BACKUP AND RECOVERY DESIGN PHILOSOPHY

There are a number of technologies that offer various options for backup and recovery implementations. The decision-making process for the selection of a specific technology needs to be based on the business requirements and SLAs defined by the organization for each of the services provided by its data center. For example, a messaging service might be considered more of a mission-critical service compared to another service provided by a data center. Thus, an SLA for a messaging service would have more resources associated with it than the SLA of another service. SLAs need to be defined in cooperation with the users of each service.

After performing a detailed analysis of business requirements and having defined mutually acceptable SLAs, the technical aspects of the backup and recovery solution can be explored. The following sections discuss the different backup modes, types, topologies, and factors that need to be taken into account while designing backup and recovery solutions.

Backup Modes

Backup mode determines how the backup is carried out in relation to the data that is to be backed up. There are two ways in which data backups can take place:

- **Online backups:** Backups are taken while data is still accessible to users.
- **Offline backups:** Backups are made of data that is first rendered inaccessible to users.

Online Backups

Online backups are performed when the system is online, thereby providing a least interruptible strategy. They are commonly used for applications that must be available 24 hours a day such as Microsoft® Exchange and Microsoft SQL Server, Oracle which support online backups.

Advantages

Advantages of online backups include:

- **No service interruption:** Applications and data remain fully available to users during the backup process.
- **Out-of-hours backup not required:** Online backups can be scheduled during normal operating hours.
- **Complete or partial backup:** Backups can be either complete or partial.

Disadvantages

Disadvantages of online backups include:

- **Server performance:** During the backup process, there may be performance degradation on production servers.
- **Open files:** Depending upon the applications that are active during the backup

process, some open data files may not be backed up.

Offline Backups

Offline backups are performed by taking the system and services offline. They are used in cases where point-in-time images of the system need to be taken, or where the application does not support online backups.

Advantages

Advantages of offline backups include:

- **Complete or partial backup:** With offline backups, it is possible to choose between complete or partial backups.
- **Performance:** Offline backups result in better backup performance because the server can be dedicated to the backup task.
- **All files backup:** All data is backed up because there are no running applications, which keep files open during the backup process.

Disadvantage

Service interruption: The disadvantage of offline backups is that data is not accessible to users while the backup process is running.

Backup Types

Various types of backup can be used for online and offline backups. An individual environment’s SLA, backup window, and recovery time requirements determine which method or combination of methods is optimal for that environment.

Full Backups

A full backup captures every piece of data round the clock, including files on all hard drives. Each file is marked as having been backed up; that is, the archive attribute is cleared or reset. One up-to-date full backup tape can be used to restore a server completely at a given point in time.

Advantages

Advantages of full backups include:

- **Full copy of data:** A full backup means that a complete copy of the data can be easily made available if a system recovery is needed.
- **Rapid access to back up data:** There is no need to search through several tapes to find the file that is to be restored because full backups include all the data on the hard disks at a particular point of time.

Disadvantages

Disadvantages of full backups include:

- **Redundant data:** Full backups hold redundant data, because both changed and unchanged data is copied to tape every time a full backup is performed.
- **Time consuming:** Full backups take longer to perform and can be very time consuming.

Incremental Backups

An incremental backup captures every piece of data that has changed since the most recent full or incremental backup. A full backup tape (no matter how old) and all subsequent sets of incremental backups must be used to restore a server. An incremental backup marks files as having been backed up; that is, the archive attribute is cleared or reset.

Advantages

Advantages of incremental backups include:

- **Efficient use of time:** The backup process can be carried out in less time because only data that is modified or created since the last full or incremental backup is copied to tape.
- **Efficient use of backup media:** Incremental backup takes up less tape space as compared to other types of backup because only the data that is modified or created since the last full or incremental backup is copied to tape.

Disadvantages

Disadvantages of incremental backups include:

- **Complex full restores:** A full system restore may involve restoring data from an incremental set of multiple tapes because the data may be spread over multiple tapes since the last backup.
- **Time consuming partial restores:** Carrying out a partial restore often means searching through several tapes to find the required data.

Differential Backups

A differential backup captures data that has changed since the last full backup. A full backup tape and the most recent differential tape are needed to perform a full system restore. It does not mark files as having been backed up (that is, the archive attribute is not cleared).

Advantage

Rapid restore: The advantage of differential backups is that they are faster than incremental backups because there are fewer tapes involved. A full restore requires two tape sets at the most—the last full backup and the last differential backup tape.

Disadvantages

Disadvantages of differential backups include:

- **Longer and larger backups:** Differential backups require more tape space and more time than incremental backups because the longer it has been since a full backup, the more data must be copied to the differential tape.
- **Backup time increases:** The amount of data that is backed up increases each day after a full backup.

Backup Topologies

Originally, the only type of storage technology that required backup involved hard disks connected directly to storage adapters on servers. Today, this kind of storage is known as direct-attached storage or DAS. The backup and recovery landscape has changed markedly with the development of technologies such as SAN and NAS. SAN environments in particular provide a significant opportunity to optimize and simplify the backup and recovery process.

Backup and recovery topologies can be classified according to the storage technology (DAS, NAS, or SAN) that needs to be backed up. The topologies covering each storage type are local server backup, LAN-attached NAS backups, and SAN-based systems, respectively.

Local Server Backup and Recovery

In a local server backup configuration, each server connects to its own backup device, usually through a SCSI bus. Local area network (LAN) bandwidth is not consumed in this case but storage media must be managed manually on the local server.

The following figure depicts a typical local server backup and recovery mechanism.

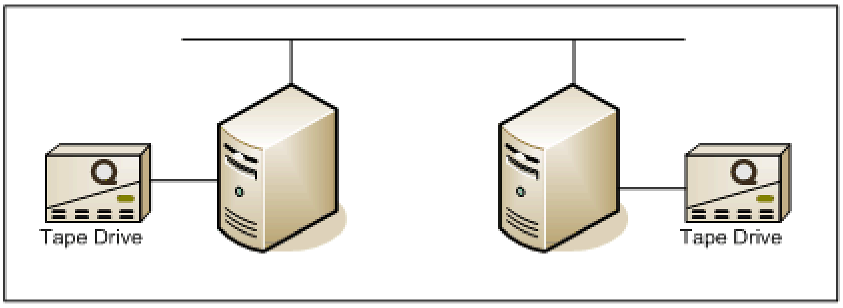

Figure 1. Local Server Backup and Recovery

Advantages

Advantages of local server backup and recovery include:

- **No network resource consumption:** Local server backup and recovery configurations do not use network bandwidth because servers are connected to tape devices that are usually connected through a SCSI interface.
- **Faster backup and recovery:** These backups can be relatively faster than other backup configurations because data does not have to travel through the network.

Disadvantages

Disadvantages of local server backup and recovery include:

- **Limited capability for centralized management and scalability:** The local server backup and recovery configuration does not offer scalability and centralization capabilities because media management has to be managed locally at each server.
- **Higher costs for backup software and tape hardware:** This configuration can significantly increase the cost of backup software licenses and tape devices because each backup configuration is configured for each server and managed individually.

