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

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

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

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

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

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

©1999-2017 Commvault Systems, Inc. All rights reserved

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

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

Legal Notices .......................................................................................................................... 2  
Table of Contents .................................................................................................................. 3  
Introduction .................................................................................................................................. 6  
Commvault® Core Fundamentals Course Preliminaries ................................................................. 7  
   Education Advantage ................................................................................................................ 8  
   Class Resources ....................................................................................................................... 9  
   CVLab On Demand Lab Environment ....................................................................................... 10  
   Commvault® Education Career Path ....................................................................................... 11  
Education Services V11 Certification ............................................................................................ 12  
Automated Proactive Solutions System (APSS) ........................................................................... 15  
   Welcome to Commvault ........................................................................................................... 16  
   Course Overview .................................................................................................................... 17  
Commvault® Software Overview .................................................................................................. 18  
   A New Vision for Data and Information Management ............................................................ 19  
   Where Does Commvault Fit? ................................................................................................... 20  
Commvault® Software Overview .................................................................................................. 22  
Content Store .............................................................................................................................. 23  
Physical Architecture .................................................................................................................. 24  
Logical Architecture .................................................................................................................... 26  
Module 1: CommCell® Administration ....................................................................................... 27  
CommCell® Administration Overview .......................................................................................... 28  
   CommCell® Console ................................................................................................................ 29  
   Admin Console....................................................................................................................... 32  
Security .......................................................................................................................................... 33  
   User and Group Security ........................................................................................................... 34  
   Role Based Security ................................................................................................................ 35  
   User Quotas ............................................................................................................................ 36  
   Client Computer Group Quotas ............................................................................................... 37  
   Exchange Mailbox Backup Quotas ........................................................................................... 38  
CommCell® Administrative Tasks ................................................................................................. 39  
   CommServe® DR Backup ........................................................................................................ 40  
   CommCell® Update Process ...................................................................................................... 42
<table>
<thead>
<tr>
<th>Subclient Design Strategies</th>
<th>.................................................................</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module 5: Data Protection and Recovery</td>
<td>........................................................................</td>
<td>113</td>
</tr>
<tr>
<td>Data Protection</td>
<td>........................................................................</td>
<td>114</td>
</tr>
<tr>
<td>Data Protection Overview</td>
<td>........................................................................</td>
<td>115</td>
</tr>
<tr>
<td>Job Initiation</td>
<td>........................................................................</td>
<td>118</td>
</tr>
<tr>
<td>Synthetic Full and DASH Full Jobs</td>
<td>........................................................................</td>
<td>119</td>
</tr>
<tr>
<td>Auxiliary Copy and DASH Copy Jobs</td>
<td>........................................................................</td>
<td>121</td>
</tr>
<tr>
<td>Using Schedules and Schedule Policies</td>
<td>........................................................................</td>
<td>123</td>
</tr>
<tr>
<td>Automatic Schedules</td>
<td>........................................................................</td>
<td>129</td>
</tr>
<tr>
<td>Managing Active Jobs</td>
<td>........................................................................</td>
<td>131</td>
</tr>
<tr>
<td>Controlling Job Activity</td>
<td>........................................................................</td>
<td>133</td>
</tr>
<tr>
<td>Data Recovery</td>
<td>........................................................................</td>
<td>137</td>
</tr>
<tr>
<td>Data Recovery Overview</td>
<td>........................................................................</td>
<td>138</td>
</tr>
<tr>
<td>Using Find</td>
<td>........................................................................</td>
<td>140</td>
</tr>
<tr>
<td>Using Browse</td>
<td>........................................................................</td>
<td>141</td>
</tr>
<tr>
<td>Pie Chart Browse View</td>
<td>........................................................................</td>
<td>143</td>
</tr>
<tr>
<td>Additional Recovery Methods</td>
<td>........................................................................</td>
<td>144</td>
</tr>
<tr>
<td>Module 6: Monitoring</td>
<td>........................................................................</td>
<td>146</td>
</tr>
<tr>
<td>CommCell® Monitoring Resources</td>
<td>........................................................................</td>
<td>147</td>
</tr>
<tr>
<td>Alerts</td>
<td>........................................................................</td>
<td>150</td>
</tr>
<tr>
<td>Reports</td>
<td>........................................................................</td>
<td>152</td>
</tr>
<tr>
<td>Thank You</td>
<td>........................................................................</td>
<td>154</td>
</tr>
</tbody>
</table>
Introduction
Commvault® Core Fundamentals Course 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 Commvault® 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!
Class Resources

Log on to EA 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.

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.
**CVLab On Demand Lab Environment**

**CVLab Details:**
- Available during and after class
- Available for purchase in blocks of four hours
- Use to practice labs or as a sandbox to test configurations

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 Commvault® 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.
Commvault® Education Career Path

Suggested learning path for administrators and engineers

The Commvault next generation platform leapfrogs legacy solutions in capabilities and functionality fully modernizing the performance, security, compliance, and economic benefits of a holistic data management strategy. The key concepts covered in this first step learning module highlight the core features of Commvault’s new platform. To realize the full value of these features, Commvault provides multiple levels of education and certification from core training, through specialized learning sessions, from introductory modules for those new to Commvault to master level training for Commvault power-users.

Additional Training Offerings:
- Commvault New Features Course
- eDiscovery Compliance Search
Education Services V11 Certification

Commvault's Certification Program validates expertise and advanced knowledge in topics, including Commvault Core Fundamentals, Implementation and Maintenance, and more advanced Specialist, Engineer 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, Engineer-level, and Master-level certifications. This Program provides certification based on a career path, and enables advancement based on an individual’s previous experience and desired area of focus. It also distinguishes higher-level certifications such as Engineer and Master 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.
- The Commvault Certified Professional Exam Prep course is also available.
- Students may take the online certification exam(s) any time after completing the course.
- Although it is recommended to attend training prior to attempting an exam, it is not required.

Commvault Version 11 Certification Exams

- Core Fundamentals
- Implementation and Maintenance
- V11 Professional Upgrade Exam
Advanced Infrastructure Design
Virtualization Specialist (June, 2016)
Commvault Master Exam (June, 2016)
Master Exam Upgrade Test (June, 2016)

Retired exams:
Disaster Recovery Specialist

Commvault Certified Professional

A Commvault Certified Professional certification validates the skills required to install, configure, and administer a CommCell® environment. It proves a professional level skillset in all of the following areas:

- CommCell Administration – user and group security, configuring administrative tasks, conducting data protection and recovery operations, and CommCell monitoring.
- Storage Administration – deduplication configuration, disk library settings, tape library settings, media management handling, and snapshot administration.
- CommCell Implementation – CommServe® server design, MediaAgent design and placement, indexing settings, client and agent deployment, and CommCell maintenance.

Certification status as a Commvault Certified Professional requires passing two exams: Commvault® Core Fundamentals and Implementation and Maintenance Exams.

Commvault Certified Engineer

A Commvault Certified Engineer validates advanced level skills in designing and implementing Commvault software.

- Advanced Infrastructure Design – this exam validates expertise in deploying medium and enterprise level CommCell® environments with a focus on storage design, virtual environment protection, and application data protection strategies.

Certification status as a Commvault Certified Engineer requires certification as a Commvault Certified Professional and passing the Advanced Infrastructure Design exam.

Commvault Certified Specialist

A Commvault Certified Specialist validates skills in a specific area of expertise:

- Virtualization – This exam validates expertise in protecting and managing virtual environments using the Virtual Server Agent, application agents, hardware snapshots, Virtualize Me and VM lifecycle policies.

Certification status as a Commvault Certified Specialist requires certification as a Commvault Certified Professional and passing the Virtual Data Management exam.

Commvault Certified Master

A Commvault Certified Master validates expert level skills in specific areas of expertise. This is the highest achievable level of certification.

Certification status as a Commvault Certified Master requires certification as both a Commvault Certified Professional and Certified Specialist, and successful completion of Master certification requirements. These Master certification requirements include attending a Master class and passing the Master Certification exam.

Additional benefits of attaining the Master Certification include:
• Opportunity to attend free invitation only training events
• Opportunity to attend free early release training courses
### Automated Proactive Solution System (APSS)

**APSS Features:**

- Real-time health monitoring
- Notify administrators on conditions in their environment
- Provide automated or user initiated healing measures
- Dashboard provides comprehensive high level view of CommCell health

---

The Commvault® Automated Proactive Solution System (APSS) is a revolutionary tool providing real-time monitoring and automated healing capabilities. The system uses workflows and custom scripts to collect and analyze data and proactively provide solutions to issues in a CommCell® environment. This active system will notify Commvault administrators on health issues and allow them to enable APSS automatic healing.

Commvault administrators can view issues and APSS solutions using the Proactive Support icon in Maintenance Advantage. When issues are detected by the APSS system, a pop-up notification is displayed in MA allowing the user to dismiss the notification or display solutions. Automated solutions can be applied by downloading and deploying the corresponding APSS solution workflow.

The APSS dashboard provides a comprehensive overview of their CommCell environment. CommServe database health, SLA charts, job summary, system alerts, and open incidents can be viewed. Additional custom widgets can be added to the dashboard.

To start using APSS, log on to Maintenance Advantage (MA) and complete your user profile. Download and install the APSS application.
Welcome to Commvault

Benefits:

- Sent out with Maintenance Advantage Welcome Message
- Assist new customers and administrators with:
  - Maintenance Advantage
  - Education Advantage
  - Commvault Terminology
  - Installation
  - Additional Resources

The WELCOME TO COMMVAULT interactive introduction provides web-based information to help you get the most of your total Commvault experience. This program is intended for those new to Commvault and enables you to better use our support processes, knowledge materials, and learn the basics of Commvault® software. This 20 minute program is your map to understanding Commvault's support, education, and online resources and immediately improves our success in working together. Click the graphic below to get started.

http://download.commvault.com/unsecure/welcome-to-commvault/
Course Overview

Module Breakdown:

1. CommCell® Administration
2. Storage Configuration and Media Management
3. Storage Policies and Retention
4. Client Administration
5. Data Protection and Recovery
6. Monitoring

Course Objective

This course is intended for personnel responsible for day-to-day administration and management of Commvault® software. The course covers essential concepts, details, options, and best practices for user security and management, system settings, policy configuration and use, media and library management, job activity and status monitoring, and job management. Students also learn how to efficiently and effectively manage data movement (backup, archive, auxiliary copy, and restore) within a CommCell® group.

This course is intended for personnel responsible for day-to-day administration and management of Commvault® software. The course covers essential concepts, details, options, and best practices for user security and management, system settings, policy configuration and use, media and library management, job activity and status monitoring, and job management. Students also learn how to efficiently and effectively manage data movement (backup, archive, auxiliary copy, and restore) within a CommCell® group.
Commvault ® Software Overview
A New Vision for Data and Information Management

Commvault® Next Generation Platform

Proactively addressing industry needs

1. Open standards-based infrastructure
   - Instant access to data via industry standards-based interfaces

2. New recovery mandates
   - Always on and always available

3. Traditional backup increasingly unable to meet today’s demands
   - Too much data to protect, manage and secure

4. Extensible analytics built-in
   - More value from data via secure global federated search & analytics

5. Access & collaboration
   - Seamless, universal secure access to all copies of users’ data

6. Governance from inception
   - From moment data is created, it needs to be under managed control

Commvault’s next generation platform fundamentally redefines data protection, archive and cloud data management, creating a platform where everything is application aware, backup windows are significantly reduced, and instant recovery is standard. Through advanced data analytics, block level intelligence, and robust automation and orchestration capabilities, Commvault assists customers of all sizes in the transformation from traditional legacy and point products to a modern hyper-converged infrastructure.
Where Does Commvault® Fit?

How does Commvault’s next generation data management platform enable your enterprise to be successful in its transformation to a services oriented architecture?

Consider legacy and point products which focus on traditional protection methods such as tape and disk storage with off-site copies for disaster recovery purposes. These solutions may lack complexity but in a modern world, fail to align with the overall realities of a modern IT infrastructure.

Data management is only as valuable as the effective ability to access the data. High availability solutions including clustering, replication, snapshots and virtualization provide added value through quick recovery times and more frequent recovery points. The complexity to manage all of these solutions, however, increases without a centralized management system.

Cloud solutions enhance high availability and disaster recovery even though the platform is still sufficiently “new”, there is a lack of standards on information management and protection.

Commvault software overcomes the complexity in managing data protection and data access through its next generation platform. The industry’s largest supported number of hardware vendors, cloud providers, and virtualization solutions are all managed through Commvault’s central platform improving data availability and recovery times.

Data protection and access, however, only tell “half the story”. The ability to share data across all devices, including mobile BYOD devices and endpoint access from any system, using native applications such as Windows Explorer, Outlook, or standard web browsers should be ubiquitous for end users. Commvault software provides all of these capabilities with intuitive “instant learn” end user features.
Finally, for many organizations, especially those with hybrid data services with content in the data center, as well as hosted or As a Service, Compliance of managed data may be the most complex solution to implement but it provides the highest value. Intelligent legal holds, records management, analytics, eDiscovery and data loss prevention can all be centrally managed through Commvault’s next generation platform.
Commvault® software streamlines all data and information management operations within a centralized platform called the Common Technology Engine. This engine functions at the core of Commvault - integrating software components that protect, store, index, and retrieve data. The indexing layer provides seamless access to data regardless of where the data is stored. Administrators manage backend functions such as backup and recovery, scheduling, and monitoring using a single graphical user interface. End users can access protected data using web browsers, or perform tasks using their mobile device.

Commvault comprises the following data and information management capabilities:

- **Data Information and Access** – Documents and messages are retrieved seamlessly from mobile devices, web pages, and native application tools.
- **Storage** – Data is protected and stored on disk, tape, and cloud storage locations. Advanced features such as deduplication to disk and tape, job and object retention, and independent multiple copy management are used to meet all Disaster Recovery (DR) and compliance requirements.
- **Indexing** – A distributed self-protecting indexing structure maintains metadata information for all protected data. Additionally, content indexing can be used to provide detailed content searches for files and Email.
- **Data Protection** – File system and application agents are deployed to production systems to protect all major operating systems and applications.
- **Administration** – Administrative tasks are centrally managed through a single administrative interface. Tasks can also be performed from mobile devices and web pages.
- **Management** – All activity is centrally controlled and managed using a common code base. Whether using traditional backups, replication, archiving, or snapshots to protect physical or virtual environments; the same core technology is used providing a solid and flexible management platform.
The Commvault next generation platform structures all managed data in virtual containers using the Content Store. The content store is a storage abstraction that allows for data that resides within it to be viewed as a single entity, no matter where that data is otherwise stored.

Data in the Content Store is protected and retained in the storage layer. Functionality, including deduplication, archiving, hardware snapshot management, and FIPS certified encryption, securely protect data to disk, tape and cloud storage. Protected data can be replicated, mirrored, and synchronized to secondary storage devices for near instant access.

The indexing layer of the Content Store maintains lightweight metadata indices for object management and retrieval, as well as content indices for end user and compliance searches.

All protected data and indices are accessed through the security layer which features full role-based access control security. Commvault security provides granular access control and distributed security roles, allowing users access only to what they need and managers to assign permissions to their groups.

Access is granted to users to retrieve or restore data using web consoles, mobile devices and endpoint applications. Compliance tools include content-based eDiscovery, Case Manager, Legal Hold, and data analytics. And all data managed in the Content Store is sharable through the security layer and accessed at the console or any number of secure endpoints.

The Commvault next generation platform provides a fully integrated software suite guaranteeing flexibility in infrastructure, platform, compute, and storage providers. Now, with a basic understanding of Commvault’s value and Content Store architecture, let us review the core technologies of the Commvault platform.
Physical Architecture

Commvault software is deployed in a cell-like structure called a CommCell® environment. One or more cells can be deployed to manage small to enterprise global environments. The central component of a CommCell environment is the CommServe server which coordinates, manages and monitors all CommCell activity. Production data is protected by installing agents which directly communicate with the operating system or application being protected. Any production server with an agent installed is referred to as a client. Data is protected by transferring data through MediaAgents to storage which can be disk, cloud or tape.

CommServe Server

The CommServe® Server is the central management system within a CommCell environment. All activity is coordinated and managed by the CommServe server. The CommServe system runs on a Windows platform and maintains a Microsoft SQL metadata database. This database contains all critical configuration information. It is important to note that Commvault software does not use a centralized catalog system like most other backup products. This means the metadata database on the CommServe Server will be considerably smaller than databases that contain catalog data. Due to the small size of the database, an automated backup of the database is executed by default every morning at 10:00 AM.

MediaAgents

A MediaAgent moves data from production systems to protected storage during data protection jobs and moves data back to production systems during recovery operations. It is a software module that can be installed on most operating systems. All of its tasks are coordinated by the CommServe server. MediaAgents are also used during auxiliary copy jobs when data is copied from a source library to a destination library such as off-site DR copies.

