Copyright

Information in this document, including URL and other website references, represents the current view of CommVault Systems, Inc. as of the date of publication and is subject to change without notice to you.

Descriptions or references to third party products, services or websites are provided only as a convenience to you and should not be considered an endorsement by CommVault. CommVault makes no representations or warranties, express or implied, as to any third party products, services or websites.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious.

Complying with all applicable copyright laws is the responsibility of the user. This document is intended for distribution to and use only by CommVault customers. Use or distribution of this document by any other persons is prohibited without the express written permission of CommVault. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of CommVault Systems, Inc.

CommVault may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from CommVault, this document does not give you any license to CommVault’s intellectual property.

COMMVAULT MAKES NO WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, AS TO THE INFORMATION CONTAINED IN THIS DOCUMENT.

©1999-2014 CommVault Systems, Inc. All rights reserved

CommVault, CommVault and logo, the “CV” logo, CommVault Systems, Solving Forward, SIM, Singular Information Management, Simpana, CommVault Galaxy, Unified Data Management, QiNetix, Quick Recovery, QR, CommNet, GridStor, Vault Tracker, InnerVault, QuickSnap, QSnap, Recovery Director, CommServe, CommCell, IntelliSnap, ROMS, Simpana OnePass, CommVault Edge and CommValue, are trademarks or registered trademarks of CommVault Systems, Inc. All other third party brands, products, service names, trademarks, or registered service marks are the property of and used to identify the products or services of their respective owners. All specifications are subject to change without notice.

All right, title and intellectual property rights in and to the Manual is owned by CommVault. No rights are granted to you other than a license to use the Manual for your personal use and information. You may not make a copy or derivative work of this Manual. You may not sell, resell, sublicense, rent, loan or lease the Manual to another party, transfer or assign your rights to use the Manual or otherwise exploit or use the Manual for any purpose other than for your personal use and reference. The Manual is provided "AS IS" without a warranty of any kind and the information provided herein is subject to change without notice.
Table of Contents (R10.4)

Introduction ............................................................................................................................. 7
Preliminaries ........................................................................................................................... 8
Education Advantage ............................................................................................................. 9
Customer Education Lifecycle ............................................................................................. 10
CommVault Certification ....................................................................................................... 11
CommVault Advantage ......................................................................................................... 12
Course Building Blocks ....................................................................................................... 13
Course Objective .................................................................................................................. 14
Common Technology Engine ............................................................................................... 15
Training Environment .......................................................................................................... 17

Module 1 – Planning a CommCell Architecture ................................................................. 19
Topics ..................................................................................................................................... 20
Common Technology Engine Architecture ......................................................................... 21
CommCell Architecture Overview ....................................................................................... 22
CommServe Server ............................................................................................................... 23
Indexing Structure ............................................................................................................... 25
Common Technology Engine Best Practices ....................................................................... 27
Architecting a Storage Solution ............................................................................................ 29
Simpana Deduplication ......................................................................................................... 32
Understanding Simpana Deduplication ............................................................................... 33
Deduplication Building Block Guidelines ........................................................................... 36
Deduplication Storage Options ............................................................................................ 38
Partitioned Deduplication Database ..................................................................................... 40
Enterprise Building Block Guidelines .................................................................................. 41
SILO Storage ......................................................................................................................... 42
Advanced Deduplication Configurations ............................................................................ 45
Deduplication Best Practices ............................................................................................... 47
Designing a Sound Data Protection Strategy. ..................................................................... 50

www.commvault.com

The Information contained in this document is subject to change without notice. No unauthorized use, copy or distribution.
<table>
<thead>
<tr>
<th>Module 1</th>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disaster Recovery Concepts</td>
<td>51</td>
</tr>
<tr>
<td>Business Continuity Concepts</td>
<td>55</td>
</tr>
<tr>
<td>Protection Methods</td>
<td>57</td>
</tr>
<tr>
<td>Data Description</td>
<td>60</td>
</tr>
<tr>
<td>Data Availability</td>
<td>62</td>
</tr>
<tr>
<td>Protected Storage Requirements</td>
<td>64</td>
</tr>
<tr>
<td>Designing a Sound Data Protection Strategy</td>
<td>65</td>
</tr>
<tr>
<td>Understanding Client Agents</td>
<td>66</td>
</tr>
<tr>
<td>Protecting Virtual Environments</td>
<td>67</td>
</tr>
<tr>
<td>The VSA Backup Process</td>
<td>69</td>
</tr>
<tr>
<td>Protecting Applications</td>
<td>71</td>
</tr>
<tr>
<td>Snapshot Management</td>
<td>73</td>
</tr>
<tr>
<td>Data Protection Best Practices</td>
<td>76</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Module 2 - CommCell Environment Deployment</th>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>CommCell Deployment Process</td>
<td>83</td>
</tr>
<tr>
<td>New CommCell Deployment Process</td>
<td>84</td>
</tr>
<tr>
<td>Existing CommCell Upgrade Process</td>
<td>85</td>
</tr>
<tr>
<td>CommCell Disaster Recovery Process</td>
<td>86</td>
</tr>
<tr>
<td>Environment Requirements</td>
<td>89</td>
</tr>
<tr>
<td>Installing CommServe Software</td>
<td>90</td>
</tr>
<tr>
<td>Installing MediaAgent Software</td>
<td>94</td>
</tr>
<tr>
<td>Index Cache Configuration</td>
<td>96</td>
</tr>
<tr>
<td>Library Detection and Configuration</td>
<td>98</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Module 3 – Advanced Configurations</th>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Policy Design</td>
<td>113</td>
</tr>
<tr>
<td>Storage-Based Design Strategy</td>
<td>114</td>
</tr>
<tr>
<td>Business Based Design Strategy</td>
<td>115</td>
</tr>
<tr>
<td>Deduplication’s Impact on Policy Design</td>
<td>116</td>
</tr>
<tr>
<td>How Many Storage Policies do I really need?</td>
<td>119</td>
</tr>
</tbody>
</table>
Implementation & Maintenance
The value of this course comes from three distinct areas – first, the content of the material which guides your exploration and understanding of the product. Second, the skill of the instructor to expand on those areas of interest and to add value from their experience with the product. And lastly, you, the student whose questions and own experiences help not only yourself but others in understanding how Simpana® software can help you with your data management requirements.
The CommVault Education Advantage product training portal contains a set of powerful tools to enable CommVault customers and partners to better educate themselves on the use of the CommVault software suite. The portal includes:

- Training Self-Assessment Tools
- Curriculum Guidance based on your Role in your CommVault Enterprise
- Management of your CommVault Certifications
- Access to Practice Exams and Certification Preparatory Tools
- And more!
Customer Education Lifecycle

• Available at: http://services.commvault.com/education
• Provides recommended training Pre / Post deployment and at various levels of Simpana® software expertise

Before customers install CommVault® Simpana® software, they should have a basic understanding of the product. This learning timeline illustrates the role of product education over the early years of owning CommVault Simpana software. A lifecycle ranging from the pre-installation review of the "Introduction to Simpana Software" eLearning module, to the pursuit of Masters Program certifications.
CommVault's Certification Program validates expertise and advanced knowledge in topics, including: CommVault Core Fundamentals, Implementation and Maintenance, Preparing for Disaster Recovery and more advanced Specialist and Master technologies. Certification is a valuable investment for both a company and the IT professional. Certified personnel can increase a company's productivity, reduce operating costs, and increase potential for personal career advancement.

CommVault's Certification Program has been re-designed to now offer Professional-level, Specialist-level and Master-level certifications. This new Program provides certification based on a career path, and enables advancement through the program based on an individual's previous experience and desired area of focus. It also distinguishes higher-level certification from lower-level certification as a verified proof of expertise.

**Key Points**
- Certification is integrated with and managed through CommVault's online registration in the Education Advantage Customer Portal.
- Cost of certification registration is included in the associated training course.
- Practice assessments are given in class at the end of each module.
- Students may take the online certification exam(s) any time after completing the course.
- Previous training course students (as validated by the registrar) can also request an opportunity to take the online assessment exam at no charge.
- For those that feel they do not require training, an online assessment opportunity for each certification level may be purchased separately from the training course.
CommVault® Advantage is your profile as a CommVault consumer and expert. The CommVault Advantage system captures your certifications, participation in learning events and courses, your Forum participation, Support interaction and much more. Through your CommVault interactions your awarded Profile Points are collected and compared with other CommVault consumers worldwide. These Profile Points allow our users to thoroughly demonstrate their Simpana® software expertise for personal and professional growth. Login to CommVault Advantage to check your progress and compare yourself to the Global CommVault community or create an account today.
Course Modules

- Planning a CommCell Architecture
- CommCell Environment Deployment
- Advanced Configurations
- Performance Tuning
Course Objective

To provide knowledge for designing and implementing a CommCell® environment. Focus is placed on the most common technical features including deduplication, virtualization, Simpana® agent configurations and advance policy design.
The CommCell® environment is the logical management boundary for all components that protect, move, store and manage the movement of data and information. All activity within the CommCell environment is centrally managed through the CommServe® server. Users log on to the CommCell® Console Graphical User Interface (GUI) which is used to manage and monitor the environment. Agents are deployed to clients to protect production data by communicating with the file system or application requiring protection. The data is processed by the agents and protected through MediaAgents to disk, tape or cloud storage. Clients, MediaAgents and libraries can be in local or remote locations. All local and remote resources can be centrally configured and managed through the CommCell console. This allows for centralized and decentralized organizations to manage all data movement activities through a single interface. All production data protected by agents, all MediaAgents and all libraries that are controlled by a CommServe server is referred to as the CommCell environment.

**Physical Architecture**
A physical CommCell® environment is made up of one CommServe® server, one or more MediaAgents and one or more Clients. The CommServe server is the central component of a CommCell environment. It hosts the CommServe database which contains all metadata for the CommCell environment. All operations are executed and managed through the CommServe. MediaAgents are the workhorses which move data from source to destination. Sources can be production data or protected data and destinations can be disk, cloud or removable media.
libraries. Clients are production systems requiring protection and will have one or more Agents installed directly on them or on a proxy server to protect the production data.

Logical Architecture
CommVault’s logical architecture is defined in two main areas. The first area depicts the logical management of production data which is designed in a hierarchical tree structure. Production data is managed using Agents. These agents interface natively with the file system or application and can be configured based on specific functionality of data being protected. Data within these agents are grouped into a data set (backup set, replication set, or archive set). These data sets represent all data the Agent is designed to protect. Within the data set, one or more subclients can be used to map to specific data. The flexibility of subclients is that data can be grouped into logical containers which can then be managed independently in the CommVault protected environment.

The second area depicts managing data in CommVault protected storage. This is facilitated through the use of storage policies. Storage policies are policy containers which contain one or more rule sets for managing one or more copies of protected data. The first rule set is the primary copy. This copy manages data being protected from the production environment. Additional secondary copies can be created with their own rule sets. These rule sets will manage additional copies of data which will be generated from existing copies within the CommVault protected environment. The rule sets define what data will be protected (subclients), where it will reside (data path), how long it will be kept for (retention), encryption options, and media management options.
The CommVault Virtual Training environment, when available, can be used by students to perform course activities or explore the product’s user interface. The training environment is NOT fully resourced, nor are all components installed or available. All course activities are supported, but due to host memory (RAM and disk space) constraints, only a limited number of Virtual Machines can be operational at the same time and few tasks beyond the activities listed in the course manual can be performed. Please discuss with your instructor what other activity/tasks you can do.
Topics

- Common Technology Engine Architecture
  - CommCell® Architecture Overview
  - CommServe® Server
  - Indexing Structure
  - Common Technology Engine Best Practices
  - Architecting a Storage Solution
- Simpana® Deduplication
  - Understanding Simpana Deduplication
  - Deduplication Building Block Guidelines
  - SILO Storage
  - Deduplication Best Practices
- Planning a Sound Data Protection Strategy
  - Disaster Recovery Concepts
  - Business Continuity Concepts
  - Protection Methods
  - Data Description
  - Data Availability
  - Protected Storage Requirements
- Designing a Sound Data Protection Strategy
  - Understanding Client Agents
  - Protecting Virtual Environments
  - VSA Backup Process
  - Protecting Applications
  - Snapshot Management
  - Data Protection Best Practices
COMMON TECHNOLOGY ENGINE ARCHITECTURE
The heart of any Simpana deployment is the CommServe® server. All activity is managed from this central point and all backup and restore activity must be initiated from the CommServe server. A Microsoft SQL metadata database is used to store all CommServe configuration and job history data.

Data movement is conducted from source to destination using MediaAgents. One or more MediaAgents can be used to move data providing greater flexibility and scalability.

Production data is managed by installing iDataAgents on physical hosts, virtual hosts or on proxy hosts. The iDataAgent communicates with the file system or application being protected and uses native APIs and / or scripting to conduct data protection operations. Physical and virtual hosts with iDataAgents installed are referred to as clients.

Libraries are used to store protected data. CommVault software supports a wide range of library configurations.

The CommServe server, MediaAgents, libraries and clients that communicate with one another make up the CommCell architecture.
Within a CommCell environment there can only be one active CommServe server. For high availability and failover there are several methods that can be implemented. The following information explains each of these methods.

**Hot / Cold Standby**
A hot or cold standby CommServe server consists of a physical or virtual machine with the CommServe software pre-installed. The DR backup Export process directs metadata exports to the standby CommServe server. In the event that the production CommServe server is not available the standby CommServe server can quickly be brought online.

**Virtualization**
Some customers with virtual environments are choosing to virtualize the production CommServe server. A virtualized CommServe server has an advantage of using the hypervisors high availability functionality (when multiple hypervisors are configured in a cluster) and reduces costs since separate CommServe hardware is not required. Although this method could be beneficial, it should be properly planned and implemented. If the virtual environment is not properly scaled the CommServe server could become a bottleneck when conducting data protection jobs. In larger environments where jobs run throughout the business day, CommServe server activity could have a negative performance impact on production servers. When virtualizing the CommServe server it is still critical to run the CommServe DR backup. In the event of a disaster the CommServe server may still have to be reconstructed on a physical

**Clustering**
The CommServe server can be deployed in a clustered configuration. This will provide high availability for environments where CommCell operations run 24/7. A clustered CommServe server is not a DR solution and a standby CommServe server must be planned for at a DR site. Clustering the CommServe server is a good solution in large environments where performance and availability are critical.

Another benefit for using a clustered CommServe server is when using Simpana data archiving. Archiving operations can be configured to create stub files which allow end users to initiate recall operations. For the end user recall to complete successfully the CommServe server must be available.

**SQL Database Replication**
The CommServe database typically will not grow very large so running periodic DR backups may be adequate to properly protect the CommServe metadata. In larger environments where the databases grow to larger sizes, using SQL log shipping or Simpana’s Continuous Data Replicator (CDR) can be used where minimal CommServe server data loss (short RPO) is required. These protection methods require additional Simpana agents and additional Microsoft SQL server licenses.

**CommServe DR Backup Process**
By default every day at 10:00 AM the CommServe DR backup process is executed. This process will first dump the CommServe SQL database and the registry hive to the <install path>/CommVault/Simpana/CommServeDR folder. An Export process will then copy the folder contents to a user defined drive letter or UNC path. A Backup phase will then back up the DR Metadata, registry hive and user defined log files to a location based on the storage policy associated with the backup phase of the DR process. All processes, schedules and export/backup location are customizable in the DR Backup Settings applet in Control Panel.

**CommServe DR IP Address**
A CommCell license is bound to the IP address of the CommServe server. In situations where a standby CommServe server with a different IP address it must be included in the CommCell license information.
Simpana software uses a distributed indexing structure that provides for enterprise level scalability and automated index management. This works by using the CommServe database to only retain job based metadata which will keep the database relatively small. Job and detailed index information will be kept on the MediaAgent protecting the job, automatically copied to media containing the job and optionally copied to an Index Cache Server.

Job summary data maintained in the CommServe database will keep track of all data chunks being written to media. As each chunk completes it is logged in the CommServe database. This information will also maintain media identities where the job was written to which can be used when recalling off-site media back for restores. This data will be held in the database for as long as the job exists. This means even if the data has exceeded defined retention rules, the summary information will still remain in the database until the job has been overwritten. An option to browse aged data can be used to browse and recover data on media that has exceeded retention but has not been overwritten.

The detailed index information for jobs is maintained in the MediaAgent’s Index Cache. This information will contain each object protected, what chunk the data is in, and the chunk offset defining the exact location of the data within the chunk. The index files are stored in the index cache and after the data is protected to media, an archive index operation is conducted to write the index to the media. This method automatically protects the index information eliminating the need to perform separate index backup operations. The archived index can also be used if
the index cache is not available, when restoring the data at alternate locations, or if the indexes have been pruned from the index cache location.

**Index Cache Server**
Index Cache Server is an index cache sharing mechanism that saves an additional copy of the index cache for sharing purposes. This additional copy, the Index Cache server, is located on one of the MediaAgent computers participating in the share. This Index Cache server can be accessed by all participating MediaAgents.

Index Cache Server provides the following advantages:

- Index cache restores for data protection operations.
- Job restartability in GridStor™ Technology scenarios (when used with transaction logging).
- Index cache rebuilding in failover scenarios (when used with transaction logging).
- Maintaining a local cache prevents network disruptions from affecting the data protection operations.

**Transaction logging**
The index copy on the Index Cache server is created by either copying the original index during the Archive Index phase of the data protection job, or dynamically through transactional log replay. Transactional logs are sent at the completion of each storage chunk. In the event the local cache is lost while indexing a job, the job can be restarted at the last transaction successfully entered on the Index Cache Server.

**Shared Index Cache (Network Share)**
A Network Share is a designated location on the network where one or more MediaAgents store their index cache. The Index Cache stored in a network share can be accessed from all participating MediaAgents. You might use a network share if you have a dedicated partition created exclusively for Index Cache and you wish to use this partition for index cache sharing.

Ensure that you have enough space to accommodate the index cache from all participating MediaAgents.

**Note:** When using a network share, the local index and the shared index are one and the same. A network disruption might corrupt the index and jobs might have to be restarted due to index cache failure.

**Intermediate Index Cache**
It is highly recommended that the option **Enable Intermediate Index Cache Directory** be used when configuring Index Cache on a network share. With this option turned on the index is written to the local disk first and at commit points uploaded to the Network share. This will avoid failures due to network disruptions/failures writing to the index on the network share.
Common Technology Engine Best Practices

- CommServe® Server
- Index Cache Settings

CommServe Server
The CommServe metadata database is the most critical component within the CommCell infrastructure. If the data becomes corrupt, the CommServe server disk crashes or you are faced with a full site disaster situation, having the metadata backup readily accessible is critical.

Consider the following key points for proper metadata protection:
- Wherever you send protected data a copy of the DR Metadata should be included.
- If you have a standby CommServe server or a dedicated DR site with network accessibility set the Export phase of the metadata backup to be written to that location.
- Consider using post process scripts to copy the metadata to additional locations as needed.
- Make sure you properly secure the metadata backup since all configuration, security, licensing and encryption key information is kept in the database.
- If data protection copies to tape are typically performed during the day and finish after 10 AM consider setting a second schedule of the DR backup to ensure the most up to date metadata is sent off-site with the data tapes.
- If tapes are sent off-site prior to 10 AM consider changing the default DR backup schedule to ensure the most up to date metadata is sent off-site with backup tapes.
- If your environment is using the Erase Data feature make sure the metadata backup is going to a dedicated DR storage policy or a storage policy with the Erase Data option deselected.
Index Cache Settings

All object level data protection jobs will use indexes for all operations. These indexes are maintained in the index cache. Improper configuration of the index cache can result in job failures and long delays in browse and recovery operations.

Consider the following when designing and configuring the index cache:

- Do NOT put the index cache on the system drive. Use a dedicated drive (recommended) or a dedicated partition (for smaller environments). During MediaAgent installation the default path for the index cache is the system drive. The location of the cache can be changed by selecting: right-click the MediaAgent à select properties Catalog tab.
- Size the index cache appropriately based on the size of your environment and the estimated number of objects that will be protected. It is much better to overestimate than underestimate index cache size. Sizing guidelines are available on CommVault’s documentation-site.
- If you will be running many concurrent jobs protecting millions of objects locate the index cache on high speed dedicated disks. Backup performance can suffer during index update operations.
- The default retention time for the index cache is 15 days. If you will be frequently browsing for data older than 15 days increase this setting and allocate enough disk space for the index cache.
- Index files are automatically backed up to media after each data protection job so there is no need to perform backups of the index cache location. If you are concerned about having fast access to indexes in the event that the cache is lost consider using an Index Cache Server.
Architecting a Storage Solution

- Library Types
  - Disk Library
  - Removable Media Library
  - NDMP Library
  - Plug and Play Library
  - Cloud Storage

- Storage Connections
  - Direct Attached Storage (DAS)
  - Network Attached Storage (NAS)
  - Storage Area Network (SAN)

All data storage devices associated/configured with the Simpana® software are referred to as Libraries. All data destined to and from a library must pass through a MediaAgent (or a NAS Filer). Libraries can be shared between dissimilar OS hosted MediaAgents. Data written by the Simpana software is OS independent. This means data written by a UNIX MediaAgent can be restored via a Windows MediaAgent and vice-versa.