LAN-based Backup and Recovery

LAN-based backup installations are a common solution in enterprise scenarios and have been in use for quite some time. Enterprise LAN backup software uses a multi-tier architecture in which some backup servers kick off jobs and collect metadata about the backed up data (also known as control data) while other servers (designated as media servers) perform the actual job of managing the data being streamed to the tape drives.

Enterprise LAN backup technologies usually have three components:

- **Central backup server:** Hosts the backup engine, which controls the backup environment.
- **Media server:** Handles data movement and manages media resources.
- **Client agent:** Application-specific agents, such as for file system data, Microsoft Exchange data, Oracle, and Microsoft SQL Server data.

The following figure illustrates a logical LAN backup and recovery system.

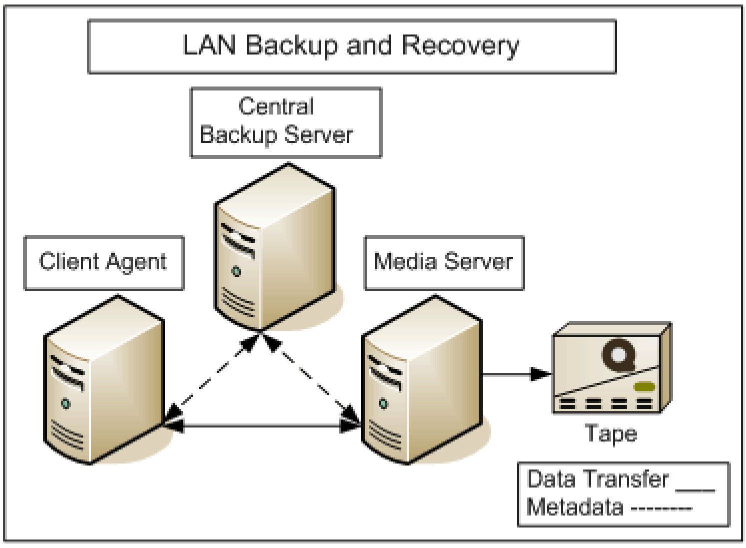

Figure 2. LAN Backup and Recovery

Advantages

Advantages of LAN-based backup and recovery include:

•Tape drives no longer need to be directly attached to servers for backup.
•Backup application runs on dedicated backup servers.
•Client agents push data over the LAN to a backup server.
•Higher level of scalability and sharing of single tape devices.

Disadvantages

Disadvantages of LAN-based backup and recovery include:

•Large data set sizes can cause performance degradation on servers and the network.
•Additional backup traffic consumes network bandwidth.
•Scheduling of backup and recovery becomes critical.

Backup of NAS devices can take place using backup agents or network data management protocol (NDMP). For further information, refer to the "Service Design for NAS Devices" section in this blueprint.

SAN-based Backup and Recovery

The ability to integrate disk space subsystems with backup and recovery provides a number of options for deploying data protection solutions in SAN-based environments. Underlying SAN technologies provide several backup and recovery alternatives for data residing in SAN storage. Details of these options are explored in the "Service Design" section in this blueprint.

The following figure illustrates a SAN-based backup scenario.

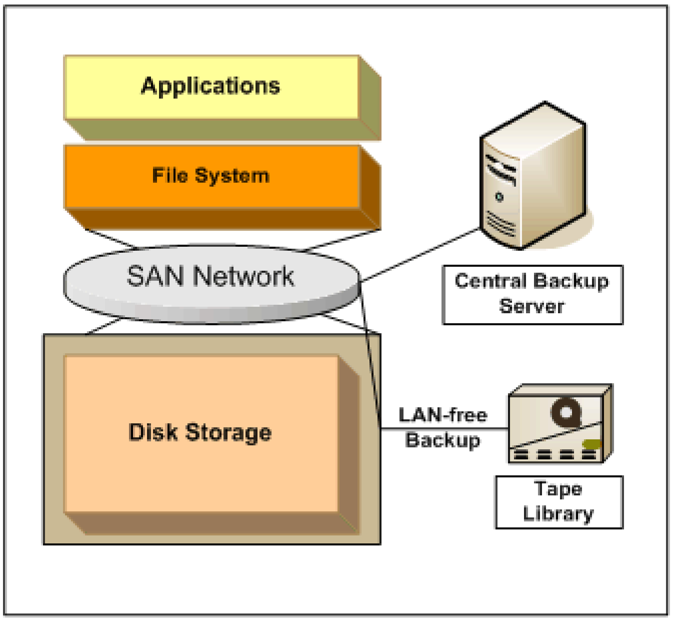

Figure 3. Sample SAN Backup Scenario

Advantages

Advantages of SAN-based backup and recovery include:

- **Reduced server load:** The path between the storage device and the backup device does not involve the server, which means load on the server is reduced.
- **Reduced LAN load:** Backups can take place without requiring data to cross the LAN.
- **Storage optimized solution:** SANs are designed to optimize the efficiency of data transfers, enabling quicker backup and recovery processes.

Disadvantages

Disadvantages of SAN-based backup and recovery include:

- **Expensive to implement:** SAN-based backup requires a SAN, which is expensive to design and deploy.
- **Device compatibility:** Backup and recovery devices must be SAN-compatible.

Using Snapshot Technologies for Backup and Recovery

A snapshot is a mechanism that provides a consistent image of a given file system or data volume at a specific point in time. When integrated with backup and recovery, snapshots can provide powerful data protection and a high-availability solution with little or no impact on production servers or network resources. A snapshot image can be used as the reference point for a backup operation, and primary data can continue being modified without affecting the backup operation once the snapshot has taken place. This approach fulfills the need for windowless backups and near-instant restores.

Snapshot technology can be broadly classified into two categories:

- **Hardware-based snapshots:** Snapshots that depend on disk subsystems and are performed at the disk space subsystem level.
- **Software-based snapshots:** Snapshots that use copy-on-write functionality and are performed at the host system level.

The choice between these two options depends on the number of host systems and production data needing the snapshot. Because the snapshot does not in itself include backup and recovery functionality, it is important to integrate and coordinate the snapshot and backup operations with the application that manages the data in order to obtain a consistent and reliable version of the data on backup media.

The following figure illustrates a software-based snapshot using a copy-on-write process.

Note: Hardware-based snapshot techniques depend directly on the selected hardware solution; therefore, they are not presented in any detail here.