There is a basic rule that all data must travel through a MediaAgent to reach its destination. One exception to this rule is when conducting NDMP dumps directly to tape media. In this case the MediaAgent is used to execute the NDMP
dump and no data will travel through the MediaAgent. This rule is important to note as it will affect MediaAgent placement.

**Indexing**

Commvault software uses a distributed indexing structure where index data is kept on MediaAgents and is also automatically copied to storage. Using a distributed indexing structure allows Commvault software to scale significantly more than legacy backup products and keeps indexes local to where data is being protected.

When data is protected, indexes are automatically generated and written to the MediaAgent’s Index Directory location. At the conclusion of the job, indexes or index logs are copied to the store location where the job resides. During restore operations, the index database within the index cache is accessed. If the index database is not available, it will automatically be restored from the storage media.

Commvault uses two primary indexing methods based on the agent being used. The traditional indexing method is currently used for all agents except file system data, Oracle and the new Exchange mailbox agent. The new V2 indexing method is used for Windows and Linux file systems.

**Libraries**

**Disk library**

A disk library is a logical container which is used to define one or more paths to storage called mount paths. These paths are defined explicitly to the location of the storage and can be defined as a drive letter or a UNC path. Within each mount path, writers can be allocated which defines the total number of concurrent streams for the mount path.

**Tape Library**

A tape or removable media library is a library where media can be added, removed and moved between multiple libraries. The term removable media is used to specify various types of removable media supported by Commvault software including tape and USB disk drives which can be moved between MediaAgents for data protection and recovery operations.

**Cloud Library**

A cloud library is a container which leverages object-based storage. It provides an easy to configure offsite copy using a supported cloud storage provider. This type of library is frequently used to replace a compliance offsite tape copy, or to protect an active server workload hosted in the cloud.
Clients and Agents

A Client is any production system that is protected by Commvault software. Clients will use agents to protect the production data by installing the agent directly on the client or using a proxy client to protect the data. When an agent is deployed to a client, the client will appear in the CommCell Browser under the Clients entity.

Agents can be deployed in several ways.

- Physical clients can have agents installed directly on them.
- Virtual clients can have agents installed directly on them or protected by the Virtual Server Agent (VSA) which would be installed on a physical or virtual proxy server.
- NAS storage devices which cannot have software installed directly on them can be managed and protect by installing NAS agents on proxy servers.

Subclients

Subclients are used to define data that will be protected in a containerized format. Each subclient container will manage specific content within a backup set. Each backup set will have one or more subclients.

Storage Policies

The Commvault® product suite offers a wide range of features and options to provide great flexibility in configuring and managing protected data. Protection capabilities such as standard backup, snapshots, archiving and replication can all be incorporated in a single environment for a complete end-to-end data protection solution. No matter which methods are being used within a Commvault® environment, the concepts used to manage the data remain consistent.
Module 1: CommCell® Administration
CommCell® Console

Key Points:

- Accessing
  - Local install
  - Web based access

- Navigating

- Customizing
  - Tabbed windows
  - Float windows
  - Hide browser

The CommCell® console is the central management graphical user interface used to configure the CommCell environment, monitor and control active jobs and view events related to all activities. The console can be accessed using local CommCell accounts or by using Active Directory integrated account authentication.

The CommCell Console is made up of the following windows:

- CommCell Toolbar provides an easy to navigate 'ribbon' to manage and configure the CommCell environment.
- CommCell Browser is the main navigation window which contains a hierarchal structure of all categories and components within the CommCell environment.
- Content / Summary window provides details based on what component is selected in the CommCell Browser.
- Job Controller provides viewing and control capabilities for all active jobs in the CommCell environment.
- Event Viewer provides information for all logged events within the CommCell environment.

Accessing the CommCell® Console

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.

Navigating the CommCell® Console

CommCell® Toolbar

The CommCell Console uses a ribbon style toolbar to provide more efficient navigation and configuration. Configuration options are organized within the toolbar to provide quick access to perform common tasks. By setting mouse focus on the toolbar, the scroll wheel on the mouse can be used to quickly move through the different toolbars available. The toolbar can also be hidden by clicking the up arrow in the upper-right corner.

CommCell® Console Browser Window

The CommCell Browser is the primary window used to navigate and configure CommCell components. The browser provides two views: Browser (default) view and Agents view. The navigation is hierarchal in nature and through properties pages, most settings can be customized through the CommCell Browser.

Content / Summary Window

The Content / Summary window provides information specific to what is selected in the CommCell Browser. Depending on what object in the browser has focus, the Content / Summary windows provide the following information:

- **Content** – displays contents contained within the object selected.
- **Summary** – displays an overview summary of the object selected.
- **Extended Summary** – when specific objects in the browser are selected the extended summary view provides greater detail than the summary view.
- **Feature View** – for specific objects, features related to the object will be displayed.

Job Controller Window

The Job Controller provides monitoring functionality for all active jobs within the CommCell® environment. Jobs will remain in the Job Controller for five minutes after the job completes, fails or is killed.
Event Viewer Window
All Commvault software related events are reported in the CommCell Event Viewer. By default, 200 events are displayed in the event viewer but the event log will maintain up to 10,000 events or 7 days of events. These options can be configured in the System Settings applet in the Control Panel.

Customizing the CommCell® Console

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.

Hide Browser Window
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.
Admin Console

Key Points:

- **Purpose**
  - Simplified administration
- **Accessing**
  - Web based access only
- **Navigating**
- **Use Cases**
  - Power users
  - System administrators

The admin console is a web based console that provides tools to configure, backup and restore client servers. It provides a simplified method of managing the Commvault environment. The purpose of the console is to provide the essential tools to administrators or power users to efficiently configure and manage backups and restores for their systems without being overwhelmed by options and tools that are irrelevant to their work. Available options and actions for each user are defined through security rules, similar to the traditional CommCell® console.

The admin console is not a total replacement for the CommCell® console, and the primary backup administrators should continue using the traditional console. The admin console currently supports the following clients and agents:

- File System (Windows and Linux/UNIX)
- Databases (Microsoft® SQL, Oracle®, SAP HANA)
- Virtualization (VMware®, Microsoft® Hyper-V, Nutanix® Acropolis Hypervisor)
- Endpoint

**Accessing the Admin Console**

Once deployed, the admin console can be accessed by using the following URL:

http://<admin console server name>/adminconsole

To access the appropriate admin console, click the switch tool icon in the upper left corner and choose the desired console.
User and Group Security

CommCell® V10 security works by assigning local users and Active Directory groups to CommCell user groups. These CommCell groups are then associated with entities in the CommCell browser to grant access to specific areas within the CommCell® console.

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.
Role Based Security

Key Concepts:

- Standard Security for V11
- Roles define permissions
- Role and user / user group associated with entity
- User group association is not required
- Users can be CommCell or Active Directory

Role based security transcends limitations of traditional user and user group security by separating the user or group from permissions.

Role based security is based on three components:

- **User or user group** – can be a local CommCell user / user group or domain user / user group
- **Role** – defines a set of permissions not tied to any user or user group
- **Entity** – the component that joins the user / user group with the associated role

The separation of user / user group (who), role (permissions), and entity (what) allows a user or user group to have different permissions depending on what their role is for a specific entity.

**Example:** A user requires backup and recovery permissions for a file server. The same user requires restore only permissions for a mail server. The user is associated with the file server entity and assigned the backup and recovery role. The same user is assigned to the mail server entity with the recovery role.

**Roles After Upgrading from Previous Version**

Prior to Commvault version 11, all permissions (formerly called capabilities) were associated with a CommCell user group. When upgrading Commvault software, a role will be created for each user group and permissions will be assigned to the role based on the capabilities of the old user group. For each user group, a role will automatically be created prefixed with `<UserGroup_Name>_Role`. These roles will automatically be assigned to entities along with the user groups.
**User Quotas**

- Applies to file system data
- Must be domain account
- Quotas can be set at group or user level
- User level quotas can override group quotas
- Warning message at 90%
- Backups stop at 110%

---

Domain users can have data protection quotas enforced for file based backups. Quotas can be set at the group or user level. If quotas are set at the group level, they can be overridden at the user level.

**How user quotas work:**

- When a user reaches 90% of their defined quotas, a warning Email will be sent to the user.
- When a user reaches 110% of quota, backups will not run for systems owned by the client.
- To fall below these thresholds, the user either must delete data or the Commvault administrator must increase the user’s quota.
Client Computer Group Quotas

Details:

- Requires to enable the use of quotas at the CommCell® level
- Desired quota is set at the client computer group level

Quotas can be applied to client computer groups. The quota is set at the client computer group level and it therefore adds up the size of each client that is a member of the group. This option is frequently used by Managed Service Providers (MSP) or in chargeback scenarios, when limited resources are shared amongst different business units or entities.
Exchange Mailbox Backup Quotas

Details:

- Applies to Exchange mailbox backup data
- Enabled at the Exchange Mailbox subclient level
- Mailboxes over the limit are skipped

Quotas can be applied to Exchange Mailbox backup data. In this case, quotas are configured at the Exchange Mailbox subclient level. Once set, the limit is applied to all mailboxes defined in the Content tab of the subclient.

How client computer group quotas work:

- When a mailbox is under the quota, it is protected as usual by the backup job.
- When a mailbox is over the quota, it is skipped during the backup job.
- To fall below these thresholds, the Commvault administrator either must delete data, increase the client computer group quota or simply remove the client computer from the group.
- When a mailbox reaches 90% of its defined quotas, a warning Email will be sent to the mailbox user.
- When a mailbox reaches 100% of the quota, an alert will be sent to the Commvault administrator.
- To fall below these thresholds, the mailbox user must delete data or the Commvault administrator must increase the subclient quota.
CommCell® Administrative Tasks
CommServe® DR Backup

Details:

- 10:00 AM default backup time
- Three phases:
  - Local DB dump
  - Export
  - Backup
- DR Backup Settings
- CommServeDisasterRecoveryGUI tool

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 to the following folder:

<installpath>\Commvault\ContentStore\CommServeDR

An Export phase 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 contains an Export Phase and a Backup Phase.

Export Phase

The Export phase 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 Phase
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 is not done the DR metadata will not be recoverable using the Media Explorer utility.
  - When storage policy secondary copy is created, ensure the DR metadata is included in the Associations tab of the policy copy.
  - Make sure you are properly running and storing media reports. This is especially 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.

**CommServe Recovery Assistant**

The CommServe Recovery Assistant tool is located in the base folder of the CommServe server. It is used to restore the metadata from the disaster recovery backup file. The CommServe Recovery Assistant Tool is used to rebuild the CommServe on the same or different server, change the name of the CommServe host and update the CommCell license.
CommCell follows a quarterly schedule for major service pack releases. Service packs are available initially for manual download from the Maintenance Advantage website and then moved to auto update via the Commvault software update cache process approximately two weeks after initial availability. Major Service packs should be deployed when available and Minor Service packs deployed when and as needed.

Commvault recommends keeping all CommCell® components up to date. Updates are released on a quarterly schedule and include all fixes and feature enhancements. An Email is sent to you when major service pack updates are available. Updates can be downloaded automatically from the CommCell console or through Maintenance Advantage.

Software and update cache locations can be configured as follows:

- Primary cache location where all CommCell resources pull software and updates unless configured to use a remote cache.
- Remote caches can be used as secondary cache locations which is beneficial for remote locations. Secondary caches can be set up on local clients at the location to pull software and updates locally avoiding additional WAN traffic.
Administrative Jobs and Schedules

- Schedule window
- CommCell schedules
  - DR backup
  - Data aging
  - Reports

The CommCell® scheduler window can be used to view all schedules.

Key points for the scheduler window:
- Filters can be applied to narrow the scope of view.
- Double-click on a day for a detailed view for all scheduled operations.
- Right-click a schedule to edit, delete or run the job immediately.
Client Computer Groups can be used to group like clients to simplify CommCell administration. Clients can be added to one or more computer groups.

There are several methods for adding clients to groups:

- During installation the client group can be selected.
- In the client group properties select the clients and include them in the group.
- In the client properties in the Group tab select the group or groups to add the client to.

Client Computer Groups provide the following benefits:

- Simplified navigation when locating clients within the CommCell console.
- Configuring user group security to manage entire computer groups.
- Simplified activity control such as enabling or disabling data protection or recovery for an entire group.
- Applying updates, bandwidth throttling, firewall configurations, etc... to entire groups at the same time.
- Executing schedule policies at the group level.
- Assigning computer groups when configuring reports and alerts will automatically add/remove clients when changes are made to the group.
Module 2: Storage Configuration and Media Management
MediaAgents and Indexing

Key Points:

- MediaAgent concepts
- Indexing
  - V1 indexing review
  - V2 indexing review
  - Index directory configuration
- CRC checks
  - Validate on media
  - Validate on network

The MediaAgent is the high-performance data mover which moves data from source to destination. It is a software module that can be installed on most operating systems. All its tasks are coordinated by the CommServe server. The MediaAgent moves data from a client to a Library during a data protection operation or vice-versa during data recovery. MediaAgents are also used during auxiliary copy jobs when data is copied from a source library to a destination library.

There is a basic rule that all data must travel through a MediaAgent to reach its destination. One exception to this rule is when conducting NDMP dumps direct to tape media. In this case the MediaAgent is used to execute the NDMP dump and no data will travel through the MediaAgent. This rule is important to note as it will affect MediaAgent placement.

Indexing

Commvault® 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 such as chunk information, which keeps the database relatively small. Detailed index information such as details of protected objects is kept on the MediaAgent managing the job.

Job summary data maintained in the CommServe database keeps track of all data chunks being written to media. As each chunk completes it is logged in the CommServe database. This information also tracks the media used to store the chunks.

How Indexing Works

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 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 Directory. 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.

There are two indexing methods in Commvault version 11 software:

- V1 indexing
- V2 indexing supported for specific Commvault agents

Traditional Indexing (V1)

Detailed index information for jobs is maintained in the MediaAgent’s Index Directory. This information will contain each object, 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 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.

Commvault Version 11 – V2 Indexing

Commvault version 11 introduces the next generation indexing called indexing V2. It provides improved performance and resiliency, while shrinking the size of index files in cache and in storage.

Indexing data is located in a persistent index database. One index database will maintain records for all objects within a backup set, so all subclients within the same backup set will write to the same index database. The database is created and maintained on the data mover MediaAgent once the initial protection job of a subclient within a backup set completes. Index databases are located in the index directory location on the MediaAgent.

During data protection jobs, log files are generated with records of protected objects. The maximum size of a log will be 10,000 objects or a complete chunk. Once a Log is filled or a new chunk is started, a new Log file is created and the closed Log will be written to the index database. By writing index logs to the database while the job is still running, the indexing operations of the job runs independent of the actual job allowing a job to complete even if log operations are still committing information to the database.

At the conclusion of each job, the log files are written to storage along with the job. This is an important distinction from traditional indexing which would copy the entire index to storage. By copying just logs to storage, indexes require significantly less space in storage which is a big benefit when protecting large file servers. Since the index database is not copied to storage at the conclusion of each job, a special IndexBackup subclient is used to protect index databases.

Index Directory Settings

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

- Index cache should be located on dedicated high speed disks, preferably solid state disks.
- Do NOT put the index cache on the system drive. The location of the cache can be changed by: right-clicking the MediaAgent and selecting the properties Catalog tab.
- Size the index cache appropriately based on the size of your environment and the estimated number of objects that will be protected. It is much better to overestimate than underestimate index cache size. Sizing guidelines are available in the Commvault Online Documentation.
  - The default retention time for V1 indexes in the index cache is 15 days. If you will be frequently browsing for data older than 15 days increase this setting and allocate enough disk space for the index cache.
  - V2 indexes are persistent and are not pruned based on index cache retention settings.
- Index files are automatically protected so there is no need to perform backups of the index cache location.

**Physical vs. Virtual MediaAgent**

Commvault recommends using physical MediaAgents to protect physical and virtual data. The advantages for using a physical MediaAgent are: better performance, more versatility as a multi-purposed data mover (protect VMs and physical data), and resiliency. A MediaAgent can be virtualized if all performance requirements including CPU, RAM, index cache location and deduplication database location are being met.

**Data Pipe**

MediaAgents can be used to backup client data over a network or dedicated where a client and MediaAgent are installed on the same server using a LAN Free or preferred path to backup data directly to storage.