The most common supported library types are listed below. For a list of specific vendor devices consult the Hardware Compatibility List on CommVault's Maintenance Advantage website. For a list of all supported library types consult CommVault's Books Online website.

**Disk library** - A disk library is a virtual library associated disk media configured for read/write access as one or more mount paths. The disk library is a software entity and does not represent a specific hardware entity. The storage capacity of a disk library is determined by the total storage space in its mount paths.

**Tape library** - Tape libraries are made up of one or more tape devices with a library controller and internal media storage. A Tape library can have mixed media and shared access with one or more MediaAgents (on NAS Filers) in the same CommCell® group. Note that Tape libraries can be configured to use WORM media.
Blind Library - A blind library is a tape library without a barcode reader, and is the opposite of a sighted library which has a barcode reader. A blind library must have all its drives (and media) of the same type. Once configured, a blind library cannot be configured as a sighted library.

IP Library - An IP Library provides LAN-based Media Management for multiple applications. Media inventory, pools, and device loading/unloading is all managed by the library software. IP Libraries are the only libraries that can be shared between CommCell entities. Example: STK ACSLS or ADICS SDLC libraries.

Stand-alone Tape Library - A single tape device with no library controller or internal storage that is accessible from a MediaAgent. Stand-alone Tape drives can be pooled together for a multi-stream job or single stream failover configuration.

NAS NDMP Library - A tape library attached to a NAS Filer for NDMP data storage. The library control and drives in a NAS NDMP library can be dynamically shared between multiple devices (NAS file servers and MediaAgents) if these devices are connected to the library in a SAN environment. The device initially having library control (media changer) would be the first configured device.

Virtual Tape Library - A software representation of a tape library using disk storage. Virtual tape libraries are supported, but not recommended because a normal disk library provides many more features and capabilities.

Plug & Play Library - Plug and Play (PnP) storage devices (e.g., FireWire, USB, SATA storage devices, etc.) can be used for storage instead of tapes. Once configured, PnP disks are treated like tapes in a Stand-Alone drive. PnP libraries are useful in locations where it is hard to configure and manage tapes due to operational issues. Only one PnP library can be configured per MediaAgent. Although multiple drives can be configured, only single-streamed jobs are supported. (Multiple drives provide the ability to span across multiple media for a single-streamed job.)

Cloud Library - A Cloud library uses online storage devices — cloud storage devices — as storage targets. Cloud libraries provide a pay-as-you-go capability for network storage. Data is transferred through secured channels using HTTPS protocol.

Removable Disk Drives
Removable Disk Drives can be configured as stand-alone drives. All operations supported by stand-alone drives are supported by such devices. Removable disks differ from PnP disks in that they are drive enclosure devices that retain a persistent drive letter in the Operating System, regardless of whether or not a disk media is loaded into the enclosure.
Storage Connections

Direct Attached Storage (DAS)
Direct Attached Storage (DAS) means the production storage location is directly attached (not SAN) to the production server. In situations where many production servers use DAS, there is no single point of failure. The primary disadvantages are higher administrative overhead and depending on budget limitations, lower quality storage being used instead of high quality enterprise class disks (typically found in SAN/NAS storage).

For some applications such as Exchange 2010 using DAG (Database Availability Groups), Direct Attached Storage may be a valid solution. The main point is that although the storage trend over the past several years has been to storage consolidation, DAS storage should still be considered for certain production applications.

One key disadvantage regarding DAS protection is that backup operations will likely require data to be moved over a network. This problem can be reduced by using dedicated backup networks. Another disadvantage is that DAS is not as efficient as SAN or NAS when moving large amounts of data.

Network Attached Storage (NAS)
Network Attached Storage (NAS) has made a strong comeback over the past few years by taking advantage of its versatility. Where NAS was once only used as file stores they are now considered good options for databases and virtual machines. NAS versatility includes the ability to attach Fibre or iSCSI connections along with traditional NAS NFS/CIFS shares and has a primary advantage of device intelligence using specifically designed operating systems to control and manage disks and disk access. From a high availability and disaster recovery aspect, disk cloning or mirroring and replication provide sound solutions. Simpana's IntelliSnap™ integration with supported hardware provides simple yet powerful snapshot management capabilities.

One key disadvantage of NAS is that it typically requires network protocols when performing data protection operations. This disadvantage can be greatly reduced through the use of snapshots and proxy based backup operations.

Storage Area Network (SAN)
Storage Area Networks (SAN) are very commonly implemented for the most mission critical systems within an environment. The ability to consolidate storage using efficient data movement protocols, Fibre channel and iSCSI provide flexibility and performance.

One key disadvantage of SAN is the complexity of configuring and managing SAN networks. Typically, specialized training is required and all hardware must be fully compatible for proper operation. Since SAN storage lacks the operating system that NAS storage has, it relies on a host system for data movement. Depending on the configuration, the load of data movement can be offloaded to a proxy and by adding Host Bus Adapters (HBA) connected to a dedicated backup SAN data can be more efficiently backed up.
Understanding Simpana® Deduplication

- MediaAgent
- Deduplication Database
- Deduplication Store
- Storage Policy
  - Dedicated
  - Global

The deduplication process contains the following key components:
- Storage Policy
- Deduplication Blocks
- Signature Hash
- MediaAgent
- Deduplication Database (DDB)
- Disk storage
- Optional client side signature cache

Storage Policy
All deduplication activity is centrally managed through a storage policy. Configuration settings are defined in the policy, the location of the deduplication database is set through the policy, and the disk library which will be used is also defined in the policy.

Deduplication blocks and Signature Generation
When data protection jobs are executed, the data is sent to the Simpana® agent from the file system or application the agent is responsible for protecting. Even though the data may be files or application data, we will process the data as deduplication blocks. The deduplication process starts by performing a calculation to generate a Signature Hash. This is a 512 bit value that
uniquely represents the data within the block. This hash will then be used to determine if the block already exists in storage.

The block size that will be used is determined in the Storage Policy Properties in the Advanced tab. CommVault® recommends using the default value of 128k but the value ranges from 32k to 512k. Higher block sizes for large databases is recommended.

Signature Hash Comparison
The block signature hash is used to determine if the block exists in storage by comparing the hash against other hashes in the Deduplication Database. By default, signature hashes are generated on the Client. This is preferred since the processing of block signatures can be distributed to many different systems. This is required when using Simpana Client Side Deduplication. For underpowered Clients that will not be using Client Side Deduplication, a subclient can be optionally configured to generate signatures on the MediaAgent.

Deduplication can be configured for Storage Side Deduplication or Client (source) Side Deduplication. Depending on how deduplication is configured, the process will work as follows:

Storage Side Deduplication. Once the signature hash is generated on the block, the block and the hash are both sent to the MediaAgent. The MediaAgent with a local or remotely hosted deduplication database (DDB) will compare the hash within the database. If the hash does not exist that means the block is unique. The block will be written to disk storage and the hash will be logged in the database. If the hash already exists in the database that means the block already exists on disk. The block and hash will be discarded but the metadata of the data being protected will be written to the disk library.

Client Side Deduplication Once the signature is generated on the block, only the hash will be sent to the MediaAgent. The MediaAgent with a local or remotely hosted deduplication database will compare the hash within the database. If the hash does not exist that means the block is unique. The MediaAgent will request the block to be sent from the Client to the MediaAgent which will then write the data to disk. If the hash already exists in the database that means the block already exists on disk. The MediaAgent will inform the Client to discard the block and only metadata will be written to the disk library.

Client Side Disk Cache An optional configuration for low bandwidth environments is the client side disk cache. This will maintain a local cache for deduplicated data. Each subclient will maintain its own cache. The signature is first compared in the local cache. If the hash exists the block is discarded. If the hash does not exist in the local cache, it is sent to the MediaAgent. If the hash does not exist in the DDB, the MediaAgent will request the block to be sent to the MediaAgent. Both the local cache and the deduplication database will be updated with the new hash. If the block does exist the MediaAgent will request the block to be discarded.
Deduplication Database

The deduplication database is the primary component of Simpana's deduplication process. It maintains all signature hash records for a deduplicated storage policy. Each storage policy will have its own deduplication database. Optionally, a global deduplication storage policy can be used to link multiple storage policies to a single deduplication database by associating storage policy copies to a global deduplication storage policy.

The deduplication database currently can scale from 500 to 750 million records. This results in up to 90 Terabytes of data stored within the disk library and up to 900 Terabytes of production in protected storage. It is important to note that the 900 TB is not source size but the amount of data that is baked up over time. For example if 200 TB of data is being protected and retained for 28 days using weekly full and daily incremental backups, the total amount of protected data would be 800 TB (200 TB per cycle multiplied by 4 cycles since a full is being performed every seven days). These estimations are based on a 128k block size and may be higher or lower depending on the number of unique blocks and deduplication ratio being attained.

A deduplication database can handle up to 50 concurrent connections with up to 10 active threads at any given time. The database structure uses a primary and secondary table. Unique blocks are committed to the primary table and use 152 bytes per entry. Duplicate entries are registered in the secondary table and use 48 bytes per entry.

Deduplication Store

Each storage policy copy configured with a deduplication database will have its own deduplication store. Quite simply a deduplication store is a group of folders used to write deduplicated data to disk. Each store will be completely self-contained. Data blocks from one store cannot be written to another store and data blocks in one store cannot be referenced from a different deduplication database for another store. This means that the more independent deduplication storage policies you have, the more duplicate data will exist in disk storage.
CommVault recommends using building block guidelines for scalability in large environments. There are two layers to a building block, the physical layer and the logical layer.

For the physical layer, each building block will consist of one or more MediaAgents, one disk library and one deduplication database.

For the logical layer, each building block will contain one or more storage policies. If multiple storage policies are going to be used they should all be linked to a single global deduplication policy for the building block.

A building block using a deduplication block size of 128 KB can scale to retain up to 96 TB of deduplicated data. This could retain approximately 40 – 60 TB of production data with retention of 30 – 90 days. The actual size of data will vary depending on the uniqueness of production data and the incremental block rate of change.

It is critical to provide adequate hardware to achieve maximum performance for a building block.

Performance starts with properly scaling the MediaAgent. There should be a minimum of 32 GB of RAM on each MediaAgent hosting the deduplication database.
The disks library can be sized up to 100 TB for a single building block. Mount paths should be configured between 2 – 8 TB.

In order to meet deduplication database IOPs requirements, high performance disks in a RAID array must be used. Enterprise class Solid State Disks or high speed SCSI disks are recommended. The disks should be configured in a RAID 0 or RAID 10 configuration. RAID 0 provides the best read / write performance but creates multiple single points of failure. If RAID 0 is going to be used ensure you are frequently protecting the deduplication database. Dedupe database backup and recovery will be covered later in this ELearning course.

Best practices for the deduplication database:
• Put the DDB on the same server as the MediaAgent
• The DDB volume needs to be on dedicated high performance disks
• DDB disk volume performance must meet IOPs required for qualifying as a disk for DDB use
• Dedicated storage adaptors - make sure MA sees the drives
• Use Simpana Cvdiskperf tool (found in software base directory) to check read/write rate
• Do not use virus scan on DDB volume
There are three methods that disk library data paths can be configured when using deduplication: Direct Attached Storage or DAS, Storage Area Network or SAN and Network Attached Storage or NAS.

Direct attached storage is when the disk library is physically attached to the MediaAgent. In this case each building block will be completely self-contained. This provides for high performance but limits resiliency. If the MediaAgent controlling the building block fails, data stored in the disk library cannot be recovered until the MediaAgent is repaired or replaced.

Keep in mind that, in this case, all the data in the disk library is still completely indexed and recoverable, even if the index cache is lost. Once the MediaAgent is reconstructed, data from the disk library can be restored.

Storage Area Networks or SANs are very common in many data centers. SAN storage can be zoned and presented to MediaAgents using either Fibre Channel or iSCSI. In this case the zoned storage is presented directly to the MediaAgent providing Read / Write access to the disks.

When using SAN storage, each building block should use a dedicated MediaAgent, deduplication database and disk library. Although the backend disk storage in the SAN can reside on the same disk array, logically in the Simpana software it should be configured as two separate libraries.
This provides for fast and protocol efficient movement of data but, as in the case of Direct Attached Storage, if the building block MediaAgent fails, data cannot be restored. When using SAN storage either the MediaAgent can be rebuilt or the disk library can be re-zoned to a different MediaAgent. If the disk library is re-zoned, it must be reconfigured in the Simpana software to the MediaAgent that has access to the LUN.

Network Attached Storage has an advantage in that the path to the storage is directly through the NAS hardware. This means that by using CIFS or NFS, UNC paths can be configured for a disk library to read and write directly to storage. When using NAS storage as a disk library, it is still recommended to configure two separate disk libraries in the Simpana software. In this case the library can be configured as a shared library, where both MediaAgents can see all storage. Separate building blocks should still be used for each MediaAgent providing Read / Write access to a disk library but Read Only access can also be granted to all libraries on the NAS storage. In this case, if a MediaAgent fails, any other MediaAgent with access to the library can conduct restore operations.
Parallel deduplication is a highly scalable and resilient solution that allows the deduplication database to be partitioned. It works by dividing signatures between multiple databases to increase the capacity of a single building block. If two dedupe partitions are used, it effectively doubles the size of the deduplication store.

In this example, two dedupe partitions have been configured, each on a separate MediaAgent. Signatures are generated on the Client and depending on the signature generated it will be directed to one of the two partitions for processing. Although either MediaAgent can process signature lookups, the data for the client will always use its default MediaAgent path. This allows all unique deduplication blocks to be protected through a single MediaAgent although duplicate blocks may have been protected by either of the MediaAgents.

Since deduplicated data can exist on either of the partitions, the disk library should be configured using NAS storage. UNC paths should be used for the NAS disk library so either MediaAgent will be able to access data even if the other MediaAgent is unavailable.

Parallel deduplication is an advanced feature for large enterprise environments and CommVault Professional Services should be consulted when designing deduplication building blocks using this solution.
When designing storage policy and building block architecture, another consideration is that certain data types do not deduplicate well against other data types. A prime example would be file system data and database data. In this case, different building blocks and storage policies can be configured to manage different data types. In this example a global deduplication storage policy has been configured with a block size of 128 KB. Two data management storage policies have been configured, one with a 30 day retention and the other with a 90 day retention. All deduplication blocks from both storage policies will deduplicate based on the global deduplication policy setting, but will be retained based on the data management storage policy retention.

A second building block using a dedicated storage policy has been configured for database backups. In this example a 256 KB block size has been configured and the storage policy has retention of 14 days.
SILO Storage

- How SILO Works
- SILO Folder
- Recovery Process

Consider all the data that is protected within one fiscal quarter within an organization. Traditionally a quarter end backup would be preserved for long term retention. Let’s assume that quarter end backup of all data requires 10 LTO 5 tapes. Unfortunately with this strategy the only data that could be recovered would be what existed at the time of the quarter end backup. Anything deleted prior to the backup within the specific quarter would be unrecoverable unless it existed in a prior quarter end backup. This results in a single point in time that data can be recovered. Now let’s consider those same 10 tapes containing every backup that existed within the entire quarter. Now any point in time within the entire quarter can be recovered. That is what SILO storage can do.

SILO storage allows deduplicated data to be copied to tape without rehydrating the data. This means the same deduplication ratio that is achieved on disk can also be achieved to tape. As data on disk storage gets older the data can be pruned to make space available for new data. This allows disk retention to be extended out for very long periods of time by moving older data to tape.

How SILO works

Data blocks are written to volume folders in disk storage. These folders make up the deduplication store. The folders have a maximum size which once reached the folder is marked closed. New folders will then be created for new blocks being written. The default volume folder
size for a SILO enabled copy is 512 MB. This value can be set in the Control Panel, in the Media Management Applet. The SILO Archive Configuration setting Approximate Dedup disk volume size in MB for SILO enabled copy is used to specify the volume folder size. It is strongly recommended to use the default 512 MB value. For a SILO enabled storage policy, when the folder is marked full it can then be copied to tape. What this really is doing is backing up the backup.

**How volume folders are moved to SILO Storage**

When a storage policy is enabled for SILO storage an On Demand Backup Set is created in the File System iDataAgent on the CommServe server. The on Demand Backup Set will determine which volume folders have been marked full and back them up to tape each time a SILO operation runs. Within the backup set a Default Subclient is used to schedule the SILO operations to run. Just like an ordinary data protection operation, right-click the subclient and select Backup. The SILO backup will always be a full backup operation and use the On Demand Backup to determine which folders will be copied to SILO storage.

**SILO storage recovery process**

In traditional recovery from tape, the tape is mounted in a drive and the data is recovered directly back to the recovery location. With SILO to tape the data must first be staged to the disk before the data can be recovered. Each volume folder that contains data blocks for the restore must be staged to the disk library for the recovery operation to complete. Since block level deduplication will result in blocks in different locations being referenced by data, multiple volume folders may be needed for a single recovery operation. This can result in a slower restore performance.

SILO storage is intended to be a compliance solution by storing data with long retention in deduplicated form. Time to recover SILO data will be longer than traditional tape or disk storage since it needs to be pre-staged to disk before recovery. SILO storage is not an option to recover data from last week but rather is a feature to recover data from last year or five years ago. Understanding this concept places Silo storage into proper perspective. This feature is for long term preservation of data to allow for point in time restores within a time period with considerably less storage requirements than traditional tape storage methods.

**How the Process works**

Let’s assume we are using deduplication and Silo storage. Our primary storage policy copy has a retention of two years. We choose to seal the deduplication store every quarter. We will have one active store, and at least one cached store on disk. This means we can perform point in time recovery of data for a period of six months from disk. We will also be using space management with disk thresholds configured that if we reach 85% of disk capacity we will prune cached volumes. If there is enough disk storage available we might be able to keep 9 – 12 months of data on disk. Beyond that point the data will need to be pulled from the tape SILO.
We could define our SLA for up to 6 months to be 2 hours. From 6 months to 1 year the SLA will be 2-4 hours. Beyond that point the SLA will be 4+ hours.

The recovery process will work as follows:

- The CommVault administrator performs a browse operation to restore a folder from eight months ago.
- If the volume folders are still on disk the recovery operation will proceed normally.
- If the volume folders are not on disk the recovery operation will go into a waiting state.
- A SILO recovery operation will start and all volume folders required for the restore will be staged back to the disk library.
- Once all volume folders have been staged, the recovery operation will run.
- To ensure adequate space for SILO staging operations a disk library mount path can optionally be dedicated to SILO restore operations. To do this, in the Mount Path Properties General tab select the option Reserve space for SILO restores.
- The procedure is straight forward and as long as SILO tapes are available the recovery operation is fully automated and requires no special intervention by the CommVault administrator.
Advanced Deduplication Configurations

- Compression
- Client side disk cache
- Variable Content Alignment
- Fragmentation considerations

Compression
It is recommended for most data types to enable compression during the deduplication process. Compression can be enabled in the storage policy primary copy or in the subclient properties. By default compression is enabled for a deduplication storage policy. You can turn compression off in the storage policy copy or you can override the use of compression in the subclient properties.

For certain application types such as Oracle and SQL which may perform application level compression you should use a dedicated deduplication storage policy with compression turned off. In some cases using application compression can cause deduplication rates to suffer. In this case you should experiment with using application compression or CommVault compression to determine which results in better deduplication ratios. For large databases it is recommended to consult with CommVault on best practices.

Client Side Disk Cache
Along with configuring Client Side Deduplication, a Client Side Disk Cache can be created. Each subclient will contain their own disk cache which will hold signatures for data blocks related to the subclient. The default cache size is 4GB. The Client Side Disk Cache is recommended for slow networks such as WAN backups. For any networks that are 1Gbps or higher using this option will not improve backup performance.
In this example a signature is generated on a deduplication block. The signature is then compared in the local client disk cache first. If the block does not exist in the disk cache, the signature is then sent to the MediaAgent and compared in the deduplication database. If the block does not exist, both the client disk cache and the deduplication database is updated and the block is written to the library.