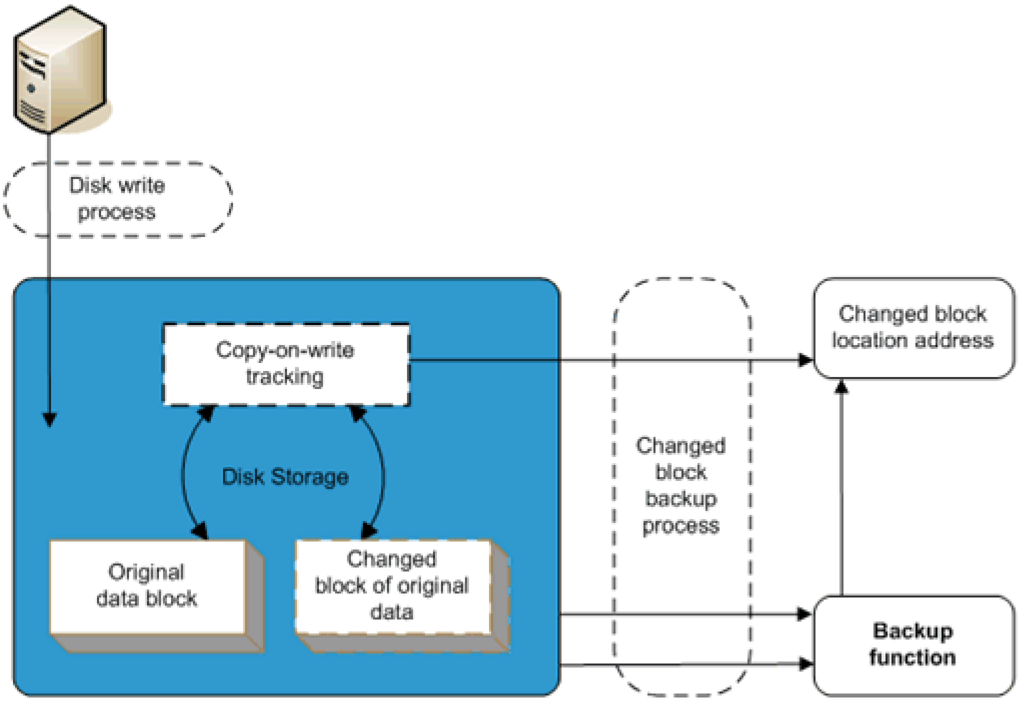

Figure 4. Software-based Snapshot Using Copy-on-Write Process

In the figure, disk writes are monitored to enable them to be replicated using a copy-on-write process. When a snapshot is taken, the changed block of data is used as the image for backup using the changed block location address identified by the copy-on-write process.

There are several approaches to using snapshot technologies in an enterprise backup and recovery solution. Volume Shadow Copy is a Windows Server 2003 feature that provides an infrastructure for creating snapshot-based point-in-time copies of single or multiple volumes.

Volume Shadow Copy Services

The ability to fully exploit the advantages of a SAN for backup has been hindered by the lack of multi-vendor, cross-platform software that can perform more sophisticated tasks for easier management. To resolve issues of compatibility and interoperability, Windows Server 2003 includes Volume Shadow Copy services.

Volume Shadow Copy is a mechanism for quickly creating copies of data and managing backups and snapshots; it provides a standard way for Windows applications to interact with point-in-time copy capabilities (hardware-based or software-based) from any vendor, making it easy for independent software vendors (ISVs) to take advantage of the capabilities offered by storage hardware. The Enterprise and Datacenter editions of Windows Server 2003 support hardware transport snapshots, provided that hardware vendors supply a provider for the Volume Shadow Copy service. In combination with Windows XP clients, Volume Shadow Copy also allows users to retrieve old copies of their files without having to request support staff to restore them, which reduces the time and cost required to retrieve old copies of files.

Using Disk for Staging Backups

Disks are low-cost viable alternatives for storing short-term data; they also allow quick retrieval of a second copy of crucial data. Although system downtime can be mitigated to a certain degree using system fault tolerance and RAID technologies, using these approaches to protect rarely used or less important data may be expensive. Therefore, one strategy that can be implemented is the staging of backups and snapshot images on a local disk or a SAN-based disk. Data can be constantly copied from disk to disk. It can be backed up to tape at fairly frequent intervals; the frequency depends on the requirements of each implementation.

Backup data staging is important because it gives administrators the option to move data to a secondary location before moving it to tape. Data copies can be scheduled to occur with minimum server and application performance overheads, while increasing the availability of data before offloading it to tape. Moving a copy of data to secondary online storage before moving it to tape ensures quick retrieval of the most recent data, which has not yet been backed up to tape. It also provides a temporary second-layer vault from which data can be moved to tape without the need for lengthy tape retrieval procedures, even if capacity is limited to keeping only 24 hours worth of data in snapshot form with online availability. Data can be moved to tape and the disk space can be cleared for the next snapshot. Backing up the snapshot copy, rather than the primary online copy, also makes the process essentially windowless.

The following figure depicts management of backup and snapshot data before archiving to tape.

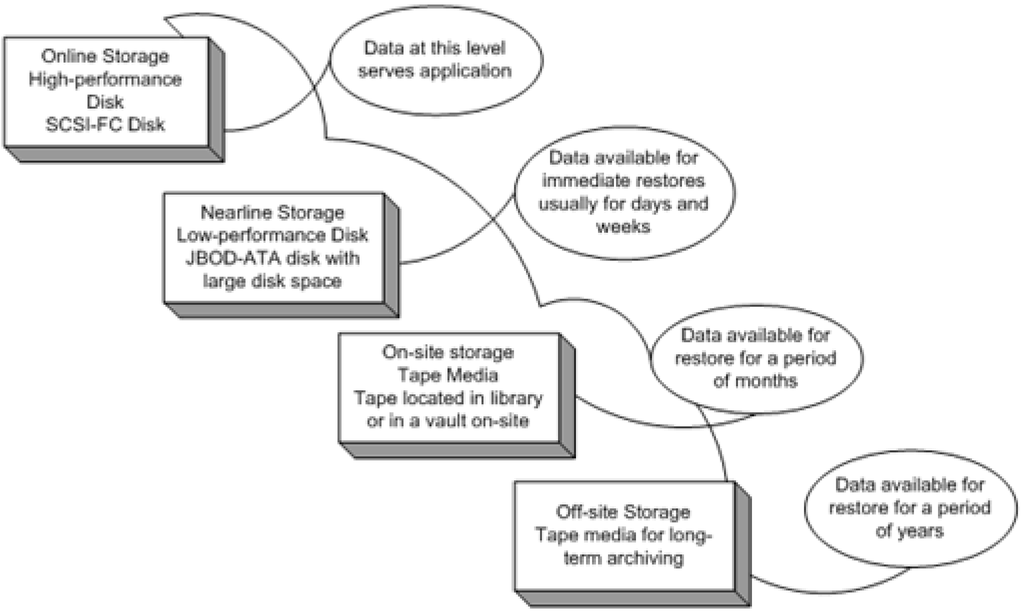
Online Storage
High-performance Disk
SCSI-FC Disk
Data at this level serves application
Nearline Storage
Low-performance Disk
JBOD-ATA disk with large disk space
Data available for immediate restores usually for days and weeks
On-site storage
Tape Media
Tape located in library or in a vault on-site
Data available for restore for a period of months
Off-site Storage
Tape media for long-term archiving
Data available for restore for a period of years

Figure 5. Backup Data Retention and Value to the Enterprise

Service Design

This section lists some of the key factors to consider when planning a backup and recovery solution.

