Core Fundamentals Training Guide

R 10.1

www.commvault.com

The Information contained in this document is subject to change without notice. No unauthorized use, copy or distribution.
# Table of Contents

Preliminaries .................................................................................................................. 9
Education Advantage ..................................................................................................... 10
CommVault® Advantage ............................................................................................... 11
Education Services Forums ........................................................................................... 12
Customer Education Lifecycle ....................................................................................... 13
CommVault Certification ............................................................................................... 14
Classroom Resources .................................................................................................. 15
CVLab and On Demand Lab Environment ....................................................................... 16
Additional Education Resources ..................................................................................... 17
Course Building Blocks .................................................................................................. 18
Course Objectives .......................................................................................................... 19
Agenda ............................................................................................................................ 20
Common Technology Engine ......................................................................................... 21

## Module 1 – CommCell Administration ........................................................................ 23

### Topics......................................................................................................................... 24
Accessing the Administrative Functions ...................................................................... 25
CommCell Console Access ............................................................................................ 26
Web Console Access ...................................................................................................... 28
Command Line Access ................................................................................................ 29

### Navigate the CommCell Console ................................................................................ 31
Parts of the CommCell Console ..................................................................................... 32
Properties, Tasks and Views ......................................................................................... 33
Customizing the CommCell® Console ......................................................................... 34

### Configure User Administration ................................................................................ 35
User Management .......................................................................................................... 36
System (Client) Owners .................................................................................................. 38
Client Computer Groups ............................................................................................... 39
CommCell Administrative Tasks .................................................................................... 40
Module 2 – Storage Configuration and Management ........................................51

Topics.................................................................................................................. 52

Configure MediaAgents......................................................................................... 53

MediaAgent Functions ............................................................................................ 54

Indexing Structure .................................................................................................. 56

Add and Configure Disk Libraries .......................................................................... 57

Understand Disk Libraries ....................................................................................... 58

Deduplication Building Blocks Guidelines .......................................................... 60

Detect and Configure Tape Libraries ..................................................................... 62

Supported Libraries and Settings ........................................................................... 63

Tape Media Lifecycle ............................................................................................... 66

Media Handling ....................................................................................................... 68

Module 3 – Storage Policies – Concepts and Design .............................................70

Topics...................................................................................................................... 71

Understanding Storage Policies ............................................................................. 72

Purpose of Storage Policies ...................................................................................... 73

Understanding the Basis of a Policy ....................................................................... 74

Storage Policy Structure ........................................................................................ 75

Simpana Deduplication ........................................................................................... 77

Dedicated Deduplication Storage Policy ............................................................... 78

Global Deduplication Storage Policy ..................................................................... 79

Storage Policy Deduplication Settings ................................................................. 80

Understanding Retention ......................................................................................... 83

What is Retention? .................................................................................................. 84
Sample Retention Policy ................................................................. 86
Data Aging and Pruning ................................................................. 87
Storage Policy Aging Rules ......................................................... 88
Data Aging Example ....................................................................... 90
Object Based (Subclient) Retention .............................................. 91
Aging Deduplicated Data ............................................................... 93
Understanding Secondary Copy .................................................. 94
Using Secondary Copies ............................................................... 95
DASH Copy .................................................................................... 97

**Module 4 – Client Administration** .............................................. 99

Topics ........................................................................................... 100

Understand Clients ....................................................................... 101
Understanding Client Structure ................................................... 102

Data Protection Methods .............................................................. 104

Configure Subclients ................................................................... 106
Identifying Data Content .............................................................. 107
Associating Subclient Content to Storage .................................... 110

Archiving with Simpana OnePass feature ................................... 112
Archiving Rules and Stub Management ....................................... 113
Application Archiving ................................................................. 115

The Importance of Filters ............................................................ 117
The Uniqueness that is System State ............................................ 119

Using a Subclient Policy .............................................................. 121

**Module 5 – Data Protection and Recovery** ................................. 122

Topics ........................................................................................... 123

Understanding Job Management ............................................... 124
What is a Job? .............................................................................. 125
Initiating a Job ............................................................................. 126
Job Priorities ................................................................................ 127
Controlling a Job ......................................................................... 128
Job States ...................................................................................... 130
Synthetic Full .................................................................................................................. 132
Dash Full ....................................................................................................................... 133
**Restore Data** .......................................................................................................... 134
Finding Data to Restore ............................................................................................... 135
Indexes and Image Files ............................................................................................... 137
Restore Options ............................................................................................................ 138
Understanding Archive Recall ..................................................................................... 140
Understanding Full System Recovery .......................................................................... 142

**Module 6 – Monitoring a CommCell Environment** ................................................ 144
Topics .............................................................................................................................. 145
Understanding Monitoring Tools ................................................................................ 146
CommCell Console Monitoring Tools ........................................................................ 147
CommVault Monitor App .............................................................................................. 149
Configuring Alerts ....................................................................................................... 150
Alert Categories and Output Options .......................................................................... 151
Configuring Reports .................................................................................................... 154
Types of Reports .......................................................................................................... 155

**Module 7 – Working with Support** ......................................................................... 157
Topics .............................................................................................................................. 158
Before you call support ............................................................................................... 159
Troubleshooting Methodology ...................................................................................... 160
Viewing Job Details ...................................................................................................... 164
Using the Event Viewer ............................................................................................... 165
Understanding Logs ..................................................................................................... 166
Submitting a Trouble Report ....................................................................................... 168
TR Submission Process ............................................................................................... 169
Support’s Top 10 .......................................................................................................... 170
Feedback ....................................................................................................................... 172
Index .............................................................................................................................. 175
Preliminaries

- Who am I?
- Who are you?
- Why are we here?
- How will this course be conducted?

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 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 Preparation Tools
- And more!
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.
Education Services Forums

- Answers to all your training questions
- Earn CVA Points when you participate

The CommVault® Education Services Forum is designed to disseminate information throughout our technical community and enhance a student’s learning experience. If you have any questions regarding our products, service, or certification program we encourage you to post your question or search for answers on our forum. The CommVault Education Services Forum not only posts questions from our customers, it also contains a wealth of knowledge from our education specialists!

To access the forums, simply log into (or create) your account on the CommVault Education Advantage website and then click on Education Services Forums on the right-side navigation pane.
Before customers install 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 Master Certification.
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 offers Professional-level, Specialist-level and Master-level certifications. This 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.
Classroom Resources

- Log in to [ea.commvault.com](http://ea.commvault.com) for:
  - Course manual
  - Activity guide
  - Launch CVLab environment
  - Start certification exam
  - Take certification practice questions
- Fill out course survey

Course manuals and activity guides are available for download for Instructor Led Training (ILT) and Virtual Instructor Led Training (vILT) courses. It is recommended to download these documents the day prior to attending class to ensure the latest document versions are being used.

Self-paced eLearning courses can be launched directly from the EA page. If an eLearning course is part of an ILT or vILT course, it is a required prerequisite and should be viewed prior to attending class.

If an ILT or vILT class will be using the CommVault® virtual Lab environment, a button will be used to launch the lab on the first day of class (see step 5 above).

CommVault® certification exams can be launched directly from the EA page. If you are automatically registered for an exam as part of an ILT or vILT course, it will be available on the final day of class. There is no time limit on when the exams need to be taken, but it is recommended to take them as soon as you feel you are ready.
The CommVault Virtual Lab (CVLab environment) is now available to our global customers. The CVLab allows you access to a vital learning tool that provides a flexible method for gaining hands-on experience with the Simpana® software platform. You will have anywhere/anytime access to a powerful lab environment to practice installations, test configurations, review current version capabilities or review any lab exercises. The CVLab shares a common console with our Education Advantage (EA) portal and is accessible 24-hours a day up to the amount of connect time purchased.

The CVLab time can be purchased as standalone on-demand CVLab time, or to extend lab time for training courses attended. Extending CVLab time must be purchased within 48-hours after class end time in order to maintain your lab progress from the training course. Whether purchasing on-demand or extending; CVLab connect time may be purchased in four hour blocks in any quantity. Access will be available for 90 days from point of purchase and is priced at just one Training Unit per four hour block.
Additional Education Resources

- eLearning Courses
  - eLearning Samples
- Ask the Educator On-Demand
- Learning Bytes
- Catalogs and Data Sheets
- Training Units Calculator

Ask the Educator Webinar Series
Review our on-demand Ask the Educator series for concept overviews and introductions to Education Services. These sessions are part of our extensive program of courseware and information assets on the Education Advantage portal and focuses on CommVault-centric valuable technology topics. Each session is presented by highly experienced CommVault Educators as a practical technical summary of the featured Simpana® software functionality.

Learning Bytes
Learning Bytes are small snippets of information on various features and functions of Simpana® Software. These small bytes of information help users understand many of the daily tasks of the CommVault® Administrator. Each Learning Byte offers information and in many cases, a demonstration of a function within a CommCell® environment. They are small and easy to understand, making it easy to grasp the many features of Simpana Software.

Training Units Calculator
CommVault® Systems Training Units enable you to stay current with the Simpana® software suite through training programs that build your technical expertise. Training Units are an easy purchase option that enable a single transaction, ensure access to courseware, and learning adapted to the needs of your business for twelve-months from the purchase date of the training unit.
Course Objective

To facilitate the understanding of the basic components, dependencies, and functionality of Simpana® software in performing data management.
Agenda

Day 1:
- User Access & System Settings
- Storage Management

Day 2:
- Storage Policies
- Clients

Day 3:
- Job Management
- Restore & Recovery
- Monitoring
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 server. 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 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 that manages both production data and data in protected storage.

**Managing Production Data**
The first area depicts the logical management of production data which is designed in a hierarchal 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.

**Managing Protected Storage**
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 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. Each storage policy can have any number of copies of the data under its management:

- **Primary copy** – is the first rule set. The Primary copy is the initial recipient of data collected by backup or archive jobs from the associated subclients. This copy manages data being protected from the production environment.
- **Secondary copy(ies)** – are additional copies created with their own rule sets. These rule sets manage additional copies of data, which are generated from existing copies within the CommVault protected environment.
Module 1

CommCell® Administration
Topics

Accessing the Administrative Functions
- CommCell® Console Access
- Web Console Access
- Command Line Access

Navigate the CommCell Console
- Parts of the CommCell Console
- Properties, Tasks, and Views

Configure User Administration
- User Management
- System (Client) Owners
- Client Computer Groups

CommCell® Administrative Tasks
- CommServe® DR Backup Process
- CommCell® Update Process

Daily Administrative Tasks
- Running Data Protection Jobs
- Viewing Job Status
- Viewing Schedules
- Alerts and Reports
ACCESSING THE ADMINISTRATIVE FUNCTIONS
The CommCell® console Graphical User Interface (GUI) can be accessed via any of the following four methods/locations:

**Local**
The CommCell® console is, by default, installed along with the CommServe® software enabling direct GUI access from the CommServe host.

**Web-Based**
The CommCell Console can be accessed remotely via any Java capable web browser. For java web access you must have installed a compatible version of the Java™ Runtime Environment (JRE). See The CommVault Online Documentation and Support Knowledge Base for latest compatible Java version information. Web-based access also requires that the CommServe host (or alternate access host in the same domain) have IIS and the CommCell Console installed.

**Alternate IIS Host**
For better security, an alternate IIS host can be used to enable web-based CommCell Console access. As with local Web-based access, the alternate IIS host requires installation of IIS and the CommCell Console.
Remote Host
The CommCell Console can be installed as a stand-alone application on any remote host (currently Linux, Macintosh, or Windows platforms are supported). Remote access in this configuration can use port 8401 to be accessible on the CommServe host. Updates to a CommCell Console installed on a remote host must be applied manually.
The Web Server and Web Console are automatically selected for installation when you select the CommServe component AND IIS is already installed. However, there is no requirement that the Web Server or Web Console be co-located on the same host as the CommServe component. Multiple Web Server components and/or the Web console component can be installed on different and separate hosts. Having multiple Web Servers or clients might be desired for performance (many end users), security (different domains) or localizing network connectivity (bandwidth).

If an alternate host is used for the Web Server component then a SQL Instance is installed automatically on that host unless one already exists.

By default, all CommCell users can access the Web console using the same credentials to access the CommCell Console (e.g., Active Directory user credentials). The user’s ability to perform tasks via the Web Console is managed by the assignment and association of appropriate CommCell User Group capabilities.

The appearance of some Tasks/capabilities on the Web console, such as Search, are dependent upon installed software components and configured capabilities of the CommServe\Web Server.
Simpana’s Command Line Interface (CLI) is used for third party integration to coordinate CommCell activity with other events and to pass information for management action.

Command line options include:

- **Qcommands** – executable utilities that enable users to perform numerous functions from the command line.
- **XML Scripts** – created via the “Save as Script” job option as input files for a qcommand. These input files along with the associated qcommand can be edited or incorporated into other scripts, management tools, or applications. The CommVault Online Documentation includes user-defined input files in XML format, as well as options in the CommCell Console that cannot be saved as XML. Simpana CLI scripts can be initiated from any CommCell component, but they are always executed on the CommServe host. This allows the use of all job management controls via the CommCell Console.

Simpana CLI scripts can be run asynchronously (“Set and forget”) or synchronously (“Wait for final status”). Synchronous execution (default) allows the administrator to have the script take appropriate and/or further action based on the results of the operation.
- **Qscripts** (pre-defined SQL scripts) – pre-defined SQL scripts that enable you to query and in some cases directly modify the CommServe database. You can execute QScripts using the `qoperation execscript qcommand`.

- **QAPI** (Application Programming Interface) – is a software development kit designed to provide programmatic interface for users to perform various operations that can be run using command line utilities or the CommCell Console. QAPI exposes C style APIs which allows users to develop customized client applications, using either C or C++, for UNIX and Windows operating systems.
NAVIGATE THE COMMCELL® CONSOLE
The CommCell Console has a ribbon **Toolbar** that includes menus to help you quickly find the commands to complete a task. Different ribbons are displayed by selecting a group from the **Main Menu**.

On the left side is the CommCell Browser which holds an expanding navigational tree of CommCell components. Expanding component levels allows the user to drill down to specific components in order to perform task or view information. The CommCell Browser has an alternate “Agents” view which presents the user with a different navigational tree organized by Agent type.

Windows on the right side of the CommCell Console display details of what is selected in the CommCell Browser, the job controller to view and manage active jobs, and the event viewer which can be used to view and search events.

The **Table Menu** is an icon made up of stacked down arrows (chevron) that is located on the top of the scroll bar in the upper right corner of the tabbed window. The Table Menu allows you to select columns, save, print, email, find and other tasks relating to the displayed information.

The **Status bar** at the bottom of the CommCell Console shows the CommCell Name (CommServe Host name), Simpana Version, and the logged in user.

Changes to the CommCell Console can be cleared by using the View | Reset Layout task. Changes can be saved through multiple logins using the Tools | User Preference options.
Properties, Tasks, and Views

Administrative action menus in the CommCell Console are accessed using either a right-click action on the component or you can use the Main Menu | View and select the Tasks View to display a window of available actions on the right side of the CommCell Console.

Actionable items are divided up into the following:

- **Tasks** – relates to either configuration, information or operational action of the selected component – or sub-components.
- **Views** – opens additional displays containing the selected information and possibly more task options.
- **Properties** – displays information pertaining to the component and possibly options to alter the components characteristics or actions.
Customizing the CommCell® Console

- Hiding the CommCell Browser
- Moving Tabbed Windows
- Floating Windows
- Setting User Preferences

Hiding the CommCell® Browser
The CommCell® Browser can be hidden by unpinning the browser window. This can free up space in the console to view more information in the Job Controller and Event Viewer windows. Once hidden, the browser window can be temporarily displayed by hovering the mouse over the browser tab on the left side of the window. To lock the browser window back, double-click the pin button on the right side of the browser window.

