between backup targets and backup resources over a network. The next step is to disconnect the backup target completely through server-free backup using SAN’s over FC or iSCSI:

Diagram 4: next generation backup: server-free, wholly contained within the SAN fabric. Backup data paths are indicated by dotted lines.
Backup is now embedded in the fabric itself, where (scsi3) extended copy engines move data to tape devices optimally located on the SAN. Backup clients are no longer involved in the backup process and data is read directly from disk and written to tape with no impact on the host or applications it serves.

What is most instructional about the last ten years of backup in the enterprise is the ongoing concern with and segmentation of the network as windows remain fixed, data grows, and tape-drives added. Increasingly the troubleshooting of a backup process is less fixed on storage and more on the network – a trend that will continue with disk-to-disk backup approaches and virtual SAN’s implemented over iSCSI and FC. At the heart of decisions around backup design and migration in the face of these new approaches is a consistent and deep understanding of the network. Where should backup devices be located on the fabric? How should I zone to optimize backup? When should I move to disk-to-disk or server-free technologies? These questions require network-level analysis and capabilities. SANPoint Control 3.6 provides these network insights and approaches needed for the entire backup lifecycle, from problem identification and resolution to design, production and re-configuration.

**Best Practice: A Backup Lifecycle**

Backup practices do not develop in a vacuum isolated from the intense pressures of running an enterprise production environment. Historically backup systems were put in place out of necessity and grew in a relatively unplanned manner, only changing when necessary. In large enterprises, however, the lack of systems engineering has reached a critical point where new types of management are required to run backup applications in a consistent, reliable, and predictable manner. To that end the introduction of SANPoint Control 3.6 into NetBackup environments creates a systematic approach to solving backup problems and planning for change. A backup lifecycle is created that integrates backup operations with the management of the network – the SAN on which NetBackup functions:

![Diagram 5: Backup and recovery application lifecycle](image)
Design

Few administrators design backups from a systems perspective simply because they have limited access or visibility into the SAN on which they are deploying. SANPoint Control 3.6 brings that perspective to NetBackup environments and can be used during a design phase to determine where on the SAN a backup system should be deployed – or whether re-configuration of the SAN may meet schedules while minimizing hardware procurement and application impact. The “context” of the backup can be captured by analyzing the trending reports available in SANPoint Control 3.6 to understand the peaks and valleys of production loads on a backup SAN, segregated from the disk SAN or connected to it. Finally, SANPoint Control 3.6 assists the backup architect in building impact studies for recovery loads and I/O paths. What happens if application X requires a full restore during production hours?

Configuration and Testing

Most customers test backup systems extensively prior to implementation. Benchmarking and tuning during this phase using SANPoint Control 3.6 provide performance metrics and baselines for end-to-end I/O capabilities over a given backup path (host-side HBA, bridge, array, tape-drive). Problem isolation in the I/O path with SANPoint Control 3.6 further qualifies the backup SAN for future troubleshooting and configuration changes.

Production Implementation

During this phase connectivity issues are often encountered, particularly in determining whether a host can see through the entire I/O path to the target backup device. SANPoint Control 3.6 provides full visibility into the path through useful tools such as SAN Traceroute and associated performance statistics. Storage Groups and Accounts within SANPoint Control 3.6 are often used as logical containers for applications running on the fabric and backup SAN Traceroute reports can be run to isolate backup performance and troubleshooting to a specific application or host. Once in production the backup system generally runs without modification while SANPoint Control 3.6 provides event management and alarm capabilities a SAN administrator can leverage to better analyze NetBackup events.

Re-configuration

New applications, new business rules and data growth rates demand re-configuration of the system. SANPoint Control 3.6 may be used to save previous configurations and then reconfigure through zoning, masking, and binding operations on the fabric and storage elements. By saving previous configurations and trending data, the newly configured fabric can be optimized and measured for efficiency improvements. In addition, SANPoint Control 3.6 can again be used in the new backup cycle introduced by a re-configuration as described above (a re-configuration best practice calls for revisiting the Design, Testing, and Implementation phases above).