Design Inputs

To determine the appropriate backup and recovery design for a particular enterprise application and data type, the following questions should be considered:

- Which is more important, fast backup or fast recovery?
- What are the available minimum backup windows for different servers and applications?
- What data should be backed up, how important is the data, and how replaceable is the data?
- When can full and partial backups be performed?
- What is required to reduce the backup windows in terms of hardware, software resources, and techniques?
- What recovery times are specified in the SLAs?
- How much time and what resources will be needed to reconstruct the data set?
- Is the data type structured (such as database systems), semi-structured (such as e-mail data), or unstructured (such as file system data)?
- What is the data size and volume?
- How often does the data change?
- What are the data retention requirements for legal, operational, or other purposes?
- What media types should be used (for example, disk, tape, or a combination of both)?
- What are the tape library requirement with regard to robotics, tape drive speeds, vendor support, interoperability with the existing environment, and supportability by the backup and recovery solution?
- What are the economic consequences of system unavailability? For example, what is the cost per hour of server downtime?
- Who is responsible for maintenance of the backup and recovery solution? What happens if the responsible personnel leave the company?
- How many clients need a backup and recovery service and what kind of backup window and SLAs are prescribed for them?

Design Goals

The design goals for an enterprise backup and recovery solution should include:

- Data recovery of a single file to complete system recovery.
- Grouping clients based on location, function, and data capacity.

Design Steps

The key design steps that follow the collation of business requirements and SLA information for a backup and recovery service implementation include:

- Carrying out a detailed system inventory.
- Understanding the environment for backup and recovery.

Detailed Inventory

A detailed inventory of all applications, servers, SANs, disk space, and network components is essential for designing an effective and reliable backup and recovery solution. Once the inventory has been drawn up, the appropriate backup and recovery systems can be evaluated and requirements for interoperability, compatibility, and common management can be included in the design. Thus, an inventory process should lead to a detailed analysis of the enterprise backup and recovery environment.

Understanding the Environment for Backup and Recovery

The backup and recovery service is dependent on the environment. Therefore, planning a backup strategy requires not only an understanding of data requirements but also an understanding of the technologies that may influence the backup and recovery architecture. Collecting information about the existing environment and taking time to understand and isolate environmental issues will result in smoother implementation and operation of the service. The following factors can influence a backup and recovery architecture:

- Application layer
- Media management layer
- Server platform layer
- Data path
- Storage layer

Application Layer

At the application layer, it is important to identify the data and the number of clients holding each type and size of data. Identifying data that is generated by each application type is important because it helps in understanding what kind of techniques, storage resources, limitations, and policies should be associated with the data. For example, in Microsoft-based environments data can be classified as:

- Active Directory.
- Messaging services, such as Microsoft Exchange.
- File system data, generated by Web servers and file servers.
- SQL Server data, generated by any application that uses a SQL Server database to store its data.

Media Management Layer

The media management layer is concerned with the physical and logical components of the backup and recovery solution. The physical components include:

- **Tape library:** The tape library and tape drives that it contains provide the offline storage for backup data. The tape library provides automated tape handling, which is a key requirement when consolidating backup across multiple servers. Sizing of tape libraries and tape drives is critical to ensure that the libraries and drives are fully utilized.
- **Medium changer:** The medium changer is the robotics within a tape library to

control the movement of tape cartridges to appropriate tape drives. Design considerations for medium changers include the type and speed of the robotics.
- **Tape drive:** The main design issues for tape drives are their speed, type (DLT, SDLT, or LTO), and the compatibility of tape cartridges.
- **Media type:** The media design considerations are whether to use tape-media, disk-media (SCSI or ATA/IDE disks) or a combination of both.

The logical components to include in the design process are policies for data retention on the media and the setting up of workable and reliable tape rotation schemes.

Server Platform Layer

The server platform layer is concerned with volume and drive management. The components that can be identified in this layer are:

- **Operating system version:** The version of the operating system is important in terms of identifying compatibility issues and using certain features, such as the Volume Shadow Copy service offered by Windows Server 2003.
- **Cluster:** Cluster identification is important, since different backup techniques and agents have to be installed based on whether a system is clustered or non-clustered.
- **Physical configurations:** It is important to determine system processor, memory, and I/O subsystems, as these affect backup and recovery performance.
- **RAID type**: Although not crucial, it can be useful to know how the data is laid out on disk.

Network Layer

The network layer is concerned with the data path from the disks (on which data originates) to the tape cartridges (or other media) on which it is backed up. In a SAN environment this layer is referred to as an interconnection network, which is the network infrastructure that connects the components of the shared storage environment. The important requirement is that it provides an appropriately high-performance scalable connectivity upon which a shared storage environment can be based. The physical layer network technologies that are widely used for this function include Fibre Channel, Fast Ethernet, and Gigabit-Ethernet. Network protocols that are used at higher layers of the protocol stack also cover a wide range, but SCSI FCP and TCP/IP are the most commonly used protocols.

In a network-based backup environment, the key issues of concern include:

- Network connectivity and bandwidth.
- TCP/IP and speed settings on the network card.
- Port mapping and speed settings at the switch or network adapter level (for example, full duplex or half duplex).

In a SAN-based backup environment, the key issues of concern include:

- Host bus adapter (HBA) settings.
- Backup zone information.
- SAN switching.

Some specific components that need to be considered when designing for a SAN-based environment include:

- **HBAs:** The HBAs are used to connect servers to Fibre Channel topologies. They provide a function similar to that provided by network adapters for access to LAN resources. The device driver for an HBA is typically responsible for providing support for any of the Fibre Channel topologies, whether point-to-point, loop, or fabric. In most cases, the device driver also provides a translation function of presenting Fibre Channel targets as SCSI devices to the operating system.
- **Switch:** A switch is a component of the Fibre Channel infrastructure that is used to construct fabrics; a fabric is a cluster formed using cascaded switches. Switches typically have an Ethernet port, which enables their management over the network by providing a means to communicate status and configuration information for the switches and their individual ports.
- **Router:** The FC-SCSI router device (sometimes referred to as a bridge) provides connection between Fibre Channel topologies and SCSI devices by presenting the SCSI devices to the SAN as Fibre Channel devices, and then relaying Fibre Channel commands to them. Routers are typically used for tape drives and tape libraries.
- **Cables and GBICs:** Three types of cables exist to connect Fibre Channel devices to each other—copper cables, short-wave or multi-mode optical cables, and long-wave or single-mode optical cables. Each type of cable provides different maximum lengths and costs. Fibre Channel devices have ports that either require a specific type of cable or a separate module referred to as gigabit interface converter (GBIC). A GBIC-based port allows the use of multiple types of cables by using the appropriate type of GBIC with it.

Storage Layer

At the storage layer, the following components need to be considered for the backup and recovery design:

- **Storage-array:** Controller, device connections, and LUN mappings.
- **Snapshots:** Snapshots are point-in-time images of data, and are either hardware-based snapshots (using split-mirror technology or clones) or software-based snapshots (using copy-on-write mechanisms).

Different Backup Types

The design options that should be considered when designing a backup and recovery solution differ depending on whether the design scope needs to include standard Windows-based servers, NAS devices, or SAN data. The following section describes the design options available for each type of backup. In an enterprise environment, it is likely that the backup and recovery design will cover options from all three types; more details on how these are commonly used in an enterprise are provided in the “Logical Design” section in this blueprint.

Service Design for Standard Windows-based Servers

A number of options exist for backup of data residing on standard Windows-based servers. These options include backing up data locally or across the network, and are discussed in the following sections.