Moving Tabbed Windows
Tabbed windows can be rearranged in any order by clicking, dragging, and dropping the tab. This can be beneficial when many windows are open at the same time.

Floating Windows
Windows can be floated where they will not be bound to the CommCell® Console. This can be beneficial when multiple monitors are being used. When a window is floated it can be dragged outside of the console windows and placed on the other monitor for a multi-screen view of the CommCell Console.

User Preferences
Various settings in the CommCell Console can be customized in the user preferences applet in the control panel.
CONFIGURE USER ADMINISTRATION
Each CommCell® User should have their own login with full or a restricted set of capabilities to view entities and/or perform tasks.

- **CommCell Users** – can be defined internally within the CommCell software or enabled externally through Microsoft’s® Active Directory or IBM’s Domino Directory Server. The ability of a user to view entities and perform tasks within a CommCell group collective is managed exclusively via membership in a CommCell User Group.

- **CommCell User Group(s)** – are associated with CommCell entities (e.g., Clients, Libraries, Storage Policies) enabling the member users to perform authorized tasks on those entities only.

- A CommCell user can be a member of any number of CommCell User Groups. The user’s ability to perform tasks on a CommCell entity is determined by the combined capabilities of the CommCell User Groups that are associated with that entity. A list of tasks and required capabilities can be found in the CommVault Online Documentation.

- **External Users/Groups** – from Microsoft’s® Active Directory or IBM’s Domino Directory Service can be associated with CommCell User Groups. Associated external group members can login to the CommCell Console using their external credentials. Single Sign on can be enabled to allow external users already logged into the domain to access the CommCell Console without re-entering their password.
**Important:** Associated external groups and users can be used as recipients for CommCell Console alerts and reports. In order to receive an alert or report, the external user must have logged into the CommCell Console at least once in order for the system to obtain the SMTP mail address of the user.
System (Client) Owners

- Access via the CommCell® Console's Control Panel
- Used to manage capabilities for Laptop Client Administrators
- Enables Web Console access to backup and restore operations

The System (Client) Owner CommCell® User Group is handled separately from other CommCell User Groups. The System Owner group dialog box with CommCell-wide implication is accessible via the Control Panel. The Client Owner group dialog box is accessible in the Client Properties dialog box.

A Name Server/Active Directory domain must be enabled/configured to authorize external users as owners. The intended members are Laptop/Desktop client administrators looking to access their mail and/or backup data via the Simpana® Web Console.

By default, the user account used to install and/or register the Laptop Backup package is automatically added as the owner. The Simpana® software can be configured to automatically add as owners any Active Directory group members or users with local profiles on the client. CommCell Administrators or CommCell Users with Client Management capability can manually add owners to a client.
Client Computer Groups

Management Scalability Tool for:
- Activity
- Security
- Operation Window
- Reporting
- Updates
- Job History
- Firewall

A Client Computer Group (CCG) is a scalability tool providing both a flexible span of control and a consistent entity for management and reporting.

Clients can be a member of any number of CCGs and inherit the properties or activities associated with each group. For example, a CCG could exist for reporting purposes. A client that joins a CCG is automatically included in the report. Membership in the CCG can be altered at any time without having to modify the report parameters.

As another example, a CCG could exist for user management purposes. A CommCell User Group with Browse and Restore capability could be associated with the CCG. New clients, Laptop Clients, and MediaAgents could then be added to this group as appropriate without having to directly modify the CommCell User Group associations. Additionally, clients can automatically be added to a CCG through a set of defined criteria.

In Enterprise environments with a larger number of clients, navigating to each client can be better facilitated through use of Client Computer Groups.
Disaster Recovery Backup protects the metadata (database, registry, and firewall configuration files) required to rebuild the CommServe host and recover data from protected storage. DR data is first exported to a specified location for quick access and then backed up to removable storage media for off-site retention.

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 following folder:

\<installpath>\CommVault\Simpana\CommServeDR

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 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 the Control Panel.
**DR Backup Phases**
The DR backup process includes several steps: Pre Scan Process, Export, Backup and Post process.

**Export**
The Export process will copy the contents of the \CommServDR folder to the user defined export location. A drive letter or UNC path can be defined. The export location should NOT be on the local CommServe server. If a standby CommServe server is available define the export location to a share on the standby server.

By default five metadata backups will be retained in the export location.

**Backup**
The backup process is used to back up the DR metadata to protected storage. This is accomplished by associating the backup phase with a storage policy. A default DR storage policy is automatically created when the first library is configured in the CommCell environment. Although the backup phase can be associated with a regular storage policy, it is recommended to use a dedicated DR storage policy to protect the DR metadata.

**DR Storage Policy**
When the first library in a CommCell environment is configured a CommServe Disaster Recovery storage policy will automatically be created. The Backup phase of the DR backup process will automatically be associated with this storage policy. If the first library configured is a disk library and a tape library is subsequently added, a storage policy secondary copy will be created and associated with the tape library.

**There are several critical points regarding the DR storage policy and backup phase configurations:**
Although the backup phase can be associated with any storage policy in the CommCell environment, it is recommended to use a dedicated DR storage policy. Using a dedicated policy will isolate DR metadata on its own set of media making it potentially easier to locate in a disaster situation.

The most common reason the backup phase is associated with regular data protection storage policies is to reduce the number of tapes being sent off-site. If the backup phase is associated with a regular storage policy consider the following key points:

- Make sure the Erase Data feature is disabled in the storage policy. If this feature is not disabled, the DR metadata will not be recoverable using the Media Explorer utility.
- When secondary copies are created, an option for the DR metadata becomes available in the **Associations** tab of the copy. Make sure every secondary copy contains the DR metadata.
- Make sure you are properly running and storing media reports. This is important when sending large numbers of tapes off-site. If you don’t know which tape the metadata is on you will have to catalog every tape until you locate the correct media which is storing the DR metadata.
Backup Frequency
By default the DR backup will run once a day at 10:00 AM. The time the backup runs can be modified and the DR backup can be scheduled to run multiple times a day or saved as a script to be executed on demand. Consider the following key points regarding the scheduling time and frequency of DR backups:

- If tapes are being sent off-site daily prior to 10:00 AM then the default DR backup time is not adequate. Alter the default schedule so the backup can complete and DR tapes be exported from the library prior to media being sent off-site.
- The DR Metadata is essential to recover protected data. If backups are conducted at night and auxiliary copies are run during the day, consider setting up a second schedule after auxiliary copies complete.
- For mission critical jobs consider saving a DR backup job as a script. The script can then be executed by inserting the path to the script in the Post Backup Process field in the subclient properties.
CommCell® Update Process

- Configuring Software and Update Cache Locations
  - CommServe® Cache
  - Secondary Cache
- Downloading Software and Updates
- Automatic Updates
- Manual Updates
- Simpana® Update Release Cycle

Updates and Service Packs are used to address specific problems, add new features and improve the overall performance of the product.

**Resource**

Service Packs and the latest software updates and hotfixes can be viewed or downloaded from CommVault's Maintenance Advantage website. Additionally, service packs and critical updates are available for automatic download to the CommServe Update Cache Directory. If unable to download files directly to the cache, manually copy to cache by using the CopyToCache utility found in the install path’s base directory, or by accessing the Add/Remove Software icon in the Tools tab of the Toolbar. The Add/Remove Software icon provides options to copy or update software packages from a specific location.

**Status**

Service Pack and installed updates can be viewed in the Client's Property dialog box or in the CommCell Configuration Report. You can also use the CommCell Configuration Report to poll all clients for latest update information. This would be appropriate if any installations, updates, or upgrades were conducted when communication to the CommServe host was not available.
Space Savings

When an update is installed, the old version of the binary is replaced with a new one. When there are many updates or Service Packs installed on the computer, these old binary versions may take up a large amount of space on the computer. Hence, to clear up space on the computer, you can expire the updates using the dUPDATEEXPIRY registry value (Windows platform only). The data for the registry value is the number of days to keep the old binary files. When the update is expired, it becomes permanent on the computer and the old binary versions are deleted.

Expiration is part of the update process. If the defined number of days has passed and there are no update installations or removals taking place, the expired update will not get removed until an actual install/removal happens.
DAILY ADMINISTRATIVE TASKS
Most data protection jobs using traditional backups or snapshots are scheduled. The frequency of scheduled jobs should be based on the Recovery Point Objective (RPO) times. For a 24 hour RPO jobs are scheduled to run daily. If a 4 hour RPO is required then jobs should be scheduled to run every 4 hours.

Different types of jobs can be scheduled to run on different days. The traditional weekly full and daily incremental is the most common schedule but not always the best. Consider scheduling jobs based on Recovery Time Objective (RTO), RPO and how frequently data should be sent off-site.

For example: If data is being backed up to disk and DASH copied to disk at a DR location, jobs could be scheduled to run more frequently throughout the day to shrink RPOs and get data off-site faster. If the disk data needs to be consolidated to tape on a monthly basis a schedule of monthly full and daily incremental with the monthly full being aux copied to tape may be adequate. An example when backing up directly to tape could be to perform nightly full backups or weekly full and nightly differential. Both of these methods could shrink RTO times.
Viewing Job Status

The Job Controller is used to monitor active jobs within the CommCell environment. Jobs will remain in the Job Controller for five minutes after the job completes, fails or is killed. The default time jobs will be maintained after finished can be modified in User Preferences applet in Control Panel.

Key features on the Job Controller:

- Provides summary and detailed information for all active jobs and jobs that have completed within a five minute period. Details for the job can be viewed by double-clicking on the job or right-clicking and selecting Detail.
- Job controller can be filtered to view specific, clients, client computer groups, and agents. Filter options can be configured, saved and selected.
- Jobs can be suspended, resumed or killed by individually selecting jobs, using CTRL or Shift keys to select multiple jobs or by right-clicking and selecting Multi-Job Control. Multi-Job Control can be used to control jobs from a client, MediaAgent or all active jobs.
- Events and log entries can be viewed by right-clicking the active job.
Client schedules can be viewed and edited from the client, agent, data set and subclient levels. When a specific level in the client tree is selected, all schedules at the selected level and all child object schedules will be displayed.

**Client schedule key points:**

- Schedules can be viewed at the CommServe®, client, agent, data set and subclient levels.
- If a schedule is associated with a schedule policy the policy name will be listed in the first column.
- Schedules can be edited, deleted, disabled or executed by right-clicking on the job schedule.
- For clients with a large amount of scheduled jobs consider using the Job Schedule report for a more consolidated view.
- Though client schedules can be viewed at the CommCell level using the Schedule icon, viewing schedules in the client tree provides a simplified view easing administration, especially in large environments.
Alerts and Reports

Alerts can be configured to provide real-time feedback about conditions in the CommCell® environment as they occur. Alerts can be emailed, saved, run a script based on the alert, and viewed in the CommCell Console using the Console Alerts view. The Alert wizard is used to configure the alert type, entities that will be monitored, notification criteria and notification method. The wizard can be accessed from the Alert icon in the Home tab of the Toolbar, select the Configure section of Control Panel or from the Advanced button when configuring data protection or recovery operations.

CommCell reports can be customized to report on all CommCell activities. Report types including job summary, job schedule, CommCell configuration and storage usage can be configured. Reports can be scheduled, saved as scripts or saved as templates. Report output formats include HTML, CSV, PDF and XML.
Module 2

Storage Configuration and Management
Topics

Configure MediaAgents
- MediaAgent Functions
- Indexing Structure

Add and Configure Disk Libraries
- Understanding Disk Libraries
- Deduplication Building Block Guidelines

Detect and Configure Tape Libraries
- Supported Libraries and Settings
- Tape Media Lifecycle
- Media Handling
CONFIGURE MEDIA AGENTS
MediaAgent Functions

- Data Mover
- Device Control
- Index Cache
- Deduplication Database

MediaAgents are the transition point for data moving on the **data pipe** to/from the Client Agent and the **data path** to/from the protected media. All data moving to/from protected storage must move through a MediaAgent. As such, resource provisioning for MediaAgent hosts (e.g., CPU, Memory, and bandwidth) must be significant and adequate for both the volume and the concurrency of data movement you expect it to handle.

A MediaAgent provides device control over media changers and removable media devices - and writers to disk devices. This control defines the path upon which data moves to/from protected storage. In addition to normal device integrity checks, the MediaAgent can validate the integrity of data stored on the media during a recovery operation and validate the integrity of the data on the network during a data protection operation.

In the case where the MediaAgent component is co-located on the same host as the Client Agent, the exchange of data is contained within the host. This is called a SAN MediaAgent configuration and has its advantages of keeping data off potentially slower TCP/IP networks by using local higher performance transmission devices (e.g., Fibre Channel, SCSI, etc.). On the other hand a MediaAgent component located on a host by itself can provide dedicated resources and facilitate exchange of data over longer distances using TCP/IP (e.g., LAN, WAN, etc.).
Device Control
With Tape libraries, MediaAgents are the primary control agent for media changers and tape devices. The Media and Library Manager service on the CommServe host determines the required tape media and its location. It then determines which MediaAgent has control of the media changer to load/unload the tape. Once loaded, the MediaAgent having the specified data path access to the tape device will mount/unmount the tape for reading/writing. In this manner a tape library can be shared with multiple MediaAgents. For IP-based libraries where the media changer is managed by 3rd party software, a MediaAgent will be the interface point of communication.

For disk libraries, data paths are either local or network. Shared disk devices can have only one local path (exception would be Global File Systems – see the CommVault Online Documentation for usage) and any number of network paths. Concurrent writes to a disk library is managed by the Common Internet File System (CIFS) protocol.

Deduplication Database (DDB)
Deduplication is also managed by a MediaAgent through the use of a Deduplication Database (DDB). Data block signatures are compared with original blocks indexed and written to storage media and duplicate blocks indexed using the location of the original block. The DDB is not used when restoring data. If multiple MediaAgents are involved, one MediaAgent can be dedicated to managing the DDB.
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 and automatically copied to media containing the job.

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.
ADD AND CONFIGURE DISK LIBRARIES
As cost of disk continues to go down, the speed and concurrency advantages of disk libraries make them the primary protected storage media of choice:

- **Dedicated** – disk libraries are created by first “adding” a disk library entity to the MediaAgent using either the right-click All Tasks menu or the Control Panel’s Library and Drive Configuration Tool. One or more “mount paths” can be created/added to the library. Mount Paths are configured as **Shared Disk Devices**. The Shared Disk Device in a dedicated disk library has only one Primary Sharing Folder.

- **Shared** – disk libraries are libraries with more than one Primary Sharing Folder configured on a Shared Disk Device. This enables other MediaAgents access to the same shared volume resource. A “shared disk library” can then be created and the Shared Disk Devices added to the library. One path to the shared folder can be direct while the others are Common Internet File System (CIFS) shared directory paths. CIFS protocol is used to manage multiple MediaAgent access to the same directory. For UNIX hosted MediaAgents, Network File Share (NFS) protocol can be used. NFS shared disks appear to the MediaAgent as local drives.

- **Replicated** – disk libraries are configured similar to a shared disk library with the exception that the Shared Disk Device has a replicated data path defined to a volume accessible via another MediaAgent. Replicated folders are read-only and replication can be configured for use with third party replication hardware.
Disk Library Settings

- **Usage Pattern** – determines how both writers and volumes are used when more than one data stream is in action. The default usage pattern is “Fill & Spill” which will use all writers and the available capacity of the first mount path before another mount path is used. The alternative is “Spill & Fill” which distributes each job stream to different mount paths which can improve performance if mount paths use different I/O devices.