**Variable Content Alignment**
Variable Content Alignment can be used in some situations to improve deduplication ratios for large data files such as database dumps. Enabling this option will read block data and align the blocks to correspond to prior data blocks that have been deduplicated. By aligning the content prior to performing the hash process, better deduplication ratios may be attained. This will however require more processing power on the Client. Since Simpana deduplication is content aware, enabling this option will not provide better deduplication for average file data. This option is only recommended for large file system data such as database dumps or PST files with low incremental rates of change.

**Fragmentation Considerations**
Since CommVault stores data in the disk library in chunks, when blocks are deleted from disk it causes empty spaces within the chunk. For Windows MediaAgents, the sparse file attribute is used to allow empty spaces within the chunk to be used to store new blocks. Since Windows uses a write next mechanism when writing data to disk, the empty spaces will only be allocated to new data when the disk starts to reach full capacity. If new data is written to the empty spaces, fragmentation could occur. This could negatively affect performance for auxiliary copy and restore operations. Scheduled fragmentation analysis operations can be configured for the disk library. This will analyze each mount path to determine the level of chunk fragmentation that exists. If fragmentation levels are too high, defragmentation operations can be run by using third party file level defrag tools. When performing defragmentation operations on a mount path, the mount path should be placed in an offline state.
Deduplication Best Practices

• General Guidelines
• Deduplication Database
• Disk Library Considerations
• GridStor™ Technology Considerations
• Deduplication Storage
• Block Size Settings
• Performance
• Global Deduplication
• SILO Storage

General Guidelines
• Carefully plan your environment before implementing deduplication policies.
• Consider current protection and future growth into your storage policy design. Scale your deduplication solution accordingly so the deduplication infrastructure can scale with your environment.
• Once a storage policy has been created the option to use a global dedupe policy cannot be modified.
• When using encryption use dedicated policies for encrypted data and other policies for non-encrypted data.
• Not all data should be deduplicated. Consider a non-deduplicated policy for certain data types.
• Non-deduplicated data should be stored in a separate disk library. This will ensure accurate deduplication statistics which can assist in estimating future disk requirements.

Deduplication Database
• Ensure there is adequate disk space for the deduplication database.
• Use dedicated dedupe databases with local disk access on each MediaAgent.
• Use high speed SCSI disks in a RAID 0, 5, 10, or 50 configurations.
• Ensure the deduplication database is properly protected.
• Do NOT backup the deduplication database to the same location the active database resides.
Disk Library Considerations
- It is recommended to use dedicated disk libraries for each MediaAgent.
- If using a shared disk library with multiple MediaAgents use NAS disk storage as opposed to SAN.
- Disk libraries should be divided into 2-4 TB mount paths.
- Use network paths as opposed to drive letters. Drive letters will limit the total number of mount paths that can be added.

GridStor Technology Considerations
- For backup and restore performance in large environments, it is not recommended to use GridStor Round Robin load balancing.
- If you choose to use the GridStor feature for data protection resiliency configure the GridStor feature in a shared disk library configuration to Failover as opposed to Round Robin.
- Do NOT use GridStor Round Robin option when using a shared disk library in a SAN environment.

Deduplication Store
- Only seal deduplication stores when databases grow too large or when using SILO storage.
- When using SILO storage consider sealing stores at specific time intervals e.g. monthly or quarterly to consolidate the time period to tape media.
- For WAN backups you can seed active stores to reduce data blocks that must be retransmitted when a store is sealed. Use the option Use Store Priming option with Source-Side Deduplication to seed new active stores with data blocks from sealed stores.

Block Size & block Processing
- Use the recommended 128 KB block size for all object level and virtual machine data protection jobs.
- For large databases use 256 KB or higher block setting. Consult with Professional Services for very large databases for best approach for data protection.
- Use compression for object level and virtual machine data protection jobs.
- For database applications that perform their own compression do NOT use CommVault compression.
- Use the Variable Content Alignment option when backing up large database dump files using the Simpana File System iDataAgent.

Performance
- Use DASH Full backup operations to greatly increase performance for full data protection operations.
- Use DASH Copy for auxiliary copy jobs to greatly increase auxiliary copy performance.
- Ensure the deduplication database is on high speed SCSI disks.
- Ensure MediaAgents hosting a dedupe database has enough memory (at least 32GB).
Global Deduplication
- Global deduplication is not a be-all-end-all solution and should not be used all the time.
- Consider using global dedupe policies as a base for other object level policy copies. This will provide greater flexibility in defining retention policies when protecting object data.
- Use global deduplication storage policies to consolidate remote office backup data in one location.
- Use this feature when like data types (File data and or virtual machine data) need to be managed by different storage policies but in the same disk library.

SILO storage
- SILO storage is for long term data preservation and not short term disaster recovery.
- Recovery time will be longer if data is in tape SILO so for short term fast data recovery use traditional auxiliary copy operations.
PLANNING A SOUND DATA PROTECTION STRATEGY
Disaster recovery or ‘DR’ is much more than backing up data and sending it off-site. Like other areas of technology, disaster recovery has been refined to a science encompassing all aspects of data protection, data preservation and data recovery. This science has been molded to a point where several key concepts and definitions are commonly used when planning, testing and implementing DR plans. The following information provides a high level overview of each of these concepts.

**Service Level Agreement (SLA)**
A *Service Level Agreement* defines a guaranteed “response time” or “resolution time” for various incidents that may occur within your enterprise. It is a contract between a business owner and the IT department. An overall SLA takes into account different objectives like Recovery Time Objective (RTO) and Recovery Point Objective (RPO). RTO and RPO will be applied on two different levels (business level and system level) and then integrated and articulated in an organizational DR Plan within an enterprise. It is important to apply different measures of RTO and RPO on these levels to determine the priority or sequence of recovery since resources such as power, hardware and bandwidth may be scarce when a disaster strikes.

**Recovery Time Objective (RTO)**
A *Recovery Time Objective* defines the time to recover a business system. Depending on the level of disaster and defined SLAs the RTO may be based on recovery time from point of disaster or from the point where the recovery process begins. This will be determined by the level of
disaster and should be quantified by business system owners and other business units. Technologies such as clustering, virtualization and disk replication/mirroring are implemented with the intention to reduce and in some cases eliminate system outages. These systems provide a level of high availability that, when planned right, can guarantee a high level of uptime. However, it is important to properly understand the type of disasters that may occur and how they might affect RTO.

**Recovery Point Objective (RPO)**

A *Recovery Point Objective* defines the frequency of recovery points that will be created and maintained. Another way of looking at an RPO is that it defines the acceptable amount of data loss that can occur. If backups are being conducted daily it will result in a 24 hour RPO. If tapes are being sent off-site weekly, then the RPO can potentially increase to seven days. Mission critical systems such as databases will typically conduct transaction log backups at short intervals (10-20 minutes) which results in shorter RPOs. Snapshots, synchronous or asynchronous replication and off-site vaulting replication technologies are also commonly implemented to shrink RPO times. RPO values are just as important, if not more than, RTO values. Not meeting an RTO could cost your company money in lost production but not meeting an RPO could result in data loss that may never be able to be recovered.

**Gap Analysis**

*Gap Analysis* is a process in which business units define SLA values for various business systems and then pass them along to technical teams. The technical teams conduct tests to establish current capabilities to meet SLAs. Gap analysis is then performed to see if the established SLAs can be met. If not the technical team must address shortcomings and adapt to better meet the business unit’s requirements. In some cases procedural adjustments can be made to better meet business’s needs. In other cases additional investments must be made to meet SLA requirements. If the business unit’s needs cannot be met or budget limitations prevent gap reduction then the business units must redefine their SLAs to be more in line with the realistic capabilities of the technical teams.

Another key point regarding gap analysis is that each business unit will always think that their systems are the most important. Fairly determining system priority and properly defining SLAs is sometimes a better fit for outside consultants or auditors. If outside consultants are to be used it is important that they do not represent specific products and technologies as they will sometimes push what they want and not provide the best solution for your situation. Auditors can be a big benefit as their knowledge of compliance requirements such as Sarbanes-Oxley can be used to push through technology upgrades and change legacy thought processes that impede progress towards providing a sound disaster recovery strategy.

**Risk Assessment**

*Risk Assessment* is a companywide coordinated effort to address the likelihood of a disaster, the effect it may have on business and the cost involved in preparing for it. Risks such as air conditioner leaks, fire, hacking or sabotage are disaster situations that every company should be prepared to deal with. Major disasters such as tornado, hurricane, volcanic eruption or terrorist attack are more complicated disasters that, depending on the nature of a business may
or may not be considered in a DR plan. This may sound contrary to what a DR course should state, but the truth is that location, disaster probability, nature of the business and data being protected will all factor in to planning a sound DR strategy.

If you work for a small company on the outskirts of Mt. Rainier, the potential of a volcanic eruption and the cost in defining short SLAs, which may be defined for an air condition leak, may not be worth the money and effort when the likelihood of an eruption is very small. In this case the cost associated with meeting short SLAs for an eruption would be substantially greater than an air condition leak. On the other hand if you work for a major bank in the same location, short SLAs would most likely be required. The point here is not that a DR plan should not be put in place, but rather the SLAs for the various levels of disaster should be realistically weighed on a cost/benefit scale before investing in meeting SLA requirements. Not all disasters are created equal so risk assessment should be considered at various disaster levels: business system outage, limited site disaster, site disaster and regional disaster.

**Total Cost of Ownership (TCO) & Return on Investment (ROI)**

*Total Cost of Ownership* is a well-known concept in the business world. Regarding DR planning and implementation TCO must be considered when assessing risk, defining SLAs and conducting gap analysis. If it is determined that short SLAs are to be defined, the TCO of designing and maintaining a DR plan including: hot DR site, bandwidth, personnel (including training and turnover), production hardware and hardware at the DR site must all be factored in to the equation. Putting a monetary value on achieving unrealistic SLAs can often be enough to readdress DR goals.

Where the TCO can usually be quantified with various calculations, *Return on Investment* (ROI) is not as easy to quantify. If two months after implementing a DR plan, disaster strikes, the ROI would be wonderful. If disaster never strikes then ROI may be thought of as being nothing. The truth is that ROI can be quantified when put into perspective. The piece of mind that a sound DR plan brings to a company can be factored into the ROI. Many companies who implement sound DR plans may receive a break on insurance, pass security and DR audits and even have an increase in customer and investor confidence. These factors should not be taken lightly and depending on the company and services they provide a sound DR plan can even be used in advertising. In overall planning of a DR strategy TCO and ROI should be taken into account to properly define SLAs.

**Cost Reduction vs. Risk Reduction**

Companies are always seeking out ways to reduce costs. In some cases reducing costs results in a compromise in effective DR planning. In other cases cost reduction can actually benefit DR planning. Consider the virtualization of data centers as a cost savings measure that actually benefits DR planning. It would be impractical to request 100 standby servers at a DR site for most companies but to request four servers to host virtual machines may be in the budget. The choice to terminate a contract with a dedicated DR facility might at first seem to be a negative towards DR planning but if the company has another facility a few towns over, it may be a perfect location for a new (and cheaper) DR facility. With bandwidth becoming considerably...
cheaper and Simpana features such as deduplication, DASH Full and DASH Copy, a branch office can be quickly and inexpensively converted into a warm or hot DR site.

In some cases cost reduction can have a negative effect on DR. Consider deduplication, being the big concept in data protection. When blocks are deduplicated they are only stored once. In this case the cost reduction in disk storage is countered by an increased risk in a corrupt block affecting the ability to recover data. This is the concept of cost reduction vs. risk reduction. Saving money in disk storage results in an increased risk. Another example is implementing archiving solutions where data is moved to secondary storage to free up space in production. Like deduplication, this results in data being stored in one location which may increase risk. Using technologies such as Deduplication and archiving can be methods of reducing risk without increasing cost. When the Simpana software is configured properly and CommVault best practices are followed, cost and risk reduction can both be achieved.
The concept of *Business Continuity* (BC) is the holistic approach of defining guidelines and procedures for the continuation of a business in the face of any disaster situation. In this case disaster may or may not even involve technical aspects or require DR planning. Business continuity is beyond the scope of an IT department and beyond the scope of this course, but it is extremely important to consider in regards to DR planning. A DR strategy may be perfectly planned and executed but without proper BC plans and procedures the effort of IT may be in vein. The primary point to consider here is that on the technical end of things you may not have the ability to design a BC strategy but you do have the power to influence. In some cases influence may include ensuring that DR aspects of a BC plan are properly being addressed such as facilities, chain of command, communication and power sources. In other cases influence might be making upper management aware that they need to create a BC plan as some companies may have no idea of how important BC planning is.

**Consider the following critical BC points and questions as they relate to DR planning:**

- **Facilities** – How secure is the main data center? Is the air conditioner right on top of the data center? How reliable is the power source? Is there a generator? How often is it tested? How much fuel does it have?
- **Chain of command** – Who is in charge when the person in charge is not there? Who’s next on the list? Who on the management team do you contact if you need to make substantial emergency purchase? What are ALL methods to contact ALL people in the chain?
• **Communication** – Who is our cell phone provider and what are their contingency plans in the event of disaster? Who is responsible for communicating with them? In the case of disaster how will management communicate with employees on status updates?

• **Contingencies** – What happens when DR plans need to be changed? How does the company deal with extended outages such as utilities where the ability to restore power or communication is out of the company’s hands.

• **Continuation of business** – how will employees work if there is no facility to work from? How will they access resources? How will they communicate?
Protection Methods

- Traditional Backups
- Archiving
  - Simpana OnePass™ Feature
- Snapshots
- Edge Data Protection
- Image Level Backups

There are several primary protection methods used in modern data centers. Each of these technologies have their advantages and disadvantages. It is important to understand that not all technologies are created equal and a holistic approach should be considered when designing a data protection strategy to meet SLAs.

Traditional Backups
Traditional backups to disk or tape protect data by backing up each object to protected storage. This is the tried and true method that has been used for decades so it is the most reliable protection technology. The main advantages when using traditional backups is that each item protected is a complete separate copy that is backed up to separate media. When using tape media the backup becomes portable. Many modern backup solutions incorporate traditional backups to disk storage which is then replicated to a DR site. CommVault’s deduplication and DASH Copy is an example of using traditional backups with a scheduled replication (DASH Copy) where only changed blocks are transmitted to the DR location. Traditional backups and restores are usually slower than some modern protection technologies which can have a negative effect on SLAs. This performance bottleneck is more severe when millions of items require protection such as large file repositories. Traditional backups are still the most common and cost effective data protection technology.
Archiving
Data Archiving is not technically a data protection technology but can be used to improve SLAs. Archiving removes infrequently accessed data from production disks and moves it to less expensive secondary storage. The archived data can be recalled by end users or Simpana administrators. By removing data from the production environment, backup and restores complete faster since less data needs to be moved improving RTO and RPO.

The Simpana OnePass™ Agent is a comprehensive solution included in Simpana® product suite that incorporates traditional backup and archiving into a single operation. It enables the movement of data to a secondary storage location and uses this data to meet both data protection and storage management archiving business objectives. Secure data recovery is available to both administrators and end-users via a platform-independent web-based console, file stub recovery and a tightly integrated Outlook add-in. Policy-driven selective stubbing and deletion from front-end storage provides storage management archiving without the need to process the data a second time.

Snapshots
Snapshots are logical point in time views of source volumes that can be conducted almost instantaneously. This allows for shortened RPOs since the snapshots can be conducted more frequently throughout the day. A snapshot is not truly considered a DR protection strategy since the protected data is not physically moved to separate media. Advanced snapshot technologies allow for data to be mirrored or vaulted to separate physical disks which can be located at off-site DR locations. Snapshot technologies are used to meet strict SLA requirements but are considerably more expensive to implement requiring dedicated hardware. Simpana’s Continuous Data Replicator (CDR) is a software based snapshot and replication technology which is a cost effective alternative to hardware snapshots. For supported hardware and CDR, SnapProtect™ technology can be used to conduct and manage snapshots.

Edge Data Protection (Desktop Laptop Option)
Edge data protection is a deduplication enhanced desktop / laptop data protection solution for protecting end user data. Edge works by using Simpana’s client side deduplication solution to backup block changes using an automatic scheduling mechanism. It allows users connected to specific networks, locally or remote, to backup data during specific time intervals based on network and system resource availability.

Replication
Replication technology is used to replicate block or object changes from a source volume to a destination volume. Replication methods can use synchronous or asynchronous replication to synchronize source and destination volumes using a one-to-one, one-to-many (fan out), or many-to-one (fan in) replication strategy. Production data can be replicated providing fast SLAs for high availability. Backup data or snapshot data can be replicated providing for a more complete DR solution. A disadvantage of replication is that if corruption occurs at the source it
may be replicated to the destination so replication should be used along with point in time snapshots.

**Image Level Backups**

Image level backups are faster than traditional backups because they read all blocks from a production disk in sequential order. When backing up large file volumes image level backups can have a performance advantage over traditional backup methods. Once the backup is complete indexes are generated from the disks metadata to allow for granular restores or full system recovery. For large file volumes, the time it takes to generate indexes can be slow causing a bottleneck but the data is backed up from the production system faster than traditional backup methods.
Data Description is based on the business data residing in the production environment. This data in some cases can be an entire server, in other cases a business system may span multiple servers and in other cases business data requiring different protection may exist on a single server. The key aspect of describing data should be its business value and not its physical location.

The **Client/Host** is the system through which the specified data set will be accessed. In the case of shared or distributed storage there may be more than one client per data set. Identifying the client(s) marks the first transition point for data movement. Data will be read from primary storage through the client host onto protected storage. Its path from the client to protected storage will be determined by the placement of MediaAgents in the final storage design.

The **location** of the data will help determine whether some protection options (such as Snap or replication) are possible and it will also determine any possible resource/data path sharing requirements. Several sets of data located on the same shared storage device but under different client management can present potential performance problems.

**Volume** information is, of course, essential to sizing protected storage, but it’s also essential to determine data movement resource requirements and potentially the need for parallel data movement to meet operation window requirements.
The **dynamics** of the data is its daily change rate and annual growth rate. Both are key data points for storage and storage policy design. Daily change quantifies both modified and new data as the minimum data volume that requires protection. This impacts the rate of protected storage growth and resources required to move the new data into storage. Annual growth rate helps determine future storage capacity which must be accounted for in any storage design.

In many IT organizations **dependency** information is captured on documents that are not dynamic and typically are not updated with any enterprise change. Additionally, dependency details are not readily available for the people who need them. Questions like "what server is your application on? What database does it use? What other applications does it depend on – or depend on it?" are being asked by operation managers, enterprise architects, change managers, service support specialists, and of course – Protected Storage architects. Dependencies are essential design information, yet many IT organizations still don't understand how to document, manage, and operate these dependencies.
Data Availability

Data Availability is the speed and ease of access to data. Understanding Data Availability options, capabilities, and limitations is essential to designing protected storage. Production disk is the primary data availability media/location. Data at that level is instantaneously and transparently available to both applications and users. It’s where the data is originally written and read from.

In Hierarchical Storage Management (HSM) availability terms, production disk is considered to be “Online”. Removable media still contained within an automated library is considered to be “Near line”. Access may be delayed, but it is still automated. Offline data requires manual intervention in order to bring it to Near line or Online status. Offline data can be as simple as tapes sitting on a shelf next to the tape library or tapes stored away in a third party vault which may require much more time to bring online.

Service Level Agreement

A Service Level Agreement (SLA) specifies the Maximum or Mean Time to Recover (MTTR) for data in protected storage. As data ages, the MTTR may increase. An example for file level or message recovery might be:

FS/MB data recovery requests < 14 days old must be recovered within (20) minutes of request. FS/MB data recovery requests > 14 days old but < 1 year old must be recovered within (24) hours of request. All versions of the data must be recoverable.
FS/MB data recovery requests > 1 year old but < 7 years old can be recovered within (24) hours of request. The data recovered will be the last monthly full iteration of the data.

**Business Continuity**
Business Continuity (BC) is the immediate availability of data as may be required to minimize the interruption of day-to-day business. This usually involves loss of a file, folder, disk, or server and is normally satisfied by restore from on-site backup data on magnetic storage. BC requirements are usually specified in media type and length of availability.

**Disaster Recovery**
Disaster Recovery (DR) provides for protection against loss of both production and on-site backup data and usually implies loss of a critical business function. DR requirements are usually specified in frequency and duration of data movement off-site.