Option 1—Backup Data Locally

The only way to carry out local server backups is through a directly attached backup system, which requires a tape drive, autoloader, or library to be directly connected to each server through a SCSI bus connection. The complete backup and recovery configuration is performed on a per server basis, and each server that needs to be backed up requires individual management and dedicated backup software. The backup software reads data from primary storage and writes it to the backup device. The administration of the backup software has the flexibility to be performed locally or remotely.

Advantages

Advantages of backing up data locally include:

- **Simple configuration:** Configuration is simple compared to other backup architectures.
- **Fast backups:** Backups are fast with high local performance rates; the time for backup is limited by the capability of the backup device.
- **Low network bandwidth consumption:** Because the servers are connected through SCSI connections, the backup process does not consume network bandwidth.

Disadvantages

Disadvantages of backing up data locally include:

- **More expensive:** Relatively expensive, as backup devices are required for individual servers.
- **High management costs:** Administration and management costs and time for managing each server individually can be significant.

Option 2—Backup Data across the Network

A network backup uses the LAN and backs up data from one or more servers; because NAS backups are a part of network backups, both LAN and NAS backups are included in this section.

Enterprise-level LAN backups require centralized and robust backup metadata and media management capabilities, which are defined as follows:

- **Backup metadata:** Backup metadata management is a critical feature of a LAN backup because it provides the search and find capabilities that are needed to quickly locate data objects for restore.
- **Media management:** Media management is critical because media is where the backup data resides. Handling of different media types (that is, disk and tape) is critical to a centralized network backup system. Furthermore, support and

management of tape libraries, tape drives, and tape cartridges are also critical aspects of media management in a network backup system.

Network backups usually make use of a dedicated backup media server that manages an automated and high-capacity tape library with fast multiple tape drives, medium changer, and bar code reader.

Advantages

Advantages of backing up data across the network include:

- **Centralization:** Unlike local server backup and recovery configuration, network backups offer centralized administration and management of the entire backup infrastructure from a central backup server.
- **Media management:** In a network backup configuration, backup media and devices such as tape drives, tape libraries, and disks can be managed by dedicated media servers**.**

Disadvantages

Disadvantages of backing up data across network include:

- **Backup traffic on corporate LAN:** Network backup causes backup data to consume corporate LAN bandwidth, which may degrade network performance.
- **Limited scalability for media management:** As compared to SAN-based backups, LAN-based backups (network backups) possess fewer media management capabilities. For instance, any server on a SAN can play the role of media server and share a single tape library, resulting in significant return on investment (ROI) on tape hardware investment.

Service Design for NAS Devices

NAS devices reside on the network with the primary purpose of providing file services. NAS devices that use standard operating systems (for example, Windows-powered NAS devices) support the installation of backup agents, and can therefore be backed up like any other file server. However, some NAS devices use a custom operating system that does not support third party backup agents. A standard backup interface for NAS devices exists in the form of the network data management protocol (NDMP), which is a backup standard for NAS devices that do not support installation of a backup agent.

The following sections discuss the backup options that are available for NAS devices.

Option 1—NAS Device with Proprietary Operating System

To back up a NAS appliance that uses a proprietary operating system which does not allow installation of backup agents, the NDMP protocol should be used. NDMP backup architectures are used predominantly in environments where appliances and specialized file servers form part of a larger enterprise backup environment. The following figure shows a NAS backup scenario using NDMP.

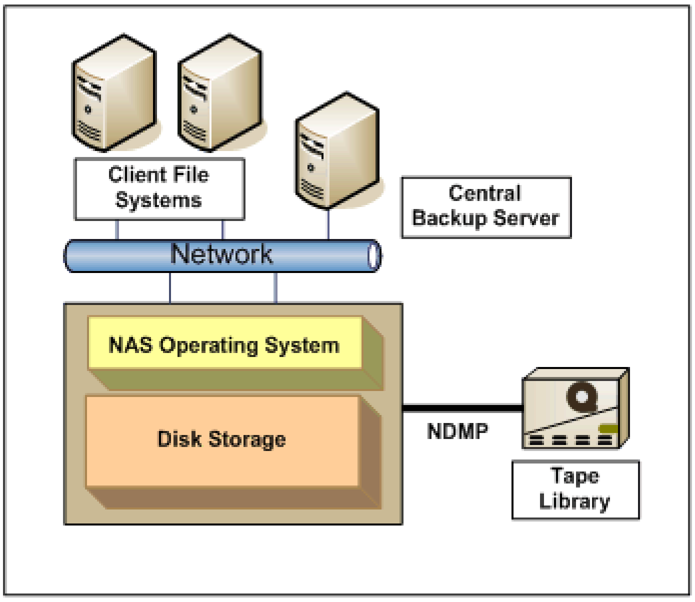

Figure 6. Sample NAS Backup Scenario Using NDMP

The main purpose of NDMP is to provide an interface to network backup software for controlling the backup and recovery functions of an NDMP-compliant server. For large NAS appliances with proprietary operating systems, NDMP currently provides the best way to connect the backup software and NAS device-attached tape drives.

Advantages

Advantages of NDMP include:

- **Better performance**: NDMP provides better network performance by removing backup traffic from LAN. Data is backed up and restored through a locally attached tape device, which enhances performance by reducing the backup window.
- **Better support:** NDMP specifies a simple, vendor-neutral standard for communication between NDMP supporting devices and backup software. Regardless of the NAS device and backup vendor, NDMP provides a standard way of backing up the NAS device as long as the vendor supports the NDMP standard.
- **Remote backup capability:** NDMP eliminates the need for data to be funneled from remote locations through a central backup server and then dumped into a single backup repository. Newer versions of NDMP standard also have provisions to use centralized tape repositories.

Disadvantages

Disadvantages of NDMP include:

- **Limited scalability of media resources:** Tape resources used by other servers on the network cannot be used for NAS devices performing NDMP backups.
- **Backup function server overhead:** NDMP-based backup might affect the NAS device performance, depending on the data being backed up.

Option 2—NAS Device Supporting Backup Agent

If the NAS appliance operating system supports installation of a regular backup agent, the second option for the NAS appliance is to back it up as any other server on the network. One example of this option is Windows Storage Server 2003 devices.

Advantages

Advantages of network backup of NAS include:

- **Better consolidation capability and performance:** Backing up multiple NAS devices can be simplified by using storage resources in the SAN.
- **Tape device optimization:** Tape resources used by other servers on the SAN can be allocated to backup sessions of NAS gateways, resulting in easier backup administration and high ROI for the tape library.

Disadvantage

Lacks NDMP support: Backups performed in this fashion are regular backups and do not benefit from standard NDMP adherence. Also, they use the network for backup functions.

Service Design for SAN Backup

A key feature of SAN backup techniques is the ability to move the actual backup copy operation from the production host to a secondary host system. The backup and recovery service can reside either in a secondary host system or any system on the storage network with access to the backup source and destination. The following section explores backup and recovery options that are available for SAN environments.

Option 1—LAN-free Backup

LAN-free backup minimizes bandwidth usage on the organization's LAN by moving backup traffic from the LAN onto the SAN. Although the bulk of the data for LAN-free backup travels through the SAN’s Fibre Channel connections, LAN-free backups still need to communicate with the central backup server over the LAN to obtain metadata (also known as control data) about the backups.