- **Usable Capacity** – is managed through settings for Reserved Capacity and Managed Threshold. Reserve capacity can be set on each mount path to allow maintenance (defragmentation) or use by other applications. Managed Thresholds are set at the library level and enabled through associated Storage Policy copies. Managed Thresholds allow the administrator to make maximum use of available capacity extending retention and thus availability of data in the disk library.

- **Allocation management** – is available through library and mount path settings for the max number of concurrent writers. Maximum number of allowed writers should be set to prevent over-saturation of MediaAgent or disk resources. Pushing too many concurrent streams with inadequate resources can be detrimental to overall throughput.

Another allocation management tool is the fragmentation setting for reserving concurrent blocks for writing. With concurrent writes to the same disk, fragmentation is a concern that can impact both restores and auxiliary copy operations.
Simpana® software offers a variety of deduplication features that drastically changes the way data protection is conducted. Client side deduplication can greatly reduce network usage, DASH Full can significantly reduce the time of Synthetic Full backups, and DASH Copy will greatly reduce the time it takes to copy backups to off-site disk storage. Additionally, SILO storage can copy deduplicated data to tape still in its deduplicated state.

When using Simpana deduplication, 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.

**Physical Layer**
For the physical layer, each building block will consist of one or more MediaAgents, one disk library and one Deduplication Database (DDB).

**Logical Layer**
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 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. For the most up-to-date requirements for MediaAgents and the DDB go to:

DETECT AND CONFIGURE TAPE LIBRARIES
Libraries
Tape libraries provide an economical means to collect and move protected data off-site.

The basic removable media type libraries are as follows:

- **Standalone tape drives** – classified and treated as libraries. The difference being that a standalone tape drive has no robotic media changer and no internal storage slots. Multiple standalone drives controlled by the same MediaAgent can be pooled together in order to support multi-stream jobs or cascade of a single stream job without having to respond to media handling requests. Media used by a Standalone library can be pre-stamped or new, and will be prompted for, by backup or restore jobs as necessary. Media Handling prompts for user action appear on the MediaAgent, CommCell Console, or can be sent as an alert if configured.

- **Robotic tape libraries** – The most common libraries used today. They consist of a media changer and internal storage slots to facilitate automatic loading and unloading of media in library drives. Barcode-ed libraries have a barcode reader and maintain an internal map/inventory of media in the library. A “blind” library has no barcode reader and is supported by the CommVault® software maintaining the map/inventory externally in the CommServe® metadata.
A common, but not required, characteristic of a robotic library is multiple drives. Drives are usually of the same type (and firmware!). A multiple drive library can be used to support either a multi-stream job, or multiple concurrent jobs. A group of drives accessible in this manner from the same MediaAgent is called a Drive Pool. This gives the software flexibility in assigning idle drives from the pool rather than requesting and waiting for a specific drive.

- **Shared Library** – A static configuration where the drives and media changer are connected to only one of several MediaAgent hosts. For example: In a library with four tape drives, one MediaAgent may have control of the media changer and two drives within the library while another MediaAgent may have control over the other two tape drives. A drive connected to one MediaAgent host is not accessible from the other MediaAgent hosts. Should the MediaAgent component having media changer control fail, no further loading/unloading of media can occur until that MediaAgent is active again. Shared libraries in today’s world of Storage Area Networks (SAN) are not common.

- **Dynamic Drive Libraries** – The most common configuration in larger environments and maximize the utility of tape libraries. In a Dynamic Library the library drives and media changer are on a SAN and can be accessed by multiple MediaAgent hosts. Drives not being used by one MediaAgent can be assigned to and used by another MediaAgent. If the MediaAgent with control of the media changer fails the control can be automatically passed to another MediaAgent. The primary advantage of a Dynamic Drive library is the use of multiple MediaAgents for processing reads/writes. Dynamic Drive capability is referred to as GridStor® Technology. GridStor technology is an option that enables load balancing and failover of data protection jobs.

**Settings**

While there are other library management settings available (and should be reviewed by the administrator), the three most important settings are:

- **Overwrite media** – prevents – or allows – the re-use of media that has been used by other applications. By default, overwrite of such media is not allowed. This is to prevent both inadvertent overwrite of important data and use of media with questionable history. Media that cannot be overwritten is logically assigned to the Foreign Media group.

- **Start new media** – determines what action is taken if media required for writing is not available within the library. Normally active media is kept in the library; however under some circumstances (exported, stuck tape) it may not be loadable. Default action is to use new media. While this allows jobs to continue without manual intervention, it may result in some tapes not being used to full capacity. (See next option!)

- **Appendable media** – allows the continued writing to previously active media that still have capacity remaining. If for some reason media was not fully used, default action is to make the unused capacity available next time new media is requested for writing.
Appendable media can only be written to by the same storage policy copy stream and only if the last previous write occurred within the specified time. These restrictions are there to ensure similarly retained data is written to the media.

**Maintenance**

Maintenance is essential in a tape library as dirty drive heads are common and can make reading/writing data difficult. Newer libraries have sensors to automatically initiate cleaning when required. Otherwise, cleaning can be scheduled or conducted based on vendor recommended thresholds for usage and errors. Selecting the correct cleaning option for your environment is important.
Removable Media moves primarily in a cycle between three logical states – **Spare** -> **Active** -> **Full**, then back to spare. New media imported into a library is considered to be **Undiscovered** until the library inventory has been updated to the CommServe database. **Appendable** media is media that is assigned to a storage policy copy; no longer active; but not yet full. There are various reasons why media might not be filled with data ranging from a user initiated command to start new media to the media not being available for the next write action. Availability of Appendable media is controlled by a library setting, configurable to an allowed time span, and restricted to the same storage policy copy stream.

Media can also be marked **Bad** by the system or user, in which case no more writes will be attempted on the tape, but readable data on the tape is still restorable. Like Bad Media, **Retired** media is no longer used for writes, but may contain aged data which is restorable. Both Retired and Bad media should ultimately be deleted from the library/CommCell environment.
Removable media states are represented by icons as shown in the graphic above. Media should move in a life cycle from an undiscovered state to a Retired state. The following characteristics help determine a media’s state:

- **Write** – Media must be in an Assigned Media Pool with Active or Appendable status before it can be written to. You cannot write to media in Spare, Retired, Overwrite Protect, and Foreign Media Pools, or an Assigned Media Pool with a Full or Bad status.

- **Read** – Media in any logical state can be read if it contains valid data. Valid data is defined as data obtained by a data protection job that has been logged into the CommServe metadata. As data is written and tracked in large contiguous files called “chunks,” this means data from any recorded chunk can be read – regardless of whether the associated job succeeded, failed, or was killed.

  **Note:** Only successful job data is copied during an auxiliary copy operation. As such, secondary copies do not contain chunks from failed or killed jobs. If numerous failed or killed jobs exist, an Auxiliary copy job can be sometimes used to consolidate data on fewer media. Data on the source copy can then be deleted and the associated media freed up for re-use.

- **Ownership** – Assigned media is “owned” by a Storage Policy copy stream. Once assigned, only that Storage Policy copy stream is able to write to that media. This ensures consistent retention and handling of data. Ownership is relinquished when the media is reclassified as spare media. However, data on aged media in the spare media pool can still be used for restore until the media has been re-assigned and written to.

- **Capacity** – Capacity is measured in two forms – Used and Available. Used capacity is reported on the properties dialog for each media and is also available in various reports. It’s important to note that with hardware compression enabled for tape drives, the size of the written data reported is an estimate. Depending upon actual compression, the available remaining capacity could be more or less than indicated. The CommVault software does not use this estimate in determining if the tape is full or not. We will always write to the End of Tape marker unless directed otherwise by system or user interaction.

  Barcodes/labels within the CommCell environment must be unique. If you are manually entering a label the system will automatically append characters to make the label unique. If a tape is introduced into the system with the same barcode as another existing tape then the second tape will be flagged as a **Duplicate Barcode** and appropriate warnings made to the administrator.
Media Handling

- Need for Unique Identity
- Media Handling Prompts
- Auto or Manual Discovery
- Export Media/Mark Media Exported
- Vault Tracker® Feature

While removable media libraries have their advantages, the task of moving media in and out is not one of them. More properly known as Import and Export tasks, the CommVault software provides numerous tools for making media handling easier for the administrator.

To facilitate locating the required data or destination media, the software must be able to uniquely identify all media storage. In a disk library, this unique identity is accomplished through Volume Folder names. With removable media, it’s accomplished through unique labels or Barcodes. This requirement for unique identity is for all media under the CommServe host control, not just within a single library.

Media handling prompts appear on the controlling MediaAgent’s host screen and optionally all CommCell Consoles (option enabled in Library properties). Event messages also appear on the CommCell Console. However, most administrators with frequent media handling requirements will enable notification via the CommCell Console’s alert feature.

Discovery is a process by which tapes imported into a library are identified and tracked by the CommServe database. The media information is permanently retained; media does not have to be rediscovered if it is exported from the library and re-imported. Auto-Discovery assumes any tape imported into the library belongs to the CommCell media pool. Manual discovery can be used to selectively add media to the CommServe database.
Export Media and Mark Media Exported are Library level tasks used primarily for moving media between libraries or CommCell control, or disaster recovery. Export Media gives the option to use the Vault Tracker® agent or manually select tapes for export. The Mark Media Exported task will put all library associated media into a logically exported status. In a disaster recovery scenario it is easier to load/use the media in different libraries if they are all in an exported state.

The Vault Tracker agent provides a policy based capability to export media from a library and track it at an export location. Vault Tracker Enterprise (licensed) provides additional job-based capability plus tracking media to/from multiple locations. Other advanced features provided by Vault Tracker Enterprise include use of containers, media repositories, transit locations, Iron Mountain reports, and alerts.
Topics

Understanding Storage Policies
- Purpose of Storage Policies
- Understanding the Basis of a Policy
- Storage Policy Structure

Simpana® Deduplication
- Dedicated Deduplication Storage Policy
- Global Deduplication Storage Policy
- Storage Policy Deduplication Settings

Understanding Retention
- What is Retention?
- Sample Retention Policy
- Data Aging and Pruning
- Storage Policy Aging Rules
- Object based (Subclient) Retention
- Aging Deduplicated Data

Understanding Auxiliary Copy
- Using Secondary Copies
- DASH Copy
UNDERSTANDING STORAGE POLICIES
A Storage policy is a single addressable entity that encapsulates the physical data paths and storage media along with the logical management and retention of one or more copies of data requiring protected storage. Production data can be easily directed to appropriate protected storage management by simply associating it with a storage policy.

The basis of a storage policy comes from the company’s retention policy. The retention policy should at a minimum define what data is being retained, for what purpose, and for how long.
A retention policy can translate easily into storage policies, as shown in this example. Policies available in Simpana® software provide an administrator with the necessary tools to easily and consistently apply various business rules for managing data. The basis for any policy design must take into account data specific to corporate needs, Government Regulations, Legal Requirements, and Resource Availability. **Policies cannot meet your business needs without this input.**

In this module we focus on Storage Policies, but there are numerous other policies available for the administrator to configure and use. There are for example - Schedule Policies that manage the timing of data movement, Subclient Policies that manage data content from multiple hosts, VaultTracker® Policies that manage the movement of exported media, and Replication Policies that manage...data replication.

The primary advantages of policies are application, flexibility, and scalability. **Application** is the ease in which a policy can be associated with an object or task. **Flexibility** means you can dynamically change how your data is managed by simply modifying the policy. Modifying the governing policy affects all managed data in the same way. **Scalability** allows the policy to grow with your data management requirements. Petabytes of data become as easy to manage as Gigabytes.
Storage Policy Structure

Types of Storage Policies
- Global Deduplication
- Standard
- Disaster Recovery

Types of Storage Policy Copies
- Primary Backup
- Primary Snap
- Synchronous
- Selective

There are three basic types of storage policies:

- **Global Deduplication** - enables deduplication across multiple storage policies using a common set of disk libraries.
- **Standard** - is the management of any data type.
- **Disaster Recovery** - is specifically for management of the CommServe® metadata and other critical data needed to re-constitute the configuration and tracking of data for the CommCell® components under CommServe management.

Each storage policy can have any number of copies of the data under its management. However, only one copy is required and it is identified as the **Primary copy**.

- **Primary Copy** - is the initial recipient of data collected by backup or archive jobs from the associated subclients.

Any number of non-primary copies can exist in a storage policy. These are called secondary copies and are classified as either Synchronous or Selective.

- **Synchronous Copy** - contains all data protection jobs for the associated subclients. This will include full, incremental, differential and log backups.
- **Selective Copy** - provides options to automatically allow only updates of full backup jobs, or for the manual selection of any job the administrator wants the Selective copy to manage.
It’s important to note that auxiliary copy updates to any secondary copy can come from any synchronous copy containing the required data. Selective copies can also use another selective copy as its data source.

For hardware snapshots of data, the hardware generated copy is identified as the **Snap Copy** and the copy made to protected storage is called the **Snap Primary Copy**. In this scenario, both the Snap Copy and the Snap Primary copy are retained by the Basic retention setting of the Snap Primary Copy. Extended retention settings can be used for the Snap Primary Copy only.
SIMPANA® DEDUPLICATION
A dedicated deduplication storage policy copy will consist of one library, one Deduplication Database (DDB), and one or more MediaAgents. For scalability purposes, using a dedicated deduplication policy copy allows for the efficient movement of very large amounts of data. Dedicated policy copies are also recommended to separate data types that do not deduplicate well against each other such as database and file system data. In this example two dedicated storage policies are used – one for file system data and one for database data.
A Global Deduplication Storage Policy works by linking storage policy copies to a single Deduplication Database (DDB) and store. This allows data to be managed independently by a specific data storage policy while maintaining a more efficient deduplication ratio by centrally managing deduplicated data through the global deduplication policy. Each policy can manage specific content and independently manage retention and additional copies. This provides for efficient deduplication ratios while providing scalability and flexibility for different data protection requirements.

Another advantage of using global deduplication policies instead of dedicated policies is that it provides more flexibility to define various retention requirements. In the example above there is a 30 day and 90 day retention requirement. By linking these two policies to a global deduplication policy if another retention setting is later required, it could also be linked to the global deduplication policy.
Storage Policy Deduplication Settings

- Block size
- Policy copy store settings
- Compression
- Store availability
- Enabling client side deduplication
- DASH full / DASH copy

Block Size
Block size is configured in the storage policy Properties under the Advanced tab. When using a Global Deduplication Storage Policy, all other storage policy copies that are associated with the global policy must use the same block size. If you change the block size for the storage policy the Deduplication Database (DDB) will be closed, the store will be sealed and a new database and store will be created.

The block size recommendations depend on the data type that is being protected and the size of the data. The current recommended setting for file and virtual machine data is 128 KB block size. This provides the best balance for deduplication ratio, performance and scalability. Though the block size can be set as low as 32 KB, deduplication efficiency only improves marginally and is therefore not recommended.

For databases the recommended block size is from 128 KB to 512 KB depending on the size. For large database servers such as Oracle which may perform application level compression deduplication ratios may be compromised. It is strongly recommended to consult with CommVault Professional Services in designing a proper protection strategy with large databases.
**Deduplication Store**

Each storage policy copy configured with a Deduplication Database (DDB) 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 DDB for another store. This means that the more independent deduplication storage policies you have, the more duplicate data will exist in disk storage.