**Cyclic Redundancy Checks (CRC)**

By default, the ‘Validation on Media’ and ‘Validation on Network’ Cyclic Redundancy Check’ options are enabled for all MediaAgents. The CRC information is used when conducting validation operations for data in protected storage. There is a minimal performance impact on protection jobs (1 – 2%) and it is strongly recommended to always leave these settings enabled. It is also recommended to regularly run data validation jobs, especially for deduplicated data.
Disk Storage

A disk library is a logical container which is used to define one or more paths to storage called mount paths. These paths are defined explicitly to the location of the storage and can be defined as a drive letter or a UNC path. Within each mount path, writers can be allocated which defines the total number of concurrent streams for the mount path.

Stream management for disk libraries is an important aspect of overall CommCell performance. Depending on the disk’s capabilities, network capacity and MediaAgent power, the number of writers can be increased to allow more streams to run concurrently during protection periods. Based on the MediaAgent hardware configuration, a specific number of concurrent streams is recommended as per Commvault Online Documentation. It is strongly recommended to follow this documentation to avoid encountering performance issues.

For more information, please refer to the following URL:


Disk Library Properties

Setting low disk space watermark

Disk library Properties | General tab

Disk Library Low Watermark can be configured with a percentage threshold that will report an event to the event viewer when total disk capacity for all mount paths reaches or falls below the specified percentage. Alerts can also be configured to notify users when the threshold has been reached.

Prevent disk content from being deleted through Windows Explorer
Disk library Properties | Mount Paths tab

Prevent accidental deletion of data from mount paths will lock disk mount paths from being deleted for Windows Media Agents. It is strongly recommended that this setting is selected.

**Determine the order multiple mount paths will be used**

Disk library Properties | Mount Paths tab

Mount Path usage determines the order in which mount paths will be written to when multiple mount paths are configured for a disk library.

**Fill & Spill** - The default setting for mount path usage will use mount paths in the order in which they were created. To view the order in which mount paths were created: Control Panel | Library & Drive Configuration | Add Media Agent for disk library | OK | expand library | view mount path order (3a)

**Spill & Fill** (load balancing) - Will load balance device streams between all mount paths in the library.

Which should you use for best performance? For disk libraries part of a bottleneck will be the disks themselves but the other part of the bottleneck will be the I/O path to the disks. The use of Fill & Spill or Spill & Fill (load balancing) should be determined by how the mount paths were created and the I/O path to each mount path.

Use Fill & Spill if the mount paths are part of the same disk array and there is a single I/O path to the mount paths.

Use Spill & Fill if the mount paths are on separate disks and/or if there is separate I/O paths to the mount paths.

---

**Tip** - If there is only one mount path in the library consider setting mount path usage to Spill & Fill. The reason for this is if an additional disk array is later added, the disk library will automatically use the mount paths in a load balancing manner. A common misconfiguration is when disks are added to a library the administrator or engineer forgets to set this option.

---

**Disk Space Thresholds for Managed Disk Space**

Disk library Properties | Mount Paths tab

Managed disk space is a Commvault feature that allows a job stored on disk to be retained beyond its standard retention settings if free space exists. Managed disk space thresholds do not apply to disk libraries using Commvault deduplication.

**Start Aging when data occupied on disk is** (High Watermark) - determines the amount of disk space consumed before aged jobs will be pruned.

**Stop Aging when data occupied on disk is** (Low Watermark) – determines the amount of disk space consumed falls to the specified value.

**Mount Path Properties**

Determine the maximum concurrent writer streams for a mount path

Mount Path Properties | Allocation Policy tab
Mount Path Allocation determines the number of concurrent write operations that will be performed to a mount path. The default setting is allow maximum.

Before modifying this setting consider the following key points:

- Increasing this setting will run more streams through the network, Media Agent and disk. For many environments increasing this number marginally may not have a negative impact on the overall environment. It is recommended to incrementally adjust this number higher (increments of three to five at a time) and carefully monitor network, MediaAgent and disk performance.

- If multiple mount paths exist in the library, consider how the mount paths have been carved out of the disks. If two mount paths are allocated from the same physical disk array then by default there would be ten concurrent write operations to the disks, five from each mount path.

- Consider the I/O path from the MediaAgent to the disks as a potential bottleneck. Depending on the disk storage being used (Fibre, iSCSI or NAS) the I/O paths can become a bottleneck.

- Increasing the number of writers could have a positive impact on overall backup performance within the CommCell by running more jobs but may slow down individual jobs due to extra network and disk load.

Determine the total amount of space used for a mount path

Mount Path Properties | Allocation Policy tab

Space Allocation specifies hard cut off limits for a mount path. By default, it is set to reserve 2 GB of disk space. By reserving this space, if a chunk is currently writing to the mount path and the threshold is reached the current chunk will complete and then the mount path will be marked full. If more reserve space is needed, increase this setting or use the ‘Do not consume more than’ setting to limit how much disk space will be allocated to write operations.

Validating a Mount Path

Mount path validation tests throughput speeds of library mount paths and is run from the CommCell console.

The validation operation is configured using the following parameters:

- MediaAgent
- File size
- Number of writers
- Block size
- Number of files
Tape Storage

Key Points:

- Library types:
  - Dedicated
  - Static shared
  - Dynamic shared

- Library operations:
  - Reset
  - Scan
  - Clean drives
  - Library properties

A tape or removable media library is a library where media can be added, removed and moved between multiple libraries. The term removable media is used to specify various types of removable media supported by Commvault software including tape and USB disk drives which can be moved between MediaAgents for data protection and recovery operations.

Removable media libraries will be divided into the following components:

- **Library** – Is the logical representation of a library within a CommCell environment. A library can be dedicated to a MediaAgent or shared between multiple MediaAgents. Sharing of removable media libraries can be static or dynamic depending on the library type and the network connection method between the MediaAgents and the library.

- **Master drive pool** – is a physical representation of drives within a library. An example of master drive pools would be a tape library with different drive types like LTO4 and LTO5 drives within the same library.

- **Drive pool** – can be used to logically divide drives within a library. The drives can then be assigned to protect different jobs.

- **Scratch pool** – can be defined to manage media which can then be assigned to different data protection jobs. Custom scratch pools can be defined and media can be assigned to each pool. Custom barcode patterns can be defined to automatically assign specific media to different scratch pools or media can manually be moved between scratch pools in the library.
Tape Media Management

Commvault® software manages all media from a physical and logical perspective. Understanding the methods used to manage media from initial discovery, throughout the media’s life and to its eventual destruction is important for effective media administration. This section details concepts and administrative tasks for proper media management.

Physical media management refers to any action performed that will physically cause actions within the library.

Common physical actions are:
- Export tapes from the library
- Import and discover tapes added to the library
- Physically erase tapes
- Load and unload tapes into drives.

Logical management of media focuses on the logical location or media group and the state of tape which is represented by a media icon. These concepts will be expanded on in the following section.

Common logical actions are:
- Move a tape to another media group
- Delete tape or delete contents of a tape
- View contents of a tape
- Retire a tape
Media Icons

All tapes within a library will have an associated status icon. The icons can be used to quickly identify key attributes of the tape.

Media Lifecycle

The lifecycle of a tape is tracked from the time of initial discovery to the time of its logical destruction. The logical lifecycle of a tape is different than the physical life. Logical management of tapes can be managed with tapes in or outside the library.

Logical management of tape media will be managed in the following media groups:

- Scratch group for new or recycled media.
- Cleaning media group reserved for library cleaning tapes.
- Retired media group for tapes that exceed usage thresholds or are manually marked bad.
- Overwrite protect media group for tapes that are manually prevented from aging.
- Foreign media group for tapes from a different CommCell® environment or a different backup vendor.
- Catalog media group for tapes that are marked to be cataloged.
- Assigned media group for tapes with active jobs currently being retained and managed by Storage Policy copies.

Tape Groups

Commvault® software logically organizes all tapes into media groups. Each media group identifies all tapes associated with the group. Since all tapes are logically managed in the Commvault environment it is important to understand each media group and group management.

Scratch Groups

Scratch groups or spare media groups are used to hold all new or recycled media. Multiple scratch groups can be used to define which tapes a job will use when it executes. When a job requires a spare tape, the tape will be pulled from a defined scratch group. The Storage Policy copy’s data path is used to determine which scratch group the tape will be selected from.

The following highlights features and key points about scratch groups:

- The terms: Scratch Pool, Scratch Group, Spare Media Group or Spare Media Pool are used interchangeably throughout Commvault documentation and the CommCell Console.
- All new and recycled tapes will be placed in scratch groups.
- Once a job is written to a tape it will be moved out of the scratch group and into the assigned media group.
- Multiple scratch groups can be created and assigned to Storage Policy copies. When a job for the policy copy runs it will automatically pick a tape from the assigned scratch group.

Cleaning Media Group

The cleaning media group will manage all cleaning tapes for a library. Tape drives can be cleaned based on drive counter usage tracked by Commvault® software or sense codes reported from the library. Drive cleaning settings are configured in the library properties under the Drive tab. Best practice guidelines are to configure drive cleaning based on the library manufacturer’s recommendations.

The following lists key points regarding the cleaning media group:
• Commvault should automatically detect and move cleaning tapes to the cleaning media group when the tapes are discovered.

• If cleaning tapes are incorrectly identified and moved to a scratch pool you can manually move the tapes or use custom barcode definitions to associate cleaning tapes with the cleaning media pool.

• Low watermarks can be defined to trigger events and optional alerts when the number of spare cleaning media reaches the low threshold.

Retired Media Group

The Retired Media group is a holding area for all tapes that have exceeded tape error thresholds or are manually marked bad. Tapes in the retired media group will remain in the group until they are manually marked good or deleted. Any tapes in the retired media group will NOT be written to. If a tape is in the Assigned Media Group and is marked bad it will NOT be moved to the Retired Media Group until all jobs have aged from the tape.

Key points for the Retired Media group:

• Only tapes that are not currently retaining job data will be placed in the retired media group. If a tape is marked bad but is currently retaining data, it will still appear in the Assigned Media Group. Once all jobs have aged from the tape it will be moved to the Retired Media Group.

• Tape counters are tracked for the life of a tape from initial discovery to deletion.

• By default, manufacturer recommended thresholds are used for all tapes. These settings can be modified in the Control Panel | Hardware Maintenance applet | Media Retirement tab. It is NOT recommended to increase the threshold values.

• As long as a tape is in the Retired Media Group it will NOT be written to.

• Tapes can be moved out of the Retired Media Group using the following methods:
  - **Delete** – This will delete the existence of the tape from the CommServe® database. The tape can then be rediscovered and reused. The tape will be treated as a brand new tape and all counters will be reset. If there are any existing aged jobs on the tape they will not be recoverable.
  - **Mark Media Good** – recommended if the tape has existing jobs that have aged but may still need to be retained. If this is the case after marking the tape good, move it to the Overwrite Protect Media Group.

Tapes should be left in the Retired Media Group until they are physically disposed of. This prevents a bad tape from accidentally being discovered and reused. If a bad tape is disposed of and being replaced with a new tape with the same barcode, delete the tape from the Retired Media Group before putting the new tape in the library.

Foreign Media Group

The foreign media group will manage all media from different CommCell® environments or tapes from a different backup vendor.
The following key points should be considered regarding the Foreign Media Group:

- Tapes from one CommCell environment cannot be directly restored into another. When a tape is loaded and the OML (On Media Label) header is read, if the CommCell ID is different than the CommCell environment reading the tape, the tape will be moved to the Foreign Media Group.
- Commvault software will not write to tapes when the OML header is not recognized as a Commvault header and the tape will be moved to the Foreign Media Group.

Overwrite Protect Media

The Overwrite Protect Media group will logically lock down a tape so it will NOT be written to or recycled. Tapes must be manually moved to the overwrite protect media group and will remain there indefinitely until they are moved out of the group.

Key points for overwrite protect media group:

- By default an overwrite protect media group will automatically be created. Additional overwrite protect media groups can be added.
- Tapes can be moved to the overwrite protect media group using the following methods:
  - For active tapes in the assigned media group – Right-click on the tape and select Prevent Reuse. The tape will appear in the assigned media and the overwrite protect media group.
  - For tapes in scratch groups – Right-click on the tape and select Move. For Media group Type select Overwrite Protect Media Group and then select the overwrite group.

Catalog Media Group

The Catalog Media group is used to hold all tapes that are actively being cataloged or are marked for catalog. A catalog operation is used to catalog job metadata from a tape and enter the metadata back into the CommServe® database. This is mainly an operation that would be performed if the CommServe database had to be restored to a point in time prior to jobs on a tape finishing. This situation can arise in cases of disaster, database corruption or if the CommServe metadata backups are not being properly managed.

Tape can be individually picked for catalog or multiple tapes can be picked and marked for catalog. When tapes are picked for catalog they will be moved to the catalog media group.

Assigned Media Group

All tapes that are actively retaining data will be in the Assigned Media group. Within a library there can only be one assigned media group. Tapes will remain in the group until ALL jobs on the tape have exceeded retention and marked as aged. During the data aging operation, the tape will then be recycled back into a scratch pool.

Key Points regarding tapes in the Assigned Media Group:

- Tapes in the Assigned Media Group cannot be deleted. Delete is considered a non-destructive operation.
- Delete Contents can be performed on a tape which is considered a destructive operation. To delete contents of multiple tapes, use the Shift or Ctrl keys to select multiple media. Note that this will recycle the tape and the jobs will be marked aged.
Common Tape Management Operations

Depending on the Media group certain administrative tasks can be performed for the group and tapes within the group. Managing tapes in different media groups provides the Commvault administrator with greater flexibility and simplifies the management of media. It is important to understand the capabilities and limitations of media management within the various logical media groups available.

The following actions can be performed on tapes in any media group:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Physically export a tape out of the library.</td>
</tr>
<tr>
<td>Move</td>
<td>Logically move tapes between media groups.</td>
</tr>
<tr>
<td>Verify Media</td>
<td>Physically verify the OML header information to CommCell tape metadata and the barcode label.</td>
</tr>
<tr>
<td>View Contents</td>
<td>Logically view active and aged jobs on a tape.</td>
</tr>
<tr>
<td>Delete</td>
<td>Logically delete the existence of a tape from the CommServe database.</td>
</tr>
<tr>
<td>Delete Contents</td>
<td>Logically delete contents by marking all jobs as aged and recycling the tape back into a scratch pool.</td>
</tr>
<tr>
<td>Erase Media</td>
<td>Physically erase data by writing a new OML header to the tape.</td>
</tr>
<tr>
<td>Mark Media Bad</td>
<td>Logically mark a tape bad to prevent it from being reused.</td>
</tr>
<tr>
<td>Media Refresh</td>
<td>Refresh active jobs on existing tapes by writing the jobs to new tapes.</td>
</tr>
</tbody>
</table>

Exporting Media

Exporting tapes is a physical operation that will send commands to the library to eject tapes to the import/export mail slots.

Key points regarding tape export operations:

- There are several methods that can be used to export tapes from a library:
  - Library export for bulk export of multiple tapes.
  - Tape export to export individual tapes.
- VaultTracker export which allows the automatic export of tapes based on criteria.
- To view the progress of export operations, use the Exports in Progress view in the library tree.
- To view tapes in the import/export slots use the I/E Ports view in the library tree.

**Logically Moving Tapes**

Tapes can be moved between certain media groups. Moving tapes between groups is a logical operation and no physical media movement will be conducted in the library. Moving tapes provides the administrator with a great deal of flexibility regarding media management.

**Key Points regarding tape movement between media groups:**

- The Move operation can be used to move tapes between scratch, cleaning, overwrite protect, foreign and catalog media groups.
- Tapes can be moved to the Retired Media Group by manually marking the tape bad. Tapes can be moved out of the retired media pool by using the option Mark Media Good or by deleting and rediscovering the tape.
- Tapes moved to the Overwrite Protect Media Group will remain there indefinitely until they are manually moved out of the group.
- Tapes cannot be manually moved to the Assigned Media Group. Tapes can logically be moved to the Overwrite Protect Media Group by selecting Prevent Reuse. The tape will exist in both the Assigned Media Group and the Overwrite Protect Media Group until all jobs age from the tape, where it will then only exist in the overwrite protect media group.
- When a tape is cataloged, or marked for catalog, it will logically appear in the Catalog Media Group.
- There are two methods that can be used when using the Move operation:
  - Specific tapes can be moved between media groups by selecting a tape or multiple tapes (using the Shift or Ctrl keys). After selecting the tapes to move, right-click and select the Move option. Specify the media group type and the specific destination pool to move the tapes to.
  - Groups of tapes can also be moved between scratch pools by right-clicking on the scratch pool and selecting Move. This method allows you to specify how many tapes to move but it does not allow you to specify which tapes will be moved.

**Deleting Tapes**

A Delete operation is a logical operation that deletes the existence of the tape from the CommCell® environment and CommServe® database. The delete operation will not physically erase any data and the tape does not need to be in the library when it is deleted. This is also considered a non-destructive operation which means a tape can only be deleted if no active jobs are currently retained on the tape. This means that the Delete option will not be available for tapes in the Assigned Media group.