Once a backup lifecycle process governs the use and administration of an enterprise backup system, standard IT accounting measures can be implemented. The lifecycle creates a consistent, repeatable, structured and reliable set of data on which to measure backup performance and impact. Measurement enables accounting:
Chargeback

A stable, consistent, and predictable backup SAN monitored by SANPoint Control 3.6 provides the detail needed to determine the cost of a particular backup: NetBackup supplying tape usage statistics and SANPoint Control 3.6 fabric use. Once cost is known the backup services can be measured and accounted for in a charge-back accounting package such as VERITAS’ CommandCentral Service http://www.veritas.com/products/category/ProductDetail.jhtml?productId=service_manager.

Service Level Agreement

By comparing SANPoint Control 3.6 fabric statistics and errors with NetBackup backup success/failure reports, a customer can build service level agreements with business units, confident in the ability to analyze root causes of backup failures (and their incidence) since a full view of the SAN in which NetBackup runs is now available.

Backup SAN Configurations

Backup SAN's are an instance of “application-specific SANs.” Configured and optimized for the sustained, streaming throughput characteristic of backup operations, they can be found connected or disconnected to the primary, on-line storage SAN. Both have advantages and disadvantages:

Diagram 6: An integrated fabric for primary storage and backup I/O.
Integrating the fabrics to create a general-purpose fabric maximizes the use of hardware. Zoning and masking keep production data and backup I/O paths segregated and safe from one another. SANPoint Control 3.6 is used to determine whether fabric saturation is reached, requiring a re-configuration. Disadvantages may include increasing hop counts faster than a segregated backup SAN when re-configuration is required over E Port expansions. Transitioning this fabric configuration to a server-free backup operation is relatively straightforward, especially if SANPoint Control 3.6 trending reports are available to help determine where xcopy-enabled backup devices should be located.

More frequently, NetBackup customers use the Shared Storage Option (SSO) on a dedicated backup SAN that is segregated from the on-line disk storage SAN. While smaller hosts continue to backup over the LAN, larger hosts contain an HBA and write directly to the tape-devices on the backup SAN in a LAN-free configuration:

![Diagram 7: A segregated SAN, commonly used to isolate backup I/O from primary storage.](image-url)
Segregating the SAN’s (much like previous IP-network approaches) offloads the production, on-line fabric. However, much of the capacity of the backup SAN remains unused outside of backup windows. As the primary fabric demands increasing backup services, SANPoint Control 3.6 can be used to re-zone and partition the excess capacity of the Backup SAN to the primary fabric, integrating the two fabrics over an E Port. With core-edge topologies becoming increasingly popular, these re-configurations will help maximize fabric utilization for backup:

No matter what topology is used to configure for NetBackup operations, SANPoint Control 3.6 provides a single point of administration for zoning and masking the fabric according to NetBackup device and class configurations. Storage units, for example, in NetBackup can map to a specific zone alias and configuration in SANPoint Control 3.6. Future versions of SANPoint Control 3.6 will be aware of NetBackup modifications to Storage Units and associated classes and will intelligently analyze current zoning to optimize how a Storage Unit is used by NetBackup on the fabric.
Common Backup SAN Problems

Troubleshooting Approaches with SANPoint Control 3.6

Most common NetBackup problems on SAN’s can be reduced to three general cases, all centered on connectivity in the SAN. To that end SANPoint Control 3.6 provides monitoring, event management, configuration, and reporting on all the elements in the SAN: hosts, HBA’s, switches, bridges, arrays, tape drives and robots. SANPoint Control 3.6 is an ideal tool to rapidly diagnose a backup failure that occurs during any phase of the backup lifecycle outlined previously.

Use Case 1: NetBackup can no longer access drives/robots

Typically found as an error 213 in NetBackup, this problem represents a loss of connectivity. The NetBackup admin will check the device monitor inside NetBackup and see it is downed. The backup job will have failed and the NetBackup admin will try to re-up the device; the backup will still fail. Next, the admin may go to the media server host and check syslog, device logs, and the NetBackup logs (looking for errors 219 and 213). But in addition, users should look for NetBackup errors 83-86 as they relate to read, write, open, and position failures to access a drive.