**Sealing the Store**

Performance of the Deduplication Database (DDB) is the primary factor in store sealing. If block lookups take too long, data protection jobs will slow substantially. Sealing the store will start a new DDB which will result in faster data protection jobs but will diminish deduplication ratios. One reason causing block lookups is that the database has grown too large. If the environment is designed and scaled appropriately this should not be a problem. Another reason is that the DDB is being stored on slow disks or using inefficient protocols such as NFS, CIFS or iSCSI. CommVault recommends using high speed dedicated disks directly attached to the MediaAgent.

*It is strongly recommended to contact CommVault support before sealing the Deduplication Store.*

**Block Compression with Deduplication**

By default when a storage policy is configured to use deduplication, compression is automatically enabled for the storage policy copy. This setting will override the subclient’s compression settings. For most data types compression is recommended. The process works by compressing the block and then generating a signature hash on the compressed block. It is important to note that using Simpana compression for data blocks will ensure the compressed blocks always results in the same signature. If other compression methods are used then the signature will be different and deduplication ratios will suffer.

**Compression and Databases**

Most database applications will perform compression on the data before handing it off to the Simpana database agent. In this case using Simpana compression is not advised as it can cause the data to expand. With some database applications it can expand considerably. CommVault strongly recommends using either the application compression or Simpana compression. If application compression is going to be used, best practice is to use a dedicated storage policy for the application and disable compression in the deduplication settings.

For Oracle databases advanced table compression is available which may result in dissimilar hashes being generated each time the database is backed up. This can negate deduplication completely. Careful consideration should be given to which compression methods should be used. Though the Oracle compression is extremely efficient it may not always be the best solution when using deduplicated storage. CommVault strongly recommends consulting with professional services when deploying CommVault software to protect large Oracle databases.
Store Availability Options
Point in time backups are configured in the advanced tab of the Deduplication settings. The Store Availability Option allows you to set recovery points for the backup of the Deduplication Database (DDB). If recovery points are not created and a Deduplication Database (DDB) becomes corrupt the store will be sealed and a new store and database will be created. This would result in all data blocks being resent to the disk library which will have a negative impact on network performance and deduplication ratio.

Client Side Deduplication
It is recommended to use Client Side Deduplication for most data protection operations. This will greatly reduce network bandwidth required to move data over time. By default, Client Side Deduplication is enabled in the storage policy copy. If it is enabled in the policy it will automatically be used by all subclients associated with the policy. If it is not enabled in the policy it can be enabled in the Client Side Deduplication tab of the Client properties.

DASH Full and DASH Copy
A DASH Full operation will simply update the index files and Deduplication Database (DDB) to signify that a full backup has been performed. No data blocks are actually read from the disk library back to the MediaAgent. Once the DASH Full is complete a new cycle will begin. This DASH Full acts like a normal full and any older cycles eligible for pruning can be deleted during the next data aging operation. DASH Full is enabled in the advanced tab of a primary copy.

A DASH Copy is an optimized auxiliary copy operation which only transmits unique blocks from the source library to the destination library. It can be thought of as an intelligent replication which is ideal for consolidating data from remote sites to a central data center and backups to DR sites. It has several advantages over traditional replication methods:

DASH Copy has two additional options; Disk Read Optimized Copy, and Network Optimized Copy. Disk read optimized copy will extract signatures from chunk metadata reducing load on the source MediaAgent. Network optimized will generate a signature from the data block and is more resource intensive on the source MediaAgent. It is recommended to use disk read optimized unless the source data is not in a deduplicated state.
UNDERSTANDING RETENTION
What is Retention?

Available at all stages of the data protection process
- Subclient (Simpana OnePass®)
- Job
- Media
- Policy

Affected by dependencies of other data or data management operations

The key to understanding how Simpana® software manages retention is that the retention criterion and actions are designed to preclude inadvertent or pre-mature data loss. While Storage Policy retention is the primary means to retain protected data, there are several other ways outside of the Storage Policy Copy’s properties to modify/set retention. These include:

- **Object based (Subclient)** – enables direct control of retention by content for backup and archive data on the primary storage policy copy.
- **Job** – enables control of retention for individual jobs. Days Retention can be configured in the job parameters. Job retention can be modified at any point after a job is started. For Snapshots you can define retention by the number of snaps (jobs).
- **Media** – enables control of retention by hosted media. For disk media you can use Managed Disk Space and for Tape media you can use the Prevent Overwrite functionality.
- **Policy** – enables control of data by each Storage Policy Copy. Basic and extended retention settings are available. Use of multiple copies along with association of subclients enables extremely flexible data management.
Retention is also affected by dependencies of one job on another (e.g., incremental/differential data) depends on the associated full job for full restore. As such, these full jobs may be retained longer if the associated dependent jobs are retained. In the case of databases, transactional log backup jobs may be retained if the associated full job is retained. An administrator has control over how retention is handled in these situations.

If other data management operations/copies require a job (e.g., content indexing, verification, secondary copies), it will be retained until all other data management requirements are met.
### Sample Retention Policy

This retention policy demonstrates the concept that all data should not be treated/retained in the same manner. It also shows the purpose of each retained copy which can drive the type of media best suited for that purpose. Disaster Recovery data should most likely be on removable media such as tape. On-site and possible archival data may be on disk for faster/transparent access.

<table>
<thead>
<tr>
<th>Data</th>
<th>Onsite Versions</th>
<th>Onsite Days</th>
<th>Disaster Recovery Versions</th>
<th>Disaster Recovery Days</th>
<th>Historical Versions</th>
<th>Historical Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Mail (Database)</td>
<td>2 cycles</td>
<td>14</td>
<td>4 cycles</td>
<td>90</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mailboxes (Standard)</td>
<td>4 cycles</td>
<td>30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mailboxes (VP+)</td>
<td>4 cycles</td>
<td>30</td>
<td>4 cycles</td>
<td>90</td>
<td>Monthly Full</td>
<td>365 1825</td>
</tr>
<tr>
<td>Mailboxes (VP+)</td>
<td>4 cycles</td>
<td>30</td>
<td>4 cycles</td>
<td>90</td>
<td>Monthly Full</td>
<td>365 1825</td>
</tr>
<tr>
<td>Finance</td>
<td>2 cycles</td>
<td>14</td>
<td>4 cycles</td>
<td>90</td>
<td>Monthly Full</td>
<td>365 1825</td>
</tr>
<tr>
<td>HR</td>
<td>2 cycles</td>
<td>14</td>
<td>4 cycles</td>
<td>90</td>
<td>Yearly Full</td>
<td>1825</td>
</tr>
<tr>
<td>User (Standard)</td>
<td>2 cycles</td>
<td>14</td>
<td>4 cycles</td>
<td>90</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User (VP+)</td>
<td>2 cycles</td>
<td>14</td>
<td>4 cycles</td>
<td>90</td>
<td>Monthly Full</td>
<td>365 1825</td>
</tr>
</tbody>
</table>
Aged data is data that has exceeded all retention requirements. Unless you have unlimited storage capacity (or are not concerned about keeping “too much” data), you’ll want to make sure data ages per your retention policy.

The Data Aging processes runs by default at 12:00pm (noon) every day. All metadata associated with the data currently in protected storage is evaluated by the Data Aging process.

Data that has aged can be pruned. Pruning is done by scheduled administrative processes or jobs. For example; aged data on disk libraries is pruned every 30 minutes UNLESS it falls under the additional criterion of Managed Disk Space. In that case pruning is only conducted when the high threshold level is exceeded and then only down to the lower threshold level or all aged data – whichever comes first.

Once all data is marked aged on a tape, the tape logically returns to its originating scratch media pool and is eligible to be overwritten or erased. Until the tape is overwritten or erased, aged data is available for restore. However, it’s not included in any browse or restore by job unless the user specifically selects to include it. This is different from managed data on a disk library which is treated the same as retained data.

Deduplicated data and snapshot data also have aging conditions. You can find these conditions for the specific agent or under Data Aging in the CommVault Online Documentation.
Policy based retention settings are configured in the storage policy copy **Retention** tab. The settings for backup data are **Days** and **Cycles**. For archived data using non OnePass enabled classic archiving agents, the retention is configured in **Days**.

**Rule 1: Both CYCLES and DAYS criteria must be met before Data will age**
Simpana software uses AND logic to ensure that both retention parameters are satisfied. Another way of looking at this is the longer of the two values of cycles and days within a policy copy will always determine the time data will be retained for.

**Rule 2: Data is aged in complete cycles by default**
Backup data is managed within a storage policy as a cycle or a set of backups. This will include the full which designates the beginning of a cycle and all incrementals or differentials. When data aging is performed and retention criteria allow for data to be aged, the entire cycle is marked as aged. This process ensures that jobs will not become orphaned resulting in dependent jobs (incremental or differential) existing without the associated full.

**Rule 3: Day is based on a 24 hour time period**
A day will be measured as a 24 hour time period from the start time of a data protection operation. Days are considered constants since regardless of a backup being performed or completed successfully the time period will always be counted. If a backup fails, backups are not scheduled or if power goes out a day will still count towards retention. This is why it is so critical to measure retention in cycles and days.
If retention was just managed by days and no backups were run for a few weeks all backup data may age off leaving no backups.

**Rule 4: A Cycle is based on the successful completion of a full or synthetic full backup**

A cycle is traditionally defined as a complete full backup, all dependent incremental, differential, or log backups; up to, but not including the subsequent full. In real world terms a cycle is all backup jobs required to restore a system to a specific point in time. To better understand what a cycle is we will reference a cycle as **Active** or **Complete**. As soon as a full backup completes successfully it starts a new cycle which will be the active cycle. The previous active cycle will be marked as a complete cycle.

An active cycle will only be marked complete if a new full backup finishes successfully. If a scheduled full backup does not complete successfully, the active cycle will remain active until such time that a full backup does complete. On the other hand a new active cycle will begin and the previous active cycle will be marked complete when a full backup completes successfully regardless of scheduling.

In this way a cycle can be thought of as a variable value based on the successful completion or failure of a full backup. This also helps to break away from the traditional thought of a cycle being a week long, or even a specified period of time. In the above example, over a two week time period there are two cycles. The first started on Friday of week 1 and finished 11 days later on Monday of week 2. This cycle was marked complete after the Tuesday full from week 2 completed successfully.
Data Aging Example – 14 Days and 2 Cycles

Protected Data in Storage at the end of Week Three

- 3 full backups = 3 Cycles
- 21 Days total elapsed time
- On week 4 on Friday at 12:00 PM – first cycle can age resulting in 14 days and 2 cycles in protected storage

First cycle can age
Object Based (Subclient) Retention

- Used for object based retention for backup and / or archive items
- Retention days is in addition to Storage Policy retention
- Backup Deletion Options:
  - Immediately – only follow Storage Policy retention
  - After nn days – carry forward with synthetic full for determined number of days
- Archive Deletion Options only applies to archived files
- Version determines number of versions to preserve for existing files

Object based retention uses the principals of synthetic full backups to create, in a way, a carry forward image file. When an object is deleted from the production environment, the object is logged with a countdown timer which is based on the subclient retention setting. The object will be carried forward with each subsequent synthetic full backup until the timer reaches zero. When the time has expired, the object will no longer be carried forward and once the synthetic full exceeds Storage Policy copy retention it is pruned from protected storage. So if the subclient retention is set to 90 days, once the item is deleted it will be carried forward with each synthetic full backup for a period of 90 days.

It is important to note that subclient retention is not used in place of Storage Policy based retention; rather the two retentions are added to determine when an object is pruned from protected storage. If an object is carried forward for 90 days upon deletion, each time a synthetic full runs it will be carried forward until the 90 days elapses. The synthetic full backups themselves are retained based on the Storage Policy copy retention rules. So if the Storage Policy copy has a retention of 30 days and 4 cycles, then a synthetic full will remain in storage until the job exceeds retention. In this instance, the object is carried forward for 90 days and the last synthetic full that copies the object over will be retained for 30 days, then the object will remain in storage from time of deletion for 120 days – 90 day subclient retention and 30 day Storage Policy copy retention.
A new tab in the subclient properties page ‘Retention’ is used to configure object based retention. The setting determines how long to keep an object from the point in which is deleted. There are three options available:

- **Delete immediately** – This does NOT mean to delete immediately. What this means is to ignore any subclient retention settings and follow Storage Policy retention. Once an object is deleted, it will not be carried forward to any synthetic full backups.

- **Keep for nnn days** – From the point in which an object is deleted, the keep for setting determines how many days the deleted object will be continued to be carried forward to new synthetic full backups.

- **Keep forever** – When the object is deleted it will be carried forward to new synthetic full backups indefinitely.
Aging Deduplicated Data

- Macro Pruning (traditional)
- Micro Pruning
  - Requires Deduplication Database (DDB)
- Requires high speed disks for DDB

During normal data aging operations all chunks referencing jobs that have exceeded their retention are marked as aged. With Simpana deduplication data blocks within chunks can be referenced by multiple jobs. If the entire chunk was aged then jobs referencing blocks within the chunk would not be recoverable. The Simpana software uses a different mechanism when performing data aging operations for deduplicated storage.

The data aging operation for deduplicated storage works by checking with the Deduplication Database (DDB) to determine if the block is being referenced by any jobs. If the block is being referenced then it will be maintained in storage. If the block is not referenced then the block will be deleted from the disk.
UNDERSTANDING SECONDARY COPY
Using Secondary Copies

Secondary Copies enable:
- Alternate Media location/type
- Alternate Data Management retention
- Subclient filtered Content
- Consolidation of Valid Data

An Auxiliary Copy operation is used to copy (or to be more specific – update) data from a source copy to one or more additional copies within the same storage policy. The term update is used since only previously un-copied data to the destination is included in an auxiliary copy operation. Auxiliary copy operations cannot be performed between two different storage policies.

Multiple Secondary Copies
If multiple secondary copies exist, the default Auxiliary copy operation is to update each copy sequentially. Depending on resource availability the administrator can choose to enable the Parallel copy option on destination copies to allow them to be updated simultaneously.

Alternate Source
By default, the Primary copy is used as the source copy for all Auxiliary Copy operations. On each destination copy you can select another secondary copy as the source. Only Synchronous copies can be used for both Synchronous and Selective Copy destinations. A Selective Copy source can be used only if the destination copy is also selective.

Subclient Filtered Content
Secondary copies have an Associations tab which can be used to exclude/include specific subclient data from the Auxiliary Copy source. This enables you to backup all data to a single copy then redistribute the data to secondary copies for different management criteria.
Data Streams
An Auxiliary copy operation is performed at the Data Stream level. All copies within a storage policy have the same potential number of data streams as defined at the storage policy level. Data written to a storage policy copy can use up to the max number of allowed streams. The number of device streams actually used in an auxiliary copy operation depends upon:

- The number of available device streams.
- Any allocation policy limiting the use of devices.
- The maximum number of device streams used to create the source copy.
- The device stream has updated data to copy.
- Use of the option Combine to <n> streams.

By default, Data Stream Randomization is enabled. This load balances the data across devices for better auxiliary copy performance.

Valid Data
Within each data stream, an auxiliary copy operation copies only Valid Data – it does not mirror media (i.e., volume for volume). Valid data is defined as data from a data protection job that has not failed or been killed. Since a source copy can contain data from failed or killed data protection jobs, an auxiliary copy operation may result in “consolidation” of the copied data on fewer medium. In fact, auxiliary copy can be used as a consolidation method to move only valid data to another copy in order to delete the less efficient source copy.