**Archive**
Archive implies long term availability of data that has value to the company. It can also mean movement of less frequently access data to less expensive storage. This data may be historical records required by legal, industry, or company requirements. The requirement for recall of archived data may be transparent (on-site magnetic storage) or limited (vaulted off-site storage) Archive requirements are usually specified in levels of availability and/or retention.
Protected Storage Requirements will determine the following:
- How many copies of data will be required
- Where will the copies be stored
- How long will the data be retained for
- Will data require encryption or content indexing

Using this chart, Storage Policies can be configured in an efficient manner. A chart such as the one above created in a spreadsheet program can be sorted by fields to determine common requirements such as storage location and retention. This can simplify the process of creating Storage Policies.
DESIGNING A SOUND DATA PROTECTION STRATEGY
The Simpana product suite uses iDataAgents or ‘Agents’ to communicate with file systems and application that require protection. Any server with an Agent installed on it is referred to as a Client. Each Agent contains code that is used to communicate directly with the system requiring protection. The Agent will communicate using APIs or scripting that is native to the file system or application. For example: A Windows 2008 file system can use VSS to protect file data so the Windows Agent will have the option to enable VSS during backup operations.

The Agent will then have a data set defined. The data set is a complete representation of all data the Agent is responsible to protect. Within the data set, subclients are used to define the actual data requiring protection. By default, a Default Subclient is used to define ALL data requiring protection within the backup set.

Additional subclients can be created to define specific content requiring protection. When content is defined within the user defined subclient, it will automatically be excluded from the default subclient. An example for a custom subclient could be defining a specific drive containing user data where VSS will be initiated for the drive during backup jobs to ensure all open files are protected.
Protecting Virtual Environments

- Hyper-V
  - VSA on Physical host
- VMware
  - VSA on physical or virtual proxy
- Agents Installed in VMs

Virtual Server Agent (VSA)
The Simpana Virtual Server Agent can be used to protect virtual machines by communicating with the hypervisor’s APIs to backup the virtual machine disks. The options available for backup include full, incremental, differential, and synthetic full. The option to Enable Granular Recovery is set by default to enable file level recovery from the backup of the virtual machine disks.

For VMware Simpana supports VMware vStorage API method (VADP) and VMware Consolidated Backup method (VCB). To support VADP backups, Change Block Tracking or CBT must be enabled. The Virtual Server iDataAgent agent will automatically check and enable CBT at the time of backup. Virtual Server iDataAgent may not be able to enable CBT for cloned or migrated virtual machines.

Agent based protection

The traditional method for protecting virtual machines is to install a file system or application agent within the virtual machine itself. There are advantages and disadvantages to using this method:
The first advantage is it is simple to deploy. When agents are installed in the virtual machine the Simpana software will treat the machine as if it is a physical client. All of the functionality for managing physical clients would be the same for the virtual clients.

The second advantage of installing an agent in a virtual machine, is the application specific functionality becomes available. For example using MAPI to conduct granular mailbox backups. Another example would be conducting transaction log backups for a virtualized database application.

There are also several disadvantages:

Installing agents within the virtual machine results in all data being granularly backed up and restored. This can be a slow process if there are many files within the machine.

The backup and recovery process will also require all data to be moved over the network which can become a bottleneck.

A third disadvantage is that all processing during the backup or recovery process will be conducted on the hypervisor. This could potentially become a bottleneck if too many virtual machines are being backed up at the same time.
This is a conceptual overview of how the VSA backup process works:

- The backup is initiated by the Simpana software for each virtual machine that will be backed up.
- The VSA communicates with hypervisor with the list of virtual machines that have been defined within the subclient contents of the virtual server agent.
- All virtual machines will have their disks quiesced. For windows virtual machines, VSS will be enabled on all of the disks to provide a consistent point in time backup of each disk.
- Once the disks for the virtual machines are quiesced, the Hypervisor conducts a software snapshot which will be used to back up the VM.
- VSA backs up the virtual machines either through the physical hypervisor or a physical proxy. With VMware, if the VSA is installed on a physical host it will be used as a proxy to back up the VMs. If a virtual proxy is being used, the VMs will be backed up through the virtual proxy on the physical hypervisor. For Hyper-V the VMs will be backed up through the physical hypervisor.
- When the backup process runs, virtual disks are indexed to provide granular recovery of files and folders within the virtual machine.
- Once the backup is complete, the hypervisor releases the software snapshot. The disk within the virtual machines are unquiesced and any transactions that were recorded while the disks were in the quiescent state are replayed.
This process ensures a consistent state of the snapshot at the time the backup was initiated.

**VSS and its role in VM backups**

For Windows virtual machines, Microsoft’s Volume Shadow Copy Service, or VSS, can be used to provide consistent point in time backups of disk volumes.

VSS is Windows’ built-in infrastructure for application backups. A native Windows service, VSS facilitates creating a consistent view of application data during the course of a backup. It relies on coordination between VSS requestors, writers, and providers to quiesce – or “quiet” – a disk volume so that a backup can be successfully obtained without data corruption.

In order for this to work the VMware Tools VSS component must be enabled. The Virtual Server agent requests VMware tools to initiate a VSS snapshot in the Guest OS. All registered VSS writers in the Guest OS get the request and they prepare its application to be backed up committing all transactions to. Once all VSS writers are finished they communicate back to your backup software which then initiates a VMware snapshot. This will make the backup application consistent.
Simpana® software supports most major applications through the use of agents installed on the application servers or on proxy servers with access to data. For unsupported applications, scripts can be used to properly quiesce application databases and then back them up as file data.

Virtualized Applications

Virtualized applications pose a challenge when it comes to data protection. Issues such as disk I/O activity, application type and application state at the time of backup can significantly affect the backup process. There are several methods that can be used to protect virtualized applications.

**Simpana application iDataAgents** – An iDataAgent installed in the VM will directly communicate with application running in the VM. Prior to the snap operation the agent will communicate with the application to properly quiesce databases. For large databases this is the preferred method for providing application consistent point in time snap and backup operations. Using application agents in the VM also provide database and log backup operations and a simplified restore method using the standard browse and recovery options in the CommCell GUI.

**VSA and VSS aware applications** – Some application such as Microsoft SQL and Exchange are VSS aware. When VSS is initiated on the virtual machine it will attempt to quiesce the VSS aware...
application to provide an application consistent snapshot. For smaller application databases with low I/O this process should be adequate for consistent snapshots. For larger database or databases with high transaction I/O this method is not recommended.

**Scripting database shutdowns** – Using external scripts which can be inserted in the Pre/Post processes of a subclient, application data can be placed in an offline state to allow for a consistent point-in-time snap and backup operation. This will require the application to remain in the offline state for the entire time of the snapshot operation. When the VM is recovered the application will have to be restarted after the restore operation completes. This method is only recommended when Simpana agents are not available for the application.
Simpana® IntelliSnap™ Technology overcomes these limitations by providing a single interface to conduct, manage, revert, and backup snapshots. The following lists the key highlights for the IntelliSnap feature:

**Application Awareness** – By using Simpana iDataAgents to communicate with hosting applications, application consistent snapshots can be performed. The application agent will communicate with the hosting application to quiesce databases prior to the snap occurring. This is a significant benefit when protecting large databases where traditional backup methods are not adequate to meet protection windows.

**Snapshot backups to reclaim disk cache space** – By managing the snapshots, Simpana software can also be used to backup the snapped data. As older snapshots are backed up to protected storage, the snaps can be released on the source disk and the space can be freed for new snap operations.

**Granular recovery** - Snapshots can be mounted for Live Browse and indexed during backup operations for granular recovery of objects within the snap. Whether using live browse or a restore from a backup, the method to restore the data is consistent. Using the proper iDataAgent you can browse the snapped data and select objects for recovery. This process is especially useful when multiple databases or virtual machines are in the same snap and a full
revert cannot be done. In this case just the objects required for recovery can be selected and restored.

**Simplified management** – Multiple hardware vendors supported by the IntelliSnap feature can all be managed through the Simpana interface. Little additional training is involved since the same subclient and storage policy strategies used for backing up data are extended when using snapshots. Just a few additional settings are configured to enable snapshots within the CommCell environment.

**Note:** The Simpana IntelliSnap feature is rapidly evolving to incorporate increased capabilities as well as expanded hardware support. Check with CommVault online documentation for current list of supported features and supported vendors.

**How IntelliSnap™ Technology Works**
IntelliSnap technology operates by interfacing with hardware APIs to conduct and manage snapshots. There are several steps required to implement the IntelliSnap feature in a CommCell environment.

**Deploy & Configure Architecture** - A IntelliSnap Architecture consists of the following components:

- Supported hardware array or Simpana Continuous Data Replicator installed on the host server.
- Host server running specific file system and application iDataAgents for the host, VSS provider (for Windows servers), and a MediaAgent. The host client must also be enabled for IntelliSnap operations.
- Proxy server to manage and backup snapshots running the same OS as the host server and a MediaAgent. VMware proxy servers must use a Windows OS and have the Virtual Server Agent (VSA) installed.

**Configure arrays** – Array information is set in the **Array Management** applet in Control Panel. Depending on the vendor different information may be required.

**Configure storage policies** – Storage policies are used to centrally manage snapshots of subclient data just like backup data. When configuring storage policies, a snapshot copy is added to the policy. For some vendors, multiple snap copies can be added. NetApp DFM enabled policies currently support multiple snap mirror/vault copies.

**Configure subclients** – The IntelliSnap capability is enabled at the client level in the **Advanced** tab of the client properties. Once enabled for the client, subclients will have a **IntelliSnap Operations** tab that can be used to enable and configure snapshots for the subclient.

**IntelliSnap Architecture**
IntelliSnap architecture is made up of host servers and proxy servers that work together to provide snap and optional backup operations.

**Host Server Agent Requirements**
The host server is the server which has direct access to data on the array. For VMware the host server will be a proxy server with the Virtual Server Agent (VSA) installed since agents cannot be directly installed on ESX hosts. Host servers will require the following agents:

**MediaAgent** – Provides capabilities to execute array functions and access to snapshots on the host. It can also be used when backing up snapshots to CommVault protected storage if no proxy is being used or if the proxy server is unavailable.

**IntelliSnap** – IntelliSnap options are built into iDataAgents and do not require additional software to be installed on the host. IntelliSnap capabilities are enabled in the Advanced tab of the client properties. This will add a IntelliSnap Operations tab to subclients to configure snap operations.

**File System iDataAgent** – provides protection for OS data.

**Application iDataAgent** – provides application integration to perform application consistent snapshots for databases.

**CommVault VSS Provider** – used to properly quiesce Microsoft applications for application consistent snapshots.

**Proxy Server Agent Requirements**

A proxy server can be used to backup snapshots and as an off host proxy to mount snapshots. The use of a proxy server eliminates load on the host server for snap mining, mounting, and backup operations. The proxy server requires the following agents:

**OS must be same as host** – For a mount or backup operation to be performed the snap must be mounted on the proxy. In order for the proxy to recognize the file system, the same OS must be used on the proxy.

**File System iDataAgent** – A file system agent is required for backup operations. When a snapshot is backed up it is treated like a file system backup job.

**MediaAgent** – Used for array access, mounting snaps on the proxy and data movement from array to CommVault protected storage.
Data Protection Best Practices

- Meeting Data Protection Windows
- Protecting Database Applications
- Virtual Machines Protection
- Meeting Media Management Requirements
- Meeting Restore Requirements

Meeting Data Protection Windows

- It is critical to meet data protection windows. If windows are not being met then restore windows may not be met. If data is scheduled to go off-site daily but it takes four days to back up the data, then the data cannot be sent off-site until the job completes.
- If you are currently meeting protection windows, then there is no need to modify anything. Improving windows from six to four hours when your window is eight hours just creates more work and a more complex environment. The following recommendations are intended to improve performance when protection windows are NOT being met.

Storage policy settings and modification to help meet protection windows:

- **Device Streams** – Increase device streams to allow for more concurrent jobs streams to write if adequate resources are available.
- **MediaAgent** – ensure MediaAgent is properly scaled to accommodate higher stream concurrency.
- **Network** – ensure network bandwidth can manage higher traffic.
- **Disk Library (Non-Deduplicated)** – ensure library can handle higher number of write operations. Increase the number of mount path writers so the total number of writers across all mount paths equals the number of device streams.
• **Disk Library (Deduplication enabled)** – if not using Client Side Deduplication enable it. Each deduplication database can manage up to 50 concurrent streams. If using Client Side Deduplication, after the initial full is complete most data processing will be done locally on each Client. This means minimum bandwidth, MediaAgent, and disk resource will be required for data protection operations.

• **Tape Library** – If tape write speeds are slow enable multiplexing. **Note**: enabling multiplexing can have a positive effect on data protection jobs but may have a negative effect on restore and auxiliary copy performance.

**Data path property settings:**

• Increase chunk size to improve performance.

• Increase the block size to improve performance. **Note**: block size is hardware dependent. Before changing the block size ensure all NICs, HBAs, Switches, routers, MediaAgent OS, and storage devices at your primary and alternate sites (including DR sites) support the block size setting.

**Subclient settings and modifications to help meet protection windows:**

**General recommendations:**

Ensure all data is properly being filtered. Use the job history for the client to obtain a list of all objects being protected. View the failed items log to determine if files are being skipped because they are open or if they existed at time of scan and not time of backup. This is common with temp files. Filters should be set to eliminate failed objects as much as possible.

For file systems and application with granular object access (Exchange, Domino, SharePoint) consider using data archiving. This will move older and infrequently accessed data to protected storage which will reduce backup and recovery windows.

**File Backup recommendations:**

• For backups on Windows operating systems ensure source disks are defragmented.

• Ensure all global and local filters are properly configured.

• If source data is on multiple physical drives increase the number of data readers to multi-stream protection jobs.

• If source data is on a RAID volume, create subclient(s) for the volume and increase the number of data readers to improve performance. Enable the **Allow Multiple Data Readers within a Drive or Mount Point** option.

• For large volumes containing millions of objects:
  • Consider using multiple subclients and stagger scheduling backup operations over a weekly or even monthly time period.
  • For supported hardware consider using the Simpana IntelliSnap™ feature to snap and backup volumes using a MediaAgent proxy server.
  • Consider using the Simpana Image Level backup agent.
Database applications

- For large databases that are being dumped by application administrators consider using Simpana database agents to provide multi-streamed backup and restores.
- When using Simpana database agents for instances with multiple databases consider creating multiple subclients to manage databases.
- For large databases consider increasing the number of data streams for backing up database.
  **Note:** For multi-streamed subclient backups of SQL, DB2, and Sybase databases, the streams cannot be multiplexed. During auxiliary copy operations to tape if the streams are combined to a tape they must be pre-staged to a secondary disk target before they can be restored.
- For MS-SQL databases using file/folder groups, separate subclients can be configured to manage databases and file/folder groups.

Virtual Machine Protection

General Guidelines
- Consider using the Simpana Virtual Server Agent (VSA).
- Determine which virtual machines DO NOT require protection and do not back them up.

When using VSA agent to protect VMware environment:
- It is preferred to use physical VSA MediaAgent proxies versus virtual server MA proxies.
- Ensure enough proxies are being used to handle load.
- Use Simpana Client Side Deduplication and DASH Full backups.
- The data readers setting determines the number of simultaneous snap and backup operations that will be performed. Increase this number to improve performance.
  **NOTE:** ensure disks where virtual machines are stored can handle the number of concurrent snapshots or the snapshot process may fail.

When using file system agents in virtual machines:
- Consider having a base vm image that will be used to recreate the virtual machine. Use the default subclient filters to filter out any volumes and folders that do not require protection.
  **Note:** It is STRONGLY NOT recommended to alter the contents of the default subclient. If you explicitly map default subclient data the auto-detect feature will be disabled. This means any new volumes added to the machine will have to be explicitly added to the content of the subclient.

When protecting applications in VMware environment:
- Use application agents inside the VMs. It is strongly NOT recommended to perform VSA crash consistent backups of application database data.
Consider the pros and cons of using Simpana compression and client side deduplication. Using application level compression may have a better compression ratio but deduplication efficiency can suffer.

Simpana IntelliSnap Technology and VSA integration:
- Define subclients by data store affinity. When hardware snaps are performed the entire data store is snapped regardless of whether the VM is being backed up.
- For smaller Exchange or MS-SQL databases (less than 500GB), application consistent snapshots can be performed using the IntelliSnap feature and VSA.
- For large databases, install the application agent in the VM and configure the IntelliSnap options in the subclient. Hardware snapshots will be performed at the database level providing better scalability and application awareness.

Meeting Restore Requirements

Considerations for tape media:

If streams from different data sets are multiplexed or combined to a tape, only one data set can be restored at a time. Consider isolating different data set streams to different media using separate secondary copies for each data set and using the combine to streams option.

For large amounts of data that are being multi-streamed during backups, do not multiplex or combine the streams to tape. If the streams are on separate tapes the Restore by Job option can be used to multi-stream restore operations improving performance.

Considerations for disk media:

When using Simpana deduplication use the minimum recommended 128k block size. Small block sizes will result in heavier data fragmentation on disk which can reduce restore performance.

Improving Recovery Time Objectives (RTO):

- Filter out data that is not required for data protection operations. The less you backup the less you have to restore.
- Strongly consider data archiving. It will improve backup and restore performance. Note that deduplication will improve backups and reduce storage requirements it can actually have a negative effect on restore performance.
- If a subclient job was multi-streamed you can restore it using multiple streams through the Restore by Job option.
- Consider assigning different RTOs for different business data. It is not always about restoring everything. Consider a database server with five databases. Each one can be defined in a
separate subclient. This will allow each database to have a separate RTO so they can be recovered by priority.

Improving Recovery Point Objectives (RPO):

• Run point in time backups such as incremental or transaction logs more frequently for shorter RPO.
• Consider prioritizing data for RPO requirements and define the data as a separate subclient and assign separate schedules. For example a critical database with frequent changes can be configured in a separate subclient and scheduled to run transaction logs every fifteen minutes. To provide short off-site RPO windows consider running synchronous copies with the automatic schedule enabled.
• Consider using hardware snapshots with the Simpana IntelliSnap feature to manage and backup snapshots.
Module 2

CommCell® Environment Deployment
Topics

- CommCell® Deployment Process
  - New CommCell Deployment Process
  - Existing CommCell Upgrade Process
  - CommCell Disaster Recovery Process
  - Environment Requirements
  - Installing CommServe® Software
  - Installing MediaAgent Software
  - Index Cache Configuration
  - Library Detection, Installation and Configuration

- Client Agent Deployment methods
  - Standard Installation Methods – Interactive
  - CommCell Console Push Install
  - Custom Installation Methods
  - Deployment Best Practices
COMMCELL® DEPLOYMENT PROCESS
New CommCell® Deployment Process

- Install CommServe® Software
- Install MediaAgent Software
- Detect Libraries
- Configure Storage Policies
- Configure Schedule Policies
- Configure Subclient Policies
- Configure Global Filters
- Install Client Agents

The first component to be installed in a new CommCell® environment will be the CommServe® server. Once it is installed the next step would be to install MediaAgent software and detect and configure libraries. Policy configuration for Storage Policies, Schedule Policies, Subclient Policies and Global Filters should be done prior to installing any client agents. When installing client agents, options to associate the default subclient for the agent with the policies can be selected so preconfiguring policies makes the agent deployment process smoother.
Prior to upgrading a CommCell® environment it is critical to perform a CommServe DR backup. In the event of problems occurred during the upgrade process, the environment can be rolled back to ensure CommCell operations can continue. The first component to be upgraded must be the CommServe server. The upgrade process can be an in-place upgrade or a fresh installation of the CommServe server software can be conducted. It is recommended that you have the CommServe database inspected by CommVault prior to upgrading. This can be done by uploading the database dump to cloud.commvault.com. Check CommVault’s documentation-site for complete instructions for CommServe database inspection.

MediaAgents should be upgraded next and libraries should be tested to ensure everything is functioning properly. Clients can then be upgraded on an as needed basis. Note that with Simpana® software, client agents up to two versions back can coexist with a CommServe server and MediaAgents at the latest version.
CommCell® Disaster Recovery Process

- Rebuild CommServe® Server
  - CommServeDisasterRecoveryGUI.EXE
- Rebuild MediaAgent
- Rebuild Libraries
  - Disk Libraries
  - Tape Library
  - Replacing Drive
  - Changing MediaAgent Hosting Library

CommServe® Server

The CommServe server must be the first machine recovered before the recovery of any production data can be accomplished. The speed and method of recovering the CommServe server ultimately depends on the combination of several factors:

- Which High Availability CommServe server option or Standby CommServe server option was configured and the access to it.
- Access to the DR Backup metadata.
- How prepared the production and DR environment is and how practiced and efficient the Simpana Administrators are at recovering the CommServe server.
- What the effect is for an actual disaster scenario you are confronting (site or regional), or what practice DR run you are simulating.