**Consider the following key points regarding tape deletion:**

- When a tape is deleted, the tape records are removed from the CommServe database. This means data on the tape would not be recoverable. If data on a deleted tape needs to be recovered the Media Explorer tool can be used to catalog and recover data.
• Since deleting a tape is a logical operation there will be no tape movement in the library and the tape does not need to be available.

• If a tape has been permanently lost or destroyed and a replacement tape with the same barcode label will replace the original tape, delete the original tape before adding the replacement tape to the library. Within a CommCell environment duplicate barcode patterns cannot exist.

• The Delete operation is useful in the following situations:
  • A tape has been lost or destroyed.
  • A tape was marked bad and has been physically removed from the environment. Note that until the tape is physically disposed of it is recommended NOT to delete the tape since a tape marked bad will not be re-used where a deleted tape rediscovered will be treated as a new tape. This concept will be discussed later in the chapter.
  • Duplicate barcodes exist in a library where an old tape has been replaced by a new tape. Note the same caveats apply in this situation as the previous one.
  • A tape was improperly marked bad. This may sometimes happen when a drive causes a tape to be marked bad.

Delete Tape Contents

Delete Contents is a logical operation that will automatically mark all jobs on a tape as aged. During a Delete Contents operation, a confirmation message will appear and then the administrator must enter erase and reuse media. The administrator will then be prompted to select a scratch group to move the tape to. Data on the tape is logically marked aged so the data can still be recovered up to the point where the tape is mounted and the OML header is overwritten.

The most common situation where the Delete Contents operation is used is when there is not enough spare media to run scheduled jobs. This typically happens when storage policies are improperly configured or retention expectations are unrealistic compared to capacity to store data. If an administrator frequently uses the delete contents option to free up tapes for jobs, consider readdressing environment configurations or purchase more tapes. Manual operations such as this add the potential of human error accidentally deleting critical data.

Erasing Tapes

Erase Media is a physical operation that will mount the tape and overwrite the OML header. Once the header is overwritten data cannot be recovered using any method Commvault® software provides. This is considered a destructive operation so it cannot be performed on any tapes where jobs are actively being retained. The option to erase media will be available in all logical groups except the Assigned Media group.

There are two methods for erasing a tape:

1. Manually erasing a tape.
2. Automatically erasing tapes after all data ages (configured through the storage policy copy).

Manually Erasing a Tape

Right-click tape | Erase Media

A tape can be erased on demand by right-clicking on the tape and selecting Erase Media. This action will then load the tape in a drive and overwrite the header physically preventing data to be recovered through Commvault® software.
Automating Erase Operations

Storage Policy copy | Media tab | enable Mark media to be erase after recycling

When tapes are recycled they can automatically be marked to be erased. This is done by selecting the *Erase Media* check box in the *Media* tab of a storage policy copy. When tapes are recycled they will be marked to be erased. An erase media operation must be scheduled for the library which will physically load each marked tape and overwrite the OML header.

Verifying Media

A Media verification operation can be conducted to physically verify the barcode label and the OML header match and the tape belongs to the CommCell environment. Since this is a physical operation the tape will be mounted in a drive and a job will appear in the job controller. When the job is initiated the operation type will be *Media Inventory*.

The Media verification operation is commonly used for the following tasks:

- To ensure that the barcode label and the OML header properly match.
- To identify potentially damaged tapes.
- To identify tapes that may belong to a different CommCell environment.
- To identify tapes that may have an OML header written by different backup software.
Additional Library Types

Cloud storage is an emerging technology that is quickly being integrated into data centers for its availability and, in some cases, lower TCO. As a DR solution however there are still significant questions on its effectiveness. The two biggest questions regarding cloud storage for DR are bandwidth availability and data security. Using advanced features such as Commvault deduplication can greatly reduce the bandwidth requirements of backing up to cloud storage. However, in a disaster situation where a significant amount of data must be restored, bandwidth can become a serious bottleneck.

USB Devices - For some environments with remote office locations connected to a main data center with limited bandwidth such as fractional T1 or satellite, USB backup devices may provide the best protection solution. USB devices are configured and recognized by Commvault software as standalone tape devices. This allows data to be protected to USB devices using MediaAgents at remote locations, removed and sent to another location and connected to a different MediaAgent where the data can be accessed and restored. Since the USB device is detected as a tape device it is considered portable and any Windows MediaAgent within the CommCell environment can recognize the device and access/restore the data. This method can also be used for seeding stores when using Commvault deduplication for remote office protection.

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

Virtual Tape Library – is a software representation of a tape library using disk storage. Virtual tape libraries are supported, but not recommended because a normal disk library provides many more features and capabilities.
**Removable Disk Drives** - is configured as stand-alone drives. All operations supported by stand-alone drives are supported by such devices. Removable disks differ from PnP disks in that they are drive enclosure devices that retain a persistent drive letter in the Operating System, regardless of whether or not a disk media is loaded into the enclosure.
Deduplication
Deduplication Overview

Key Points:

- Deduplication benefits
- High level overview
- Building block guidelines
  - Must meet hardware requirements

In any modern data center, duplicate data exists on production storage, servers, and end-user systems. Some examples include identical DLL files existing on different servers, or multiple users working on the same document—each user modifies different blocks in the file while other blocks remain unchanged. Traditionally this redundant data is stored on disk or tape, which requires a significant amount of space to protect. With Commvault® Deduplication storage techniques, a single copy of redundant data (and any subsequent references to the same data) is stored only once; reducing the amount of space needed to save data and protecting against data loss.

Benefits and Features

Commvault® software has a unique set of deduplication features that are not available with most third-party deduplication solutions. By taking full advantage of Commvault® Deduplication, you can reduce storage and network resource requirements, shrink backup windows, efficiently copy data to off-site locations, and copy deduplicated data to tape, disk, or to a cloud environment.

Commvault Deduplication offers the following benefits:

- Efficient use of storage media
- Efficient use of network bandwidth
- Significantly faster Synthetic Full operations
- Significantly faster auxiliary copy operations
- Efficient use of tape media
- Resilient indexing and restorability
The Deduplication Process and Data Protection

The following steps illustrate the deduplication process during a data protection job.

1. Production data is read from the source location and written into a memory buffer. This memory buffer is filled based on the defined block size. Note that the block size is referred to as a data block with a default of 128 KB.

2. A signature is then generated on the data block. The signature uniquely represents the bit makeup of the block.

3. The signature is compared in the Deduplication Database (DDB) to determine if the data block already exists.
   A. If it does exist, the data block in the memory buffer is discarded and pointers to the existing block in storage is referenced instead.
   B. If it does not exist, the data block is written to protected storage.

Deduplication Building Blocks

Commvault recommends using building block guidelines for simplicity and scalability when designing a deduplication solution. Use the building block approach provides the best method to ensure a deduplication solution will meet current and future needs.

For additional guidelines and the latest recommendations for deduplication building blocks refer to Commvault’s online documentation:

Components and Terminology

There are several components that comprise the Commvault® Deduplication architecture.

The **Global Deduplication Policy** defines the rules for the Deduplication Engine. These rules include:

- Deduplication Store location and configuration settings
- Deduplication Database (DDB) location and configuration settings

A **Data Management Storage Policy** is configured as a traditional storage policy, where the former also manages subclient associations and retention. Storage policy copies defined within the Data Management policy are associated with Global Deduplication storage policies. This association of the Data Management Storage Policy copy to a Global Deduplication Policy determines which Deduplication Store the protected data resides.

**Deduplication Database (DDB)** – is the database that maintains records of all signatures for data blocks in the Deduplication Store.

**Deduplication Store** – contains the protected storage using Commvault® Deduplication. The store is a disk library which contains non-duplicate blocks, along with block indexing information, job metadata, and job indexes.

**Client** – is the production client where data is being protected. The Client has a file system and/or an application agent installed. The agent contains the functionality to conduct deduplication operations, such as creating data blocks and generating signatures.

**MediaAgent** – coordinates signature lookups in the DDB and writes data to a protected storage. The Signature lookups operation is performed using the DDB on the MediaAgent.
Transactional Deduplication Database

Database components:
- In Memory logs
- DiskDB log
- Primary table
- Secondary table

Transactional deduplication database provides significant resiliency benefits. There are several components that make up the in memory deduplication database: In memory logs and disk log.

In Memory Logs

In memory logs are linked to portions of the deduplication database and are dynamically added to memory by the system. There are three memory logs; one active log, which records all database changes, a pending commit log, and merge commit log. The active log will be record changes for 20 seconds. Once the active log is closed it becomes a pending commit log and a new active log is started. While the active log receives changes and the pending commit log closes, a merge commit log is committed to an on-disk log.

DiskDB Log

The DiskDB log resides in the DDB location and receives updates from the memory logs. In addition to receiving changes from the in-memory logs, it is also used to commit records to the deduplication database. In the event of a MediaAgent unplanned shutdown, the DiskDB log is used to bring the DDB to a consistent state.
Content Aware Deduplication

How it works:

- Object based backups
- Database backups
- Database log backups

The concept of content aware deduplication is to identify what type of data is being protected and adjust how deduplication is implemented. Consider a deduplication appliance that receives data from a backup application. The appliance can’t detect files, databases, or metadata generated from the backup application. Commvault deduplication is integrated into agents so it understands what is being protected. This provides significant space saving benefits and results in faster backup, restore and synthetic full backup operations.

Object Based Content Aware Deduplication

Since most file objects are not equally divisible by a set block size, such as 128 KB, Commvault® Deduplication uses a content aware approach to generate signatures. If an object that is 272 KB in size is deduplicated, it can be evenly divisible by 128 KB with a remainder of 16 KB. In this case two 128 KB deduplication blocks will be hashed and compared. The remaining 16 KB will be hashed in its entirety. In other words, Commvault® Deduplication will not add more data to the deduplication buffer. The result is if the object containing the three deduplication blocks never changes, all three blocks will always deduplicate against themselves.

Database and Log Content Aware Deduplication

Database application often provide built in compression which will compress blocks before Commvault generates signatures on the blocks. The application level compression results in inconsistent blocks being deduplicated each time a backup runs which results in poor deduplication ratios. Using Commvault compression during backups instead of application compression, the application agent will detect the database backup and generate a signature on uncompressed data. After the signature has been generated, the block will then be compressed. This lead to improved deduplication ratios.
Log files are constantly changing with new information added and old information truncated. Since the state of the data is constantly changing, deduplication will provide no space saving benefits. During log backup jobs, the application agent will detect the log backup and no signatures are generated, saving CPU and memory resources on the production system and speeding up backups by eliminating signature lookups in the deduplication database.
Deduplication Database Reconstruction

Reconstruction options:

- Unplanned shutdown
  - DDB still available
  - Use DiskDB log to reconstruct DDB
- Database lost
  - Recovered from backup
  - Use chunk metadata to reconstruct DDB
- Database lost
  - No DDB available for restore
  - Use chunk metadata to reconstruct DDB

The deduplication database is highly resilient and reconstruct operations can rebuild the database to match the latest job and chunk information maintained in the CommServe database.

There are three methods available to reconstruct the deduplication database:

**Delta Reconstruction** – In the event of an unclean DDB shutdown due to MediaAgent reboot or system crash, the DiskDB logs can be used to bring the DDB to a consistent state.

**Partial Database Reconstruction** – If the deduplication database is lost or corrupt, a backup copy of the database is restored and the database is reconstructed using chunk metadata.

**Full Database Reconstruction** – If the deduplication database is lost and no backup copy is available, the entire database is reconstructed from chunk metadata.
Data Verification

Verification Options:
- Incremental
- Verify DDB
- Verify jobs and DDB
- Quick verification

Verification of Existing Jobs on Disk and Deduplication Database
Full verification for disk and DDB uses checksum data to verify block integrity by reading data chunks (Sfiles), uncompressing, and decrypting, and using CRC information to validate block integrity. This option also verifies chunk metadata using CRC checks. Any blocks failing the check will be marked in the DDB. New blocks generating the same signature as a block marked bad are re-written to disk and a new signature entry is written to the DDB. This verification method also verifies chunk integrity between the DDB and disk library.

Verification of Deduplication Database
The verification of the deduplication database option performs all of the same tasks as the verification of existing jobs on disk and the deduplication database except metadata chunk validation.

Quick Verification of Deduplication Database
Quick verification option verifies chunk integrity between DDB and disk library.

Incremental Verification
Incremental data verification verifies data integrity for new jobs added since the last verification job. This option is available when running ‘verification of deduplication database’ or ‘verification of existing jobs on disk and deduplication database’ options. Since this method only verifies new jobs, full verification jobs should periodically be executed.

Default Data Verification Schedule Policy
On a newly installed system, a default data verification schedule policy called System Created DDB Verification schedule policy gets created which executes a daily incremental data verification job. However, full verification is not scheduled. It therefore is recommended to periodically execute a full verification job manually or schedule it.
Module 3: Storage Policies
Storage Policies
Storage Policy Overview

Storage Policy Concepts:

- Policy based data management
- Three primary rules:
  - Subclient (What data)
  - Data path (Where will it go)
  - Retention (How long will it be kept)

A storage policy defines the lifecycle management rules for all protected data. In its most basic form, a storage policy can be thought of as a container with one or more sets of rules that define how data will be managed. These rules are called storage policy copies. Within the storage policy, multiple copies can be created, each with their own set of rules.

There are three primary rules that every storage policy copy must have defined:

- What data is determined through subclients association
- Where will it be stored is determined by the data path
- How long will it be kept is determined by the retention

Subclient (What Data)

One of the more difficult concepts for backup administrators transitioning from legacy backup products to Commvault software is that a server is not directed to a storage policy, subclient data on the server is. This is done by defining what data a subclient will manage. For most file systems and applications, a default subclient is automatically generated. For these agents, the default subclient will protect all data the agent is responsible for. Additional subclients can be created to meet performance, management and special protection requirements.

Data Path (Where data is stored)

The storage policy the subclient data is associated with determines the data path. The path is used to move data from the source location to protected storage. All active subclients must be associated with a storage policy.
A data path is made up of four components:

- Media Agent
- Library
- Drive pool
- Scratch pool

**MediaAgent**

MediaAgents are the workhorses that move data from production servers to the backup environment. They supply the processing power to receive data, arrange it in chunk format, and send it to the library. MediaAgents can also be responsible for encryption, compression, or deduplication processing.

**Library**

Libraries are logically defined and are categorized as stationary or removable media libraries. Stationary libraries define a path to a disk location such as a drive letter or UNC path. They are considered stationary since these paths do not change once defined. Removable media libraries are generally thought of as tape libraries but they can also be magnetic optical or USB storage devices.

**Drive Pool (Tape Libraries Only)**

Drive pools are a single MediaAgent’s view of allocated drives within a tape library. Use of drive pools gives the MediaAgent the flexibility of drive choice and usage within a library. Without drive pools, assigning and sending a data protection job to a specific drive will fail if the drive is broken or offline. Having a pool of drives to choose from gives the job the best chance of success.

**Scratch Pool (Tape Libraries Only)**

Scratch pools allow new and reusable media within the library to be logically grouped based on media type and intended usage. At least one default scratch pool exists for every tape library. Master drive pools can be assigned their own default scratch pools. Additional user-defined scratch pools can be created, assigned media manually or automatically and assigned to a storage policy copy’s data path.

**Retention (How long data is kept)**

Retention is defined in the Retention tab of the storage policy copy. Each copy will have its own retention configurations. This allows subclient data to be managed in multiple locations, each with their own retention settings.

In this example data is backed up to the primary copy and retained for (1) one month. A synchronous copy is created for Disaster Recovery which will be kept for (2) 3 months and a selective copy for compliance is retained for (3) seven years.
Storage Policy Structure

Storage Policy Copies:

- Primary copy
- Secondary copies
  - Selective
  - Synchronous

The concept of storage policy copies is that the data from the production environment only has to be moved to protected storage once. Once the data is in protected storage, the storage policy logically manages and maintains independent copies of the data. This allows for great flexibility when managing data based on the three key aspects of data protection: disaster recovery, data recovery, and data archiving.

There are three types of storage policy copies

- Primary Copy
- Secondary Synchronous Copy
- Secondary Selective Copy

Primary Copy

A storage policy primary copy sets the primary rules for protected data. Each storage policy can have two primary copies, a primary snap copy and primary classic copy. A primary snap is used to manage protected data using the Commvault IntelliSnap® feature and a primary classic which will manage traditional agent based data protection jobs. Most rules defined during the policy creation process can be modified after it has been created.