An auxiliary copy operation to update one or more copies can be performed within a multi-stream capable library or between any two libraries in a CommCell® environment managed by the same or different MediaAgents, regardless of their host operating system.

Inline Copy
Inline Copy enables the simultaneous updating of secondary copies as the backup data is being written to the Primary copy. A backup can have up to nine (9) secondary copies enabled for inline copy but they must all be using the same MediaAgent. Inline Copy uses the same process/code as Auxiliary Copy.

Use more Recently Full Backup
If the destination copy is a Selective type copy with automatic selection turned off, the Use most Recently Full Backup for AuxCopy option becomes available giving the administrator the ability to determine selective copy content by scheduling the auxiliary copy operation.
DASH Copy is an Auxiliary Copy option that provides a fast method of copying data by transferring only the changed data to a secondary copy (second disk target). This is extremely useful for creating secondary copies of deduplicated data.

The DASH Copy method is better than the MediaAgent Replication method as it transfers only the modified data to secondary copy.

The DASH copy option is enabled in a secondary storage policy copy’s property dialog in the Deduplication->Advanced Tab.

**Disk Read Optimized Copy**

- Source copy must be deduplication-enabled.
- Reads each signature from the respective chunk’s metadata (which contains the data block signature).
- Sends and compares each signature against the target copy’s Deduplicated Database (DDB)
- If the signature exists, the target copy’s DDB is updated for a duplicate data block.
- If the signature does not exist (unique data block) then that block is copied to the target copy. The target copy’s DDB is updated accordingly.
Network Optimized Copy

- Source copy can be deduplication-enabled or not.
- Reads object data from chunk files to be copied and generates signature.
- All signatures are forwarded to the target copy’s DDB for updating. For signatures not found, both the signature and data block are transmitted to the target copy.

Store Priming Option
Whenever a new store is created, a fresh copy of the deduplicated data blocks is created for that store. The Store Priming feature determines if any of the new data blocks existed in the previously sealed stores and if so, uses them to baseline the new store. In source-side deduplication, this saves the need for clients to transfer data blocks that are already available in the MediaAgent.

This feature is best used to reduce the data transfer between clients that have source-side deduplication enabled and connected to the MediaAgent over a WAN.
Topics

Understand Clients
- Understanding Client Structure
- Understanding Agents

Configure Subclients
- Identifying Data Content
- Associating Subclient Content to Storage
- Archiving with Simpana OnePass® feature
- Archiving Rules and Stub Management
- Application Archiving
- The Importance of Filters
- The Uniqueness that is System State
- Using a Subclient Policy
Understanding Client Structure

Clients are Simpana® software component hosts under management of a CommServe® server. Each client must be uniquely identified/accessible by IP address. Valid hosts include physical servers, workstations, or laptops, virtual servers in a cluster, virtual machines on a VMware® ESX Server, Xen Server or Microsoft® Virtual Server/Hyper-V platform, and Logical partitions configuration on UNIX servers. Logical partition support is for applications agents only. A more detailed list of hosts suitable for Agent installation can be found in CommVault’s documentation site.

Within the CommCell Console, a client has properties that provide common support to all hosted agents such as a Job Results folder, Data Interface pairs, and Job priority.

Multiple Agents (agents) of different types can be installed on the same client. Each agent has a specific type of data it is designed to manage. An Agent provides properties and functions that affect the application and data as a whole. Note that for Microsoft® software only, if the data type/application does not exist on the host, the option to install the Agent is not available.

Most, but not all Agents will have a Data Set. The names of data sets reflect their functional area – e.g., Backup Set, ArchiveSet, Replication Set, and Instance (Database). Agents that do not have Data Sets are those where only one view of the data set can exist (e.g., Microsoft Exchange Server) on a Client.
Data Set properties are used to provide a collective view of all protected volumes. The Data Set also defines any user group association and subclient policy association for file systems. For Databases, the Instance level is given the necessary identity, username and password to backup and restore the corresponding data.

Data sets are also used to provide a complete and consistent view of the managed data. With this capability, data can move between subclients and still be consistently viewed and accessed for restore from the Data Set without the user’s knowledge of what subclient managed the data at what time.

Where applicable, the user has options to create additional data sets for an Agent. These additional data sets provide another management view/opportunity for the same data or a different database/application instance.

**Subclients** are the tools used to identify data content and associate that content with a Storage Policy for management. The role and capability of subclients is discussed later in further detail.
What Agent is appropriate for my data protection requirements? It depends on your business needs and may involve more than one data protection method/Agent.

**Backup**
Backup agents are available for all supported file systems and applications. Backups make a protected storage copy of your essential data. Should your production data be lost or inaccessible, you can restore the data from protected storage. General backups are short-term in nature and used for business continuity situations (e.g., corrupt or missing production data).

**Archive**
Data archiving is usually done for two reasons – First, to free up space in front-line storage for more commonly accessed data and second, to preserve data with long term business value. Selection of data to archive is usually based on last access time and size, but other criteria can be used including user and group ownership. Archive agents are available for all supported file systems and most applications.

**Replication**
Data Replication is most likely used when peak loading of the data transport media is a concern. Remote offices connected by the internet or smaller bandwidth dedicated lines usually can’t handle full backups in a reasonable amount of time. Data Replication is designed to dynamically copy only changed data so traffic is spread out over time and more suitable to the available bandwidth. The replicated copy in this scenario is usually at a larger corporate facility with IT staff and other resources. The copy can then be used as a source for backup or other data management activities.
Snapshots
Data snapshots are best accomplished using dynamic hardware mirrored volumes that can be split apart and mounted on a proxy server. Data on the source and mirrored volume is quiesced into a stable state before the split occurs. The “snapped” mirror can then be used as a source for backup, archive, replication, or offline mining. In this manner, there is minimum disruption or resource consumption on the production host. In addition to backing up the snapped volume, the volume can also be swapped back into production should the original volume be lost.

Software snaps are also supported by CommVault and can be used to obtain stable, crash consistent backups where locked or opened files may be a concern. CommVault can manage the entire snap process for more software and hardware environments.
CONFIGURE SUBCLIENTS
Identifying Data Content

Content is defined by Subclients
- Content is mutually exclusive within a Data Set
- Default subclient includes undefined content

Content is Identified by Scanning
- Scanning determines what objects within the defined content need to be put in protected storage

Locked/Open Content handling
- Not all content is in a suitable state to be copied/moved to protected storage

Content destined for protected storage is defined using subclients. Content defined under one subclient is mutually exclusive from other subclient content meaning a content path can only be defined once in the same data set. The default subclient has a unique characteristic in that any content not defined by other subclients in the data set will be included in the default subclient.

Note: Caution should be exercised to not change the content definition of the default subclient which can void this inclusive characteristic.

Subclient content is usually pre-defined by a static data path (e.g., D:\Data) or configured set of objects such as mailboxes. For some Agent types, dynamic content can be defined using regular expressions (wild cards). Additionally, for Exchange Mailbox subclients dynamic content can also be defined using affinity (membership) in a particular Exchange storage group or Active Directory Group.

True dynamic content can be managed using an On Demand backup data set. On Demand content is defined by an external read list which can be generated in any manner at any time.

Subclient content must be accessible to the local system. Data collection processes are run using services with no network capability. For Windows File System subclients the use of UNC paths in defining content is allowed if an authorized username and password is provided. For UNIX, NFS mounted content can be included by specifically entering their mount path.
Archive subclients have additional capability to further define content using Archive rules that focus on content through characteristics such as time last used and size.

**Scanning**
Within the constraints of defined content, the actual data to be protected is identified by scanning the content for objects that meet the criteria of the job type or rules. Full backups should include all defined content. Incremental backups should include only that data that has been modified since the last backup.

Several methods are available to identify modified data.

- Windows subclient content defined on NTFS 3.0 and later can use the Change Journal as a means to track modified files. The Change Journal scan is recommended when content is an entire volume or large subset of a volume.
- The most basic scan method is Recursive Scan (formerly referred to as Classic Scan). Recursive scan uses the file/folder modification and creation times (MTIME/CTIME) to identify modified files. This scan method is recommended when content is a small number of folders/files. It is the default method if the content includes non-NTFS volumes (no Change Journal capability), UNC paths, or volumes with no drive letters.
- A third available scan method is Optimized Scan (formerly Data Classification Enabler). Optimized Scan uses a small database with background monitoring to track content. This scan method can significantly reduce scan time and resource requirements. Optimal scan is recommended when content is a larger number of files/folders.

MAKE SURE YOU SELECT THE APPROPRIATE SCAN METHOD! Inappropriate scans can delay or even hang backup jobs.

**Locked/Open Content**
Not all data is in a state ready for backup. Some files may be in an exclusive state denying the backup application access. Other files may be available, but not in a consistent state making them viable for later restore. In these cases, interaction with the file system or application is required to access the data. Microsoft® provides the Volume Shadow Copy Service (VSS) with application and file system integration specifically for this situation. However VSS is not available for all Windows versions or applications. For non-Windows file systems, the CommVault® Software provides IntelliSnap® Software which performs the same service.

Even VSS or IntelliSnap Software may not be sufficient to access some application data in a consistent state. For these situations, administrators can employ the subclient’s capability to execute pre and post process commands to make the data accessible.
For example: Microsoft® SQL Server 6.5 is no longer supported by Microsoft and CommVault software does not have an SQL 6.5 Agent (agent). However, there are still a lot of functioning applications using SQL 6.5. CommVault systems can still provide protection using a File System Agent. A subclient is created to run a pre-scan process command to create a dump of the SQL database to the defined content path. The dumped copy of the SQL database is scanned, backed up, and then a post-backup command is used to remove the dumped file. Restores are accomplished by restoring the dumped SQL database file and using SQL to read the dump file back into operation. This use of pre/post process command capability to handle applications with no specific Agent support or unsuitability to VSS or IntelliSnap Software is not uncommon.
Subclient content is moved/copied to protected storage using **Job Streams**. Each data movement event is called a job. Each job will have at least one Job Stream upon which data flows from a Client to a MediaAgent.

The number of Job Streams is defined at the subclient properties level as the number of concurrent **readers or streams**. Which data path (MediaAgent and storage) the streams use is determined by the associated Storage Policy and the available data paths. With GridStor® Technology, a Storage policy can have multiple MediaAgents and data paths.

Each subclient can define, within the constraints of the associated storage policy, which Data path it will use and in which precedence order. This user-defined data path priority can be used to override the automatic data path selection logic. This feature enables the administrator to use a single storage policy with multiple data paths where not every data path should be an alternative to a particular subclient. For example, a storage policy with Clients and MediaAgents located in different geographical locations. Locations are connected by low bandwidth transmission media. Logically, the clients in one location should not use MediaAgents in another location. Using data path override, you can specify that Clients in one location can only use MediaAgents in the same location. All still within one storage policy.

Each Job Stream is assigned to a Data Path and a Device Stream originating and accessible from the MediaAgent. For a disk library that means a mount path and a writer on that mount path. For a tape library that means a drive pool and a tape drive in that pool.
Multiple Job streams can be sent to the same mount path or drive pool. For tape devices, multiplexing allows multiple job streams to be sent to the same device stream.

Options exist on the subclient properties dialog box to facilitate the state of data before it reaches its storage destination. These options also allow the administrator to determine where that state change will occur:

- **Compression** can be enabled and is recommended to occur on Clients with low bandwidth transmission paths or those with data destined for deduplicated storage.
- **Encryption** can also be set on the subclient to occur before, during, or after transmission depending upon whether the purpose of encryption is transmission or storage related. Note that Encryption must be enabled at the client level for this option to be available.
- **Deduplication** signature generation and its location can also be enabled. This option only has affect if the associated Storage Policy is enabled for deduplication. CommVault recommends deduplication signature generation occur on the client so as to not overtax the MediaAgent processor which may be handling multiple job streams.

Job streams consume resources on the Client, MediaAgent, Data Paths, and, in the case of LAN-based Clients, TCP/IP transmission bandwidth. As often is the case, the transmission media is not dedicated to the exclusive use of the CommVault software. As such, the subclient has resource tuning features that can constrain the consumption of bandwidth used to move the data. This means we can play well with other applications using the network.
Archiving with Simpana OnePass® Feature

- Optimize disk space usage and file accessibility
- Can enable transparent recall by end user or application
- Can reduce backup volume
- Capability offered as:
  - Integrated with File System Backup Agent (Simpana OnePass®)
  - Separate File Archiving Agent

File archiving facilitates the optimization of disk space and file accessibility based on usage patterns. It also provides a transparent recovery mechanism (stub) for users and/or applications to re-access the data from the original storage location.

File Archiving with transparent recall is supported though the Simpana OnePass Agent for Windows or UNIX. This is an integrated component of the File System Agent and is enabled in the File System Agent Properties. The Driver for File Recall component must be installed. **Driverless for Simpana OnePass Agent for Windows** configuration is only supported for Windows 7, 8, and 2008. End user file recalls for the driverless configuration are supported via an add-in component to Microsoft® Explorer.

There is also a Simpana OnePass Agent for BlueArc, Celerra, and Netapp. As no drivers can be installed, recall of files archived in this manner is through the CommCell® Console.

**IMPORTANT** – Once Simpana OnePass Archiving has been enabled, it cannot be disabled. Additionally, archive retention/stub management is managed via Synthetic Full backups. Once Simpana OnePass Archiving has been enabled, only incremental or Synthetic Full job types can be executed.
Archiving Rules and Stub Management

- Capacity
- Time
  - Access
  - Modification
  - Creation
- Size
- State (Read-Only)

File Archiving is used when primary storage reaches near capacity and free disk space is required for more data. Understanding that the objective is to maximize the utility of primary storage, file archiving actions are usually governed by used or free capacity. If sufficient free capacity exists, there should be no need to archive files. However, if free capacity becomes a concern, then archiving the more infrequently accessed files would be prudent.

In order to free up this disk space, less frequently used files are migrated/archived to less costly storage based on a set of defined rules. Archived files can be replaced with a much smaller Stub file that contains the necessary recovery information. With a stub file and the recall drive installed users and/or applications can recall the file to primary storage using normal access methods. Without the recall driver installed users can recall the file using the Microsoft® Explorer add-in. The only noticeable impact may be a slight time delay in the file’s initial response time.

Archive rules enable the administrator to select files for archiving based on their last access time, modification time, size, and attribute (read-only). The best archive candidate would be a large, infrequently accessed file as this would free up the most disk space.

Archiving rules for the OnePass Agent appear under the Disk Cleanup tab of the File System Subclient Properties. The Disk Cleanup tab is only visible when Archiving has been enabled in the File System Agent Properties.
**Stub Management/Retention**

Files that are archived are deleted on the source and a stub file left in their place. By default, all archived files are retained forever. To alter this characteristic you use two features:

- Schedule Synthetic Full backups by enabling the **check for deleted stubs** option.
- Use the Subclient Properties to set the archived files retention value for when their corresponding stub has been deleted. Retention options are to delete immediately, keep for a specified number of days, or keep forever.
Simpana OnePass® Agent for Exchange Mailbox

As with the Simpana OnePass® Agent for Windows or UNIX, the Simpana OnePass Agent for Exchange Mailbox enables you to move the mailbox messages to a secondary storage and use these messages to function as both backup and archive copy. Stubs are retained on the production storage, which point to the messages that were moved as part of the backup. The archived messages are available for quick and easy retrieval to administrators and end users. This integrated agent is also able to selectively age off messages and stubs to reclaim space on primary and the secondary storage based on message age in the mailbox.