CommserveDisasterRecoveryGUI.exe (CSDR tool)

The CommServe Disaster Recovery Tool restores the metadata from the Disaster Recovery Backup file. The Disaster Recovery Backup file gets created when a Disaster Recovery backup is performed from the CommCell Console.
The CommServe Disaster Recovery Tool can be used to rebuild the CommServe server on the same or different computer, change the name of the CommServe computer, create and maintain a CommServe server in the hot-site and to update the license.

**MediaAgent**

**MediaAgents at a Disaster Recovery site**
If it becomes necessary to build a completely new MediaAgent, as in the case of complete Disaster Recovery at another location other than the production-site, there are a few things to keep in mind. Usually, this type of scenario will be using removable media as the primary source of data recovery and the MediaAgent will be new to the CommCell environment. This is not a problem for the Simpana® software. The new MediaAgent will be installed after the CommServe server Disaster Recovery has taken place and connected to a library where the media has been loaded. Restores can take place from any library; in fact one of the advanced options of a restore job is to select the desired MediaAgent and Library. Some considerations may be licensing issues. With Volume based licensing there is no issue installing an additional MediaAgent, as with a DR License as well, but if the licensing is per agent it may be necessary to release the license of an existing MediaAgent to apply a license to a new one.

**MediaAgent Data Path in a Storage Policy**
If a MediaAgent is not available and it is imperative that data be restored, the data path configured for each copy set within a Storage Policy can be changed through the properties of the copy set.
For step-by-step instructions for recovery of a MediaAgent in any scenario please refer to CommVault’s documentation web site where detailed instructions are listed for each type of restore.

**Rebuild Libraries**

**Rebuilding Disk Libraries**
The main reason for changing the hardware of a disk library is to upgrade to better devices. Most disk libraries will have fault tolerant redundancies built in to avoid major disk failures. Changing the hardware is a relatively simple process. The original CV_Magnetic folder and all its contents must be copied to the new location. After moving the physical data, the original mount path can be changed in the Library and Drive Configuration tool by right-clicking the old mount path and selecting the new location.

**Rebuilding Removable Media Libraries**

**Replacing a drive**
In the event that a drive in a library fails and needs to be replaced, the process is very simple. After the new drive is installed in the library, the MediaAgents operating system must be able to communicate with the new drive. Within the CommCell Console, open the library properties page and from the Attributes tab, choose Enable Auto Drive Replacement when new device is detected during Mount to enable the option to automatically detect the new drive. A new drive
can also be manually detected by selecting *Mark Drive Replaced* from the task menu of the replaced drive.

**Replacing a Library**

There are two reasons to replace a library, the first being an upgrade to newer hardware and the second being a major hardware malfunction. In either case it is fairly simple to replace the library. Keep in mind the new library must support the same drive type and must have the same or more drives as the original. Once the Hardware is connected and can communicate with the MediaAgent’s operating system you can move the media from the old library to the new one. Then you must use the Library and Drive Configuration tool in order to configure the new library. The procedure to *Modify* the existing library to be replaced with the new library is clearly documented in our documentation website.

**Caution:** If a library is being replaced, **Do not deconfigure the library, master drive pool or drive pool.** Doing so will lose all data associated with the library.

**Changing the MediaAgent hosting a library**

There may be instances where it becomes necessary or desired to change the MediaAgent hosting a library to another MediaAgent. This would involve connecting or presenting the library devices to the new MediaAgent first and using the Library and Drive Configuration tool to configure the change of MediaAgent host. Choosing both old and new MediaAgents in the Library and Drive Configuration tool will allow the Administrator to select the option to *Change Host* when right clicking on the Library Controller, and also on the Drive Pool.
Environment Requirements

- Hardware Requirements
- Software Requirements
- Network Requirements
- Domain and DNS Requirements

Minimum system, software, and application requirements are documented in Simpana's Books Online (BOL). If you do not see your specific OS, application, or environment don't panic. Contact your Simpana® Support group to check if you can still install the software component. BOL may not have the latest information available from our testing group. Additionally, CommVault will often authorize "Field Certification" of new versions or unique environments to allow installation and support.

Be sure to read the notes included on the System Requirements page. These notes often contain caveats or additional information essential to the installation process.
Within a CommCell environment there can only be one active CommServe server. For high availability and failover there are several methods that can be implemented. The following information explains each of these methods.

**Hot / Cold Standby CommServe Server**
A hot or cold standby CommServe server consists of a physical or virtual machine with the CommServe software pre-installed. The DR backup Export process directs metadata exports to the standby CommServe server. In the event that the production CommServe server is not available the standby CommServe server can quickly be brought online.

**When using a hot / cold standby CommServe server consider the following key points:**
It is critical that both the production and standby CommServe servers are patched to the same level. After applying updates to the production CommServe server, ensure the same updates are applied to the standby CommServe server.

Multiple standby CommServe servers can be used. For example: an on-site standby and an off-site DR CommServe server. Use post script processes to copy the raw DR metadata to additional CommServe servers.
The CommCell license is bound to the IP address of the production CommServe server. If standby CommServe server will be used purchase the CommServe DR license which allows multiple IP addresses to be associated with the standby CommServe servers.

A standby CommServe server can be a multi-function system. The most common multi-function system would be installing the CommServe software on a MediaAgent. It is important to note that the CommServe software must be installed on a system with no other CommVault agents installed. First install the CommServe software and then install other agents. When using a multi-function server the DR restore operation will not work. Contact support in the event that the standby CommServe server must be activated for instructions on how to proceed in this situation.

If a virtual environment is present consider using a virtual standby CommServe server. This avoids problems associated with multi-function standby CommServe servers and eliminates the need to invest in additional hardware. Ensure the virtual environment is properly scaled to handle the extra load that may result when activating the virtual standby CommServe server.

**Virtualization**

Many customers with virtual environments are choosing to virtualize the production CommServe server. A virtualized CommServe server has an advantage of using the hypervisors high availability functionality (when multiple hypervisors are configured in a cluster) and reduces costs since separate CommServe hardware is not required. Although this method could be beneficial it should be properly planned and implemented. If the virtual environment is not properly scaled the CommServe server could become a bottleneck when conducting data protection jobs. In larger environments where jobs run throughout the business day, CommServe server activity could have a negative performance impact on production servers.

When virtualizing the CommServe server it is still critical to run the CommServe DR backup. In the event of a disaster the CommServe server may still have to be reconstructed on a physical server. Do not rely on the availability of a virtual environment in the case of a disaster. Follow normal CommVault best practices in protecting the CommServe metadata.

**Clustering**

The CommServe server can be deployed in a clustered configuration. This will provide high availability for environments where CommCell operations run 24/7. A clustered CommServe server is not a DR solution and a standby CommServe server planned for at a DR site. Clustering the CommServe server is a good solution in large environments where performance and availability are critical.

Another benefit for using a clustered CommServe server is when using Simpana data archiving. Archiving operations can be configured to create stub files which allow end users to initiate recall operations. For the recall to complete successfully the CommServe server must be available.
SQL Database Replication
The CommServe database typically will not grow very large so running periodic DR backups may be adequate to properly protect the CommServe metadata. In larger environments where the databases grow to larger sizes, using SQL log shipping or Simpana’s Continuous Data Replicator (CDR) can be used where minimal CommServe data loss (short RPO) is required. These protection methods require additional Simpana agents and additional Microsoft SQL server licenses.

Standby CommServe Options
DR Backup Phase 1 (export copy) configured directly to the standby CommServe server (physical or a virtual machine).

How to configure:
Pre stage a CommServe server at a hot-site and/or locally with a different host name and a different IP address with all Simpana services stopped. The DR Backup export phase is configured run directly to this server via a network share.

A CommCell license is tied to the IP address of the production CommServe server. It is recommended that you obtain a Dual IP License for the CommCell environment instead of obtaining an additional license for the CommServe server in the disaster recovery site. The Dual IP License can have two IP addresses assigned to it; a primary IP address for the production CommServe server and secondary IP address for the standby CommServe server staged in the disaster recovery site. Without the Dual IP License in place, if the IP address on the DR standby CommServe server is not exactly the same as the production CommServe server, Simpana services will NOT start after restoring the SQL database.

Reinstalling Software:
Ideally the standby DR CommServe server has the OS and the CommServe module preloaded with all of the CommServe services stopped. You should never run two CommServe servers at the same time in the same CommCell environment with their Simpana services running.

If the CommServe module is not preinstalled, install only the CommServe module, install the same Service Pack and patches as the production CommServe server and recover the CommServe server using the CSDR tool outlined below.

After recovering the CommServe server you can install the MediaAgent Module on the same machine if that is desirable.

Service Packs & Patches
It is critical that the production CommServe server and the target recovery CommServe server be at the same service pack and patch levels to avoid recovery issues.
Installing MediaAgent Software

- Installing on a Physical Host
- Installing on a Virtual Host
- Installing in a Clustered Environment

A MediaAgent component can be located on the same host as the CommServe component, the same host as an iDataAgent component, or on a separate host by itself.

The MediaAgent component can be installed in any order after the CommServe component has been installed.

Normally, at least one MediaAgent is installed with a configured library prior to installing iDataAgents, but it is not required.

Non-clustered MediaAgent components can be installed interactively from the installation media or pushed from the CommCell Console.

**Host Name resolution**
Proper Host Name resolution, both forward and reverse are the single most common installation problems. Verify proper host name resolution of all components before starting an install. IP addresses can be used in place of a Host Name if DNS is slow or unreliable.

**Client(s) access path**
If the client data will transit over a LAN, verify the expected access path is available and addressable. This data path may be different from the control/coordination path used for the install. Such paths can be set up using Data Interface Pairs.

Data path(s) to Library(ies)
The MediaAgent host must have access to all libraries to which you expect to read/write data from that MediaAgent. Multiple libraries under a single MediaAgent control are supported.

Index Cache Size and location
During installation you will be asked to select the location for the Index Cache (Default - <software install path>\IndexCache.) For performance reasons the index cache should be located on a separate disk of sufficient size. The estimation of index cache size is based on a number of assumptions, which include the following:

- Average full path name to the indexed object
- Average incremental percentage of the files being backed up
- Job frequency and type
- The retention time for the Index Cache

Calculations for sizing the index can be found on the documentation web site. However, a SWAG of 4% of protected indexed volume is often used to size the Index Cache for “average” environments. For most cases this is more than adequate.

After installation, the location of the Index Cache directory can be changed. Multiple MediaAgents can share a common Index Cache directory.
CommVault software uses a two-tiered distributed indexing structure providing great resiliency, availability, and scalability. **Job summary** data is maintained in the CommServe metadata database and requires minimal space to retain the data. The job summary information will be maintained as long as the data is being retained. An **Index Cache** maintains detailed indexing information for all objects being protected. Multiple index caches can be used for more efficient index scaling and to keep index files in close proximity to the MediaAgents. Index data is maintained in the cache based on retention settings of days or disk usage percentage. Each subclient will have its own index file and new index files are generated by default during a full data protection operation. Index files are copied to media automatically at the end of each job.

**Sizing the Index Cache**

The index cache should be sized based on the need to browse back in time for data to be recovered. The farther back in time you need to browse, the larger the cache should be. If the index cache is undersized, index files will be pruned sooner to maintain a default 90% disk capacity. When you attempt to perform a browse or find operation and the index file is not in the cache it will automatically be restored from media. If the index file is in magnetic storage there will be a short delay in recovering the index but if it is on removable media the time to recover the index can be much longer.
To properly size the index cache, consider the following:
The index file size is based on the number of objects being protected. Estimate 150 bytes per object. The more objects you are protecting the larger the index files will be.
Each subclient will contain its own index files within the cache.

The index cache should be on a dedicated disk or partition with no other data being written to the disk.

To reduce the probability of pulling an index file back from media use a large index cache location.

**Maintaining the Index Cache**
The index cache is self-maintaining based on two configurable parameters: Index Retention Time in Days and Index Cleanup Percent. Index files will be kept in the cache for a default of 35 days or until the cache disk reaches 90% disk capacity. A smaller index cache location may result in index files being pruned before the 35 day time period expires if the cleanup percentage is reached first. Index files will be pruned from the index based on least recently accessed.

A Minimum Free Space can also be configured to reserve space in the index cache location. The cleanup percent setting would be based on the allocated space to the index cache. So if you had a 100 GB partition and wanted to reserve 10 GB of space, the cleanup percent would be based on 90GB.

**Index Cache Location**
**Shared Index Cache**
A shared index cache is when multiple MediaAgents connect to a central cache location. This is required for GridStor® technology load balance configuration and in some cases is also required for a failover configuration.

To configure a shared index cache, one MediaAgent will host the index cache. The other MediaAgents will connect to it. The index cache location can be a local drive, SAN disk space, or a NAS device.
Library Detection and Configuration

• Adding Libraries from the CommCell® Browser
• Adding Mount Paths from the CommCell Browser
• Library and Drive Configuration Tool

Using the Library & Drive Configuration Tool

Libraries are either detected (e.g. tape device, library controller) or added (e.g. disk, cloud, IP-based controller). Essential to both is the ability of the MediaAgent to correctly see/access the device. Prior to any detection or adding of devices to a MediaAgent, the Engineer should confirm the physical and logical view of the device from the operating system. If multiple similar devices are involved (e.g. a multi-drive library), all such devices should be at the same firmware level.

Detection
The system only detects devices for which device drivers are loaded. A detected device may have the following status:

• Success indicates that the system has all of the information necessary to use the device.
• Partially configured, detect fail - connection error status when the detection fails due to an error connecting to the MediaAgent
• Partially configured, detect fail - device not found status if the detection fails due to a missing device
Note: that some devices (e.g., the library associated with a stand-alone drive) have no detection status, since they are virtual entities and as such have no hardware components that can be detected.

Exhaustive Detection
Modern tape drives have serial numbers which are used by the Simpana software to properly place a drive physically and logically within a library. Older drives without serial numbers require manual locating. Exhaustive detection is a process of associating drive numbers to its correct SCSI address. This is done by mounting a media to each of the drives in the library to obtain the drive’s SCSI address.

Adding
Logical libraries (e.g. Disk, Cloud, PnP) are added by user allocating assets and/or access to devices. This usually involves the grouping of devices (mount paths) identified by providing data paths and user access authority.

A hybrid library requiring both addition and detection would be an IP-based library. The IP address for the library control is added while the tape devices used by the MediaAgent(s) are detected and logically associated with the IP-based library.

Configuration
Added or Detected devices can be configured as new libraries or added to existing libraries (e.g. adding an additional tape drive in an already detected/configured library.) Configuration gives the device an identity within the CommCell environment and, as appropriate, an association with other devices for management/control (e.g. tapes drives in an automated library, new mount paths).
CLIENT AGENT DEPLOYMENT METHODS
Interactive Install

Interactive installation can be performed directly from the installation software disc by running the setup.exe command. Optionally you can copy the installation files to a disk or a network share accessible to the client and execute the setup.exe command from the client.

The SQL Server instance for the CommServe component cannot be installed from a UNC path. The path must be a mapped drive letter. The user performing the installation must have administrator privileges on the client to install software.

Any number of components can be selected for installation at the same time. For a new client, the Base Agent (not visible in the component list) will automatically be selected and the first item installed. The Base Agent provides files needed for communication with the CommServe component.

While every effort is made to not require a reboot of the host during or after the installation, the state of the system at the time of install may require a reboot. If this happens, you will be presented with an option to not reboot at that time.
Common questions asked during the interactive installation are:

- Installation Path
- Authorized user/password to interact with an application for backup/restore (Application Agent only)
- Firewall access (if required)
- Computer Group membership
- Default Storage Policy
- Filter Policy
- Include patches/service packs
- Update Schedule

Use a common installation path for all clients if possible, this will help with re-installation and/or a full system restore should it become necessary.
You can manage the installation of agent and component software packages on client computers or even on network computers not yet a part of the CommCell environment, from the CommCell console.

The required software packages can be downloaded or copied to the CommServe Cache Directory and then pushed to selected computers. Remote Software Cache directories may also be configured and used to locate installation software closer to their prospective targets or for different access privileges.

Remote caches can be configured for automatic synchronization with the CommServe cache directory. This entire process is all conveniently managed from the CommCell console.

Remote software cache directories can be created and managed via the Add/remove Software Configuration applet located in the CommCell cconsole's control panel.

Prior to configuring the installation of software packages to specific computers to build your CommCell environment, you must copy or download the required software packages to the CommServe cache directory. The directory is configured to serve as a holding area for software and update packages. To install from any of the software cache directories the directory must be a shared network directory with permissions set to write to the directory.
The CommServe cache directory can be populated during install of the CommServe host, by FTP download, or by using the **Copy Software** task found in the install path's base directory. Remote cache directories can be populated using the synchronization feature or the **CopyToCache** utility.

Client computers that are not in the same domain as the domain in which the CommServe cache is located must have bidirectional trust in place.

**If Authentication for Agent Install** is enabled for the CommCell environment, installation from the CommCell Console is restricted to only those users belonging to a user group assigned with **Administrative Management** capabilities for the CommCell computer or an existing Client computer within the CommCell environment. However, if it is a new computer, not yet part of the CommCell group, you must have Administrative Management capabilities for the CommCell group.

During configuration, computers within the domain that are not yet part of the CommCell group can be selected for installation. Users accessing these computers must have administrative privileges required for installing software.

Software packages are intelligently pushed to the computers. This means that a windows package pushed to the domain consisting of both Windows and UNIX computers will only install on the Windows systems. Additionally, application package software will only install on systems with the prerequisite software installed.

Install options include "For Restore Only" and the optional "CommServe Host Name" which, if left blank" leaves the client in an un-registered state. Either of these options will not consume a license until the client is either registered and/or enabled for data protection.

---

www.commvault.com

The Information contained in this document is subject to change without notice. No unauthorized use, copy or distribution.
Custom Installation Methods

- Decoupled Install
- Custom Package Install
- Restore Only Agent
- Silent Install

Decoupled Install
Decoupled install is performed without involving the CommServe server until you are ready to add the Client and/or MediaAgent to the CommCell environment. Once all necessary physical connections are established, the computer can be added to the CommCell environment. This feature will be useful when you want to pre-image computers with the software at a central location and later ship them to the environment where you plan to use them.

Custom Package Install
Custom Packages enable you to push smaller install packages through a network, which is useful for reducing WAN/LAN payload while installing remote clients.

Custom packages can be configured from the Simpana Installer's Advanced options. For UNIX systems, select the cvpkgadd's Advanced options menu choice.

Using Custom packages, you can do the following:
• Select the necessary components to build the custom package. This enables you to build smaller packages based on needs of the client computer.
• Create a self-extracting executable file for installing the custom package in the client computer. This enables you to easily deploy the software with a one-click deployment procedure.
• Save the installation options in the current deployment setup so it can be reused later.
Installation involves copying the custom package .exe file to the target host and executing to expand the installation files and start the silent install process. Upon completion, a success message will be displayed.

For UNIX, copy the folder to the target host and execute the cvpkgadd command.

**Restore Only Agent**
To install agents software for restore only, select **Restore Only** checkbox in Selected Platforms dialog during the installation as shown in the sample screen image. Installing Restore Only agents allows you to install the agent software without consuming any license. There may be different steps involved for Ddecoupled Installation based on the agent being installed. Check CommVault’s online documentation for step-by-step guides for installing agents in restore only mode.

**Silent Install**
A Silent install consists of the following distinct phases:

- **Recording Mode** - In this phase, an install is recorded, saving your install options to an .xml file.
- **Playback Mode (XML input file)** - In this phase, the .xml file is played back by the install program. The software components are installed as per the recorded options without prompting for any user inputs. Through this method, the deployment of the software can be automated.