Secondary Copies

There are two types of secondary copies:

- Secondary Synchronous
- Secondary Selective
Synchronous Copy
A synchronous copy defines a secondary copy to synchronize protected data with a source copy. All valid data (jobs that completed successfully) written to the source copy will be copied to the synchronous copy via an update process called an auxiliary copy operation - this means all full, incremental, differential, transaction log, or archive job from a source copy will also be managed by the synchronous copy. Synchronous copies are useful when you want a consistent point-in-time copy at any point within the cycle of all protected data available for restore.

Synchronous copies are used to meet the following requirements:
- Consistent point-in-time copies of data required to restore data to a particular point-in-time within a cycle.
- Copies that are required to be sent off-site daily.
- To provide the ability to restore multiple versions of an object from a secondary copy within a cycle.

Selective Copy
A selective copy allows automatic selection of specific full backups or manual selection of any backup for additional protection. Selective copy options allow the time based automatic selection of: all, weekly, monthly, quarterly, half-year, and/or yearly full backups. Advanced options allow you to generate selective copies based on a frequency of number of cycles, days, weeks, or months. You can also choose the Do Not Automatically Select Jobs option which allows you to use auxiliary copy schedules to determine when copies of full backups will be made.

Selective copies are used to meet the following requirements:
- Data being sent off-site weekly, monthly, quarterly, or yearly.
- Archiving point-in-time copies of data for compliance and government regulations.
Storage Policy Configuration

Key Points:

- Storage policy wizard
- Policy options:
  - Device streams
- Copy options:
  - Retention
  - Data path settings
  - Subclient association
  - Multiplexing
  - Combine to streams
  - Compression

The Storage Policy Wizard is used to create storage policies for a CommCell environment. Once the policy is configured, most options can be customized in the property settings.

Storage Policy Type

Storage Policies can be used for CommServe Disaster Recovery Backups or standard data protection. CommServe disaster recovery storage policies are only used for protecting the CommServe metadata database, the CommServe registry, configuration files, and specified log files. No standard data can be protected by a CommServe DR policy. Standard data protection policies will be used for protecting all production data within an environment.

Storage Policy Name

The name of the storage policy can be defined at time of creation and later modified in the Storage Policy Properties. The name should be descriptive and reflect what is being protected and any key configuration options.

In the following example this policy will be protecting Windows servers to a 10 TB shared RAID array using deduplication with a 128 KB block factor. It any of these options later change, simply change the name of the policy.

Global Deduplication Policy

This determines if the storage policy will use a global deduplication storage policy. If Yes is selected, the option to perform Client Side Deduplication can be enabled. If Client Side Deduplication is enabled, it will override settings at the Client level and perform client deduplication for all subclients associated with the policy.
Default Library

This defines the default library which will be used by the primary copy. The path can later be changed in the primary copy’s Data Path tab. The library that will be used is a 10TB Shared RAID library using the CS and EX Media Agents.

Selecting the Media Agent

This allows you to specify which Media Agent will be used to write to the library. During the policy creation process, only one Media Agent can be specified. Additional Media Agent paths can later be added in the primary copy’s Data Path tab.

For a tape library with multiple drive pools, the drive pool to be used for the primary copy can also be selected.

Scratch Pool

For tape libraries, the scratch pool to be used for the primary copy can be selected.

Retention and Stream Settings

Device Streams

Device streams determine how many concurrent write operations will be performed to the library. This setting should equal the number of tape drives or the total number of writers for all mount paths in a disk library. If the number of drives or writers change, the Device Streams setting can be modified in the storage policy’s properties.

Agent Backup Data Retention

Standard retention for backup data is based on cycles and days. This is because standard backups run full and full dependent operations (incremental, differential, and log). The default retention for a storage policy primary copy is 15 days and 2 cycles. The default retention for a secondary copy is 30 days and 4 cycles. The retention is set during the policy creation process and can later be modified in the policy copy’s retention tab.

Data Archive / Compliance Archive Retention

Archiving retention is based on days. When archive jobs run they determine what will be archived based on defined criteria in the subclient. Full and dependent jobs are not used in this case so the cycle criterion is not needed. Note that this retention setting does not apply to OnePass® Archive.

Storage Policy Settings

Storage Policy Device Streams

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

Secondary Copy Settings

Combine to Streams

A storage policy can be configured to allow the use of multiple streams for primary copy backup. Multi-streaming of backup data is done to improve backup performance. Normally, each stream used for the primary copy requires a
corresponding stream on each secondary copy. In the case of tape media for a secondary copy, multi-stream storage policies will consume multiple media. The *combine to streams* option can be used to consolidate multiple streams from source data onto fewer media when secondary copies are run. This allows for better media management and the grouping of like data onto media for storage.

**Example:** You backup a home folders subclient to a disk library using three streams to maximize performance. The total size of protected data is 600GB. You want to consolidate those three streams onto a single 800GB capacity tape for off-site storage.

**Solution:** By creating a secondary copy and setting the Combine to Streams setting to 1 you will serially place each stream onto the media.

In some cases, using the combine to streams option may not be the best method to manage data. Multi-streaming backup data is done to improve performance. When those streams are consolidated to the same media set they can only be recovered in a single stream operation. Though combining to streams has a media consolidation benefit it will have a negative effect on restore performance.

Another reason not to combine to streams is for multi-streamed backups of SQL, DB2, and Sybase subclients. When these agents use a single subclient with multi-streaming enabled the streams must be restored in the same sequence they were backed up in. If the streams are combined to the same tape, they must be pre-staged to disk before they can be recovered. In this case not enabling combine to streams and placing each stream on separate media will bypass the pre-staging of the data and also allow multiple streams to be restored concurrently making the restore process considerably faster. Note that this only applies to subclients that have been multi-streamed. If multiple subclients have been single streamed and combined to media, they will NOT have to be pre-staged prior to recovery.
Storage Policy Administration

**Administrative Tasks:**

- Job management
  - Change job retention
  - Delete job
- Hide storage policy
- Delete storage policy
- Storage policy and subclient association

---

**Job Management**

Jobs can be managed by viewing the job history for a storage policy copy.

**Key points for job management in storage policy copies:**

- Retention can be changed for a job.
- A job can be deleted.
- A job can be picked or re-picked to be included in an auxiliary copy job.
- Use the browse or find options to recover data.
- Pick a job for data verification.

**Hiding Storage Policies**

Storage Policies can be hidden from view within the CommCell Console by selecting the Hide Storage Policy check box in the Storage Policy Properties. Once hidden it will not appear in the Storage Policies list and more importantly, subclients cannot be associated with a hidden Storage Policy. In order to hide a Storage Policy, no subclients can be associated with the policy.

Hiding Storage Policies is an important feature because if a Storage Policy that is managing protected data is deleted, all the managed data will be pruned during the next data aging operation.
Show Hidden Storage Policies

To make hidden Storage Policies visible use the Show Hidden Storage Policies configuration parameter in the Media Management applet in Control Panel. Setting the parameter value to 1 will show hidden policies but subclients will not be able to be associated with the policy.

Deleting Storage Policies

If a Storage Policy is deleted, all protected data associated with the Storage Policy and all policy copies will be pruned during the next data aging operation. It is strongly recommended to hide the Storage Policy instead of deleting it.

To delete a Storage Policy, perform the following:

1. In the Storage Policy properties view the Associations tab to ensure no subclients are associated with the policy. A Storage Policy cannot be deleted if subclients are associated with the policy.

2. On the Storage Policy, right-click | select View | Jobs. De-select the option to Specify Time Range then click OK. This step will display all jobs managed by all copies of the Storage Policy. Ensure that there are no jobs being managed by the policy and then exit from the job history.

3. Right-click on the Storage Policy | Select All Tasks | Delete. Read the warning dialog box then click OK. Type erase and reuse media then click OK.

Associating Subclients to Storage Policies

Subclient Properties

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

Storage Policy Level

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

Policies Level Subclient Association

If subclient associations need to be made for more than one storage policy you can use the Subclient Associations option by expanding Policies, right-click on Storage Policies and select Subclient Associations. The windows will display all subclients for the CommCell environment. Select the subclient and use the drop down box under the storage policy field to select the storage policy. You can use the Shift or Ctrl keys to select multiple subclients then use the Change all selected Storage Policies to drop-down box to associate all selected subclients to a specific storage policy.
Global Secondary Copy policies allow multiple storage policy copies using a tape data path to be associated with a single global secondary copy. This is based on the same concept as global deduplication policies, but global secondary copies only apply to tape copies. If multiple secondary copies require the same retention and encryption settings, using a global secondary copy reduces the number of tapes required during auxiliary copy operations and improves performance.
Retention
Retention Overview

<table>
<thead>
<tr>
<th>Reasons for data retention:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Disaster Recovery</td>
<td></td>
</tr>
<tr>
<td>Data Recovery</td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Retention set at the following:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage policy copy</td>
<td></td>
</tr>
<tr>
<td>Job schedule</td>
<td></td>
</tr>
<tr>
<td>Job history in storage policy copy</td>
<td></td>
</tr>
<tr>
<td>Subclient</td>
<td></td>
</tr>
<tr>
<td>Manually by moving tapes to the ‘Overwrite protect media’ pool</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Storage policy copy retention notes:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary copy default retention: 15 days and 2 cycles</td>
<td></td>
</tr>
<tr>
<td>Secondary copy default retention: 30 days and 4 cycles</td>
<td></td>
</tr>
</tbody>
</table>

The heart of every data protection strategy should be data retention. This strategy should not be based on a simple one-dimensional approach though, as multiple copies of data may be required with each copy having different retention requirements. Commvault software makes this strategy straightforward to implement by using storage policies with multiple policy copies. Each copy can independently manage subclient content and have specific retention settings defined. Retention settings will include the basic rules of how long data will be retained and additional rules can be set to determine how many complete sets or cycles to keep, whether grandfather/father/son media rotation will be used and for specific storage policy copy types, which backup jobs will be selected to be retained such as end of month or end of year copies.

There are three primary reasons data is retained:

- Disaster recovery
- Compliance and archiving
- Data Recovery

**Disaster Recovery** policies should always be implemented based on how many complete sets of backups should be kept. A set is referred to as a cycle and it will include all data protection jobs required to restore an entire system to a specific point-in-time. In this case, the number of cycles should be used to determine retention policies.

**Compliance and Archiving** copies are usually point-in-time copies of data that will be retained for long periods of time. Month, quarter, or year end point-in-time full backups are usually retained for months, years or indefinitely. In this case the length of time is the key factor in determining retention, not the number of cycles.
Data Recovery is the ability to go backward in time to a certain point to recover specific data at that point. It could be a file a user deleted two months ago, or an Email message. Data recovery policies may include all data for a specific length of time so keeping full and incremental backups may be required. In this case which copies and the length of time they will be kept for should determine retention policies.

Destroying Data when retention policies expire is a critical component of some organizations. Unfortunately, this aspect of retention policies is often overlooked. Moving data throughout it’s useful lifecycle and then destroying beyond that period can not only help an organization from legal and compliance standpoints, but from a technical aspect old data being destroyed will free up space on production storage.

Storage Policy Copy Retention Rules

Policy based retention settings are configured in the storage policy copy Retention tab. The settings for backup data are Days and Cycles. For archive data the retention is configured in Days. Retention can also be set through schedules or applied retroactively to a job in a storage policy copy.
Sample Retention Policy

<table>
<thead>
<tr>
<th>Data</th>
<th>Onsite</th>
<th>Disaster Recovery</th>
<th>Historical</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Versions</td>
<td>Days</td>
<td>Versions</td>
</tr>
<tr>
<td>E-Mail (Database)</td>
<td>2 cycles</td>
<td>14</td>
<td>4 cycles</td>
</tr>
<tr>
<td>Mailboxes (Standard)</td>
<td>4 cycles</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>Mailboxes (VP+)</td>
<td>4 cycles</td>
<td>30</td>
<td>4 cycles</td>
</tr>
<tr>
<td>Finance</td>
<td>2 cycles</td>
<td>14</td>
<td>4 cycles</td>
</tr>
<tr>
<td>HR</td>
<td>2 cycles</td>
<td>14</td>
<td>4 cycles</td>
</tr>
<tr>
<td>User (Standard)</td>
<td>2 cycles</td>
<td>14</td>
<td>4 cycles</td>
</tr>
<tr>
<td>User (VP+)</td>
<td>2 cycles</td>
<td>14</td>
<td>4 cycles</td>
</tr>
</tbody>
</table>
**Job Based Retention Rules**

- **Days**
  - Defined as 24 hour time
  - Constant whether jobs run or not

- **Cycles**
  - Dependent on successful completion of full backup
  - Active cycles
  - Complete cycles

Policy based retention settings are configured in the storage policy copy **Retention** tab. The settings for backup data are **Days** and **Cycles**. For archive data the retention is configured in **Days**. Retention can also be set through schedules or applied retroactively to a job in a storage policy copy.

**Days**

A day is a 24-hour time period defined by the start time of the job. Each 24-hour time period is complete whether a backup runs or not. In this way a day is considered a constant.

**Cycles**

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.
Days and Cycles relation

A rule of thumb that has been followed for years was that cycles and days should directly or indirectly equal each other. 2 cycles and 14 days with weekly full backups. 4 cycles and 30 days being approximately 1 month. 12 cycles and 365 days for month end fulls being retained for a year. But what about 52 cycles and 365 days? In situations like this it is rather irrelevant how many cycles are set. The truth is, 2 cycles and 365 days is good enough. You will meet your retention requirements since you will be keeping data for one year and if backups don't run for over a year you are still guaranteed to have at least 2 cycles of data in storage based on the aging entire cycles rule.

When setting retention in the policy copy, base it on the primary reason data is being protected. If it is for disaster recovery, ensure the proper number of cycles are set to guarantee a minimum number backup sets for full restore. If you are retaining data for data recovery, then set the days to the required length of time determined by retention policies. If the data recovery policy is for three months, 12 cycles and 90 days or 1 cycle and 90 days will still meet the retention requirements.
How Retention Works

**Example:**

- **Retention Settings:**
  - 14 days
  - 2 cycles
- **Job Schedule:**
  - Weekly full
  - Daily incremental

<table>
<thead>
<tr>
<th>Week 1</th>
<th>S</th>
<th>M</th>
<th>T</th>
<th>W</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td>FULL</td>
<td>INC</td>
<td>INC</td>
<td>INC</td>
<td>INC</td>
<td>INC</td>
</tr>
</tbody>
</table>

1 Cycle 7 Days

<table>
<thead>
<tr>
<th>Week 2</th>
<th>S</th>
<th>M</th>
<th>T</th>
<th>W</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td>FULL</td>
<td>INC</td>
<td>INC</td>
<td>INC</td>
<td>INC</td>
<td>INC</td>
</tr>
</tbody>
</table>

1 Cycle 7 Days

<table>
<thead>
<tr>
<th>Week 3</th>
<th>S</th>
<th>M</th>
<th>T</th>
<th>W</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td>FULL</td>
<td>INC</td>
<td>INC</td>
<td>INC</td>
<td>INC</td>
<td>INC</td>
</tr>
</tbody>
</table>

1 Cycle 7 Days

Can any jobs be aged?

Data Aging for Non-Deduplicated Data

There are two processes that will be performed during a data aging operation. **Aging** simply marks jobs that have exceeded retention as aged. **Pruning** will physically delete eligible disk jobs or recycle a tape when all jobs on it have been marked aged.

The **Data Aging** process will compare the current retention settings of the storage policy copy to jobs in protected storage. Any jobs that are eligible to be aged will be marked aged. By default, the data aging process runs every day at 12PM. This can be modified and multiple data aging operations can be scheduled if desired.

**Pruning** is also part of the data aging process. How Pruning occurs depends on whether jobs are on disk or tape. For jobs on a disk library, they will be pruned. This will physically delete the data from the disk. If deduplication is being used, job blocks that are not being referenced by other jobs will be deleted. If Managed Disk Space is enabled, the jobs will remain until the Disk library reaches the upper watermark threshold defined in the Library Properties.

For tape media, when all jobs on the tape have been marked as aged, and there are no auxiliary copies dependent on the jobs, the tape will be moved into a scratch pool and data will be overwritten when the tape is picked for new data protection operations. In this case the data is not deleted and can still be recovered by browsing for aged data, until the tape label is overwritten. If the storage policy copy option ‘mark media to be erased after recycling’ has been selected or if the tape is manually picked to be erased, the data will physically be destroyed. This is done by overwriting the OML header of the tape making the data unrecoverable through the CommCell environment or using Media Explorer.
Rules for Aging Data

There are several rules that are applied during the data aging process

1. Both days and cycles criteria must be met for aging to occur.
2. Data is aged in complete cycles.
3. Days criteria is not dependent on jobs running on a given day.

Rule 1: Both CYCLES and DAYS criteria must be met before Data will age

Commvault 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.