The Simpana OnePass Agent feature for archiving mailbox messages is enabled from the General tab of the File System Subclient Properties.
**Domino Mailbox Archiver Agent**

The Domino Mailbox Archiver Agent periodically moves unused or infrequently used Lotus Notes Mailbox messages on a host computer to secondary storage. The Domino Mailbox Archiver Agent provides support for two distinct archiving scenarios:

- **Migration Archiving** – Used to reduce the number of messages routinely backed up to primary storage by the Lotus Notes/Domino Server Agent.
- **Compliance Archiving** – Used to index messages copied to the journaling mailbox to meet security and compliance standards.

The Domino Mailbox Archiver Agent provides data protection support for all .nsf mail databases visible to the Domino Server. However, only databases with alphanumeric names are supported.
The Importance of Filters

Filters
- Save Backup Time
- Save Storage Space
- Save Restore Time

Exclusion Filters defined
- By Policy
- By Subclient

• Exceptions to Filters defined
  • At Subclient Policy or Properties Level

Users and applications generate a lot of non-essential data. Such data is not required to be retained or not needed for business continuity/system recovery purposes. Such data is usually temporary in nature (e.g. cache files, working files), non-business related (personal files), or data protected by other means (install source files, database files). This data should be filtered from the results of the content scan.

Filters are evaluated during the Scan phase to produce the final list of data to be protected within the scope of the subclient content.

Filtering data achieves three key objectives:

- First, it reduces the data collection time by excluding the movement of non-essential data.
- Second, it reduces the protected storage footprint from eliminating non-essential data.
- And lastly, it reduces the system restore time by not having to restore non-essential data.

DO NOT UNDERESTIMATE THE VALUE OF FILTERS!

Exclusion filters can be defined on a broad scale by Global, Replication, or Subclient policy, or locally within the subclient’s properties. The application of the Global Filter policy is part of the Agents installation process.
Exceptions to the exclusion filters can be defined only within the Subclient policy or properties. Exceptions allow you to make broader exclusions but still include data within the scope of that exclusion. Example: You can exclude all Temp folders — with the exception of .log files within the temp folders.

Getting the proper filters in place can be challenging. Always check your backup content after applying a filter. You want to make sure the filters are not too restrictive as to exclude some essential data from being available in protected storage. The CommVault Online Documentation has a list of recommended filters you can try.
The Uniqueness that is System State

- Uses VSS for System State backup
- Domain Controller System State includes Active Directory® Directory Service
- Option to only backup System State during full backups

System state is unique to Microsoft’s® Windows Operating Systems and is critical to recovery of applications that depend on it (e.g., Exchange 2007/2010). By default, System State is protected with the default File System Agent subclient. Administrators have the option to protect the System State separately with its own subclient combined with other data such as the system disk.

On a domain controller running Windows Server 2003/2008/2012, the System State data consists of the system startup files; the system registry; the class registration database of COM+ (an extension to the Component Object Model); the SYSVOL directory; Certificate Services database (if installed); Domain Name System (if installed); Cluster service (if installed); and Active Directory. A more detailed list can be found in CommVault Books Online.

Note that if you do not use Active Directory-integrated DNS, you must explicitly back up the zone files. However, if you back up the system disk (Windows directory) along with the system state, zone data is backed up as part of the system disk.

A domain can have multiple domain controllers. It is recommended that at a minimum you should back up two domain controllers in each domain, one of which should be an operations master role holder (excluding the relative ID (RID) master, which should not be restored). Unprotected failed domain controllers can be recovered through reinstall, promotion, seizure of operational roles and/or enabling of global catalog, and replication. Note that in a multi-domain environment, the restoring of a global catalog server from backup requires more time than restoring a domain controller that does not host the global catalog.
A system state backup is always a full backup whether you select full, incremental, or differential backup for the subclient that includes the system state. You can filter out some components from system state backup. And you can restore individual system state components/services or the entire system state in place – or out of place. If a synthetic full is conducted then the first backup after the synthetic full will include the system state.

A backup that is older than the tombstone lifetime set in Active Directory is not a good backup. At a minimum, perform at least two backups within the tombstone lifetime. The default tombstone lifetime is 60 days. Active Directory incorporates the tombstone lifetime into the backup and restore process as a means of protecting itself from inconsistent data.
Using a Subclient Policy?

- Scalability tool for defining subclient properties
- Locks down subclient properties from local client changes

Subclient Policies provide a way for you to configure many similar file system clients within a CommCell environment from a central template. For example, you can attach the same storage policy to several Windows server clients all at once using a subclient policy. This alleviates the need to manually set up similar file system clients for data management tasks.

A primary Subclient Policy use case would be laptop clients where you have many clients with a subset of data (documents) that you want protected.

Another use case would be several clients where there is only minor variance in the subclient properties. In this case you can build and associate a Subclient Policy with all the common settings. You can then disassociate the policy and the subclients will retain the settings allowing you to individually adjust each subclient as necessary.

Another use of a Subclient Policy would be to separate and manage System State backups as a separate subclient.
Topics

**Understanding Job Management**
- What is a Job?
- Initiating a Job
- Job Priorities
- Controlling a Job
- Job States
- Synthetic Full
- DASH Full

**Restore Data**
- Finding Data to Restore
- Indexes and Image Files
- Restore Options
- Understanding Archive Recall
- Understanding Full System Recovery
UNDEFRSTANDING JOB MANAGEMENT
What is a Job?

Definition

- A Job is a task consisting of one or more phases executed and managed via the Job Manager Service and appearing in the Job Controller window.

Types

- Data Management
- Data Recovery
- Administrative

A Job is a task consisting of one or more phases executed and managed via the Job Manager Service and appearing in the Job Controller window. An exception to this are VaultTracker Policy jobs which are called “actions” instead of jobs and these actions appear in the CommCell® Browser’s Storage Resources->VaultTracker->Actions window.

Types of jobs include:

- **Data Management jobs** – are those jobs that involve collecting data or information from an Agent on a client. These include Backup, Archive, Replication, Offline Content Indexing, and Data Collection. Some Data Management Jobs are also referred to as Data Protection jobs. Where applicable, Data management jobs can be further broken down into full and non-full job types. Non-full job types are those that cover only new or changed data. This can be object level changes (e.g. backup) or block level changes (Intellisnap).

- **Data Recovery jobs** – are those jobs that involve sending data to an agent. This does not necessarily mean the same agent that provided the data. Data Recovery jobs include Restore, CDR Recovery, Stub Recall, and Search Restore.

- **Administration jobs** – are any other jobs not classified as Data Management or Data Recovery. Some key Administrative jobs include DR Backup, Auxiliary Copy, Data Aging, Data Verification, and Backup Copy.
Jobs are initiated by the user as either on demand (immediate) or scheduled events. Scheduled jobs are initiated at the set time and frequency by the Job Manager Service. Some jobs can be saved in script form and executed from the command line. Command line execution allows for integration with other management applications and coordination with external events.

**Scheduling a Job**

In the act of defining a job, the user will be given Job Initiation options which include scheduling. Various schedule patterns and options can be defined. Alternatively, a Schedule Policy for a job type can be created and then associated with an object. Viewing job schedules is available at the CommCell level down to the Subclient level. At the CommCell level, the Scheduler tool can be used to edit an existing job pattern, delete, clone, disable a job schedule, run immediately, or decouple a Schedule Policy. Decoupling frees a job schedule from the originating Schedule Policy making the schedule independent and editable for the associated object. The Scheduler tool also has the option to filter the view by desired scheduled items on a daily basis per month.

Some administrative jobs (Data Aging, DR Backup) are automatically scheduled by default for a new CommCell environment. When installing components, adding new subclients or adding Storage Policy copies, the user will be prompted to schedule the appropriate job. The Job Schedule Report can be used to list all scheduled jobs. The Job Summary report can also report schedule information as well as any subclient that has not been scheduled for a job.
Job priority determines the numerical precedence in which the Job Manager assigns storage resources to a task. Think of it as being served at a Deli counter that uses a ticket system. It also determines preemption precedence when resources are limited. This means a higher priority jobs can preempt a currently running job if there are no other resources available.

In the example shown, two jobs are running with the default priority. There are two jobs queued and are waiting for resources to be freed to start.

When a new job is started with a higher priority (lower number), the job moves to the head of the queue and it will be the next job to run when resources are available.

If the “Backups pre-empts other backups” option in the Control Panel’s Job Management applet is selected, the job manager will look for pre-emptible jobs. Only indexed jobs are pre-emptible. It finds a pre-emptible job, suspends it, and frees up the resource. In this example it will unload the tape, find the assigned active tape for the new job and load it. When that job completes, the previous tape gets loaded back and the suspended job will resume.
There are two primary means to control job start – **Activity Control** and **Operation Window**.

- **Activity control** – disables or enables certain operations. For example, you want to prevent backups from running while doing maintenance on a server or you don’t want users running restore jobs to that server.

  Activity control is available at multiple levels starting from the CommCell® environment level (CommServe® Properties) all the way down to the Subclient Properties level. Various types of job activity can be controlled, with more choices at the CommCell environment level than at subsequent lower levels.

  Disabling activity at a higher level has a cascading effect down to the subclient level. Jobs that fail to start due to the activity being disabled will be identified as such in the Event Log. As to whether the job queues waiting for the activity to be enabled is determined by options set in the Control Panel’s Job Management applet.

- **Operation Windows** – limits the start and duration of an operation. Operation Windows are also available at the CommCell environment level (Control Panel Applet) all the way down to the Subclient task level.
“Do Not Run” rules can be defined in an Operation Window for a specific job, day of the week, interval of dates, and from/to time. Operation Windows set as descending levels can optionally ignore rules set at higher levels. Jobs to which the operation window rules apply will not start in the “Do Not Run” intervals. Jobs currently running may be suspended for the interval or allowed to complete. This depends upon the type of job and the options set in the Control Panel’s Job Management applet.

There is also a job option that will start a job in a **suspended state**. Its primary use case would be in an event-driven scenario where the event cannot be determined by a computer (i.e., human intervention required). In this case, the job must be manually started (resumed) by a user.

The **Job controller** allows the user to monitor and control jobs in progress. For scalability, when many jobs are in progress, the user can filter the view of jobs in the controller and take action on multiple jobs at the same time.

The columns viewed in the Job Controller can be re-ordered, re-sized, removed or added, and used as sort criteria for displaying jobs.

User action includes; changing the job priority, adding/deleting/modifying job alert, suspending the job, resuming the job, killing the job, or resubmitting a failed job. Additional Job details beyond what is seen in the Job Controller can also be viewed.
Job States

States
- Running, Waiting, Pending
- Suspended, Queued, Killed, Failed
- Completed, Completed with warning, or Completed with Error

Job History
- Used to view jobs no longer in the Job Controller

While in the job controller, a job can have various states. These include Running, Waiting, Pending, Suspended, Queued, Killed, Failed, Completed, Completed with warning, or Completed with error. Transient states include Dangling Cleanup, Interrupt Pending, Kill Pending, Suspend Pending, and System Kill Pending. Detailed explanation of each of these states can be found in the CommVault Online Documentation. Running and Waiting are natural job progress states. Pending indicates a phase of the job has failed to complete successfully and is waiting to be retried. The Queued, Suspended or Killed state can be initiated by the user or the system. Failed state is when all job retries have been exhausted. A Dangling Cleanup is a failed phase waiting for the Job Manager Service to finish associated processes.

Note that jobs that have been Killed, Failed, or Completed with or without Warning or Error remain visible in the Job Controller for 5 minutes or until the Job Controller view is refreshed – whichever is earlier. This visibility retention time can be modified in the Control Panel’s User Preference applet.

If the job is no longer visible in the Job Controller, how do I know its final state?

Once a job has completed, failed, or been killed, its final state can be seen in the Job Summary Report or viewed in Job History. The Job History view is available from the CommCell level down to the subclient level. By default, Job History for failed or killed jobs is retained for 90 days. This retention setting can be changed in the Control Panel’s Media Management applet in the Data Aging tab. Completed job history is retained as long as the associated data is retained. However, some job details (e.g. list of protected files) which are drawn from the JobResults folder on the client are retained less due to space constraints.
What's the relationship between Job Phases, Pending state, and Job Retries?

As defined in the question – What is a job? – a job is made up of one or more phases. The job manager service initiates each phase and reviews the phase’s reported completion or failure before starting the next phase in the job. Failed phases put the job into a pending status. Depending upon the type of job and phase that fails, the job phase that failed will be retried – or an earlier phase will be the restart point – or the job as a whole will be failed.

Default Job Retry settings are defined in the Control Panel’s Job Management applet. These settings can also be defined within each job. You may want to increase the Job Retry interval or reduce the number of attempts. In addition to retries, the overall time it takes to complete a job can be defined. This helps to prevent jobs from entering an extended waiting state which may affect the client system, application, or production data.
A Synthetic Full synthesizes a full backup by copying objects from previous backups into a new backup. You could consider a synthetic full as a restore into a backup. Synthetic full backups can greatly reduce network traffic and load on the client by eliminating the need of moving all the data from a production server.

A Synthetic Full works by using image files to determine which objects need to be protected. Each time a data protection operation is run for a client (full/incremental/differential), an image file is generated. This image is a view of the folder structure for a subclient at the time of backup. This will include all folders, files, data/time stamp and journal counters. When a synthetic full is performed the most recent image file is used to determine which objects need to be protected. They are copied from previous backups into the new synthetic full.

A Synthetic Full is considered a valid full backup and a successful completion will begin a new cycle. It will also result in the creation of a new index file. If any objects are missing from the Synthetic Full you can use the Verify Synthetic Full option in the advanced backup options. This will check what is in the Synthetic Full against the most recent image file. If any objects are missing the next incremental backup will automatically backup those objects.
DASH Full is a Synthetic Full backup option available on a dedupe-enabled primary storage policy copies.

A traditional Synthetic Full job determines what objects existed on the source subclient at the time of the last backup. It uses this list to read the data from the primary copy vice the source client and re-writes the data to the copy.

With deduplicated data, a DASH Full job works much the same way as a traditional Synthetic Full with the exception that since all the data comes from existing data blocks in the library – no new duplicate data blocks would be written. Only the reference points in the Deduplication Database (DDB) and the index for restore are updated. The savings in time and resources are significant.
RESTORE DATA
Finding Data to Restore

Find
- Uses MediaAgent indexes
- Metadata only

Search
- Uses Content Indexes
- Metadata and text

Restore Browse
- Uses MediaAgent indexes
- Expanding Hierarchical display of data structure

There’s a big difference between doing a full system restore from the latest backup copy and restoring a single object (file/folder/document/message) that someone just noticed missing. Odds are you’ll be doing more of the later. So, how do you locate that missing file when you’re not sure when it was lost, where it last was, and what exactly was its name? And if there were changes to the file resulting in multiple versions in backup storage, which version is the right version?

**FIND**

Your first and best tool in locating data within protected storage is **Find**. The Find task is available at the data set level and within the Restore Browse. Find can scan multiple indexes within a specified range of backup time looking for a specific filename or pattern (wildcards). You can also limit your scope of search to a specific folder or folder structure. Matching results are displayed, including all versions of the file within the specified time range. You can select to restore any, all, or specific version(s) of the found file.

Note that if multiple versions are restored, each version will have a sequential number appended to the filename starting with 1 for the most recent version of the file.