When recording an install, note the following:
- The install program only records your choices, it does not execute the install.
- No license is consumed when recording an install.
- All Agents are selectable when recording an install.
- Review the System Requirements and the Installation procedures for each component you are installing.
- If you intend to play back this recorded install on multiple computers, choose options that are applicable to all those computers. For example when specifying an installation folder, be sure it exists on all target computers.
- Playing back a recorded installation installs the software with the options saved in the .xml file you created during the record procedures.
**Deployment Best Practices**

- CommServe® Server
- MediaAgents
- Index Cache
- Libraries
- Clients

**Key points regarding the CommServe server:**
- For CommServe server availability consider staging a standby CommServe server.
- In some environments virtualizing the CommServe server can provide high availability.
- In large environments consider clustering the CommServe server for high availability.
- It is ABSOLUTELY CRITICAL that the CommServe database is properly protected. By default every day at 10 AM a CommServe DR backup job is conducted. This operation can be completely customized and set to run multiple times a day if required.
- All activity is conducted through the CommServe server therefore, it is important that communication between the CommServe server and all CommCell resources always be available.
- Do not install the CommServe database on the system drive. Consider a SSD or high performance 15RPM dedicated disk drive.
- If the CommServe server is configured on a Virtual Machine (VM), then it typically operates at a range of 60% efficiency as compared to a comparable physical server.
- Follow the CommCell Scalability Guide in BOL for the minimum requirements for a CommServe processor and memory specifications depending on your scale variables.
MediaAgents

- If the MediaAgent is configured on a Virtual Machine (VM), then it typically operates at a range of 60% efficiency as compared to a comparable physical server.
- Follow the CommCell Scalability Guide in BOL for the minimum requirements for a MediaAgent processor and memory specifications depending on your scale variables.
- There are (3) separate disk drives typically on a MediaAgent that need to be sized and have sufficient I/O specifications to meet the SLA for data protection and recovery operations as well retention requirements. They are the disk library, the DDB drive, and the Index Cache drive.
- Format the disk library at minimum 64KB blocks per sector. The Index Cache and DDB drives should be left at the default values.

DR MediaAgents

- A DR MediaAgent is installed and preconfigured at a DR location. The most common implementation of DR MediaAgents is in the use of replica libraries or a secondary disk library using Simpana deduplication and the DASH Copy feature. By having an active and registered MediaAgent configured with a library at a DR location RTOs can be more realistically achieved. Incorporating a DR MediaAgent with a standby CommServe server provides a ‘ready to go’ DR infrastructure which can expedite recovery procedures in the case of disaster.
- Another use of the DR MediaAgent is the ability to pre-stage recovery operations at a DR location. This is most commonly implemented in virtual environments. CommVault provides documentation on the proper implementation on pre-staging the recovery of virtual machines in DR environments.

Index Cache

Sizing the Index Cache

- The index cache should be sized based on the need to browse back in time for data to be recovered. The farther back in time you need to browse, the larger the cache should be. If the index cache is undersized, index files will be pruned sooner to maintain a default 90% disk capacity. When you attempt to perform a browse or find operation and the index file is not in the cache it will automatically be restored from media. If the index file is in magnetic storage there will be a short delay in recovering the index but if it is on removable media the time to recover the index can be much longer.
- To properly size the index cache, consider the following:
  - The index file size is based on the number of objects being protected. Estimate 150 bytes per object. The more objects you are protecting the larger the index files will be.
  - Each subclient will contain its own index files within the cache.
  - The index cache should be on a dedicated disk or partition with no other data being written to the disk.
  - To reduce the probability of pulling an index file back from media use a large index cache location.
Maintaining the Index Cache

- The index cache is self-maintaining based on two configurable parameters: **Index Retention Time in Days** and **Index Cleanup Percent**. Index files will be kept in the cache for a default of 35 days or until the cache disk reaches 90% disk capacity. A smaller index cache location may result in index files being pruned before the 35 day time period expires if the cleanup percentage is reached first. Index files will be pruned from the index based on least recently accessed.

- **A Minimum Free Space** can also be configured to reserve space in the index cache location. The cleanup percent setting would be based on the allocated space to the index cache. So if you had a 100 GB partition and wanted to reserve 10 GB of space, the cleanup percent would be based on 90GB.

Libraries

**Consider the following key points for library connections:**

- For client servers where the source data is in a SAN or DAS environment and target storage can be made directly accessible to the client, install a MediaAgent on the client server to provide LAN free backups.

- When backing up to disk storage attached to a network use a dedicated backup network for library read/write operations. Do not use the same NIC that is receiving data from a client to write the data to the library.

- If using Fibre SAN storage with an iDataAgent and MediaAgent installed on the same system use separate HBAs to receive the source data and write the data to storage.

- If using iSCSI ensure the iSCSI initiator and target systems being used are enterprise class. Consider using a TCP/IP Offload Engine (TOE) NIC card to reduce CPU load on the server. Do not use the same NIC receiving the data to write the data to storage.

- If considering using a Virtual Tape Library (VTL) carefully weigh the advantages and disadvantages. Simpana disk features such as deduplication and DASH operations will not work if disk storage is configured as a VTL.

- If using a shared disk library, where the library will be shared between multiple MediaAgents and Simpana’s deduplication, it is strongly recommended to use NAS storage instead of SAN storage.
Topics

• Storage Policy Design
  • Storage Based Design Strategy
  • Business Based Design Strategy
  • Deduplication's Impact on Policy Design
  • How Many Storage Policies do I Really Need?
  • Advanced Storage Policy Features
  • Storage Policy Design Best Practices
• Advanced Job Control
  • Controlling Data Protection and Recovery Jobs
  • Firewall Configuration
  • Network Control
  • Stream Management
  • Configuring Data Encryption
• Advanced Media Management
  • Retention
  • Data Aging
  • Tape Media Lifecycle
  • Vault Tracker® Technology
STORAGE POLICY DESIGN
This strategy starts with the assumption that protection for the largest data set for a particular data type is the biggest challenge. For example; if you have hundreds of Oracle databases that drive your business then their protection should be handled first, even though the databases cross business function lines. Once you get that storage policy in place, you deal with the next largest data set. This strategy is driven more by resources than protection requirements.
As the title says, this strategy approaches your data from the business side. Build the storage policies you need for your mission critical data/business function first. These storage policies become your core set. As you review other data sets and business groups look to see which can be incorporated/covered by existing storage policies and which need new policies. This policy is driven by protection requirements rather than resources. It often results in the purchase of more storage and data transmission resources.
Deduplication’s Impact on Policy Design

- Block Factor
- Data Types
- Location
- Global Policies
- Compression

Block Factor
When using Simpana Deduplication, the dedupe block factor is a primary concern when developing storage policy strategies. The smaller the block size the more entries are made to the dedupe database. Currently the database can scale from 500-750 million records. The total volume of data being protected, which is relatively simple to estimate and the estimated number of unique blocks, which is certainly not easy to estimate, should be taken into consideration when determining block size. The following recommendations for block factor settings are based on the following:

128 KB – All object level protection, virtual machines and smaller databases.

128 KB – 512 KB – Current recommendation for database backups depending on size of all database data managed by the policy. For large databases it is recommended to engage CommVault Professional Services for proper deployment.

In this case different storage policies should be configured for the different block factors. It is not recommended to use a single policy for all data when mixed data types are involved since different data may not deduplicate well in mixed dedupe stores.

Another factor that should be considered is how long the data will be retained. Longer retention will result in larger databases. Since different data types typically will have different retention
settings, it would require separate storage policies to manage the data so separate dedupe databases will be used. It is NOT recommended to use global deduplication for long retention or large volume protection.

**Dissimilar Data Types**
Dissimilar data types that require different block settings should have separate policies. In some cases data types that do use the same block size should still have their own dedicated policies. This is the case when considering databases since different database applications typically organize and compress data using specific algorithms. Using the same dedupe policy will not necessarily result in better deduplication ratios. Also considering databases can contain large amounts of data, using a single dedupe policy may result in large dedupe databases which can lead to scalability issues. It is recommended to use different storage policies dedicated to different data types. For applications that perform their own compression, it is typically recommended to disable Simpana compression in the dedupe policy copy. This could lead to poor deduplication ratios if compressed blocks contain different data each time they are protected. Check with CommVault for current best practices when considering using Simpana compression or application compression and deduplication.

**Deduplication Database Scaling**
A single deduplication database can scale to 750 million records. Based on estimated dedupe efficiency a single deduplication database can manage up to 120 TB. Total volume would be the size of data times the number of cycles the data will be retained. In environments managing large amounts of data, it is recommended to use multiple storage policies, each with their own dedupe database to provide for the highest level of scalability.

When determining the number of policies that will be needed in large environments, data growth projections should be considered. Although a single dedupe database may be able to manage all current data, if the data growth rate is expected to change significantly, you may find yourself scrambling to redesign your policies at the last minute to accommodate changes in your environment. This will have a negative effect on deduplication efficiency especially when data is being retained for longer periods of time.

**Global Deduplication on Primary Copy**
If different retention settings are required for the primary copy but the disk location and block factor are the same, a global deduplication storage policy can be used to achieve a better deduplication ratio. Associating a global dedupe policy with a primary copy will result in a single dedupe database and dedupe store being used across multiple copies. Because of this, consider the volume of data that will be protected and ensure the deduplication database will be able to scale to meet current and future data growth.

The use of global dedupe policies are mainly for consolidating small amounts of data with different primary retention needs or for consolidating remote location data to a central location. Global deduplication policies should NOT be used across the board for everything in your datacenter. You can quickly grow out of the database maximum size which will then require a
complete redesign of your storage policy structure. Realize that policy copies attached to a
global dedupe policy cannot be unattached. New policies will have to be created and the old
policies cannot be deleted until ALL data has aged from the policies.

**Global Deduplication on Secondary Copies**
The most common implementation method for global deduplication Storage policies is
consolidating remote data to a central disk library. Secondary Copies for remote storage policies
can be associated with a global deduplication Policy with a data path at the main data center.
This will allow multiple remote locations to be consolidated into a single deduplication store at
the main data center. Create any global deduplication policies prior to creating secondary copies
for the remote location.
A general rule of thumb has been – “The more storage policies you have, the more management is required.” This is not entirely true. Following the rule of thumb you would think the ultimate solution would be to have just one storage policy. While possible, the problem with this is the potential complexity of this single storage policy and the efforts needed to handle any additional data/clients.

Storage policies need to reflect your storage organization and business needs. If that means have 5, 10, or even 100 storage policies then that’s the correct number of storage policies you need.

From the previous design strategies you always start with one storage policy. Within a storage policy you can add, delete, and modify copies by just moving data around. You can’t move/re-associate existing data between storage policies.
Understanding Alternate Paths

Alternate Data Paths
Each storage policy copy has a default data path which will be used to perform backup operations.

You can also define alternate data paths in each storage policy copy to ensure the success of backup and other operations conducted using the storage policy. In addition, alternate data paths provide the following advantages:

• Automatic switch-over to an alternate data path, when one of the components in the default data path is not available.
• Utilization of available libraries and drives in the event of failure or non-availability of these resources.
• Minimizes media utilization by routing backup operations from several subclients to the same storage policy and hence the same media; instead of creating several storage policies which in turn utilizes a different media for each subclient.
• Load balancing (round robin) between alternate data paths provides the mechanism to evenly distribute backup operations between available resources.
• Facility to define a subset of the data paths at the subclient level within the selected storage policy and its data paths.

Alternate data paths are supported for both the primary and secondary copies associated with storage policies for all libraries.
**Data Interface Pairs**

Use Data Interface Pairs whenever network traffic for control or data needs to be routed on a network connection other than the default connection used during installation. Control traffic will also use the Data Interface Pair network connection. You can also configure Data Interface Pairs between the CommServe server and other components for control traffic.

Data Interface pairs are stored in the CommServe database, and are communicated to the clients via the FwConfig.txt file. When a Data Interface Pair configuration changes, the CommServe software automatically generates the appropriate FwConfig.txt and pushes it to all affected parties. There is no requirement that a firewall needs to be configured. It was for efficiency only that the same file was used for holding both firewall and Data Interface Pair configuration information on the client.
## Advanced Storage Policy Features

- Incremental Storage Policies
- Hide Storage Policy
- Copy Precedence
- Erase Data
- Content Indexing
- Legal Hold Storage Policy
- Subclient Associations

### Incremental Storage Policy

An *Incremental Storage Policy* links two policies together. The main policy will manage all Full backup jobs. The incremental policy will manage all dependent jobs (incremental, differential or logs). This is useful when the primary target for full backups needs to be different than dependent jobs. Traditionally this has been used with database backups where the full backup would go to tape and log backups would go to disk. When performing log backups multiple times each day, replaying logs from disk during restore operations is considerably faster than replaying the logs from tape.

### Hide Storage Policy

If a storage policy managing protected data is deleted, then all of the data associated with the policy will be aged and subsequently deleted. If a storage policy is no longer going to be used to protect data, the option *Hide Storage Policy* in the General tab of the policy properties can be selected. This will hide the policy in the storage policy tree and also hide the policy in the subclient drop down box in the Storage Device tab. In order to hide a storage policy no subclients can be associated with it.

If hidden storage policies need to be visible in the storage policy tree, set the *Show hidden storage policies* parameter to 1 in the Service Configuration tab in the Media Management applet.
Copy Precedence
Copy precedence determines the order in which restore operation will be conducted. By default, the precedence order specified is based on the order in which the policy copies are created. The default order can be modified by selecting the copy and moving it down or up. This changes the default order. Precedence can also be specified when performing browse and recovery operations in the Advanced options of the browse or restore section. When using the browse or restore precedence the selected copy becomes explicit. This means that if the data is not found in the location the browse or restore operation will fail.

Erase Data
Erase data is a powerful tool that allows end users or Simpana administrators to granularly mark objects as unrecoverable within the CommCell environment. For object level archiving such as files and Email messages, if an end user deleted a stub, the corresponding object in CommVault protected storage can be marked as unrecoverable. Administrators can also browse or search for data through the CommCell Console and mark the data as unrecoverable.

It is technically not possible to erase specific data from within a job. The way Erase data works is by logically marking the data unrecoverable. If a browse or find operation is conducted the data will not appear. In order for this feature to be effective, any media managed by a storage policy with Erase Data enabled will not be able to be recovered through Media Explorer, Restore by Job, or Cataloged.

It is important to note that enabling or disabling this feature cannot be applied retroactively to media already written. If this option is enabled, then all media managed by the policy cannot be recovered other than through the CommCell Console. If it is not enabled, then all data managed by the policy can be recovered through Media Explorer, Restore by Job, or Cataloged.

If this feature is going to be used it is recommended to use dedicated storage policies for all data that may require the Erase Data option to be applied. For data that is known to not require this option, disable this feature.

Content Indexing
Content indexing allows selected object level data to be indexed for eDiscovery, Records Management, and compliance purposes. Simpana software allows data to be proactively or retroactively indexed. This means any jobs being retained in the CommCell environment can be indexed. Content director schedules can be set to index new data as it is protected, or jobs currently managed by a storage policy can be selected and indexed.

Subclients can be defined to protect specific data required for indexing. This allows for several key advantages when using CommVault content indexing:

Selected data and users can be defined in specific subclients for investigative purposes.
When using the Intelligent Archiving Agent, data can be defined based on file type in separate subclients for Information Lifecycle management policies. This allows specific data types to be removed from production storage and set in a standard lifecycle management policy where the data will be retained and destroyed based on retention policies. Indexing of the data can be conducted to associate relevant search results with specific retention policies to manage data based on content throughout its useful lifecycle.

Data can be defined in separate subclients for records management policies. This allows data to be searched based on content and ownership and move relevant information to ERM (SharePoint), export for 3rd party analysis tools, or moved into separate legal policies for data preservation.

The **Content Indexing** tab allows subclient data to be selected for indexing. This allows for a policy retaining protected data to selectively index relevant data while adhering to standard retention policies.

**Legal Hold Storage Policy**

When using the Simpana Content Indexing and Compliance Search feature, auditors can perform content searches on end user data. The search results can be incorporated into a legal hold. By designating a storage policy as a Legal Hold policy, the auditor will have the ability to associate selected items required for legal hold with designated Legal Hold policies. It is recommended to use dedicated Legal Hold policies when using this feature.

Legal Hold Storage Policies can also be used with Content Director for records management policies. This allows content searches to be scheduled and results of the searches can be automatically copied into a designated Legal Hold Policy.

**Subclients Associations**

**Subclient Properties**

In order to protect a subclient, it must be associated with a storage policy. During an iDataAgent install, a *storage policy* can be selected for the Default Subclient. When creating additional Subclients you must select a storage policy. The policy defined to manage the subclient is configured in the **Storage Device** tab – **Data Storage Policy** sub tab. Use the *storage policy* drop down box to associate the subclient with a policy.

**Storage Policy Level**

All subclients for a specific *storage policy* can be associated with another policy in the **Associated Subclients** tab of the **Storage Policy Properties**. You choose *Re-Associate All* to change all policies, or you can use the Shift or Ctrl keys select specific subclients and choose the *Re-Associate* button to associate selected subclients to a new policy.

**Policies Level Subclient Association**
If subclient associations need to be made for more than one storage policy you can use the Subclient Associations option by expanding Policies, right-click on Storage Policies and select Subclient Associations.
The windows will display all subclients for the CommCell environment. There are several methods that can be used to associate subclients to storage policies.

Select the subclient and use the drop down box under the storage policy field to select the storage policy.
You can use the Shift or Ctrl keys to select multiple subclients then use the Change all selected Storage Policies to drop down box to associate all selected subclients to a specific storage policy.
Storage Policy Design Best Practices

- Approaching Storage Policy Design
- Four Key Rules:
  - Keep it Simple
  - Meet Protection Requirements
  - Meet Media Management Requirements
  - Meet Recovery Windows
- Considerations for Subclient Definitions
- Retention Considerations
- Protection Requirements for Data Types
- Library Considerations
- Deduplication Considerations

Consider these four basic rules for approaching storage policy design:

**Rule #1: Keep it Simple**
This section will describe several different methods for protecting data. It is designed to provide in-depth explanations and solutions for the most complex environments. But before overanalyzing and over-architecting the CommVault environment, use this one simple rule: **KEEP IT SIMPLE**! If rules 2 – 4 are being satisfied then there is really no reason to change anything. A complex environment leads to more complex problems.
**Rule #2: Meet Protection Requirements**

Data protection requirements MUST be met. Though it is true the only reason we protect data is to recover it, if you are not meeting your windows then you are not protecting data. You cannot recover something that never finished backing up, so ensure protection windows are being met. In the following sections methods to improve performance will be discussed. Performance always starts with an adequately designed physical environment. Before tweaking CommVault software to improve performance, ensure that Clients, MediaAgents, and networks are scaled appropriately.

**Rule #3: Meet Media Management Requirements**

In an ideal world data would simply be preserved forever. With the dropping cost of disk storage and deduplication, most data can be retained longer. As with anything this comes at a price. The best way to approach media management is to ensure the business end understands your capabilities and limitations for preserving data. Sometimes a ‘Pie in the Sky’ vision of protecting data can be brought right down to reality through a little education and a cost association of the business requirements. Although you understand the capabilities and limitations of your storage, the non-technical people may not. Provide basic guidance and education so they better understand what you and the Simpana product suite are capable of doing. You may not have the power to make the final decisions but you do have the power to influence the decision process.

**Rule #4: Meet Recovery Windows**

Recovery windows are made up based on Service Level Agreements (SLA).

For data protection and recovery an SLA is made up of three components:

- Protection Windows
- Recovery Time Objectives (RTO)
- Recovery Point Objectives (RPO)

When designing a CommCell environment focus should always be placed on how data will be recovered. Does an entire server need to be recovered or only certain critical data on the server require recovery? What other systems are required for the data to be accessible by users? What is the business function that the data relies on? What is the associated cost with that system being down for long periods of time? The following sections will address RTO and RPO and methods for improving recovery performance.

**Requirements for Custom Content Definitions (Subclients)**

The Simpana software suite offers powerful features to provide great flexibility in managing data. One of the most powerful features is the ability to logically address content requiring protection by using subclients. Subclients allow content to be explicitly defined such as files, folders, mailboxes, document repositories, or databases. Although most environments only use the Default subclient to protect all data managed by an agent, custom subclients can provide granular management of data which can be used to improve performance, make more efficient
Consider using custom subclients for the following situations:

- When custom retention settings are required for specific data such as a folder, virtual machine or a database.
- When special storage requirements exist for specific data such as isolating financial data onto separate media from other data being managed by the agent.
- When special file handling must be performed such as using VSS or Simpana QSnap to protect open files.
- When specific files must be protected and managed independently from other data in the same location such as PDF and DOC files requiring specific retention or storage requirements.
- When scripts need to be used to place data in a specific state prior to backup such as quiescing a database before backing it up.

When Simpana software is initially deployed in most environments, only a default subclient is used. In the KISS philosophy of keeping things simple, unless there are predefined reasons for protecting specific data, this step may be skipped. Modifying, adding or deleting subclients is a simple process that can be performed at any time.

Retention Considerations

Retention Requirements for Contents

Retention requirements should be based on specific contents within a file system or application. All too often, determining retention requirements is not easy, especially when data owners do not want to commit to specific numbers.

Considerations for Retention Requirements:
Keep it simple. Unless specific content within an application or file system requires special retention requirements, don’t over design subclients.