The admin will then try a robot test to determine connectivity and if this fails, a hardware problem may be the root cause. However, a quick check for fabric health is also required since an error in the I/O path through the SAN could have caused the backup failure. The user should configure NetBackup to launch SANPoint Control 3.6 in-context from within the NetBackup management console. A rapid view of fabric health and recent events quickly narrows the analysis. In-context launching of applications such as NetBackup can be found on p. 120ff in the SANPoint Control 3.6 Administrator’s Guide.

Use Case 2: NetBackup device discovery cannot see a robot/drive

The visibility of devices to NetBackup is one of the most frequent troubleshooting issues. Typically a NetBackup admin installs a new device and runs device discovery to configure it. When device discovery is run it fails to see the newly installed device. Again, launching SANPoint Control 3.6 at this time will generate a view of fabric health to check for SAN connectivity problems. But more importantly, SANPoint Control 3.6’s SAN Traceroute utility (found under the Wizards menu option in the console) should be used to make sure the full I/O path is functional. Select SAN Traceroute within SANPoint Control 3.6 and define the two endpoints: the host being backed up and the target tape device. If the I/O path trace route fails, SAN Traceroute will reveal where the failure occurs and the admin can focus investigation on the connectivity in the hardware at the final point in the trace route.

The ability to see through the full I/O path on the backup SAN is particularly useful for snapshot (using NetBackup FlashSnap) classes. In these configurations, the NetBackup media server must be capable of seeing all devices it orchestrates for the backup: disk array, disk cache, data mover, library, and drive. Connectivity must be correct. In addition, the third-party copy command in NetBackup generates a configuration file that drives the backup orchestration, using WWN’s — and if the SAN has been modified these WWN’s may not reflect the changes, causing the backup to fail. SANPoint Control 3.6 contains all current WWN’s in the fabric and can be used to determine whether fabric changes require modifications to NetBackup’s config file for third-party copy commands (bptpc).
Use Case 3: Intermittent drive failure

A drive fails and causes a backup failure; yet when the admin looks at the drive everything looks fine. The admin will continue to up the drive, seeing it respond correctly when the backup is re-initiated. Launching SANPoint Control 3.6 in context at this time will add a broader context to the view of drive status – to see whether the drive remains attached to the fabric. Once verified that connectivity is established, the NetBackup admin can look at the SANPoint Control 3.6 event logs for the fabric, analyzing events around the time of the drive failing.

Troubleshooting Examples

Example 1: A bank continued to experience drives being downed. This was critical to resolve as inline tape copy was being used to conduct concurrent backups, one locally and one for disaster recovery purposes across a DWDM to a remote site. Write failures continued to accompany the downed drives in the NetBackup logs. Standard troubleshooting procedures were followed: watching the drive mount, the write initiation, then watching the command time out, sometimes with SCSI errors. A launch of SANPoint Control 3.6 revealed intermittent errors in the DWDM, which proved to be the culprit in generating higher-level errors at the SCSI layer, which in turn caused the drive time-outs. The DWDM component was replaced and backups ran successfully.

Example 2: A financial services company continued to experience error 213s on an intermittent basis. Investigations into the NetBackup media server HBA and target backup drives did not reveal problems. Looking at SANPoint Control 3.6 events and reports, however, showed a switch port going offline intermittently, which produced SCSI transport error messages.

Example 3: An insurance company administrator (working separately from the backup administration team) re-zoned a portion of a general-purpose fabric, causing error 213s. The NetBackup administrators noticed the failures and used SANPoint Control 3.6 to analyze fabric changes that broke backup operations. Today they coordinate their zoning operations through SANPoint Control 3.6 for systematic change management.