With E-mail, you can also use Find to search on data within the From, To, and Received fields of the message. Note that not all Agents support the Find task and the scope is restricted to a single Client/data set.
SEARCH
The next best tool for locating missing data is **Search**. The search task is available as a Web Search capability for offline data (data on production storage). Search requires and is limited to data that has been Content Indexed. The advantage of using Search in locating data in protected storage is the expansion of the search field to include the text body of the file, document, or message. The original location of the data becomes irrelevant in the search. All content indexed data regardless of which client or data set it originated from is scanned by a Search task.

BROWSE and RESTORE
Browse is probably the most common method used for locating a missing object to restore. It’s also the slowest as it requires the system to first compile and display the browse tree. The user must then expand and visually search through the browse tree to locate the missing object. As this is a familiar and easy way for data search, users are most comfortable with this method.

Restore Browse performance can be improved by narrowing the starting point of the search. For example; if you know the file was in the F:\Users folder structure, do you really need to include the C:\, D:\, and E:\ drives in the browse tree? You can also change or expand the browse to cover other backup times or indexes. These options are discussed later in this module.

Restore Browse is available at the Client, Data Set, and the subclient task menus. There is also a Restore Browse icon available on the CommCell Console Tool bar that allows you to select any Client level browse.
Indexes and Image Files

- Image and No Image Browse
- When to use Image Browse
- When to use No Image Browse (show deleted items)

The “index” used to restore file is actually an efficient database with numerous indexes used to efficiently retrieve files. Each backup does two indexes – an “image” index which is a list of all objects found in the subclient and a “collect” index which is what objects were actually collected by that job.

For a full backup, the image and collect indexes would be the same (assuming all objects successfully backed up). For an incremental backup, the collect index would be most likely significantly smaller than the image index (assuming only a subset of the data has changed since the last backup).

Normally (by default) a full backup starts a new indexing database. Subsequent incremental or differential backups update the database with new objects and add new image and collect indexes.

When you do a “Browse” of data, you’re looking at the image index from the most recent backup relative to the date selected. If multiple subclients exist within the backup set and you browse at the backup set level or higher, then the indexes from each subclient are merged in order to present a complete listing of objects.
Direct
Supposing you know precisely what file you want to restore. Do you need to go through the effort of Find, Search, or Browse? No, you do not. A data set level task of Restore is available for File System Agents. Just enter the specific path and filename - or you could use wild cards (e.g. *.doc).

Restore By Job
The Restore by Job feature provides the facility to select a specific backup job or set of jobs to be restored. This method of restoring data is faster under some circumstances as it reads continuously from protected storage and retrieves the data independently rather than using the indexing subsystem which does individual seek offsets on the media.

A key advantage of restore by jobs is restoration of any successfully written data in failed or killed jobs.

If multiple job streams were used in parallel for the data protection job, then restore by Job can use those same multiple streams in parallel for the restore. The degree of parallelism would be a factor of the degree of multiplexing for the jobs involved. The higher the multiplexing, the more “parallel” the restore. Restore by Job cannot be used to restore the Windows System State data.
**Restore Browse**
A standard browse/index-based restore provides a more granular restore capability and may be more appropriate for anything less than a full system restore. For smaller sets of data the Restore Browse can be faster by not restoring unnecessary objects. However, an index-based restore is single stream only, regardless of how many streams may have been used in parallel by the data protection job.

**Copy Precedence**
Restore will use highest copy precedence containing a copy of requested data. Use of other copy precedence can be forced for data path or to avoid questionable/unavailable copy. By default, the Primary copy is assigned the first Restore Precedence. Restore precedence is defined at the Storage Policy copy level.
The recall or non-browse recovery feature provides the facility to transparently and either temporarily or permanently brings an object back from an export location for a specific operation. Transparency is provided by a stub object substituting for the actual object which initiates the recall automatically when accessed through normal means. The temporary capability is useful if you need an object for a specific purpose or length of time and do not wish to reset the object’s archive criteria. A permanent recall is useful if the object being recalled will be used multiple times and you wish to reset the object’s archive criteria.

**Note:** For Microsoft® Windows, stub recovery is handled through CommVault’s Driver for Recall which passes the access action to CommVault for processing. If the Driver for Recall is not installed on a Windows host then the user can use the Microsoft Explorer Add-in to initiate file recovery. In all cases, archived files can be selected and restored using the CommCell Console. For Network Appliance, automatic recalls can be handled using their Fpolicy feature. For Celerra, this can be handled using their Virtual Data Mover feature.

When performing a non-browse recovery of archived data from magnetic media or tape, the system maintains a common open pipeline known as a **persistent pipeline** between the target client and the protected media source for multiple stub recall requests. The pipeline stays persistent for 24 hours (by default) to reduce the time to open a pipeline for each individual stub recall request. The initial object being restored may take a few seconds more time as the pipeline is established. Subsequent restores are very quick.
When performing a non-browse recovery of archived data from a stub, keep in mind that the data can only be recovered in-place to the same path/destination on the same client from which the data was archived.

Stubbed, non-browsed restores can only be recalled in-place to the item’s previous location. However, for Exchange the restore destination can be the same mailbox, a different mailbox, or a PST file on another Exchange Server within the same organization and site with a compatible Exchange Mailbox Agent installed and operational.

**Working with Stub Files**

When data is archived from a server to another location, a pointer - or what we call a stub - is left in place of the file. This stub enables transparent recalls of the data. Although the data has been moved, it is still available to the user or application as if it was still on the server. After a stub has been recalled, the icon will change back to the normal icon for the respective file type. The only visible difference between a stub and the file is the icon representing the file. The icon is changed to denote the archived status of the data. The icon doesn’t change much, the original application icon will still appear but with a small clock in the left bottom corner. This represents a potential delay in accessing the file while it's being recalled from remote storage.
Understanding Full System Recovery

Similar/Different Hardware Issues
- Configuration and size of Mass Storage devices
- Dealing with device driver issues

Windows System State
- Optional and partial restore supported
- Domain Controller/Active Directory restore modes

UNIX/Linux Root Partition
- Default install on different partition

The difference between a normal restore and a full system restore is the severity of the problem. Normally, if data is lost or removed it can be recovered from the archives using the normal restore procedures. However, when a normal restore operation cannot correct a software and/or hardware corruption problem, some level of full system restore is required.

If the root directory of a UNIX system or the System State of a Windows system is lost, a Full system restore is required. Full system recovery procedures can be found in the CommVault Online Documentation within the appropriate client’s Disaster Recovery section.

Hardware
Hardware failure is the most prevalent cause of a full system restore. In this case most likely one or all of the hardware components are new. For Microsoft platforms, both the CommVault® and Microsoft® software makes a best effort to reconcile hardware differences at the time of restore or recovery. However, there are no guarantees since some hardware differences may cause issues that are beyond the software’s control. In fact officially, Microsoft does not support restore to different hardware. As such, having similar - if not identical - hardware is essential to a trouble-free full system restore. A solution to this would be CommVault’s 1-Touch feature which enables full system recovery to different platforms.

Regardless of different hardware, unless you intend to restructure your data during a full system restore, you will need, at a minimum, the same number/configuration of volumes and volume size. You can’t restore 100 GB of data to a 20 GB volume!
Software
When you perform a full system restore, the client computer must have a functional and compatible
version of the Operating system. With UNIX, the default install partition should not be on the same disk
partition that will contain the restored root file system. For Windows you must have the same OS and
service pack level installed along with the File System Agent. Hot fixes can be pre-applied before or
during the restore.

System State
The decision to restore the System State as part of the full system restore should be based on hardware
differences and application support. Do not restore the system state if there are significant hardware
differences. Not restoring the system state may require you to re-install applications. Note that you can
set restore filters to do partial system restores.

For Domain Controllers, restoring the System State includes the Active Directory. Depending upon the
presence of other Domain Controllers and the desired resultant state of the domain you need to select
Primary (first/only), non-Authoritative (sync with others), or Authoritative mode (sync with me). In
some cases, rebuilding and promoting another Windows Server may be faster.

Application Restores
An application is made up of its managed data set and supporting executable and configuration files.
The application must be functional in order to restore its managed data. In some cases this may require
using a File System restore to get necessary supporting files in place. Additionally, the application must
be in a recovery state in order for a restore and full recovery to work successfully.

For example; With Exchange the System Attendant Service must be running in order to restore
databases. The System Attendant Service will run without the presence of the databases. However, if
the databases do exist they must be enabled for overwrite by a restore. This can be done using
Exchange admin tools, or it can be done automatically by selecting the appropriate option during an
Exchange database restore.

On the other hand, SQL Server service will not run without the master, model, msdb and temp
databases. In order to do a full application recovery of SQL Server you must build suitable replacement
databases in order to start the SQL Service - and then restore your original databases from protected
storage. Microsoft provides utilities to rebuild the necessary databases.

The key thing to remember is that restoring an application to full functionality requires cooperation
between many parts. Understanding and practicing application recovery is essential to successful
recovery.
Module 6

Monitoring a CommCell® Environment
Topics

Understanding Monitoring Tools
- CommCell® Console Monitoring Tools
- CommVault Monitor App

Configuring Alerts
- Alert Categories and Output Options

Configuring Reports
- Types of Reports
UNDERSTANDING MONITORING TOOLS
Other than the Event Viewer, there are four basic features of the CommCell Console that provide valuable information to the administrator:

**Job Controller**
The Job Controller allows you to monitor and view detailed information about jobs as well as job events and the media used for each job. Once a job is finished, more information about that job is obtainable using the Job History.

**Job Updates**
By default, the system updates the information in the Job Controller every time a chunk is written, every 5 minutes, and every 2048 MB (2 GB) of data transferred. These values can be changed by opening the Control Panel and selecting the Job Management control – Advanced tab. We don’t recommend you decrease the value as the more frequent updates will compete for resources and could impact job performance.

**Job Status Levels**
A job in the Job Controller window may show the more common and self-explanatory status of Completed, Failed, Killed, Waiting, Stopped, or Running. A Pending state indicates a phase failure waiting to restart or waiting for the appropriate point to perform the requested operation by the user or system.
It may show one of less common status levels of:

**Completed with One or More Errors**
The job has completed with errors indicates some components of the job were not protected such as locked files, deleted files, or virtual machines when using the VSA agent.

**Dangling Cleanup**
An expected response has been missed and the job has been terminated by the job manager. The job manager is trying to locate and kill all associated processes before killing the job.

**Queued**
The job conflicted with other currently running jobs (such as multiple data protection operations for the same subclient), and the **Queue jobs if other conflicting jobs are active** option was enabled from the General tab of the Job Management dialog box. The Job Manager will automatically resume the job only if the condition that caused the job to queue has cleared.

**Storage Resources**
Tape Device can provide average and recent throughput information. Tape devices can also provide usage and error information. Mount paths and Media properties can provide both used and available space information. Note that tape media usage with compression enabled is an estimate.

**Content**
Jobs on Media can be viewed to determine which jobs, if any can be manually removed in order to make the media available for re-use.

**Resource View**
The Resource displays all the drives in the library and the Job ID, media used, and current operation being performed by each drive. If the media in the drive is not being used by a job the resource view displays the Job ID as Cache Mounted. In addition, the resource view also displays the slot information in the library and information on media that is currently in the process of being exported. For disk libraries, the status and free space information for the mount path is displayed.

**Job History**
Admin, Backup, and Restore Job History is available in hierarchical format from the data set level up to the CommCell level.

**Policies**
You can view both jobs and media associated with each storage policy. These views also allow you to manipulate the jobs or media as may be required to facilitate reuse of media and availability of jobs for recovery.
CommVault Monitor enables you to use your smart device to view, manage and monitor backup jobs on a CommCell environment. The application can display information on jobs classified by their status including running, waiting, pending, succeeded, or failed. You can view job progress, attempts, and top reasons for Job Delay (waiting or pending) and failure. You can also take action to kill, suspend, or resume a job.
CONFIGURING ALERTS
CommVault’s® Alert feature provides real time notification on events occurring within a CommCell environment. These conditions can range from minor occurrences that do not require intervention to severe occurrences that need immediate intervention. The system detects conditions within two minutes of the occurrence. Alert coverage is defined for each alert created and is hierarchical covering all sublevels of the defined object. Alerts can be configured for any object that can be seen by the user creating the alert.

**Alert Output Options**

Alerts can be sent to their intended recipients by email/pager; to the CommServe’s application log accessible from the Windows System Event Viewer; by SNMP Trap(s) to a SNMP capable monitoring application; or initiate a command line program, executable script or batch file, save to disk (CommServe host folder and/or file), sent to a RSS feed, or displayed as a console dialog box.

Alert wording can be customized by the user. Relevant, localized information can be added to reports such as responsible persons to contact or appropriate action/steps to take. To help with customization of variable data in an alert, tokens representing the variables are provided. Tokens can also be passed as arguments for the command line script. Command line arguments support the use of all tokens except attachments (e.g., `<PROTECTED_OBJECTS>`) or lists (e.g., `<MEDIA_LIST>`).
E-mail alerts can be sent to a CommCell User Group, External User Group, or to individual users. In order for a user to receive an alert, the user must be enabled and have a valid SMTP address. If the mail server is down, the system will attempt to send alert e-mail notification for the next four hours. If after four hours, the mail server is still down, these alerts will be removed from the system, and will not be sent to the recipient. Additionally, an individual alert notification can be generated rather than multiple alerts being generated within a single alert notification.

In the event that an alert condition persists, an escalation notice can be generated via alternate means.

**Testing Alerts**
An alert can be tested to verify if the notification is configured correctly so that all intended recipients of the alert receive the notification messages. This can be accomplished in the Alert Dialog box by right-clicking on the alert and selecting Test from the submenu that appears. The TestSendMail utility in the Resource Pack can also be used from the command line to test the mail connection for sending alerts.

**Recommended Alerts**

**Insufficient Storage**
Media Management | Library Management

The most common reason for data protection job failure is no spare media. You run out of magnetic disk space or have no spare media inside the library. This is particularly prevalent during weekends when large data protection jobs are usually scheduled and no one is about to monitor the status of spare media.

The Insufficient Storage alert is dependent upon the *Low Watermark* threshold value assigned to the disk library, Scratch, and Cleaning Media Pools. Ensure you set these values high enough to allow the alert to give you ample warning to replenish the media before jobs start to fail.

**Phase or Start Job Failure**
Job Management | Data Protection

A Data Protection job consists of two or more phases and requires network connection in order to initiate the job on the Client. If a phase fails, or the Client can't be reached the job will enter a pending state and retry. If the condition that caused the failure is transitory, a retry may succeed. If not, the entire job will eventually fail if nothing is done to overcome the reason for the network or phase failure. You can be pro-active in setting alerts for repetitive phase and/or network failure to take appropriate action before the entire job fails.
<Device> Offline

Media Management | Device Status

Library, mount paths, or tape devices that are taken offline intentionally, or by themselves due to some problem can have significant impact on your ability to complete jobs in a timely manner. CommVault’s CommCell Readiness Report checks for device status and should be run before each data protection window. However, for more real time notification we recommend you set an alert for offline status of key devices.

**Best Practices**

When possible, configure alerts to cover Client Computer Groups vice individual clients and when using the E-mail output option, use group e-mail addressing vice individual users. Groups are more consistent and won’t require you to modify alerts when individual Clients or users are removed or added.
CONFIGURING REPORTS
A variety of reports can be created, each tailored to a particular aspect of data management. Through filter criteria, you can customize each report to include only the data that is required. Report templates can be customized and are available to you to save, run, schedule, edit and view.

Classic reports on the CommCell Console collect comprehensive information about jobs, storage, data growth, and cost that administrators can use to troubleshoot the environment and ensure that service level agreements are consistently met. Reports on the Web Console are tailored for basic users and allow you to access job, storage, and cost information.