Consider using default retention policies providing several levels of protection. Provide the options to the data owners and allow them to choose. Also stipulate that if they do not make a choice then a primary default retention will be used. Also state a deadline in which they must provide their retention requirements. It is important to note that this is a basic recommendation and you should always follow policies based on company and compliance guidelines.
Consider defining retention rules for the following:

- Disaster Recovery requirements should be based on the number of Cycles of data that should be retained. This should also include how many copies (on-site / off-site) for each cycle.
- Data Recovery requirements should be based on how far back in time (days) that data may be required for recovery.
- Data Preservation/Compliance should be based on the frequency of point-in-time copies (Monthly, Quarterly, Yearly) and how long the copies should be kept for (Days).

**Protection Requirements for specific data types**

Managing different data types such as file systems and databases typically require special design considerations for storage policies. These factors should be considered in the initial design strategy.

**Consider special protection requirements for different data types in the following situations:**

- Typically different data types such as databases and files will require different retention settings which will result in different policies being used to protect the data.
- If the primary storage target is a tape library and multiplexing will be used it is not recommended to mix database and object level backups to the same media. Using different storage policies will force different data types to use different media.
- When using Simpana deduplication it is recommended to use different policies to manage various data types. This should be done for three reasons:
  - Different block sizes may be recommended for different data types depending on the volume of data requiring protection.
  - Different data types do not always deduplicate well against each other.
  - It provides for greater storage scalability since each policy will maintain their own dedupe database.

**Library Considerations**

**Library and Data Paths**

For simplicity of managing a CommCell® environment, different libraries as well as location of the libraries may require separate storage policies. This will allow for easier policy management, security configurations, and media management.

**Consider the following when determining storage policy strategies for libraries and data paths:**

When using Simpana deduplication, for performance and scalability reasons different policies should be used for each MediaAgent data path. This will allow the deduplication database to be locally accessible by each MediaAgent providing better throughput, higher scalability, and more streams to be run concurrently.
If a shared disk (not using Simpana deduplication) or shared tape library is being used where multiple Client / MediaAgents have LAN free (Preferred) paths to storage, a single storage policy can be used. Add each path in the **Data Path Properties** tab of the **Primary Copy**. Each Client / MediaAgent will use the LAN Free path to write to the shared library. This will allow for simplified storage policy management and the consolidation of data to tape media during auxiliary copy operations.

If a shared disk (not using Simpana deduplication) or tape library is protecting LAN based client data where multiple MediaAgents can see the library, each data path can be added to the primary copy. GridStor Round Robin or failover can be implemented to provide data path availability and load balancing for data protection jobs.

**Deduplication Considerations**

When using Simpana deduplication careful planning is essential. Whether a policy will use deduplication or if a policy copy will be associated with a global dedupe policy must be determined during the initial configuration of the policy copy. Although the block size specified during the policy creation can be modified, it will seal the store which will have a negative impact on dedupe ratios and backup performance.

**Consider the following when using Simpana Deduplication:**

- Deduplication gets the best benefit from data that deduplicates well with other data and from subsequent full backups that protect the same data over time. Not all data will deduplicate efficiently. For data that will be written to non-deduplicated disk storage, use a separate storage policy. It is also recommended to use a separate disk library for deduplicated and non-deduplicated data.
- Use separate storage policies for data types that require different block settings and for data that does not deduplicate well with other data types. This provides for better performance and scalability.
- If global deduplication is going to be used for Primary or Secondary copies, create the global dedupe policy before creating the other policy copies. Associating a policy copy to a global dedupe policy must be done during the initial creation.
- In environments with ‘Big Data’ consider scaling out the environment to accommodate current data volume and future growth estimates. This may require using dedicated storage policies which will use independent dedupe databases allowing for higher volumes of data to be managed. Each database can handle up to 750 million records.
- If certain data will also be placed in SILO storage then dedicated policies should be used to separate SILO required data from non-SILO required data.
ADVANCED JOB CONTROL
Controlling Data Protection and Recovery Jobs

- Firewall Configurations
- Network Control
  - Network throttling
  - Data Interface pairs
  - Robust Network Layer
- Job Control
  - Activity Control
  - Operation Windows
  - Holidays
- Stream Management
Understanding Ports and Services

- Static Ports for Base Services can be changed
- Dynamic port usage range can be defined

Several services used by Simpana software are designed to listen for incoming network traffic on specified network ports; thus the CommServe server, MediaAgents, and Agents within the CommCell environment communicate with each other. Essential CommServe services are automatically assigned registered static port numbers during installation. MediaAgents, Agents, and other software components can utilize the same default static port numbers, or any static port numbers specified during installation.

CommVault® Services are broken down into five (5) groups:

- **Base Services** - common to all hosts
- **CommServe® Services** - CommServe Only
- **MediaAgent Services** - MediaAgent Only
- **Client/Agent Services** - Client/Agent Only
- **Search Engine Services** – Search Engine Only

Those services assigned static ports are constantly listening for commands/results from other services.

Those services assigned dynamic ports are only active when required.
Port usage can be curtailed through defining Firewall port restrictions. However, restricting port usage can negatively impact performance during concurrent operations.

CommVault Services are listed here:

**Base Services**

**Communications Service (CVD)**
Provides the ability to fetch or save metadata on the CommServe® server when data protection or data recovery operations are in progress.

**Client Event Manager (EvMgrC)**
Forwards events generated on the local machine to the CommServe server. In addition it helps the CommServe server to browse the application data on local machine.

**Server Event Manager (EvMgrS)**
Responsible for communicating with CommCell Console and receive the events from the Clients and/or Media Agents.

**CommServe Services**

**Application Manager (AppMgrSvc)**
Provides access to server and client configuration for local and remote processes. This service is essential for the CommServe server.

**Job Manager (JobMgr)**
Responsible for running and controlling jobs and also communicate with the available resources.

**Media & Library Manager (MediaManager)**
Responsible for controlling the hardware devices that are part of a CommCell® environment.

**Commands Manager (QSDK)**
Responsible for servicing command line requests and is therefore essential for command line operations.

**Monitor (QNServer)**
Present only if CommNet Server is installed. Responsible for communicating with CommCell servers (including SRM) and the CommNet Browser for CommNet Server components. Uses static port 8403.
MediaAgent Services

*Media Mount Manager (CVMountd)*
Responsible for interacting with the hardware devices that are attached to the local host and are part of the CommCell environment.

*NDMP Remote Server*
Responsible for interacting with NDMP servers for backup, restore, and snapshot management.

Client/Agent Services

*HSM Recaller (GXHSMService)*
Installed on clients with a Migration Archiver Agent. Responsible for archiving or recovering the files based on rules defined for the migration archiving operation.

*Replication Service (CVRepSvc)*
Installed on Clients with ContinuousDataReplicator. Responsible for replicating data from one client computer to another client computer.

*VSS Provider Service (VSS_SWPROV_SVC)*
Makes use of the Volume Shadow Service feature of the Windows Server 2003 operating system. This service is not managed by the Service Control Manager. The Cluster Administrator must be used to control this service.

*Cluster Plugin (GxClusPlugin)*
Provides notification regarding whether or not the cluster group goes into an active or passive state. This service is essential for system functionality.

*NAS Recaller Service (GxHSMServiceNTAP)*
Provides for recall files functionality on a NAS Share.

*Tomcat Service (GxTomcat)*
Installed on Clients with either the Web Search Server or Web Search Client. Provides web services for web browser connectivity functionality. Port numbers are assigned during installation. Default ports are 80 and 81.
Direct Connections Using port Tunnels

Direct connection with port restrictions is a setup where at least one of any two communicating computers can establish a one-to-one connection towards the other on specific ports. The connection route should not include a proxy or an intermediate port-forwarding gateway.

Port Forwarding gateways

There are cases where direct connectivity setups do not work. Imagine a situation where the CommServe server and MediaAgent are located inside a company’s internal network, and the entire network is exposed to the outside world through a single IP address. Typically this IP address belongs to a firewall/gateway that works as a NAT device for connections from the internal network to the outside.

In scenarios like this, you can establish a port-forwarding at the gateway to forward incoming connections on specific ports to certain machines on the internal network (on specific ports). You can then configure the client to open a direct connection to the port-forwarder’s IP on a specific port to reach a particular internal server. This creates a custom route from client towards the internally running server(s).
**Demilitarized Zone (DMZ) using a Simpana proxy**

Simpana proxy is a special proxy configuration where a dedicated iDataAgent is placed in a Demilitarized Zone (DMZ), and the firewall(s) is configured to allow connections (from inside and outside networks) into the DMZ. The proxy, which is the agent running in the DMZ, authenticates, encrypts, and proxies accepted tunnel connections to connect the clients operating outside to clients operating inside.

The Simpana proxy acts like a Private Branch Exchange (PBX) that sets up secure conferences between dial-in client calls. With this setup, firewalls can be configured to disallow straight connections between inside and outside networks.

The diagram on the right illustrates a DMZ setup where a client from outside communicates to the CommServe server and MediaAgent operating in an internal network through the Simpana proxy.

**HTTP proxies (Wi-Fi connections)**

You are in a public location like a coffee shop, airport, hotel, or other such remote locations where internet access is using public Wi-Fi through a HTTP proxy. If you are a roaming user who travels frequently, you might operate the software in this scenario.
Network Control

- Network Communications
- Data Interface Pairs
- Robust Network Layer
- Job Control
  - Activity Control
  - Operation Windows

Network Communication
Communication within a CommCell® environment is based on TCP/IP. It is recommended to use hostnames for communication between agents and with the CommServe server. Due to this recommendation, a properly configured DNS environment with forward and reverse lookup zones should be used. Hosts files can also be used in situations where DNS is not available or not reliable. If using hostnames is not preferred, IP addresses can be used to bypass host name resolution all together.

During agent software installation you will be prompted to choose the hostname of the server you are installing the software on. The hostname will automatically be populated in the drop down box. If there are multiple interfaces you can use the drop down box to select the preferred interface. You can also enter an IP address in place of the hostname though this can lead to communication problems when IP addresses are changed.

Data Interface Pairs

Data Interface Pairs (DIP) are used to explicitly define the physical IP network path the data will take from source to target. This is done by specifying source and destination network interfaces using host name or IP address. When multiple paths from source to target exist, multiple DIPs can be configured allowing multi-stream operations to use separate network paths for streams.
This will permit the aggregate bandwidth of multiple DIPs source-to-target physical connections to improve data movement performance.

Data Interface Pairs can be configured in several different ways:
Tab of client properties – can be used to configure source and target paths for a client.
Data Interface Pairs applet in Control Panel – can be used to configure source and target paths for clients and MediaAgents.
DataIFPairs.exe – a resource pack utility that allows bulk entry of multiple DIPs using an answer file.

**Robust Network Layer (Network Retries)**
During data protection operations, communication is maintained between the agents moving data (MediaAgent and client agent) and the CommServe server. This communication is required to keep job status updates. In situations where communication is lost between the agents and the CommServe server.

**Job Control**

**Activity Control**

**Rules for Activity Control**
If activity is **Disabled** at any parent level object, all activity in any child levels of the object will also be disabled. If activity is disabled at the CommCell level, then the entire CommCell environment activity is disabled.
If activity is **Enabled** at any parent level object, child objects can override that setting and disable activity at the child object.

**What Activity can be Controlled**

**CommCell Level**

- All activity for the entire CommCell environment can be enabled / disabled.
  - Disabling activity will disable all activity for the CommCell environment.
  - Enabling (default) allows activity to be controlled at child levels.
- Data management (data protection) can be enabled or disabled

**Operation Windows**
Operation windows allow the CommVault administrator to designate blackout windows in which designated operations will not run. These rules can be set at the global, client computer group, client, iDataAgent and subclient levels.

Different operation windows can be defined for data protection jobs, recovery jobs, copy jobs and administrative jobs. Each defined operation window can have one or more **Do not run intervals** defined.
Different operation rules can be specified for the same operation type to define specific time intervals for different days of the week.

Key Points

Job starts during an operation window blackout period
If a job starts and an operation window is currently preventing jobs from running it will be placed in a Queued state. This will apply to both indexed and non-indexed jobs. Once the operation window is lifted and jobs are able to run, the jobs will change to a running state.

Job is running and an operation window blackout period become active
If a job is currently running and an operation windows blackout period becomes active indexed and non-indexed jobs will behave in the following ways:
Indexed based jobs will finish writing their current chunk then be placed in a waiting state. When the blackout period is lifted the job will continue from the most successfully written chunk,
Non-Indexed jobs will continue writing and will ignore the operation windows blackout period.

Allow running jobs to complete past the operation window
The behavior of actively running jobs can be configured in the Job Management applet in Control Panel. The setting Allow running jobs to complete past the operation window can be selected to allow all currently running indexed based jobs to continue running even when blackout windows become active.
Data Interface Pairs

- Use with Multiple NICs
- Route control and data traffic off default network

A client computer with multiple Network Interface Cards (NIC) and networks can route control and data traffic using Data Interface Pairs.

Data Interface Pairs can be configured in the CommCell Console’s Control Panel or on the Job Configuration tab of the Client’s Properties dialog page.

Data Interface Pairs can use the NIC’s host name (ex: client.backup.net) or IP address. In situations where name resolution is slow or erratic, use of an IP address can improve performance.
Network Throttling

- Throttle by day and time
- Relative and absolute throttling
- Different rules can be set for client computer groups and clients

The network traffic for Clients and MediaAgents can be throttled based on the network bandwidth in your environment. This is useful to regulate network traffic and minimize bandwidth congestion.

By default, network throttling is disabled. You can enable the throttling options for an individual client, a client group consisting of multiple clients, and/or a MediaAgent. Once configured, the throttling options are applied to all data transfer and control message operations, such as Backup operations including Laptop Backups, Copy operations including DASH copy, Restore operations, etc.

The throttling values setup in the throttling rule regulates the rate at which the data is sent and received.

You can also setup relative bandwidth throttling to ensure performance when the client machine connects with limited bandwidth. Multiple rules can be created for same client/client group, however the lowest values set up in different rules takes precedence for each time that intersects.
**Configuring Data Encryption**

- **Inline Encryption**
- **Offline - Copy Based Encryption**
- **Hardware Encryption**
- **Media Password**
- **Best Practices**

**Inline encryption**
Enable client encryption: Client properties | encryption tab
Apply encryption: Subclient properties | Encryption tab
Data can be encrypted as it is being backed up using inline encryption. Encryption can take place on the client or on the MediaAgent. There are two steps to implement inline encryption:
Enable encryption for the client - encryption can be enabled to use specific encryption algorithms and bit length. Options to place keys on media and use a pass phrase can also be configured.
Encryption is applied at the subclient level - Choose which subclients will be encrypted. This allows you to specifically define data that will be encrypted.

**Offline Copy Based Encryption**
Secondary Copy Properties | Advanced tab
Data can be encrypted during auxiliary copy operations. This is useful when the primary location that data is being backed up to is disk and secondary locations are tapes which will be sent off-site. This method has the advantage that it will not impact primary backup performance.
Hardware Encryption
Storage Policy Copy Properties | Data path tab | Data path properties
Simpana software supports LTO standards for data encryption. For LTO generation 4 and above drives the LTO standard includes AES encryption. In this case the drive will perform all encryption and decryption. The Simpana software can manage encryption keys in the CommServe database and optionally include the keys on the media for recovery through the Media Explorer tool.

Media Password
The Media Password is a CommCell and/or storage policy level password that is written to all media. When using Media Explorer or the catalog feature and a Media Password has been set, the administrator must enter the password before media catalog operations can be conducted. It is strongly recommended a Media Password is always set.

When using LTO hardware encryption or Simpana offline copy based encryption there is an option to place the encryption keys on the media. If the keys are placed on the media, a Media Password must be set or encrypted data will be recoverable without entering any password.

Encryption Best Practices
Use custom subclients to separate data requiring encryption from data that does not require encryption. This will improve overall performance by only encrypting data that must be secured. Carefully consider the option to place the encryption keys on the media. Placing the keys on the media makes direct access using Media Explorer possible but is a little less secure. Not placing the keys on the media means that the CommServe server must be available to recover data. If keys are not placed on media ensure proper protection of the CommServe database as that will be the only location where the keys are stored.

Ensure the media password is configured. The CommCell level media password is set in the System settings in control panel. Optionally, a media password can be configured for specific storage policies.

If the encryption keys will be placed on the media for recovery using Media Explorer, ensure that any storage policies where data may need to be recovered using Media Explorer has the Enable Erase Data option deselected. If this option is enabled, Media Explorer can NOT be used to recover data.

If a Pass-phrase is going to be used for inline encryption, ensure the password is properly documented. If the password is not known when recovering data through Media Explorer, the data cannot be recovered. If the option for regular restore access With a Pass-Phrase is enabled and the pass-phrase is not known then no data can be recovered using any means.
Base Folder and Resource Pack Tools

- Process Manager (GxAdmin)
- DBMaintenance
- IOMeter.org (Base Folder)
- CommServe® Disaster Recovery GUI (Base Folder)
- Media Explorer (Available from Support)
- TapeToolGUI (Base Folder)
- Archive Prediction Tools (Base Folder)
- CVping
- CVIPinfo

Using GXAdmin

The GXAdmin.exe utility located in the <install folder>\Base directory is used by Engineers and Support personnel to monitor Simpana services and processes during troubleshooting. The GXAdmin.exe utility’s Log Params tab replaces SetLogParamsGUI.exe utility used to set Log size, retention, and verbosity (debug) parameters.

**General** – Client information

- Instance Name
- Client Host Name
- Software Version
- Installation Path
- Drive Space
- Key Folder
Available Actions:
Select **Retrieve Remote Clients** to enable view/management of other client's info/settings

**Services** - Show all Simpana Services and current status.
Available Actions:
• Start a Service
• Stop a Service
• Restart a Service

**Processes** - Monitor Simpana processes use of resources.
Available Actions
• Dump Process info
• Kill Process
• View Logs for Process

**Log Params** - Set Log Parameters for troubleshooting
  • **DBGLevel** - (0 - 100) verbosity level reported by module. Higher means more info.
  • **LogFileSize(MB)** (0 - 100) Default 5. Max file size of log before creating new log
  • **LogFileMaxVer** (0 -100) Default 2. # of past log copies to keep before overwriting.
  • **DbgWaitTime** (0-600) Seconds to wait before DbgLevel attaches to process/service (0)

**Utilities** – Display contents of process dump file.
Actions:
• Get Call Stack

**Warning** – **Utilities tab is for Development use only**

**DBMaintenance**
DBMaintenance utility can be used to perform the following maintenance tasks on the CommServe database:
• Check the database for inconsistencies
• Re-index all database tables
• Shrink the database

This utility is located at <Software Installation Path>/Base directory. From the command prompt, run dbmaintenance with appropriate parameters from the list of available parameters. Running the utility without any parameters will give the complete list of supported parameters. The CommCell services must be stopped before performing database maintenance.

**Using CommServeDisasterRecoveryGUI**
Disaster Recovery Backup data can be restored at any production-site or a hot-site any time using the **CommServe Disaster Recovery Tool**; however, the operation must be run on a CommServe machine that does not have any other platforms installed, e.g., MediaAgents,
iDataAgents. Running the restore on a CommServe-only machine ensures that conflicts caused by mismatched product versions or dynamic-link library (DLL) files are avoided. The backup data can be restored from the Export Destination (Disaster Recovery Backups on disk) or the Backup Destination (Disaster Recovery Backups on media).

Besides restoring the CommServe database, the CommServeDisasterRecoveryGUI.exe utility can perform the following:

- Restore the CommNet Server Database
- Restore the SRM Server Database
- Change the Name of the CommServe server
- Activate the License
- Perform Post-Recovery Operations

The CommServeDisasterRecoveryGUI.exe utility can be found in the <install path>\Base directory.

**TapeToolGui.exe** - TapeToolGUI is used for both troubleshooting and performance analysis of tape devices. The latest version of the TapeToolGUI.exe utility incorporates the DiskRead.exe utility also found in the CommVault Resource Pack. With this integration you can measure throughput performance from magnetic disk to tape – or tape to tape – without the CommVault software involved.

Selecting the Disk Read option, run the tool on the MediaAgent and specify a UNC path to a source folder on the Client. This will yield full end-to-end throughput performance. The tool gives you the option to use the Windows ReadFile API to give you an environmental benchmark for real achievable performance levels.
Topics

- Performance Basics
  - Establishing Benchmarks
  - Storage Performance
  - Performance Parameters
- Stream Management
  - Data Streams
  - Deduplication Stream Management
PERFORMANCE BASICS
Establishing Benchmarks

- Understand the process
- Identify the resources involved
- Minimize outside influence
- Sample, Sample, Sample
- Write it down!