Example: Retention for a storage policy copy is set to 3 days and 2 cycles. Now this example doesn’t make sense in the real world but it is being used to logically prove the statement that both days and cycles criteria must be met for data to age. By Monday, 3 full backups have been performed. If we were to age Friday’s full there would be two 2 fulls left meeting our criteria of 2 cycles. However, the days’ criteria calls for 3 days and if the Friday full was aged only 2 days would be counted. The Friday full would therefore age on Tuesday.
Rule 2: Data is aged in complete cycles

Backup data is managed within a storage policy copy 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.

Example: This is another retention example used to prove the rule. Retention is configured for 7 days and 2 cycles. Fulls are being performed on Fridays and Mondays, and incrementals on all other days. On Saturday, the cycle criteria of 2 has been met since there are 3 full backups. If a cycle is removed there would be 2 left, a complete cycle (Monday – Thursday) and the full on Friday night. However, since we prune entire cycles we would have to age the Friday full and the incrementals from Saturday and Sunday. This would result in only 5 days which does not meet our days’ retention requirements of 7. So on Monday when the data aging operation runs (default 12PM daily) there will now be 7 days and 2 cycles which will allow the first cycle to be aged.

---

**Retention has been defined for 7 Days and 2 Cycles. When the data aging operation runs on Saturday, the cycles criteria has been met but not the days criteria.**

---

**Retention - 7 Days and 2 Cycles**

<table>
<thead>
<tr>
<th>Week 1</th>
<th>F</th>
<th>S</th>
<th>S</th>
<th>M</th>
<th>T</th>
<th>W</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FULL</td>
<td>INC</td>
<td>INC</td>
<td>FULL</td>
<td>INC</td>
<td>INC</td>
<td>INC</td>
</tr>
</tbody>
</table>

| Week 2 | FULL | INC | INC | INC | INC | INC | INC |

Saturday – Cycles met but not Days

---

**Retention has been defined for 7 Days and 2 Cycles. When the data aging operation runs on Monday both cycles and days criteria have been met and the first cycle will be marked as aged.**

---

**Retention - 7 Days and 2 Cycles**

<table>
<thead>
<tr>
<th>Week 1</th>
<th>F</th>
<th>S</th>
<th>S</th>
<th>M</th>
<th>T</th>
<th>W</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FULL</td>
<td>INC</td>
<td>INC</td>
<td>FULL</td>
<td>INC</td>
<td>INC</td>
<td>INC</td>
</tr>
</tbody>
</table>

| Week 2 | FULL | INC | INC | INC | INC | INC | INC |

Monday – Both criteria met first cycle aged
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.

Example: During a Friday night backup power is lost in the building. Power is restored on Sunday resulting in two days elapsing and counting towards retention. Note that since the Friday full failed the cycle continues into the next scheduled full (following Friday). This illustrates the importance of defining retention in both days and cycles.

---

A FAILURE OF A FULL BACKUP ON FRIDAY DUE TO A POWER OUTAGE RESULTS IN A CYCLE CONTINUING UNTIL A VALID FULL IS COMPLETED.

---

[Diagram showing a week with backups on Monday, Tuesday, Wednesday, Thursday, and full backup on Friday, with no backup performed on Saturday and Sunday.]
Additional Retention Settings

Retention Settings:

- Spool copy
- Extended retention
  - Do not use with dedupe disk storage
- Managed disk space
- Job based retention:
  - Retention set in schedule
  - Retention applied to job
- Enable / disable data aging

Spool Copy

The Spool Copy option can be used to take advantage of fast disk read/write access and its multi-streaming capabilities when there is limited capacity available on the disks. A spool copy is a no retention copy. Data is spooled to disk and then copied to a secondary copy. Once the data is successfully copied to the secondary copy, the data on disk will be pruned and the space will immediately be available for new backups. The spool copy option is not available when using deduplication.

Extended Retention

Standard retention allows you to define the length of time based on cycles and days that you want to retain data. Extended retention allows you to define specific retention in days that you want to keep full backups for. It allows you to extend the basic retention by assigning specific retention to fulls based on criteria configured in the extended retention settings. Basically it allows you to set a grandfather, father, son tape rotation scheme.

Example: You want to retain backups for 4 cycles and 28 days. You also want to retain a monthly full for three months, a quarterly full for a year, and a yearly full infinitely.

To accomplish this, you configure retention as follows:

- Standard retention is set for (4,28)
- Extended retention is configured for:
  - For 90 days keep monthly fulls
  - For 365 days keep quarterly fulls
  - For infinite keep yearly full
Extended retention rules are similar to selective copies in that they only apply to full backups. However, a selective copy creates an additional copy of a full and assigns it a specific retention. Extended retention applies retention to an existing full and does not create an additional copy. Determine which is the more appropriate solution when planning retention strategies. Note that it is not recommended to enable extended retention on a deduplicated copy. This exponentially inflates the size of the deduplication database, and could potentially lead to issues.

**Managed Disk Space**

*Managed Disk Space* is a feature used with disk libraries not using Commvault deduplication, which allows data to reside on the disk beyond its retention settings. This allows you to increase the chances of recovering data faster from primary storage on disk without changing retention settings. Managed data on disk is treated the same as retained data for data recovery.

Managed data will be held on the disk beyond the standard retention settings until an upper space threshold is reached. A monitoring process will detect data exceeding the upper threshold and then delete aged jobs from the media until a lower space threshold is reached. It is important to note that only aged jobs will be pruned. If all aged jobs are pruned and the lower threshold is not met, no more pruning will occur.

Managed disk thresholds are configured in the disk library properties and can be enabled in each storage policy copy.

As a general rule of thumb the upper threshold should be set to allow one hour of backups to run after the threshold is reached. The lower threshold should be set so that the managed disk space pruning operation will not run more than once in a backup time period as the pruning operation will have a negative effect on the performance of backups. For more information on configuring library settings for managed disk space, see Commvault’s online documentation.

**Job Based Retention**

Typically, retention is based on company policy and therefore managed through storage policy retention settings that affect all data being managed by the policy. There may be situations where job retention would need to be individually set. There are two methods to apply job based retention: through schedules or through storage policy copy job history.

**Retention Set Through Schedules**

Retention can be extended beyond the defined storage policy primary copy retention through a schedule or schedule policy. This is done by setting the *Extend Job Retention* options in the **Media** tab of Advanced Options. The default setting is to use storage policy primary copy retention settings. You can set schedule based retention for a specified number of days or infinitely retain the data. Retention settings at the schedule level cannot be shorter than the retention defined in the storage policy primary copy.

**Retention Applied to Job in Policy Copy**

Retention for a job in a primary or secondary storage policy copy can be retroactively modified by going to the job history for the copy. This can be done by selecting the storage policy copy where the job is located, right-click the copy and select View | Jobs. Specify the time range of the job then click OK. Right-click on the job and select Retain Job. The job can be retained infinitely or until a specific date. The job icon will change to reflect that the job has been pegged down.
Module 4: Client Administration
Client Tree Structure

Client Components:

- Client
- Agent
- Instance
- Backup set
- Subclient

Commvault software uses agents to communicate with file systems and applications that require protection. Any server with an Agent installed on it is referred to as a Client. Each Agent contains code that is used to communicate directly with the system requiring protection. The Agent will communicate using APIs or scripts that are native to the file system or application. For example: A Windows 2008 file system can use VSS to protect file data so the Windows Agent will have the option to enable VSS during backup operations.

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

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

Client Tree Structure

The Client Tree Structure defines a hierarchy for arranging various components of a client. This hierarchy will remain consistent throughout clients with different agents installed which results in simplified administration of a CommCell® environment.

Each component in the client tree structure provides specific functionality to properly configure, manage and protect production data. Each of these components has specific features and properties that can be configured to provide a comprehensive protection strategy.
The client tree structure will consist of the following components:

- Client identifies the client system by CommCell Client name and Host name or IP address.
- Agent is installed on the client or a proxy client to protect specific data such as files, databases or virtual machines.
- Instance is used with specific agent types such as database application or hypervisors to define specific configuration for an instance.
- Backup Set is a complete representation of all content the agent is responsible to protect.
- Subclient defines the actual data within the backup set that requires protection.
Client Administrative Tasks

Common Tasks:

- Check connectivity
- View schedules
- Job history
- Release license
- Activity control
- Update status

Check client connectivity (check readiness)

Connectivity to a client and all Storage Policy data paths for configured subclients within the client can be checked and reported on at the client level. This is actually a mini version of the CommCell Readiness report. It will ensure that the CommServe server can communicate with the client machine. It will also check data path connectivity to all MediaAgent and library paths for Storage Policies that are associated with subclients configured for the client.

View client schedules

Client schedules can be viewed and edited from the client, agent, backup 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 client, agent, backup set and subclient levels.
- If a schedule is associated with a schedule policy, the policy name is 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.

View client job history

Job history for data protection and restore operations can be viewed from the client, agent, backup set and subclient level.
Job history can be used to perform the following:

- View status of backup and restore jobs.
- View media used for the job.
- View items that successfully backed up or failed to back up.
- Browse a completed job.

**Releasing a License**

Releasing a license is a logical operation that can be applied to clients or agents. Releasing a license will ‘grey out’ the client or agent so data can still be recovered.

**Release License key points:**

- The client or agent will appear greyed out in the CommCell console. This means that data will still be retained and restored (out of place) in protected storage but the client cannot be backed up unless the license is re-applied.
- If the CommCell licensing structure is agent based, the license will be available to install on another system.
- If the CommCell licensing structure is capacity based, the size of data for the de-configured client or agent will not count against the capacity usage of the CommCell environment.
- Released licenses can be re-applied to the client by using the Reconfigure option.
- Agents and the client can be completely removed from the CommCell environment by using the Delete option. However, deleting a client results in deleting all the data that belongs to the client from the Content Store.

**Client Activity Control**

Data protection and data recovery jobs can be enabled or disabled in the Activity Control tab in the Client Properties. If activity is disabled, an Enable after a Delay button will be displayed. This can be used to automatically enable the activity on a specific date and time. Client activity control is useful when a client will be offline, since any scheduled operations are by default ignored if activity is disabled.

**Client Update Status**

Update status for clients can be viewed by selecting the Client Computers entity in the CommCell Browser or through the Client Properties page in the Version tab.

**Summary Update Status View for all Clients**

The current Commvault software version, service pack level, update status and operating system platform can be viewed for all Clients by selecting Client Computers icon in the CommCell Browser. This will display all clients in the CommCell environment providing summary information on their status.

**Checking Detailed Update Status for a Client**

The Version tab will display the current version of software, service pack level and status of each package installed on a client.

**Update status key points:**

- Installed packages will contain the status of Up to Date, Needs Updating or Ahead of cache. The Ahead of cache may appear in situations where updates have been applied to the system prior to their general release.
- Commvault recommends keeping all software up to date.
• If updates need to be applied to a client: Right-click Client | All tasks | Add/remove software | Install updates.
## Commvault® Agents

<table>
<thead>
<tr>
<th>Methods for Protecting Data:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard Backup Agents</strong></td>
</tr>
<tr>
<td>▪ File system backup</td>
</tr>
<tr>
<td>▪ Application backup agents</td>
</tr>
<tr>
<td>▪ Virtual Server Agent</td>
</tr>
<tr>
<td><strong>Archiving Agents</strong></td>
</tr>
<tr>
<td>▪ OnePass® Agent</td>
</tr>
<tr>
<td>▪ Classic archiver agent (not supported in V11)</td>
</tr>
<tr>
<td>▪ Compliance archiver agent</td>
</tr>
<tr>
<td><strong>Additional Agents and Protection Methods</strong></td>
</tr>
<tr>
<td>▪ Laptop and end user backup</td>
</tr>
<tr>
<td>▪ IntelliSnap® Technology</td>
</tr>
<tr>
<td>▪ Continuous Data Replicator</td>
</tr>
</tbody>
</table>

### Data Protection Methods

The backup and recovery system uses agents to interface with file systems and applications to facilitate the transfer of data from production systems to the Commvault protected environment.

#### File System Backup & Recovery

File system backups provide the fundamental data protection strategy in all data centers. File backups are supported for all major operating systems and include inherent file system capabilities based on the operating system being protected.

#### Application Backup & Recovery

Application protection uses application aware backups providing consistent point-in-time protection for application databases. Granular application protection for Exchange, SharePoint and Lotus Notes can be done to provide flexible data protection strategies and simplified recovery methods.

#### Virtual Environment Backup & Recovery

The Virtual Server Agent (VSA) provides complete virtual machine protection and granular recovery of virtual machine data without the need to install traditional agents within a virtual machine. The Virtual Server Agent can protect entire virtual machines or filters can be put in place to protect specific disks within the VM.
File & Application Data Archiving

Data archiving removes infrequently accessed data from production storage reducing backup and recovery windows and providing a greater return on investment by reducing production storage requirements. File system data, NAS data, Exchange mailbox, and SharePoint documents can be archived based on user defined rules.

Compliance Archiving

For Microsoft Exchange and Lotus Notes Domino server, Email messages being journaled can be protected with Commvault’s compliance archive component. This extends the retention on application based journaling indefinitely by protecting journaled data and then removing it from the production Email server. Journaled massages can be content indexed for legal discovery.

Laptop and End User Backup

For data not being centrally managed on servers, protection is still required. End user desktop and laptop systems can be protected using Commvault’s Desktop Laptop Option and deduplication features which will only protect changed blocks reducing backup requirements. Data can be defined based on data type (file extension) to protect critical user data. Automatic scheduling can be configured to backup data based on specific criteria such as subnet, bandwidth utilization, or disk consumption.

IntelliSnap® Snapshot Management

IntelliSnap technology integrates regular protection methods with hardware based snapshot technologies to coordinate and manage disk snapshots. The integration allows for application aware snapshots to be conducted for application data and virtual machines.

Continuous Data Replicator (CDR)

Continuous Data replicator (CDR) provides asynchronous replication of production data for mission critical applications. Data is replicated to secondary locations and point-in-time snapshots can be conducted for frequent recovery points. CDR can also integrate with the IntelliSnap® feature to provide software based snapshots if IntelliSnap feature does not support the disk hardware being used.
Subclients Overview

Key Points:

- What is a subclient
- Default Subclient

Subclients are used to define data that will be protected in a containerized format. Each subclient container will manage specific content within a backup set. Each backup set will have one or more subclients.

Key points for subclients:

- Subclient contents can be defined as drives, folders, files or UNC paths.
- Storage policy used to manage the subclient can be defined.
- Scripts can be inserted prior to scan and after backups.
- Filter settings can be configured for global and local filters.
- IntelliSnap® technology can be enabled and storage array managing subclient data can be defined.
- Data transfer options including compression, deduplication and encryption can be configured.

Default Subclient

By default, most Agents will have a Default Subclient. During the initial installation of the agent software an option to associate agent data with a storage policy is provided. This determines the storage policy that will manage the Default Subclient data. All subclients must be associated with a storage policy to protect the data.

The default subclient acts as a catch all for all data managed within a backup set. This means the default subclient will automatically detect and protect all data the agent is responsible to protect. When custom subclients are defined, any data managed by the custom subclient will automatically be excluded from the default subclient. This is the concept of mutual exclusiveness of contents within a backup set. Data is mutually exclusive to the subclient in which it is defined and data cannot be defined in multiple subclients within the backup set. The concept of Commvault software is to Copy Once and Reuse Extensively (CORE). In other words, protect the data to the storage policy and use secondary
copies to create additional copies of data. There are situations where protecting data from the source location multiple times may be required. To accomplish this you can create additional backup sets.

Modifying Contents of the Default Subclient

The content of the default subclient is represented by a slash (backslash for windows based agents and forward slash for Linux/Unix based clients). It is strongly NOT recommended to modify the contents of the default subclient. Modifying this content will disable the auto detect functionality of the default subclient. If this is done any future content required for protection must be explicitly added to the subclient contents.
Subclient Configuration

File System Agents:

- **Content**
  - Drives, folders, files
  - Content library
- **Data Readers**
  - Multiple readers in drive or mount path
- **Storage policy**
- **VSS**
- **Scan type**

Defining Contents

The Contents tab is used to define the content for the subclient. There are several important points that should be understood before configuring subclient content:

- The contents of a Default Subclient for most backup agents is a \ (windows based) or / (Linux/Unix based). This represents an auto detection functionality that will protect any newly added volumes. If the default subclient’s content is modified the \ or / will be removed and auto detection will be disabled. It is NOT recommended that the contents of the default subclient be modified. If only certain drives are to be protected, use the Filter tab to exclude the drives.
- Content can be added by browsing (Browse button) or manually entered (Add Paths button).
- Use the Add Paths button to enter UNC paths to protect data on systems that do not have Commvault agents installed. An impersonate user box will prompt you to enter a user account with proper permissions to read the data from the shared location. This feature is only recommended when protecting small amounts of data.
- The option to Backup System State can be used to protect system state data for Windows servers. By default, the default subclient will automatically protect system state data. If required, a separate subclient can be defined to specifically protect system state. Only one subclient within a backup set can be designated to protect system state data.