**Recommended Reports**

**CommCell Configuration Report**

The CommCell Configuration (formerly CommCell Summary) Report provides the properties of the CommServe® system, MediaAgents, clients, agents, subclients, and storage policies within the CommCell environment based on the selected filter criteria.

**Job Summary Report**

The Job summary report can be filtered to display jobs that are, or have been run in the CommCell environment.
Data Retention Forecast and Compliance Report
The Data Retention Forecast and Compliance Report provides a history of data protection jobs, associated media, data aging forecast and recyclable media based on the selected filter criteria. Note that regardless of the filter options selected for this report, the report always checks retention in days.

Media Information Report
The Media Information Report provides detailed information about the media that is associated with storage libraries, the media repositories and/or locations, and the media that has been written to or reserved by storage policy copies, all within a specified time range.

CommCell Readiness Report
The CommCell Readiness Report provides you with vital information about the condition of your CommCell environment that can serve as a tool to warn you about potential problems that can impact your operations before they occur.
Module 7

Working with Support
Topics

Before you call Support
- Troubleshooting Methodology
- Viewing Job Details
- Using the Event Viewer
- Understanding Logs

Submitting a Trouble Report
- TR Submission Process
- Support's Top 10
BEFORE YOU CALL SUPPORT
Chefs can create tasty dishes without a recipe; Mechanics can diagnose and fix cars without fancy machines or manuals; and artists can create wonderful paintings without paint-by-number guides.

**What do they have that we don’t?**
They have experience to guide them - experience that comes with time and practice.

Without experience we can still solve problems. We just need to substitute something for experience. For chefs it’s a recipe; for mechanics it’s a manual; and for troubleshooting, this guidance is called a methodology. It’s really all the same. While it might seem tedious and time-consuming at first, it will always find a solution.

Without a methodology, troubleshooting efforts will be different each time. While this may sometimes solve problems, it’s a hit-or-miss proposition that does little towards reducing future troubleshooting efforts or contributing to your collective experience.

The basic Troubleshooting Methodology is universal. Following the sequence of steps each time leads you closer to a solution. Documenting each solution in terms of symptoms and cause helps you to more quickly resolve a problem in the future when similar symptoms arise.
Gather Information

Time and description of problem
Note when the error first occurred since this is a key identifier in tracking down relevant information from other sources – both in and outside of the Simpana® software. Describe the problem both in general terms and in specifics as reported by the software. This would include the exact text of the error that alerted you to the problem in the first place.

Pertinent Job details
Note the type of job, job id, start time, phase, state, etc. These details along with the time and problem description will help you when you try to narrow down the probable source of the problem.

Applicable Events
Find any and all events that may be applicable to the error.

Involved Resources/Components
Identify all involved hardware and software components.

Relevant Log Entries
Collect all log entries relevant to the job/task that had problems.

Other Concurrent Activity
Look at events/status from other jobs that were running at the same time.

Environment
Look for any external factor (e.g., storm, power failure, or other system issues) that may be a factor.

Narrow Probable Source

Is this a known problem?
There is nothing worse than expending time and effort troubleshooting a problem that is known and already has a solution – or no solution. Check your documentation, product knowledge base, product release notes, patches, and documentation.

Is this a pattern/re-occurring problem?
Does this error occur repeatedly? Does it occur at the same time? Same place? Is there a pattern? What is common in the pattern? Elusive, sporadic errors are the most difficult to isolate.

Has it worked before?
Look at the job history. If the operation/procedure has worked successfully before, then something has changed to make it fail. If it has never worked before, the problem is most likely in the installation or configuration of one of the components involved.
What’s changed since it last worked?
Have you changed security (e.g. password/permissions); paths (IP address, hostname, data locations, MediaAgent, library, and media); job characteristics (content, filters, storage policy, encryption, compression, etc.). If the working environment has changed since the last successful job, it would be the probable source of the problem. If not, then the problem may be an unknown change or component related.

Do other jobs work from/to the client?
If this problem has to do with data protection/restore, do similar jobs to/from client work? If not, the client is the probable source of the problem. If other jobs do work, then the problem may be Agent or subclient specific or it may be somewhere outside the client.

Do other jobs from/to that MediaAgent work?
If this problem involves a MediaAgent, do other similar job to/from that MediaAgent work? If not, the MediaAgent is the probable source of the problem. If other jobs do work, then the problem may be with a particular drive or media or it may be somewhere outside the MediaAgent.

Eliminate Simple Causes
Always check the simple causes first. These usually take the least amount of time.

- Check that all devices have power and are in a ready operational state.
- Check that all required services are started and running correctly.
- Check cabling, connectors, controls, zoning, masking, and ports. Can all devices see each other properly?
- Check that both forward and reverse host names are resolved correctly.
- Check that all drivers and firmware are up to date and compatible with each other.
- Check OS and application access.
- Check that sufficient spare media is present and that it’s good spare media.

Apply one Solution at a time
Changing multiple settings/conditions at the same time may fix the problem, but it will not enable you to determine the cause and take preventive action against future errors of that nature.

Always record the current state. In some cases, an applied solution may cause additional errors. Now it’s a battle to get back to your previous state and your original problem.

Try the most probable solution first. If this is not an easy solution, you may want to try other solutions that are easier or least disruptive first in order to eliminate them.

Always record the effect of a solution. Even if it does not solve the problem, it may have either positive or negative effect on the application. If new errors are generated, you can then associate them with the current state.
If applicable, back out each solution before trying the next. If all the simple causes have been eliminated, and any software changes identified and addressed - rarely will an error be the result of multiple concurrent software conditions.

**Document**

Documentation records the history of errors, troubleshooting efforts, and solutions. Some errors can only be resolved by recognizing patterns. For example; backups run fine for a client except on the first Friday of each month. It just so happens that another application runs a particular process on that day that causes port conflicts. The offending process may not be found without recognizing that there is a pattern of errors.

To give users a better chance of resolving future errors quicker, maintain good troubleshooting records.
Viewing Job Details

General
• Reason for job failure

Details
• Data Transfer statistics

Attempts
• Phase status
• Number of Attempts

Events
• Related Events

In gathering information for troubleshooting, one of your prime sources of information will be the Job Details dialog box. Job Details is available by right-clicking on the job in the Job Controller (if it’s still there) or in the History view and selecting Job Details.

• **General** Tab you may see a Reason for job Failure.
• **Details** Tab you can see job statistics and if there were any objects that failed to backup or restore.
• **Attempts** Tab you can see which phases of the job completed and which phases may have required multiple attempts to complete – or failed to complete.
• **Events** Tab you can see any job related Events.

Note that job failures may be caused by external events not associated with the job directly. While Job Details is the place to start looking, the information you need may require expanding your search.
The Event Viewer allows you to monitor multiple activities that are occurring within the CommCell® environment over a period of time. In your quest to gather information, the event viewer can help you know if there are issues outside of a particular job that may be causing problems.

Events are displayed in the Event Viewer with the severity levels of Information, Minor, Major, and Critical, along with additional information, such as the subsystem that generated the event. You can modify the types of events to be displayed based on the severity level by setting filters in the User Preference control applet.

By default, the number of events displayed in the Event Viewer is 200. You can modify this number in the User Preference control applet. A max of 1000 events can be displayed. The default total number of events retained is 10,000. This value can be changed in the Control Panel’s System applet. You can search events by job ID, severity, and/or time frame. The search will include all retained events. A more in-depth search using Find can be run in the search results window if you want to search for word/phrase patterns.

Some search queries can be saved and selected at any time from the Select from this search query field. A search query based on a particular Job ID cannot be saved.

As part of preventive action against future occurrence of similar problems, you can set alerts to be sent if a particular event happens again.
Understanding Logs

Operation Logs
- Found in <Install Path>\Log_Files directory
- Self Maintaining

Installation Logs
- Found in %TEMP% directory or
- %PROGRAMDATA%\Galaxy\Log_Files

Most Common Errors
- Host name resolution
- Insufficient space
- Permissions

Logs enable experience support/development personnel to view a job’s historical detail software processes and their results. Logs are not intended to be read/interpreted by customers.

CommVault® software Log files can be classified into four functional areas:

- **Service** – Record of installed services interaction with hardware, OS, applications, and other CommCell hosts.
- **Job Phase** – Record of Task level activity required to execute a job.
- **Administration** – Record of activity associated with the CommCell environment internal operations such as licensing, updates, data aging, firewalls, and metadata protection.
- **Installation** – Record of component installation activity.
CommVault software Log Files are present on each component. On Windows hosts, the log files can be found in the `<Install Home>\Simpana\Log Files` directory. On UNIX\Linux hosts, the log files can be found in the following directory:

`/var/log/galaxy/Log_Files`

In NetWare, log files can be found in the following directory:

`(SYS:\Simpana)`

**Self-Maintaining**

Log files have a default maximum size of 5 MB and most have a default version retention level of 1. Version retention means the number of full logs kept plus the active log. Once an active log reaches maximum size, it is renamed to `<filename>_#.log` where # represents the version. If only one version is being retained, the next full log will overwrite the previous full log.

Because of the expected activity levels, the communication service (CVD) and media management logs have a default version retention level of 3. CVD Log sizes and version retention can be changed via registry values. Media Manager log size and version can be changed via the Service Configuration tab of the Media Management control in the CommCell Console.
SUBMITTING A TROUBLE REPORT
Having exhausted your own troubleshooting efforts, you may want to open a Trouble Report (TR) with your support group. A TR can be initiated by phone or via e-mail. You can create an e-mail TR from the CommCell Console itself. Alternatively you can use the e-mail TR form available on CommVault’s web site. If you use the form via the Maintenance Advantage portable, the key information fields will automatically be populated.

Each TR passed through a Level I support review to see if the problem is procedural in nature, or is a known problem with a solution. TR’s that pass through Level I are assigned to a specialty area (Level II) for a more focused look into the problem. If Level II support cannot identify or resolve the problem, then Level III escalation into development is made.

The most common thing asked for by support when troubleshooting will be the log files. These will enable support to recreate the events leading up to and during the problem. Since the cause of the problem may be peripheral to the event itself, all logs from the CommServe and any involved component hosts are usually requested. In the CommCell Console, at the CommCell level of the browser, you’ll find the “Send Logs” task.
The following is a list of common problems based on the number of calls made to customer support.

10. Known Problems
   - Documented in Release Notes
   - Documented in the CommVault Online Documentation
   - Usually, no resolution. Sometimes possible workaround

9. Software Conflicts
   - Anti-virus
   - Other Backup products
   - Previous Simpana® software Installations

8. Anomalies
   - Works fine the second time
   - Erratic – no pattern of failure
   - Possibly attributable to timeouts
   - Reboot/Restart Services/Process to correct

7. Permissions Related Issues
   - Install or first use problem
   - CommServeDR or Mapped Drive Access
   - Exchange Login ID/Password
   - SQL Login ID/Password
   - Oracle Login ID/Password
6. Network Related Issues
   - DNS
   - NIC Drivers
   - NIC Hardware Problems
   - NIC Software Settings
   - Multiple NICs

5. Services / Job Management
   - Failed to restart on reboot
   - Improper start order
   - Dependency services not running
   - Conflict with other services

4. Performance Issues
   - Expectations vs. Reality
   - Inadequate resources
   - Competition for resources

3. Library/Drive/Media
   - Library/Drive offline
   - Drive dirty/error
   - Mount/Unmount Error
   - Timeout
   - Physical/Logical inconsistency
   - Out of Spare Media

2. Restore/ Index Issues
   - Index not available
   - Index Cache corrupt
   - Timeouts

1. User Training
   - Lack of understanding for Storage Policies
   - Lack of understanding for Subclients
   - Lack of understanding for Content Indexing
   - Lack of understanding for Deduplication
   - Lack of understanding for Restore options/steps
   - Lack of understanding for Media Management
Please give us your feedback!

To give us feedback on your course:

- Login to your EA account (ea.commvault.com)
- Select the lab for Courses Completed
- Click on the icon to fill out the Course Evaluation

Thank You!
Index

Active Directory, 119
Activity Control, 128
Administration jobs, 125
Alerts, 50, 151
Archive, 104
Archiving, 113
  Application Archiving, 115
  Domino Mailbox, 116
  Exchange Mailbox, 115
Ask the Educator, 17
Backup, 104
Backup Set, 102
Certification, 14
chunks, 56
Client Computer Group, 39
Clients, 102
Command Line Interface, 29
CommCell console, 26, 33, 147
  CommCell browser, 32
  Event Viewer, 165
  Floating Windows, 34
  Hiding the CommCell® Browser, 34
  Job controller, 147
  Moving Tabbed Windows, 34
  Viewing Job Details, 164
CommCell Updates, 44
CommCell User Group, 36
CommCell Users, 36, 58, 59
Common Technology Engine, 21
CommServe, 41
  Disaster Recovery Backup, 41
  DR Storage Policy, 42
CommVault® Advantage, 11
Compression, 111
Copy Precedence, 139
CVLab, 16
DASH Copy, 82, 97
  Disk Read Optimized, 97
  Network Optimized Copy, 98
DASH Full, 82, 133
data pipe, 54
Data Protection, 47
Data protection jobs, 125
Data Recovery, 125
  Browse, 136
  Find, 135
  Full System Recovery, 142
  Restore by Job, 138
Deduplication, 78, 111
  block size, 60
  Block size, 80
  Client Side, 82
  Compression and databases, 81
  dedicated deduplication storage policy, 78
  Deduplication Building Blocks, 60
  Deduplication Database, 55
  Deduplication Store, 81
  Global Deduplication, 75
  Global Deduplication storage policy, 79
  Sealing the Store, 81
  Store Priming, 98
Disk libraries
  Fill & Spill, 59
  mount path writers, 59
  Replicated, 58
  Shared disk libraries, 58
  Spill & Fill, 59
Disk Libraries, 58
Education Advantage, 10
Education Services Forum, 12
Encryption, 111
filters, 117
Image Files, 137
Indexing, 56
  Index Cache, 56
Java™ Runtime Environment, 26
Job controller, 129
  Viewing Job Status, 48
Job Controller, 48
Job priority, 127
Job Streams, 110
Learning Bytes, 17
Logs, 166
MediaAgent, 54
OnePass, 112
Operation Window, 128
Qcommands, 29
Replication, 104
Reports, 50, 155
Restore, 135
Restore By Job, 138
Retention, 84
  Aging Deduplicated Data, 93
  Aging Rules, 88
  Data Aging, 87
  Object Based (Subclient) Retention, 91
  Pruning, 87
  Sample Retention Policy, 86
Schedules, 49
Scheduling, 126
Security
  External Users, 36
  System (Client) Owner, 38
  User Group, 36
Service Packs, 44
Snapshots, 105
Storage Policies, 73
  Disaster Recovery, 75
  Secondary Copies, 95
  Selective Copy, 75
  Snap Copy, 76
  Standard, 75
  Synchronous Copy, 75
Subclient Policy, 121
Subclients, 103, 107, 121
  Identifying Data Content, 107
  Scanning, 108
Synthetic Full, 132
System state, 119
Tape libraries, 63
  Dynamic Drive Libraries, 64
  Maintenance, 65
  Robotic, 63
  shared, 64
  Standalone, 63
Tape media, 66
  Appendable, 66
  Assigned Media Pool, 67
  Capacity, 67
  Duplicate Barcode, 67
  Export Media, 69
  Media Handling, 68
  Undiscovered, 66
TR Submission Process, 169
Training Units Calculator, 17
Troubleshooting, 160
Vault Tracker, 69
Web Console, 28
Windows, 119