Advantages

Advantages of LAN-free backup include:

- **Network performance:** Removing backup traffic from the LAN increases performance by reducing the backup window; data is backed up and restored through a 1-2 Gbps Fibre Channel-based SAN rather than across a 10/100 Mbps Ethernet network.
- **Tape drive optimization:** Tape resources can be dynamically allocated to backup sessions on each server and intelligent scheduling can optimize the use of shared tape drives. These features allow for sharing of a single tape library among several media servers and a high ROI for the tape library.

Disadvantages

Server overhead: The main disadvantage of LAN-free backup is the server overhead; it does not solve the problem of production server overhead during a backup process.

Option 2—Server-free Backups

Server-free backups offload the backup process to a specialized backup appliance that acts as data mover. The extended **copy** command (also known as third party copy) is used, which is a SCSI-3 command to copy data from one set of devices to another. These devices can be disks, tapes, or other types of storage devices. This SCSI protocol command can be used on devices connected through SCSI cables or Fibre Channel connections.

Advantages

No overhead on production servers: The main advantage of server-free backup is that it does not incur a backup overhead on production servers. With server-free backups, production systems do not suffer any performance degradation caused by the backup and recovery process.

Disadvantages

Requirement for special devices: The main disadvantage of server-free backup is that it requires specialized devices. Server-free backups require the use of intelligent devices that support the SCSI-3 Extended Copy command set.

Option 3—Hardware-based Snapshot Backups

Hardware-based snapshots use split-mirror technology, or cloning, to provide a complete copy or exact duplicate of the original volume. Split-mirror technology provides an easier way to backup production data that experiences high transaction rates.

Backup is accomplished by mirroring the data and performing a physical backup of the mirror. Steps for this method include:

1. Before the backup process can begin a backup, the database application must establish a quiescent data image. An application is said to be quiescent when it has been temporarily paused and all writes to disk are completed, with the system cache being flushed to capture a consistent data state. A quiescent data image provides a transactional consistent image that can be remounted without file system (or database consistency) checks.
2. The mirror is detached so that the static image of the data is maintained separately from the live data; the backup system can now back up the detached snapshot.
3. When the backup is complete, the mirror is reattached and the mirroring mechanism synchronizes the two disk images.

Advantages

Advantages of hardware-based snapshot backups include:

- **Data availability:** Hardware-based snapshots provide the most highly available data because they are exact duplicates of the original volume.
- **Backup speed:** Very fast backup and recovery times, usually measured in seconds.
- **Low backup overhead:** Backups are performed with minimal workload degradation.
- **Near-instantaneous restores:** If the production disks are resynchronized with the clone in the background, the restore is almost instantaneous. This eliminates the single most time-consuming phase of the restore and recovery process and is the most important benefit of this technology.
- **Flexible restores:** Hardware-based snapshots provide for flexibility of restoring to the same or a different server on the SAN. Restores can be accomplished very quickly.

Disadvantages

Disadvantages of hardware-based snapshot backups are as follows.

- **No partial backups:** The major drawback of split-mirror technology is that it does not provide for partial backups, such as incremental or differential backups. In a split-mirror backup, the entire volume must be backed up as a single entity; thus, split-mirror backups are most useful when the entire device must be backed up.
- **Hardware-dependent:** Split-mirror technology is dependent on the hardware vendor.
- **Cost:** Split-mirror technology is more expensive than software-based snapshots.

Option 4—Software-based Snapshot Backups

Software-based snapshots, also referred to as metadata copies, use a copy-on-write mechanism, which provides a quick snapshot capability that can mount an additional file system as a read-only snapshot of the original volume. This type of snapshot can be done while the original volume is still active and available. Software-based snapshots ensure that any blocks from the original file system are copied out to a special area (a designated pool of storage set aside for the snapshot) before the block is changed on disk. A copy-on-write mechanism moves the original data block to the snapshot before a write is allowed to that block, which keeps the snapshot data consistent in time with the exact time that the snapshot was taken. A metadata copy is faster than backups because it only copies the pointers to where the original data is stored. Because copy-on-write snapshots are not complete copies of the original data, a much smaller amount of additional disk space is required to activate the snapshot capability. Snapshot volume read requests to unchanged data blocks are redirected back to the original volume, while read requests to data blocks that have been changed are directed to the copied blocks in the snapshot.

Advantages

Advantages of software-based snapshot backups include:

- **Applicability:** Software-based snapshot techniques can be used on all classes of storage and are not dependent on vendor-specific hardware technologies.
- **Efficient use of storage:** Snapshots use storage efficiently because only the changes

are tracked (instead of complete copies of data).

Disadvantages

Low performance: The main disadvantage of software-based snapshot backups is that metadata snapshots affect performance, because write requests to the original volume must be copied to the snapshot before being completed.

Logical Design

Many data centers can have multiple backup and recovery processes to support each unique application and server platform. Thus, a backup and recovery solution is a combination of several software and hardware components.

When planning a backup and recovery solution for an organization, it is important to take into account the backup requirements of clients residing in remote data center locations. This process involves planning the networking requirements to meet the backup window as well as other considerations. There is no one-size-fits-all-solution because of the different varieties and configuration possibilities of enterprise networks. A backup and recovery solution for a distributed environment entails a carefully devised plan for a successful network backup infrastructure.

Even with the latest networking technologies, network bandwidth tends to lag behind for wide area network (WAN) connections. Even when bandwidth is available, it is very expensive to use it fully just for backup purposes. Because of these cost and network bandwidth issues, finding ways to satisfy backup requirements of remote locations is a challenge.

When designing a backup and recovery solution, an organization needs to identify and divide the servers and their data into different categories based on their business requirements and SLAs. Important considerations include which data center scenario is involved.

The following figure shows a logical design that incorporates various considerations for an enterprise organization’s backup and recovery solution.