Benchmarks can be divided into two kinds, component and system. Component benchmarks measure the performance of specific parts of a process, such as the network, tape or hard disk drive, while system benchmarks typically measure the performance of the entire process end-to-end.

Establishing a Benchmark focuses your performance tuning and quantifies the effects of your efforts. Building a benchmark is made up of the following 5 steps:

1. **Understand the process**
   You can’t document or improve something if you don’t know what’s going on. More importantly, you need to understand what phases a job goes through and how much each phase affects the overall outcome.

   For example: a backup job over a network to a tape library takes 2 hours to complete. You think it should take a lot less and you spend time, effort, and money to improve your network and tape drives and parallel the movement of data. The job now takes 1.8 hours to complete. You gained a 10% improvement.

   Looking at the job in more detail we find that the scan phase of the job is taking 1.5 hours and the rest is the actual data movement. Switching the scan method reduces the scan phase time to 12 minutes. The job now takes .4 hours. You gained a 78% improvement.
Knowing what phases a job goes through and how much each phase impacts the overall performance can help you focus your time, effort, and money on the real problems.

2. Identify the resources involved
Each hardware component is going to have a theoretical performance limit and a practical one. Attempting to get improvement beyond these limits without changing the resources involved is a waste of time. For example; a SDLT 320 tape drive has a vendor listed sustained throughput of 16MB/second. In practical application you should get at least 70% of that throughput or about 11MB/sec. Major efforts with fine tuning may get the performance up to 14 or 15MB/second, but you’ll most likely never see the 16MB/sec and you certainly won’t see performance above 16MB/sec.

Another example would be a Gigabit Ethernet with a theoretical throughput of 125Mb/sec. In the real world, accounting for overhead and given a dedicated link, you would expect to see about 90 Mb/sec of actual throughput. That’s about 11MB/sec and you can keep a SDLT 320 tape drive busy.

Knowing the reasonable and available performance expectations out of each resource or component involved can help you avoid wasted effort on improving that which cannot be improved.

3. Minimize outside influence
Large data movements are usually done during non-production hours for two reasons – one, they can degrade production work, and two, production work can degrade the movement of data. You want to minimize competition for resources in order to get a fair benchmark of what performance is actually achievable. In those cases where competition cannot be eliminated, you must accept the impact to performance or invest in more resources.

4. Sample, Sample, Sample
A single measurement is not a benchmark. Tape devices have burst speeds that are not sustainable over the long run. Networks have various degrees of bandwidth availability over a period of time. A single snapshot check of bandwidth will not give you a realistic expectation. Do periodic testing over the actual usage of a resource to determine it's average performance. Try to level out the peaks and valleys - or at least try to identify what causes these variations.

5. Write it down
The hardest lessons are the ones you have to learn twice. Once you’ve established your acceptable and/or expected performance levels for each resource and end-to-end, write them down and use them as the baseline for comparing future performance.
Storage Performance

- Storage Connections
- Disk Performance
- Tape

TCP/IP
TCP/IP is the most common network transmission protocol and the least efficient of the three. Factors that can degrade TCP/IP performance are:

- **Latency** - Packet retransmissions over distance take longer and negatively impact overall throughput for a transmission path.
- **Concurrency** - TCP/IP was intended to provide multiple users with a shared transmission media. For a single user, it is an extremely inefficient means to move data.
- **Line Quality** - Transmission packet sizes are negotiated between sender/receiver based on line quality. A poor line connection can degrade a single link’s performance.
- **Duplex setting** - Automatic detection of connection speed and duplex setting can result in a half-duplex connection. Full duplex is needed for best performance.
- **Switches** - Each switch in the data path is a potential performance degrader if not properly configured.

SCSI/RAID
SCSI is the most common device protocol used and provides the highest direct connection speed. Current max SCSI speed for a SCSI controller device is 640MB/sec. An individual SCSI drive’s speed is determinant by spindle speed, access time, latency, and buffer. Overall SCSI
throughput is also dependent on how many devices are on the controller and in what type of configuration. The limitation of SCSI is the distance between devices and the number of devices per controller.

RAID arrays extend the single addressable capacity and random access performance of a set of disks. The fundamental difference between reading and writing under RAID is this: when you write data in a redundant environment, you must access every place where that data is stored; when you read the data back, you only need to read the minimum amount of data necessary to retrieve the actual data—the redundant information does not need to be accessed on a read. In a nutshell—writes are slower than reads.

RAID 0 (striping) or RAID 1 (mirror) or RAID 1+0 with narrow striping are the fastest configuration when it comes to sequential write performance. Wider striping is better for concurrent use. A RAID 5 configured array regardless of the striping has the worst write performance. It’s even worse than single disks. Of course the tradeoff is redundancy should a disk fail.

Note that fine tuning a RAID controller for sequential read/write may be counterproductive to concurrent read/write. A compromise needs to be worked out if backup/archive performance is an issue.

**iSCSI/Fibre Channel**

iSCSI or Fibre Channel protocol (FCP) is essentially serial SCSI with increased distance and device support. SCSI commands and data are assembled into packets and transmitted to devices where the SCSI command is assembled and executed. Both protocols are more efficient than TCP/IP. FCP has better statistics than iSCSI for moving data, but not by much. Performance tuning is usually setting the correct Host Bust Adapter configuration (as recommended by the vendor for sequential I/O) or hardware mismatch. Best performance is achieved when hardware involved is from the same vendor. Given that configuration and hardware is optimum, then for both iSCSI and FCP, performance is inhibited only by available server CPU resources.

A key tuning setting for iSCSI/FCP on windows is:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnds\Parameters\Device\NumberOfRequests
```

NumberOfRequests is a generic Windows parameter that specifies the maximum number of outstanding requests allowed from any initiator. To maximize performance of iSCSI or FCP, the NumberOfRequests registry parameter should be increased from the default value to 256.
Disk I/O

Defragment source volume
Performing I/O to disks is a slow process because disks are physical devices that require time to move the heads to the correct position on the disk before reading or writing. This re-positioning of the head is exacerbated by having a large number of files or having fragmented files. You can significantly improve read performance of the source data by de-fragmenting the data on a regular basis.

Use 64K block size for target volume
The standard buffer size used by the CommVault software and most transmission methods is 64Kb. The standard block size used by Windows NT File System is 4Kb. UNIX and Netware Files systems use a standard of 8Kb. The low block size is for backward compatibility with smaller disks (< 2GB). When writing a 64Kb buffer to smaller disk blocks, there is overhead involved in acquiring and writing each block. If you use 64Kb block sizes there is no additional overhead. CPU loading is reduced with potential for improved I/O.

Optimize Readers/Writers
Parallel reads and writes are possible on disk devices. Adding additional readers and writers can improve throughput. At some point, there are diminishing returns from adding more reads or writes. For a single disk, the best speed is obtained by having no more than 2 readers/writers. Additional throughput may be achieved by adding additional readers/writers, but the speed of each data stream and the amount of improvement will diminish. For example: Two readers @ 24Mb/sec can move approximately 20GB/hour. Adding an additional reader may drop the speed of each stream to 20Mb/sec and move 27GB/hour. The throughput is higher, but the speed of each stream is lower.

RAID devices use multiple disks so more parallel I/O streams are possible. The CommVault software recommends a max of 5 readers/writers for a RAID 5 volume. This will give you the fastest performance per stream. Again, more streams may improve the overall throughput, but slow the individual streams. Consider what’s on the other end of the stream.

Tape
Tape I/O

Limit drives per controller
With today’s fast tape drives it is often difficult for a single controller to keep a single tape drive running at optimum speed. The more tape drives you have on a single controller, the less performance you’ll get from each tape drive. A general rule of thumb is to have no more than one tape drive per 16 bits of the controller. So a 32bit controller card can support 2 tapes drives. A 64bit controller can support 4 tape drives. Always consult with the vendor on what is the optimum controller/drive ratio.
**Limit drives per MediaAgent**
Reading or writing concurrent data streams to tape devices puts a stress on the CPU, memory, and bus capacity of the MediaAgent host. Factor in possible multiplexing of job streams and you’re keeping a MediaAgent very busy. Over utilization of the host resources can have a dramatic effect on performance. Have you ever had the experience of slow performance when your CPU utilization rate approaches 100%? For optimal performance of all data streams to tape devices you should limit the number of concurrent data streams to tape to no more than 6 per MediaAgent. If more than 6 drives are accessible to the MediaAgent, you can set this lower limit on the Master Drive Pool properties page.

**Keep buffers filled**
Tape drives are dependent on the write buffers to feed a continuous stream of data. As the write buffer low watermark is approached, the tape drive must take action to prevent gaps of no data on the tape. For static speed tape devices (e.g. DLT), the drive will stop, re-position, and wait for the write buffer to fill before continuing. This can reduce a tape device throughput performance by as much as 50%. A variable speed tape device (e.g. LTO) will slow as the write buffer gets lower and uses its speed variation to maintain the buffer level within a certain range. You still get reduced performance, but the impact is a lot less than that of a static drive.

So how do you keep the tape’s write buffer filled? Match the buffer input of data to the output of data. This can be done by providing sufficient fast individual job streams or by multiplexing slower job streams together. **Note:** that excessive input to a tape write buffer impacts the previous buffer and operation. Do not multiplex for the sake of just having more parallel data streams and then be concerned about poor performance.

CommVault’s TapeTool.exe or TapeToolGUI.exe utility located in the `<Install home>\Base directory of the MediaAgent can be used to determine the achievable read/write throughput for a tape device.
Data Path Parameters

Chunk Size
A chunk is the unit of data that the MediaAgent software uses to store data on media. For sequential access media (tape), chunk is defined as data between two file markers. The default chunk size for indexed data on Tape is 4 GB and for non-indexed data (databases) is 16 GB. For disk libraries the default chunk size for this type of media is 2 GB. NDMP Libraries use 4GB chunks.

The Chunk size set on the Data Path Properties will have an impact only when backing up the tape.

A higher chunk size will give you better data throughput for backups, but granular restores (e.g., single file restore) will be slower. On the other hand large restores, like a full machine rebuild will be a bit faster. Recommended values are: 4 GB, 8 GB, 16 GB or 32 GB.

A lower value is recommended for frequent checks of slower data protection operations, especially when data is moving across a WAN link. A chunk size can be set as low as 32KB, but we do not recommend a chunk size below 512KB.
Block Size
CommVault software uses a default block size of 64 KB for tape devices, 32 KB for Centera devices, and whatever the formatted block size used on disk. MediaAgents can write to media using different block sizes if the MediaAgent host Operating System and media device supports that block size.

With tape devices, the higher the block size, the better the performance. CommVault software can write block sizes up to 256 KB and can automatically read block sizes up to 512 KB. If the block sizes are larger than 512 KB, read operations from the media will fail and such media will be over written and re-used if the When Content Verification Failed option is enabled in the Library Properties (Media) dialog box.

With magnetic file systems, the recommended block size is 64 KB.

Ensure that the device hardware and MediaAgent host Operating System supports higher block sizes. If block sizes are not supported the data cannot be restored.

Subclient Parameters
Compression
Data compression options are provided for data secured by data protection operations. Compression reduces the quantity of data sent to storage, often doubling the effective capacity of the media (depending on the nature of the data). Hardware compression is usually available on tape devices and is the recommended method of compression. If hardware compression is not available or not enabled, then software compression can be configured to occur on the Client or on the MediaAgent. If the data is later restored/recovered, the system automatically decompresses the data on the Client and restores it to its original state. Software compression is CPU intensive. We recommend using it only for WAN-based Clients writing to disk libraries with compression enabled on the Client.

As compressed data often increases in size, if it is again subjected to compression, the system only applies one type of compression for a given data protection operation. You can redefine the compression type at any time without compromising your ability to restore/recover data.

Setting Concurrency Parameters

Magnetic Writers
The previous section on disk I/O contains more detailed discussion on configuring the number of magnetic writers. Setting the number of magnetic writers is a balance between MediaAgent capacity, drive configuration, data stream speed, and overall throughput.

Multiplexing factor
The previous section on tape I/O contains a more detail discussion on setting a multiplexing factor. However, a few more things to note:
• Multiplexing factor is effective only for the Primary copy and to a secondary copy with Inline copy enabled.
• Multiplexing factor for tape libraries has no impact on the max number of streams for the storage policy.
• Multiplexing factor for magnetic libraries has impact on the max number of streams for the storage policy. So if you enable multiplexing for magnetic libraries, adjust as appropriate the max number of streams for the storage policy

Network Agents
Network Agents are parallel processes that read/write buffers to the transmission path. If not fully used, they consume resources that might be used elsewhere. If LAN Optimized the number of Network Agents is automatically set to 1. Changing the setting has no affect.

If LAN Optimization is not checked we recommend-
• For subclients writing over a WAN, or Netware subclients set the number of Network Agents to 1.
• For all other conditions, if memory allows and all other tuning actions have been taken, then increase the number to the max possible for the shared memory available.

Pipeline buffers
CommVault’s data pipe technology in a Non-LAN optimized configuration uses by default thirty (30) - 64KB buffers in shared memory to transmit/receive data. For large databases writing to tape devices, increasing the number of buffers to 150 or 300 can improve performance. The amount of shared memory available and the impact to other production processes must be considered before increasing this value.
STREAM MANAGEMENT
Data Streams are what CommVault software uses to move data from source to destination. The source can be production data or CommVault protected data. A destination stream will always be to CommVault protected storage. Understanding the data stream concept will allow a CommCell environment to be optimally configured to meet protection and recovery windows. This concept will be discussed in great detail in the following sections.

Job Streams
Content requiring protection is defined within a subclient. Each subclient will contain one or more streams for data protection jobs. For most iDataAgents, it is possible to multi-stream subclient operations. Depending on performance requirements and how the data is organized in the production environment, multi-streaming source data can be done by adding more subclients or increasing the streams for an individual subclient.

Multiple Subclients
There are many advantages to use multiple subclients in a CommCell environment. These advantages are discussed throughout this book. This section will focus only on the performance aspects of using multiple subclients.

Running multiple subclients concurrently allows multi-stream read and data movement during protection operations. This can be used to improve data protection performance and when using multi-stream restore methods, it can also improve recovery times. Using multiple subclients to define content is useful in the following situations:
Using multiple subclients to define data on different physical drives – This method can be used to optimize read performance by isolating subclient contents to specific physical drives. By running multiple subclients concurrently each will read content from a specific drive which can improve read performance.

Using multiple subclients for iDataAgents that don’t support multi-stream operations – This method can be used for agents such as the Exchange mailbox agent to improve performance by running data protection jobs on multiple subclients concurrently.

Using multiple subclients to define different backup patterns – This method can be used when the amount of data requiring protection is too large to fit into a single operation window. Different subclients can be scheduled to run during different protection periods making use of multiple operation windows to meet protection needs.

Multi-Stream Subclients
For iDataAgents that support multi-streaming individual subclients can be set to use multiple read streams for data protection operations. Depending on the iDataAgent being used this can be done through the Data Readers setting or the Data Streams setting.

Data Readers
Data Readers determine the number of concurrent read operations that will be performed when protecting a subclient. By default, the number of readers permitted for concurrent read operations is based on the number of physical disks available. The limit is one reader per physical disk. If there is one physical disk with two logical partitions, setting the readers to 2 will have no effect. Having too many simultaneous read operations on a single disk could potentially cause the disk heads to thrash slowing down read operations and potentially decreasing the life of the disk. The Data Readers setting is configured in the General tab of the subclient and defaults to two readers.

Allow multiple readers within a drive or Mount Point
When a disk array containing several physical disks is addressed logically by the OS as a single drive letter, the Allow multiple readers within a drive or mount point can be used as an override. This will allow a backup job to take advantage of the fast read access of a RAID array. If this option is not selected the CommVault software will use only use one read operation during data protection jobs.

Data Streams
Some iDataAgents will be configured using data streams and not data readers. For example, Microsoft SQL and Oracle subclients use data streams to determine the number of job streams that will be used for data protection operations. Data Streams are configured in the Storage Device tab of the subclient. Although they will be configured differently in the subclient, they still serve the same purpose of multi-streaming data protection operations.
Device Streams
As Job Streams are received by the MediaAgent, data is put into chunk format and is written to media as Device Streams. The number of device streams that can be used will dependent on the library type, library configuration and storage policy configuration.

Storage Policy Device Streams
Device streams are configured in the properties of the storage policy. The general rule of thumb is that the number of device streams configured in a storage policy should always equal the number of drives or writers of all libraries defined in the storage policy primary copy. Having fewer number of streams may be used to throttle parallel throughput, but that doesn’t make maximum efficient use of the devices and there are other means to restrict allocation of devices. If the number of device streams is greater than the total number of resources available no benefit will be gained. The CommVault software uses a throttling mechanism to always use the lowest stream value throughout the data movement process.

Disk Library Device Streams
For disk libraries the number of device streams is based on the total number of mount path writers for all mount paths within the library. If a disk library has two mount paths with ten writers each, a total of twenty device streams can write to the library. It is important to note that since disk libraries allow multiple write operations multiplexing is not recommended. By increasing the number of mount path writers, more job streams can be written to device streams on a one-to-one ratio. If network, MediaAgent and disk resources are adequate increasing the number of writers for a mount path will have a positive effect on data protection performance.

Tape Library Device Streams
For tape libraries one sequential write operation can be performed to each drive. If there are eight drives in the library then no more than eight device streams will be used. By default each job stream will write to a device stream. To allow multiple job streams to be written to a single tape drive, multiplexing can be enabled. The multiplexing factor will determine how many job streams can be written to a single device stream. If a multiplexing factor of four is set and there are eight drives a total of thirty two job streams can be written to eight device streams. The following diagram illustrates multiple job streams being multiplexed into device streams within the MediaAgent. Multiplexing to tape libraries can improve write performance by keeping drive buffers filled allowing the drives to write faster.
Library and Storage Policy Stream Settings
Stream management using Simpana deduplication is important to achieve best data protection performance. Considering most data after the first full backup will be deduplicated, library performance becomes less critical and more streams can be written to storage. Using client side deduplication also significantly reduces network traffic. Considering both of these advantages, considerably more streams can be used during data protection jobs allowing for more concurrent operations to be conducted.
When using deduplication, the primary bottleneck in most environments will be the deduplication database. If the deduplication database is properly designed, 50 streams should be configured to maximize data protection throughput. Stream settings will be configured in two primary areas: the storage policy and the disk library.

Storage Policy Stream Settings
In the General properties tab of the storage policy, the Device Streams setting should be set to 50. If global deduplication storage policies are being used, this option should be set in the global deduplication policy. For best performance, the storage policy device stream setting should NOT be set higher than 50.
Disk Library and Mount Path Stream Settings
Library and mount path stream settings should be configured to allow up to 50 streams in a spill and fill load balanced configuration. This will be configured in two primary locations: the library properties and mount path properties.

Library Property Settings
The default stream setting for a disk library is set in the Mount Path Allocation Policy option in the Mount Paths tab and is configured by default to allow maximum streams. Setting allow maximum streams is suitable since the storage policy maximum streams will be set to 50. However, it is critical to note that when following standard building block guidelines where one storage policy writes to one MediaAgent and library, this configuration is adequate. The problem is when CommVault best practices are not followed and many storage policies write to the same MediaAgent and library. The result could be a significant degradation in performance. Because of this, a recommendation of setting the library streams to 50 could be used to avoid potential bottleneck problems from future misconfigurations.

Most disk libraries will be comprised of multiple mount paths. In order to load balance between mount paths, it is recommended to set the Mount Path Usage option in the Mount Paths tab to use Spill and Fill. By setting the number of streams to 50, storage policy streams to 50 and the mount path usage to spill and fill, maximum performance can be achieved.

Mount Path Settings
In the Allocation Policy tab of the mount path properties, the Mount Path Allocation Policy option can be used to determine how many write streams will be allowed for the mount path. This option is set to Maximum Allowed Writers by default and for most situations, should be left at the default setting. By setting the mount path to maximum allowed writers, the throttling is taken care of by the library and storage policy stream settings. In certain cases where a mount path may be under performing, allocating a specific number of writers can be used to throttle down the number of write operations to the mount path.
PLEASE GIVE US YOUR FEEDBACK!

To give us feedback on your course:
- Login to your EA account (Ea.commvault.com)
- Select the tab for Courses Completed
- Click on the icon to fill out the Course Evaluation

Post Class Survey
- In 45 days you will receive a follow-up survey, take the opportunity to let us know how you are doing!

Thank You!