Example 4: A large retailer experienced backups failing because of intermittent bridge failure. Periodically the bridge panic'd when too many hosts were zoned to it. SANPoint Control 3.6 was used to determine the zoning threshold to work with the vendor to correct the firmware bug as well as to coordinate the reconfiguration of the SAN as an interim work-around.

Example 5: A telecommunications provider found periodic backup failures. A launch of SANPoint Control 3.6 and the use of SAN Traceroute between the host and the target backup device indicated a prompt failure at the HBA of the host. A quick glance at the HBA configuration through SANPoint Control 3.6 and how it was configured to the fabric indicated a device driver mis-configuration -- preventing NetBackup’s bptm requests from being issued to the tape drive.
Techniques for Troubleshooting VERITAS NetBackup using VERITAS SANPoint Control 3.6

The following SANPoint Control 3.6 techniques can be used for rapidly diagnosing NetBackup errors. In general, a backup failure on a SAN should be investigated using SANPoint Control 3.6 in the following order:

Check the current fabric state:

Step 1: Launch SANPoint Control 3.6 from within NetBackup to check fabric health
Step 2: Launch SAN Traceroute to isolate problems in I/O path

Check past fabric state:

Step 3: Check SANPoint Control 3.6 events and reports for fabric events around the time of the NetBackup error log entry
Step 4: Check event alerts sent from SANPoint Control 3.6 to NetBackup administrators
Step 5: Check fabric changes around the time of the NetBackup error

Details on each are provided below:

Launching SANPoint Control

The ability to launch SANPoint Control 3.6 from within NetBackup (or launching NetBackup from within SANPoint Control 3.6) is valuable for determining root cause problems quickly when related to SAN connectivity. In addition, NetBackup administrators and SAN administrators often work in different groups; SANPoint Control 3.6 provides a common troubleshooting approach that diminishes time to resolution. SANPoint Control 3.6 can be configured to launch in view-only or administrative modes, depending on the user’s role definition. To configure launching of SANPoint Control 3.6, make sure you have installed the SANPoint Control 3.6 web engine to provide browser based access to the server. This will permit view-only operations to NetBackup operators to gain immediate connectivity and alarm information required for rapid problem resolution.

Connectivity/device check

Within SANPoint Control 3.6 set up alarm policies on all NetBackup devices in the SAN. Include these and other general fabric health alarms to send alerts to NetBackup administrators via email or SNMP traps to another general console. Within SANPoint Control 3.6 you should also make certain to set an alarm policy on the NetBackup Mediaserver hosts to alarm on stale O/S handles for the backup devices they manage. Changes to these devices will cause backups to fail. This speeds up the troubleshooting process.

Log Correlation

With NetBackup 213s and 80s errors, the user should look at timestamps and launch SANPoint Control 3.6 to open the event monitor and reporting interface. Queries should be conducted around the NetBackup timestamp range to correlate NetBackup errors with SAN events that may be the root cause. Once the SANPoint Control 3.6 console is open, go to Window Reporter and select the Alerts reports.
SAN Traceroute

Once SANPoint Control 3.6 shows the fabric to be healthy but the backups continue to fail, the user should launch SAN Traceroute (from the Wizards menu option in the console) and initiate a test of the I/O path from host to target tape device.

Configuration management

Zone changes may break backup configurations. Device changes can change WWN settings on which NetBackup third party copy depends. SANPoint Control 3.6 should be launched to determine what fabric and device changes have occurred around the time of the backup failure. SANPoint Control 3.6 maintains a complete picture of the SAN on which backups operate that can be exported periodically and saved to check for modifications. Frequently operators will mistakenly reconfigure elements on the fabric without notifying other users: hosts, drives, hubs, zones may change without administrative coordination, causing backups to fail. It’s important to be able to detect the connectivity changes and then be capable of viewing the older configuration to determine what has changed. To export your SAN configuration, simply go to the SANPoint Control 3.6 console under the File|Export|Objects to File. This will save your environment to an XML file for subsequent viewing. You can also programmatically dump your environment using the vxsalcmd get hinv command (see p. 246 of the SANPoint Control Administrator’s Guide)

Future considerations for Backup SANs

Your topology WILL change. Having a SAN management solution like SANPoint Control 3.6 in place before business requirements demand change adds tremendous value to troubleshooting, optimizing, and configuring your backup SAN. Now is the time to gather all statistics possible to understand the environment in which your backup systems operate and to plan and prove the business case (with a quantitative baseline) for future reconfigurations or hardware and software procurement. In addition, SANPoint Control 3.6 reduces the number of failed backups while speeding problem resolution through root cause isolation and facilitating common approaches between NetBackup administrators and SAN managers.