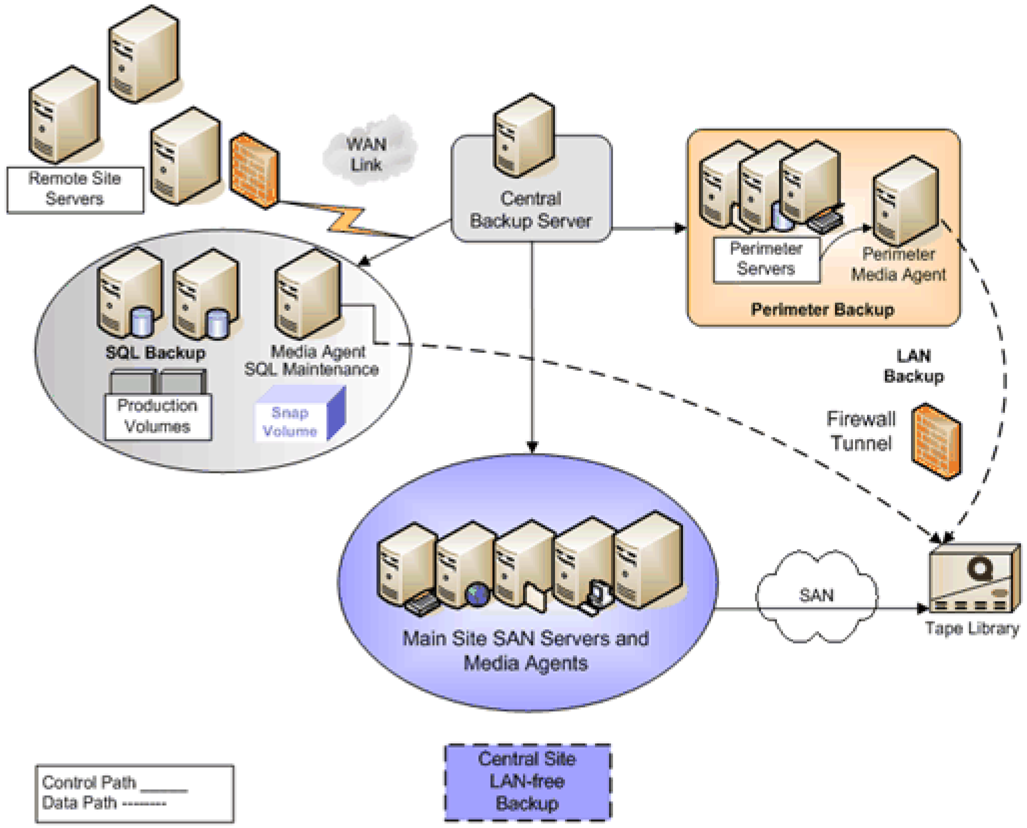

Figure 7. Enterprise Backup and Recovery Logical Design

Hardware Requirements

A backup and recovery application may require significant disk and network I/O resources, particularly where there are significant amounts of data. Therefore, it is important to carefully plan for hardware and network capacity. Backup and recovery should be considered a primary application in the enterprise environment so that sufficient resources are allocated to this critical service.

System Memory

Backup relies on system memory for the following:

•**Interprocess communication (IPC):** Shared memory is used to implement communication between various backup and recovery processes.
•**Virtual memory (VM) cache:** Memory is used when buffering file system data in the VM cache. If data is cached in VM faster than old pages can be purged, system performance may be seriously degraded. More system memory may forestall this situation temporarily. For efficient backup and recovery, a certain amount of shared memory should be configured per device and data stream.

File System Cache

Backups are more efficient when the file system buffer cache is avoided. The buffer cache can be bypassed by either using direct I/O to access individual files or backing up the raw volume rather than the file system. In either case, the result is rapid backup of raw blocks.

Tape Drive and Tape Formats

One of the important considerations for hardware requirements in an organization’s backup system is the tape drive and tape formats used. The tape drive determines the transfer rate at which data can be written to tape media. The tape media determines the amount of data that can be retained on a single tape. The following section outlines the commonly used tape drives and tape capacities.

- **DLT tape drives:** DLT format is the most popular tape format used in tape backup systems. DLT format tape drives can transfer data to tape media at 6-10 MB/sec.
- **Super DLT tape format:** Super DLT (SDLT) is the newer version of DLT; it is faster and has more capacity than DLT tape cartridges. The new SDLT format tape drive has a data transfer rate of 10-16 MB/sec native and 12-32 MB/sec compressed. SDLT is also backward read compatible with existing DLT tape drives.
- **Linear Tape Open (LTO) tape drives:** The LTO standard was developed by a consortium of IBM, Seagate, and Hewlett-Packard. It supports two formats: Accelis and Ultrium. Accelis is in development and will be designed for applications that require exceptionally fast access time. The Ultrium format is the more commonly used LTO format and is a viable alternative to the conventional DLT tape format. LTO provides higher capacity backups, restores, and tape archive capabilities than the DLT format and is capable of supporting LTO cartridges of varying capacities—up to 200 GB of compressed data. Unlike SDLT, LTO is not compatible with earlier versions of DLT.

The following table outlines most commonly used tape formats, capacities, and speeds.

Tape Format	Native Capacity (GB)	Compress Capacity (GB)	Max Transfer rate (MBps)
Mammoth-2	60	150	30
DLT	40	80	6-10
SDLT 220	110	220	22
SDLT 320	110	320	32
AIT-3	70	260	31.2
LTO	100	200	20-40

Table 2. Tape Media Formats, Capacities, and Speeds

Availability

For high availability of data, the backup and recovery system and the data it manages must be highly available.

Considerations for high availability of the backup and recovery system include:

- The hardware on which backup and recovery system runs must provide redundant components and clustering failover capabilities.

- Backup data retention requirements must include the period for which tape media backups need to be retained. The media resources being used should support these retention requirements, which should be determined based on business, legal, and industry requirements.
- The backup and recovery system must provide alternate backup server and tape device failover support. It is important that the system is capable of detecting failure during its functions and providing an automatic switchover to different backup servers or devices.
- The backup and recovery system should have capability to automatically restart failed backup and restore jobs from the point of failure because these jobs could fail midstream for any number of reasons. The backup system should automatically restart the job from the point it left off.

Security

The growth in the use of geographically dispersed data centers, segmented networks, vertical application services, and remote access means that information systems (IS) are no longer hidden within private corporate networks. There are, therefore, potential threats to corporate data due to virus attack, hacking, intrusions, and denial-of-service (DoS) attacks. Thus, security is crucial to ensure that a data center provides its services in a secure manner. Because backup and recovery data can span many networks and sites, it is more important than ever to secure the backup and recovery components and their communications.

Service Security Design

A backup and recovery system can be secured at the following levels:

- **Secure communications:** A backup solution should be able to offer support for different encryption algorithms and sophisticated network port blocking. In addition, packet filtering techniques should be used to prevent unauthorized access between servers. For example, when a central backup server communicates across a firewall or locked down switch, it should be able to communicate over any user-defined ports. Backup software should log all failed attempts to access the server and these logs must be regularly reviewed by the system administrator. Remote administration of the backup server must be carried out using encrypted management links.
- **Authorized access:** A backup solution should support security policies to control access and provide secure management of backup and recovery applications.
- **Media protection:** A backup solution should support password protection for media. In addition, policies should be in place to ensure that all media are properly protected and stored.

Security Lockdowns

The backup and recovery solution should make use of the underlying system security employed on the servers on which backup components are installed. Through the use of security policies and access control lists (ACLs), the servers, devices, and data should be protected to ensure that only authorized users and applications are able to access it.

Scalability

The storage systems in any infrastructure must be designed from the beginning to scale to larger data capacities without major effort. The storage system should be chosen on the basis that it will grow as the environment data increases. The backup and recovery architecture should be flexible enough to be able to scale and handle enormous volumes of data. The backup application should allow flexibility in terms of scaling up and scaling out the backup and recovery infrastructure.

Scalability in the backup infrastructure can be evaluated at the following levels:

- **Master backup server:** The main command center of the backup. The backup application should support clustering and other fault-tolerant technologies to support scaling-up capability. Furthermore, more relevant for large installations, the backup application should be able to scale-out and group multiple master backup servers under one central management configuration.
- **Media servers:** Provide data transfer function in the backup architecture. As the amount of data to transfer increases, the backup application should provide scale-out capability for adding media servers and hardware capacity.
- **Media management:** In terms of media management, the backup application should support a scaled-up large tape library with multiple tape drives and tape slots**.** Also, it should support multiple tape libraries for scale-out capability.