Data Readers

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

Allow multiple readers within a drive or mount point

When a disk array containing several physical disks is addressed logically by the OS as a single drive letter, the Allow multiple readers within a drive or mount point can be used as an override. This will allow a backup job to take advantage of the fast read access of a RAID array.

Storage Policy Association

Traditionally data protection has always been approached at the server level where an entire server is protected as one piece. Commvault software handles data protection at the subclient level where each subclient when protected will run as a separate job. If three subclients are defined within a backup set, if they all run at the same time, three jobs will appear in the job controller.

Content defined at the subclient level is directed to storage through a Storage Policy. This means that data defined in different subclients on the same server can be directed to different storage and have different retention settings.

System State for Windows Subclients

For Windows operating systems, ensuring proper protection of System State is critical when performing full system restores. VSS should be used for System State backups to ensure all components are properly being protected.

System State and Domain Controllers

For Domain Controllers, System State backups will backup the Active Directory database. This will be used when restoring Domain Controllers which can be restored in an Authoritative or Non-Authoritative restore mode. Although Microsoft recommends and many administrators will choose to rebuild Domain Controllers, the ability to use the Commvault software to restore a Domain Controller is critical, especially in a disaster situation.

Adding Subclients

Backup set | All tasks | New subclient

Notes on adding subclients:

- When new subclients are added, the content defined in the new subclient is automatically removed from the default subclient.
- Content within a backup set cannot be defined in more than one subclient.

Deleting Subclients

Right-click on Subclient | Delete

Notes on deleting subclients:

- Deleting a subclient will NOT result in data already protected for the subclient being deleted.
- When a subclient is deleted the content that was defined for the deleted subclient will automatically be included in the default subclient in future data protection jobs.
- To browse previous backup job for the deleted subclient, simply browse at the backup set level.
### Filtering

#### Global and Subclient Filters:

- **Global filters**
  - Use global filters on all subclients

- **Subclient filters**
  - On
  - Off
  - Global settings

- **Filter exceptions**

Filters are defined at the global and subclient level to remove specific folders and objects that do not require protection. Global filters defined in the Global Filters applet in Control Panel can be automatically or manually associated with subclients. If global filters are associated with a subclient, the choice to override the global filters will be available.

**Global and subclient filter key points:**

- Global filters can be defined for Windows, UNIX, Exchange and Virtual Servers.
- To enforce global filters to subclients enable the Use Global Filters on all Subclients check box.
- Subclient settings to inherit global filters are configured as:
  - On – always use global filters
  - Off – never use global filters
  - Cell Level Policy – only use global filters if Use Global Filters on all Subclients check box has been enabled.
- Subclient filters include exclusion and exception filter entries:
  - Exclusion filters determines which folders and/or objects will be excluded from the subclient.
  - Exception is an override for exception and global filters. This means any folders and/or objects defined in the exception entry will be protected by the subclient.

Subclient Design Strategies

Reasons for custom subclients:

- Special protection needs:
- Different retention requirements
- Performance requirements
- Special filters
- Open file handling
- Pre / Post process scripts

Defining custom subclients allow for much greater flexibility in crafting a comprehensive protection strategy. User defined subclients allow data to be explicitly defined within a subclient container. This subclient container can then be protected and managed independently within Commvault protected storage. There are many advantages to using custom subclients. The following list highlights the primary advantages of using custom subclients:

- Allows for better media management by meeting protection needs based on specific content.
- Better performance by using multiple streams within a subclient, protecting multiple subclients concurrently or by stagger scheduling subclients over a longer time period.
- Allow for custom configurations for specific data such as open file handling, filtering or Pre/Post Process scripts.

Special Protection Needs

Data being protected by an agent is by default protected by the Default Subclient. Custom subclients can be explicitly defined to manage specific data such as a folder or database. Each subclient container can be managed independently in protected storage. This can reduce the amount of data that needs to be protected by associating just subclient data to the storage policy copy to meet protection requirements.

Example: A file server with 800 GB of data has a file share containing critical financial data that must be retained for 10 years. The folder containing the data can be defined in a separate subclient and the subclient can be associated with a storage policy copy with a 10 years retention. The result is instead of keeping all 800GB of data for 10 years; only the financial data will be kept for the required period.
Performance Requirements

Each defined subclient will be an independent job and use independent streams when being protected. There are several reasons why this will improve performance:

Multiple Stream Backups

A subclient can be configured to use multiple streams for supported agents. This is useful when data is being stored on a RAID array. To take advantage of RAID’s fast read access; multiple streams can be used to improve the performance of data protection operations.

Multiple Subclients running concurrently will result in multiple stream data protection operations. This is especially useful when the application does not inherently support multi-stream backups such as Exchange message level backups or archives.

Stagger Schedule Backups

By creating separate subclients, you can stagger schedule data protection operations. Instead of trying to get a full backup done in one night, different subclients can scheduled to run full backups throughout the week or month and incremental backups on other days. This can be especially useful for virtual machine backups or Network Attached Storage with large file counts.

Filters

Filters can be applied through the Global Filter applet in Control Panel or locally at the subclient level. If specific folder locations require special filters, a dedicated subclient should be used. Define the subclient content to the location where the filters will be applied and configure local filters for that subclient. The option to use Global Filters can still be used allowing the global and local filters to be combined.

If global filters are being used but specific subclient data should not have certain filters applied, define the content in a separate subclient. Global filters can still be enabled for the subclient but the exclusions list can be used to override the global filter settings for specific file/folder patterns.

Open File Handling

Open file Handling using Microsoft VSS or Commvault QSnap can be used to ensure open files are protected. VSS is an available option for Windows 2003 or higher agents. Non-Windows agents can use Commvault QSnap to ensure open files are protected.

Pre/Post Scripts

Pre/Post Process scripts can be used to quiesce applications prior to protection. This is very useful when protecting proprietary database systems or for quiescing databases within virtual machines prior to using the Commvault Virtual Server Agent for snapping and backing up the virtual machine.
Module 5: Data Protection and Recovery
Data Protection
Data Protection Overview

Backup Types:

<table>
<thead>
<tr>
<th>Standard Backup Types:</th>
<th>Full Backup Types:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full</td>
<td>Incremental</td>
</tr>
<tr>
<td></td>
<td>Differential</td>
</tr>
<tr>
<td></td>
<td>Synthetic Full</td>
</tr>
<tr>
<td></td>
<td>Auxiliary Copy</td>
</tr>
<tr>
<td>Deduplication Enhanced:</td>
<td>DASH Full</td>
</tr>
<tr>
<td></td>
<td>DASH Copy</td>
</tr>
</tbody>
</table>

Backup Types

Full

A full backup will protect all data within a subclient each time it is run. This provides the most complete level of protection by backing up all data every time the job runs. This will also provide for the fastest recovery time since all data is contained within a single job. Full backups will require the most storage space and take the longest time to complete.

Incremental

Incremental backups protect all data that has been added or modified since the last successful backup operation. Based on the average incremental rate of change and growth the incremental backups should remain consistent in size. An incremental backup is considered a dependent operation as it is dependent on previous incremental backups and the full backup which started the cycle. For a full restore of data the full and all incremental backups will be required.

Differential

A differential job backs up all data that has been modified or added since the last full backup job. The first differential job following a full backup would just contain incremental changes since the full backup completed. As subsequent differential backups are run the backup size will increase since all changed and added data will be backed up in each differential. As the cycle progresses and more differential backups are run they will continually increase in size requiring more storage until the next full backup runs. Restores will be slower than a full but faster than using incremental jobs since only the full and most recent differential will be required for complete restore. Another
advantage of differential jobs is that modified data is being redundantly stored throughout the cycle as each differential completes. This could potentially limit data loss if a differential job is lost or damaged.

**Synthetic Full**

A synthetic full backup synthesizes full backup operations by copying previously backed up data into a new full backup job. It works by using the Image file from the most recent backup. The image file contains a list of all objects that existed at the time the backup operation was run. The synthetic full uses the image to determine which objects require protection and copies the objects from previous backup jobs into a new synthetic full backup. No data is backed up from the production client.

For synthetic full backups to work properly, an initial full must be run which provides the foundation in which the synthetic fulls will be based on. Incremental backups must be run after the initial full and subsequent synthetic full to ensure all required objects are in protected storage. When the synthetic full runs, it copies all required objects into a new synthesized full backup which will then become the foundation for the next synthetic full backup.

**DASH Full**

A read optimized synthetic DASH Full uses the Commvault deduplication feature to logically perform synthesized full backups without moving any data. This can be accomplished because Commvault deduplication tracks the location of all blocks on disk storage. After the initial foundation full is run and subsequent incremental jobs are run, all block data required for the synthetic full is already present in the deduplicated disk storage location. Since deduplication will only store a unique block once in storage, the DASH Full operation will only make references to the blocks in storage and not actually copy them. The DASH Full operation will generate a new index file signifying that a full backup was run and update the deduplication database with block record data that is used for data aging purposes. DASH Full backups are the preferred method of running full backup jobs and can dramatically reduce backup windows.

**Auxiliary Copy**

Auxiliary copy operation allows you to schedule, run on-demand, save a job as a script, or set an automatic copy. When configuring Auxiliary copy operations there are several options you can configure:

- Allocate number of drives to use during auxiliary copy
- Which secondary copies you want to include in the auxiliary copy
- Start new media and mark media full which can be used to isolate jobs on media
- VaultTracker options which can be used to export and track media using VaultTracker™ policies and reports
- Job priorities to assign different job priorities for auxiliary copies

**DASH 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.
DASH Copy has several advantages over traditional replication methods:

- DASH Copies are auxiliary copy operations so they can be scheduled to run at optimal time periods when network bandwidth is readily available. Traditional replication would replicate data blocks as it arrives at the source.

- Not all data on the source disk needs to be copied to the target disk. Using the subclient associations of the secondary copy, only the data required to be copied would be selected. Traditional replication would require all data on the source to be replicated to the destination.

- Different retention values can be set to each copy. Traditional replication would use the same retention settings for both the source and target.

DASH Copy is more resilient in that if the source disk data becomes corrupt the target is still aware of all data blocks existing on the disk. This means after the source disk is repopulated with data blocks, duplicate blocks will not be sent to the target, only changed blocks. Traditional replication would require the entire replication process to start over if the source data became corrupt.
Job Initiation

Initiation Methods:

- Run immediately
- Schedule
- Schedule policy
- Save as script

Scheduling

Most data protection jobs using traditional backups or snapshots are scheduled. The frequency of scheduled jobs should be based on the 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 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 methods could shrink RTO times.

Scripting

When jobs are configured in the CommCell console they can be saved as scripts. This provides the advantage of executing jobs on demand. For example: A Database Administrator dumps database files each night. The dump process finishes at different times each night and there is a risk that a scheduled backup may run before the dump operations are complete. If the backup of the dump location is saved as a script, the DBA can call the script once the dump operations complete ensuring the data is properly protected.
Synthetic Full and DASH Full Jobs

Key Points:

- Synthetic full
  - Synthesizes full by consolidating data from previous backups
- DASH full

A synthetic full backup synthesizes full backup operations by copying previously backed up data into a new full backup job. It works by using the Image file from the most recent backup. The image file contains a list of all objects that existed at the time the backup operation was run. The synthetic full uses the image to determine which objects require protection and copies the objects from previous backup jobs into a new synthetic full backup. No data is backed up from the production client.

For synthetic full backups to work properly, an initial full must be run which provides the foundation in which the synthetic fulls will be based on. Incremental backups must be run after the initial full and subsequent synthetic full to ensure all required objects are in protected storage. When the synthetic full runs it copies all required objects into a new synthesized full backup which will then become the foundation for the next synthetic full backup.

Synthetic Full key points:

- Synthetic full backups are useful for large volumes or Exchange mailbox backups where many objects require protection or when the production client has very short operation windows.
- Synthetic full backups work best on non-deduplicated disk storage. When using Commvault deduplication use DASH Full backups instead of traditional synthetic full backups.
- Using Synthetic full backups on appliance based deduplication devices can have a negative impact on performance. In some cases, the performance can be slower than running regular full backups. Test this option before implementing if using 3rd party deduplication solutions.

Read Optimized Synthetic DASH Full

A read optimized synthetic DASH Full uses the Commvault deduplication feature to logically perform synthesized full backups without moving any data. This can be accomplished because Commvault deduplication tracks the location of...
all blocks on disk storage. After the initial foundation full is run and subsequent incremental jobs are run, all block
data required for the synthetic full is already present in the deduplicated disk storage location. Since deduplication will
only store a unique block once in storage, the DASH Full operation will only make references to the blocks in storage
and not actually copy them. The DASH Full operation will generate a new index file signifying that a full backup was
run and update the deduplication database with block record data that is used for data aging purposes. DASH Full
backups are the preferred method of running full backup jobs and can dramatically reduce backup windows.
Auxiliary Copy and DASH Copy Jobs

Key Points:

- Does not require indexes
- Auxiliary Copy Options:
  - Automatic copy
  - Inline copy
  - Parallel copy
  - Deferred copy
- DASH copy
  - Disk read optimized
  - Network optimized

Auxiliary copy operation allows you to schedule, run on-demand, save a job as a script, or set an automatic copy. When configuring Auxiliary copy operations there are several options you can configure:

- Allocate number of drives to use during auxiliary copy
- Which secondary copies you want to include in the auxiliary copy
- Start new media and mark media full which can be used to isolate jobs on media
- Vault tracker options which can be used to export and track media using VaultTracker™ policies and reports
- Job priorities to assign different job priorities for auxiliary copies

Automatic Copy

Most jobs run once during a day and a normal schedule can be used for auxiliary copies. The automatic copy allows you set a check interval for source data to be copied. This can be a great advantage when jobs are being run multiple times per day or if you are unsure when the source data will be available for copy.

Example: A critical database is running transaction log backups every four hours. You want to run an auxiliary copy of the source transaction logs to a secondary location, in this case a disk library off-site.

Solution: Schedule the transaction logs to backup every four hours. Then set the automatic copy option to check for source data. If source data is present, the auxiliary copy will run creating an additional copy of the data.

Note: A System Created AutoCopy schedule policy gets created when Commvault software is installed. Any created secondary copy will be associated to that schedule policy by default.
Inline Copy
The Inline Copy feature allows you to create additional copies of data at the same time you are performing primary backups. This feature can be useful when you need to get two copies of data done quickly. Data is passed from the client to the MediaAgent as job streams. The MediaAgent then creates two sets of device streams, each going to the appropriate library. This can be a quick method for creating multiple copies but there are some caveats:

- Inline Copy is not supported if Client Side Deduplication has been enabled.
- If the primary copy fails, the secondary copy will also fail.
- Since both copies are made at the same time twice as many library resources will be required which may prevent other jobs from running.
- Since backup data is streamed, data will be sent to both libraries simultaneously, which may cause overall performance to degrade. Basically, your job will run as fast as the slowest resource.

Parallel Copy
A parallel copy will generate two secondary copy jobs concurrently when an auxiliary copy job runs. Both secondary copies must have the Enable Parallel Copy option enabled and the destination libraries must be accessible from the same MediaAgent.

Deferred Copy
Deferring an auxiliary copy will prevent a copy from running for a specified number of days. Setting this option will result in data not aging from the source location regardless of the retention on the source until the auxiliary copy is completed. This option is traditionally used in Hierarchal Storage Management (HSM) strategies where data will remain in a storage policy copy for a certain period of time. After that time period, the data will be copied to another storage policy copy and deleted from the source once the copy is completed. Although this method was implemented since traditional HSM solutions worked this way, with Commvault software it is recommended to copy data to multiple HSM copies to provide for disaster recovery as well as HSM archiving.

DASH Copy
A DASH Copy efficiently copies data to secondary storage locations by only transmitting unique blocks to the destination MediaAgent. Disk Optimized is the most efficient copy method and should be used when the source library is deduplication enabled. Network Optimized should only be used if the source library does not have deduplication enabled. To schedule an auxiliary copy job as a DASH Copy, first go to the Secondary Copy Properties Deduplication tab and, from the Advanced sub tab, ensure the ‘Enable DASH Copy’ check box is checked and ensure that ‘Disk Optimized’ is also checked.

Once Enabled:
1. Right-click the Storage Policy.
2. Select All Tasks and then Run Auxiliary Copy.
3. The Auxiliary Copy can be run immediately, scheduled, or set to run at automatic time intervals.
Using Schedules and Schedule Policies

Commvault® software uses a standard scheduler which is used for scheduling all operations within the CommCell® environment. The following is a list of operations which can be scheduled within a CommCell environment:

1. Data protection operations
2. Data recovery operations
3. CommServe DR backup
4. Reports
5. Data Aging

Schedule Frequency

Jobs can be configured to run once or repeat based on set frequencies.