Here are future developments related to backup SAN’s where SANPoint Control 3.6 can help plan, design, configure, manage, and monitor:

Mixed Fabrics

Enterprises are moving to core-edge topologies as they consolidate storage. As a consequence, legacy switching technology is leveraged by being placed at the edge or to re-constitute the backup SAN. However, not all switching vendors interoperate well with zone configuration exchanges or state change information. SANPoint Control 3.6 is important for monitoring the health of these mixed fabrics.

VSANs

By the end of 2004 most switch vendors will offer the ability to zone across E Ports, creating a “Virtual SAN” which spans two or more switches. This type of zoning may prove to be very useful for segmenting portions of the fabric for dedicated backup, using the VSAN capabilities in the switch to segregate the backup SAN where it had previously been physically separated. SANPoint Control 3.6 is a requirement in these environments because of the need to “de-virtualize” the VSAN in order to troubleshoot, optimize, and manage it.
Server-free

It is likely that xcopy engines will be embedded in switches in the next generation of products being brought to market in 2004 and 2005. When combined with VSAN capabilities, determining optimal zoning configurations and I/O paths for the "virtual" backup SAN will require fabric-wide visibility and statistical analysis using SANPoint Control 3.6.

Security

Standardizing and coordinating fabric configuration management will be needed to coordinate NetBackup operations with SAN management, especially as fabrics contain mixed products and the separation of the backup SAN from the primary online SAN is virtual and not physical.

Disk-to-disk

One potential for backup revolution involves emerging disk-to-disk (D2D) backup technologies. By introducing a staging platform for backup and recovery between the primary online SAN and the backup SAN (which takes staged data to tape) I/O can be optimized for both backup and recovery, while VSAN capabilities present the staging area to both SAN’s. With a new layer of I/O – a kind of giant cache – between the primary online SAN and backup SAN, management and monitoring of events in and around this new layer will be required. How should the D2D tier be configured? Where should it reside on the SAN? Answers to these network architecture questions require the type of visibility and quantitative data available in SANPoint Control 3.6.

Backup and Restore Optimization

Server-free, VSAN's and disk-to-disk bring with them a new type of optimization for backup operations. NetBackup administrators using SANPoint Control 3.6 will have three knobs to turn (before reconfiguring the SAN or purchasing additional hardware): zoning, masking, and binding. SANPoint Control 3.6 provides these knobs and the measuring tools to continue refining the SAN configuration to meet business requirements for backup and recovery. In addition, NetBackup administrators can look at SANPoint Control 3.6 reports and trending data to analyze what impact a restore may have if required during peak production hours. Where resource contention exists the data may provide the business case for re-configuring the SAN or adding more hardware to insure capacity in the event of a massive restore requirement.

Policy based SAN backup

Once a SAN has been optimized and observed over time it may be possible to implement policies for automating the temporary rezoning of a switch to accommodate a backup during slow production times. One example is the use of pre- and post-backup scripts to alternate use of the snapshot platform. Policy driven backup in this case may delay the need for additional hardware purchases.

Summary

Backup SAN's were among the first in the market and remain central to enterprise SAN development. These same SAN's are now undergoing fundamental changes driven by new business demands and new market economics. Management and measurement of backup performance requires a SAN management approach enabled by SANPoint Control 3.6 and integrated with NetBackup. With the visibility provided by SANPoint Control 3.6 into the underlying capabilities of the SAN, a backup lifecycle can be implemented to build utility-like quality and accounting for NetBackup.