Performance

Performance in a backup and recovery system can be achieved at different levels. Some of the areas that can affect performance directly are discussed in the following sections.

Using Compression for Performance

Benefits of compression can vary with the data being compressed as well as with the compression mechanism being used. The level of compression depends on how much redundancy can be identified and remapped in the data with the amount of time available. Some types of data, such as streamed video data, have little or no redundancy to eliminate. Therefore, this type of data does not compress well, regardless of the compression scheme used. There are two types of compression—hardware compression and software compression. Hardware compression is the most commonly used.

Hardware compression is usually located in the tape drive and relies on a buffer in which data is temporarily held while it is being compressed. One constraint of hardware compression is that it is limited to the hardware buffer size.

Software compression compresses the target data on the system by using compression algorithms, which are often supplemented with backup applications. Software compression can put a heavy load on system memory while performing the compression. However, software compression programs have better performance than hardware compression because they are not dependent on buffer size in the tape drive. Software compression is well suited if the data is backed up over slow links.

Metadata Overhead

Backup planning should allow for a certain amount of metadata overhead in addition to the data that is being backed up and restored. Metadata is information maintained by the backup application about the data residing on tape, and includes disk and tape catalogs that are used to locate files during recovery. Typical backup applications use one to four percent of the disk space being backed up for metadata.

Restore Performance

Restore performance is not identical to backup performance. Although performance varies depending on the particular environment, restores typically take between 25 percent and 50 percent longer to perform when compared with the amount of time needed for backing up the same data. With proper tuning of the backup software and for certain data types, data sizes, and hardware, it is possible to perform data restores so that they take less than 10 percent more than the backup time.

One of the factors for increased restore time is the browse delay introduced at the start of the backup job request. When a restore request is issued initially, the backup software needs to browse the file record database and locate all records that need to be retrieved, which may take some time for a large data set.

Reduce Network Traffic Caused by Backups

One of the ways to reduce backup network traffic is to isolate the network carrying backup traffic. Another technique could be grouping subnets and deploying media servers per subnet to keep the backup traffic at subnet level.

Consolidation

Consolidation in a backup and recovery solution can be achieved at various levels. For instance, SAN and NAS technologies produce centralization of storage, thus providing consolidation benefits for backup and recovery functions.

Consolidation at the media management level can be achieved by using large tape libraries and sharing tape drives within the tape library for tape backups.

A centralized backup and recovery solution should be an integrated combination of scalable hardware and software components. Consolidating DAS into a giant, single, and logical pool of storage and then allocating and reallocating this capacity as needed is a huge consolidation benefit for all storage-related functionality, including backup and recovery.

Using the underlying strengths of the SAN for tape backup provides significant payback. Storage consolidation streamlines the tape backup process in the following ways:

•Integration of mirroring and snapshot technology with backups.
•Single, centralized backup management of all storage volumes.
•Flexibility of performing LAN-free and serverless backup and recovery.
•Sharing of multiple tape drives within a single automated tape library.
•Centralized, easier media management.
•Significant reduction in backup and recovery window time.

To achieve these benefits, a consolidated tape backup requires careful upfront planning to correctly classify the data and size the backup tape system, media, and storage.

Interoperability

It is important to identify what hardware, platforms, and applications are supported by a backup and recovery solution and which hardware and software vendors' products will interoperate. Technologies to assess for interoperability include backup hardware and software, server hardware, HBAs, switches, hubs, operating systems, and applications. The solution must allow sufficient product integration so that products from a range of vendors can support backup and recovery requirements across heterogeneous environments.

Previous Service Versions

It is important that the backup and recovery solution provide a clear road map for upgrades, not only for its own releases but also as support for previous versions of server platforms and applications.

Another area to focus on in a backup and recovery infrastructure is compatibility of media. For example, if DLT tapes are used to change newer types of technologies such as SDLT or LTO, a migration path should be defined because the DLT tapes are not compatible with LTO tapes. For further information, refer to the "Tape Drive and Tape Formats" section in this blueprint.

Supportability

Media management for tapes, tape drives, and tape libraries is the most important aspect of supportability in a backup and recovery system. The issues that affect supportability of a backup solution include:

•Does the media management provide indexing, tape labeling, detection of tape libraries, initialization of remote media, adding and deleting media to and from libraries, or use of bar codes in the media?
•Is tape library sharing among several media servers supported?
•Does the backup software support the entire life cycle of data on disk and tape media?

- What tape libraries and tape drives are currently supported by the backup and recovery software?
- Does the backup software provide the ability to view the usage of tape cartridges, tape drives, and libraries regardless of their physical location?

Best Practices

Tape-based backups are run on a daily basis with little or no assurance that the data forming the lifeblood of the organization is appropriately protected and recoverable. Restore drills should be performed to verify that backups are recoverable. In addition, a complete backup and recovery process should be documented and a backup and recovery manual should be created that is customized to your environment.

The backup and recovery solution should be designed proactively based on business needs, application and server requirements, and data growth. One of the most overlooked aspects of backup and recovery is that it is not seen as part of planning process when an application or server is deployed. Making backup and recovery a key part of the planning process before deploying any application and server in the environment can eliminate many issues.

Service Dependencies

The following table lists the services on which the backup and recovery service depends.

Service Dependency Name	Specific Requirements
Name Resolution	Functioning Domain Name System (DNS) or host files.
Network Architecture	Connectivity to backup clients.
Storage Services	Fibre Channel connectivity to tape libraries and storage devices.
Firewall Services	The number of firewall ports needed depends on the number of clients that need backup services. The specific port ranges used are vendor-specific and depend on the backup solution that is deployed.

Standards and Guidelines

An organization’s backup and recovery solution should adhere to applicable industry standards, including SCSI and NDMP.

SCSI

The backup and recovery service depends on SCSI technology for connections and data transfer between devices. It is important to use compatible SCSI interfaces when designing a SCSI-based backup system and to ensure that the distance limitations of these interface types are adhered to.

The four types of connections for SCSI include:

- Single ended (SE)
- High voltage differential (HVD)
- Low voltage differential (LVD)
- LVD/SE combination

The following SCSI types are compatible with each other:

- HVD (differential) to HVD (differential)
- LVD/SE to LVD
- LVD/SE to SE
- LVD to LVD

These SCSI connection types have different restrictions on how long the data connection can be. These distance limitations are as follows:

- **Single ended (SE):** The distance limitation is 3 meters.
- **High voltage differential (HVD):** The distance limitation is 25 meters.
- **Low voltage differential (LVD):** The distance limitation is 12 meters.

NDMP

As introduced earlier in this blueprint, NDMP is an open-standard protocol for enterprise-wide backup that is used to manage the backup of devices such as NAS-dedicated file servers (also known as filers). NDMP provides a standard interface for devices and backup and recovery software, eliminating the need for vendors in both categories to support multiple interfaces and operating systems. In operation, NDMP reads from a disk or tape and produces an NDMP data stream that can be read or written by another NDMP device. The NDMP architecture also supports separating the control and database functions from the file system and the devices. Normally, the control and associated database are handled by the backup software, which is usually centrally located and may handle many files and file systems.

For more information on NDMP, including the latest versions of the specification and which products support NDMP, refer to the NDMP Web site at:

www.ndmp.org