Job frequency can be set for the following:

- Daily
- Weekly
- Monthly
- Yearly
- Automatic
Daily jobs can be set to start and end at a certain time each day. A repeat interval can be configured to have the job run multiple times per day with an hour and minute recurrence interval.

Weekly jobs can be configured to run on specific days of the week. Jobs can also be set to repeat every set number of weeks and an exception can also be added. For example: A job needs to be scheduled to run every Friday except for the last Friday of the month. Set the weekly schedule to run on Friday, repeat every week and set an exception for the last Friday of the month.

Monthly jobs can be configured to run based on the following criteria: On the first, second, third, fourth or last day of a month. The day of the month specified can be a day of the week, day, weekday or weekend day.

Yearly jobs can be configured to run based on the following:

- Specific day of a specific month.
- On the first, second, third, fourth or last day of a specific month.
- The day of the month specified can be a day of the week, day, weekday or weekend day.

Automatic schedules are used for protecting end user workstations or automatically scheduling specific database applications log backups such as SQL or Oracle.

Schedule and Schedule Policy Settings

<table>
<thead>
<tr>
<th>Schedule Type:</th>
<th>One Time</th>
</tr>
</thead>
</table>
| Select date and time of one time job | You can specify to the minute when you want a job to start. The date can be selected through a drop-down calendar box. In the date box use the inner arrows to switch between months and the outer arrows to switch between years.  
This can be useful when a specific backup has been requested at some point in the future. Instead of remembering to initiate the job at the requested time, you can just schedule it. |
| Time Zone | By default, the time zone used will be the time zone of the CommServe server. If you have clients in other time zones use this option to set the correct time zone for the client. |

<table>
<thead>
<tr>
<th>Schedule Type:</th>
<th>Daily</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>Set the start time for the job.</td>
</tr>
<tr>
<td>Range of Recurrence: Start</td>
<td>The start date will default to today’s date. You can select a specific future date for the schedule to begin. The date can be selected through a drop-down calendar box. In the date box, use the inner arrows to switch between months and the outer arrows to switch between years.</td>
</tr>
<tr>
<td><strong>Range of Recurrence:</strong></td>
<td>Makes this schedule permanent.</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td><strong>Range of Recurrence:</strong></td>
<td>Allows you to terminate the schedule after a specific date and time.</td>
</tr>
<tr>
<td><strong>End By</strong></td>
<td>Allows you to determine how many times the job will be run before the schedule is terminated.</td>
</tr>
<tr>
<td><strong>Repeat Every nn Days</strong></td>
<td>This defaults to 1. You can change this option to specify how many days the job will wait before it runs again.</td>
</tr>
<tr>
<td><strong>Repeat Every nn Hours and xx Minutes</strong></td>
<td>This determines how frequently the job will be run. This is useful for frequent backup requirements such as transaction logs or point-in-time incremental backups. For example, you can schedule a daily transaction log backup to begin at 7:00 AM and repeat every 1 hour until 8:00 PM.</td>
</tr>
<tr>
<td><strong>Time Zone</strong></td>
<td>By default, the time zone used will be the time zone of the CommServe server. If you have clients in other time zones use this option to set the correct time zone for the client.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Schedule Type:</strong></th>
<th><strong>Weekly</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>This schedule option multiple days in a week that a job will run. This schedule will repeat on a weekly basis. This can be useful for backups that you want to run multiple days in a week except for certain days. For example, you can schedule incremental backup jobs to run Monday through Thursday but not Friday through Sunday.</td>
<td></td>
</tr>
<tr>
<td><strong>Start Time</strong></td>
<td>Set the start time for the job.</td>
</tr>
<tr>
<td><strong>One These Days</strong></td>
<td>Select which days you want the job to run each week. The options default to Sunday through Thursday.</td>
</tr>
<tr>
<td><strong>Range of Recurrence:</strong></td>
<td>The start date will default to today’s date. You can select a specific future date for the schedule to begin. The date can be selected through a drop-down calendar box. In the date box use the inner arrows to switch between months and the outer arrows to switch between years.</td>
</tr>
<tr>
<td><strong>End</strong></td>
<td>Makes this schedule permanent.</td>
</tr>
<tr>
<td><strong>Never End</strong></td>
<td>Allows you to terminate the schedule after a specific date and time.</td>
</tr>
<tr>
<td><strong>End After</strong></td>
<td>Allows you to determine how many times the job will be run before the schedule is terminated.</td>
</tr>
<tr>
<td>Repeat Every nn Weeks</td>
<td>Allows you to specify how many weeks will be skipped before the weekly schedule is run again. This defaults to one week.</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Advanced Button</td>
<td>Use this to exclude a particular day within the month. The options are: first, second, third, fourth, or last day and the day can be selected as a day of the week, weekend day, week day, or day. This offers tremendous flexibility in the scheduler. For example, you can schedule a weekly full backup to run every Friday except for the last Friday of the month. The last Friday full that runs in the month can then have special attributes associated with it such as isolating the job on specific media, forcing the creation of a new index file, or automatically exporting the tape after the job completes.</td>
</tr>
<tr>
<td>Repeat Every nn Hours and xx Minutes</td>
<td>This determines how frequently the job will be run. This is useful for frequent backup requirements such as transaction logs or point in time incremental backups. For example, you can schedule a daily transaction log backup to begin at 7:00 AM and repeat every 1 hour until 8:00 PM.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>By default, the time zone used will be the time zone of the CommServe server. If you have clients in other time zones use this option to set the correct time zone for the client.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Schedule Type:</th>
<th>Monthly</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Monthly backup schedules are useful for special backup types such as month end or quarter end operations. Very specific schedules can be set up to meet corporate and government compliance requirements. The monthly schedule options can be fully customized to accomplish these requirements.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Specific time the job will begin.</td>
</tr>
<tr>
<td>On Day</td>
<td>Specify a particular day of the month you want the job to run.</td>
</tr>
<tr>
<td>On The</td>
<td>You can specify a particular day of the month you want the job to run. The options are: first, second, third, fourth or last day and the day can be selected as a day of the week, weekend day, week day, or day. This option can be used to customize operations to run on specific points in the month for compliance requirements. For example, you can specify a job to run on the last weekday of the month. This will result in a backup on the last business day. Note that weekday will not account for time periods ending on a holiday and business is closed. You can use custom calendars to overcome this.</td>
</tr>
<tr>
<td>Range of Recurrence:</td>
<td>The start date will default to today’s date. You can select a specific future date for the schedule to begin. The date can be selected through a drop-down calendar box. In the date box, use the inner arrows to switch between months and the outer arrows to switch between years.</td>
</tr>
<tr>
<td>Range of Recurrence: Never End</td>
<td>Makes this schedule permanent.</td>
</tr>
<tr>
<td>Range of Recurrence: End By</td>
<td>Allows you to terminate the schedule after a specific date and time.</td>
</tr>
<tr>
<td>Range of Recurrence: End After</td>
<td>Allows you to determine how many times the job will be run before the schedule is terminated.</td>
</tr>
<tr>
<td>Repeat Every nn Months</td>
<td>This can specify how many months to skip before repeating the job. This is a very powerful option for monthly schedules. For example, you can set a schedule to run on the last weekday of the month, specify the start date of the schedule to be the last day of the quarter, and have the job repeat every three months. This configuration will result in a quarter end backup job.</td>
</tr>
<tr>
<td>Repeat Every nn Hours and xx Minutes</td>
<td>This determines how frequently the job will be run. This is useful for frequent backup requirements such as transaction logs or point in time incremental backups. For example, you can schedule a daily transaction log backup to begin at 7:00 AM and repeat every 1 hour until 8:00 PM.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>By default, the time zone used will be the time zone of the CommServe server. If you have clients in other time zones use this option to set the correct time zone for the client.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Schedule Type:</th>
<th>Yearly</th>
</tr>
</thead>
<tbody>
<tr>
<td>A yearly backup can be defined to run a once a year backup. This is also useful for the compliance type of operations.</td>
<td></td>
</tr>
</tbody>
</table>

| Start Time | Determines the time the job will begin. |
| On Day | Allows you to specify a particular day of a particular month. |
| On The | You can specify a particular day of the year you want the job to run. The options are: which month, the first, second, third, fourth or last day and the day can be selected as a day of the week, weekend day, week day, or day. |
| Range of Recurrence: Start | The start date will default to today’s date. You can select a specific future date for the schedule to begin. The date can be selected through a drop-down calendar box. In the date box use the inner arrows to switch between months and the outer arrows to switch between years. |
| Range of Recurrence: Never End | Makes this schedule permanent. |
| Range of Recurrence: End By | Allows you to terminate the schedule after a specific date and time. |
| **Range of Recurrence:**<br>**End After** | Allows you to determine how many times the job will be run before the schedule is terminated. |
| **Repeat Every nn Hours and xx Minutes** | This determines how frequently the job will be run. This is useful for frequent backup requirements such as transaction logs or point in time incremental backups. For example, you can schedule a daily transaction log backup to begin at 7:00 AM and repeat every 1 hour until 8:00 PM. |
| **Time Zone** | By default, the time zone used will be the time zone of the CommServe server. If you have clients in other time zones use this option to set the correct time zone for the client. |
Automatic Schedules

Use Auto Schedules for:

- **Laptops**
- **Databases**
  - SQL
  - Oracle / Oracle RAC
  - SAP on Oracle
  - IBM Notes
- **Auxiliary Copy**

Commvault® software provides the ability to control the execution of jobs using an automatic schedule. The automatic schedule uses criteria which, when met, triggers the execution of the task automatically. Automatic schedules can be used for three specific scenarios:

- Laptop backups
- Database backups
- Auxiliary Copy

**Automatic Laptop Backup**

The protection of mobile users’ laptops can be controlled through an automatic schedule that uses criteria such as available bandwidth, AC power, if the laptop is idle, and more. This ensures that backups are executed when the computer is under ideal condition.

When setting up the criteria for laptop backups, two values must be set for interval between jobs, which are as follows:

- **Minimum interval between job** – This is the minimal time between two consecutive backup jobs. The default value is 15 minutes. If the laptop has been protected more than 15 minutes ago, and if it meets all requirements such as available bandwidth, AC power, etc., it will get protected.

- **Maximum interval between job** – This is the maximum acceptable time between backup job. The default value is 72 hours. This means that if a laptop has been protected more than 72 hours ago, even if it does not meet the requirements such as available bandwidth, AC power, etc., the system will try to back it up. This prevents
a computer to go for a long period without being protected, such as scenarios where the user frequently use it on battery, or the bandwidth is limited.

**Automatic database log backups**

The automatic backup schedule for databases allows to set a space usage threshold for the volume where the database log files reside. If the space usage is reached, a backup is triggered, which implies truncating the logs at the end of the backup. It will therefore free up space on the volume. This is a useful tool to prevent database log volumes to fill up if backups are not scheduled to run frequently enough. When setting up the criteria for database backups, two values must be set for interval between backup jobs, which are as follows:

- Minimum interval between job – This is the minimal time between two consecutive backup jobs. The default value is 15 minutes. If the database has been protected more than 15 minutes ago, and its log volume space usage reaches the defined usage threshold, it will be protected.

- Maximum interval between job – This is the maximum acceptable time between backup job. The default value is 72 hours. This means that if a database has been protected more than 72 hours ago, even if log volume space usage has not reached the defined threshold, the system will protect it.

**Automatic Auxiliary Copy Schedule**

An automatic schedule can be used to run an auxiliary copy. When using an automatic schedule, a frequency such as every 30 minutes must be defined. In such case, every 30 minutes, the system will establish if there are completed jobs in a storage policy primary copy that have not yet been copied to a secondary copy. If this is the case, the auxiliary copy job will start copying these jobs.

Using an automatic schedule has a significant advantage over a traditional auxiliary copy schedule that runs after the backups. Since it is executed every 30 minutes, if there are completed jobs, they will be copied even if other backup jobs are still running. This provides the shortest auxiliary copy window possible.

By default, when Commvault® software is installed, a schedule policy named *System Created Autocopy schedule* is implemented. When a storage policy secondary copy is created, it automatically gets associated with that schedule policy that will execute auxiliary copies every 30 minutes.
Managing Active Jobs

Job Controller Functions:

- Changing job state:
  - Suspend
  - Resume
  - Kill
  - Commit

- Job details

- Job filtering

The *Job Controller* in the CommCell console is used to manage all active jobs within the CommCell environment. Regardless of which method is used to initiate a job (schedule, on demand or script), the job will appear in the job controller. The job controller is the most effective tool within the CommCell console for managing and troubleshooting active jobs. The functionality and customization features will be discussed in the following section.

The following lists the common actions that can be conducted from the job controller:

- Suspend / Resume / Kill / Commit
- Change job priority
- View events
- View logs
- Add a job alert
- View job details
- Apply job controller filters
Working with Job Controller Fields

The job controller is completely customizable through the following actions:

- **Move a field** – Click and drag the field to the desired location in the job controller.
- **Resize the field** – Click the outer edge of the field and drag to the desired size.
- **Sort the field** – Click on the field and an arrow on the left side will appear. You can sort in order or reverse order for the field.
- **Add/remove field** – Fields can be added and removed. This will be discussed in the next section.

Adding / Removing Fields

Select double down-arrow in the upper left corner | choose columns | select desired columns

- Fields can be added and removed by using the menu arrow in the upper left corner.
- Fields recommended to be added to the job controller:
  - **Number of Readers in use** – this field will display the number of streams per job that are being used for the operation. Note that the ‘readers in use’ field only displays a number during the backup phase.
  - **Current throughput** – displays the current throughput in GB per hour.
  - **Priority** – displays the job priority for the operation.

Changing Job Status

Right-click job | select Suspend, Resume or Kill

Multi-Job Control

When changing status for multiple jobs at the same time there are two methods that can be used:

- Select multiple jobs using the Shift or CTRL keys.
- Use the multi-job menu option.

Change job status of multiple jobs

Select multiple jobs using Shift or Ctrl keys | Right-click | Suspend, Resume or Kill

The status of multiple jobs can be changed by using the Shift or CTRL keys to select multiple jobs and then right-clicking on one of the selected jobs.

Filtering the Job Controller Window

Right-click in the Job Controller window | Filters. To add a new filter, Select New Filter button. To apply an existing filter, from the Filters drop-down box select the filter.
Controlling Job Activity

Activity Control Methods:

- Activity control
- Job priorities
- Operation rules

<table>
<thead>
<tr>
<th>Activity Control Methods</th>
<th>Activity that can be enabled or disabled</th>
<th>CommCell</th>
<th>Client Group</th>
<th>Client</th>
<th>Agent</th>
<th>Backup Set</th>
<th>Subclient</th>
</tr>
</thead>
<tbody>
<tr>
<td>All activity</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Data Management</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Data Recovery</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Auxiliary Copy</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Data Aging</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Schedule Activity</td>
<td>Yes</td>
<td>No</td>
<td>Yes (enabled/disabled through schedule view for client)</td>
<td>Yes (enabled/disabled through schedule view for IDA)</td>
<td>Yes (enabled/disabled through schedule view for Backup Set)</td>
<td>Yes (enabled/disabled through schedule view for subclient)</td>
<td></td>
</tr>
</tbody>
</table>

Commvault software offers a great deal of flexibility for controlling job activity.

Job Activity Key points:

- If activity is disabled in a parent object of the CommCell tree, activity is automatically disabled for any child objects.
- Activity can be disabled until manually enabled or set to automatically re-enable at a specific date and time.
- If activity is enabled for a parent object in the CommCell tree, activity can be enabled or disabled for any child objects.
- When activity is disabled or enabled, the icon where the activity was set will change to reflect the current activity state.
What Activity can be Controlled

CommCell Level

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

<table>
<thead>
<tr>
<th>Activity that can be enabled or disabled</th>
<th>CommCell</th>
<th>Client Group</th>
<th>Client</th>
<th>Agent</th>
<th>Backup Set</th>
<th>Subclient</th>
</tr>
</thead>
<tbody>
<tr>
<td>All activity</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Data Management</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Data Recovery</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Auxiliary Copy</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Data Aging</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Schedule Activity</td>
<td>Yes</td>
<td>No</td>
<td>Yes (enabled / disabled through schedule view for client)</td>
<td>Yes (enabled / disabled through schedule view for iDA)</td>
<td>Yes (enabled / disabled through schedule view for Backup Set)</td>
<td>Yes (enabled / disabled through schedule view for subclient)</td>
</tr>
</tbody>
</table>

Enabling or Disabling CommCell Activity

Disabling Job Activity

If job activity is disabled at any level within the CommCell tree it will automatically disable activity for any child objects within the tree. Activity cannot be overridden at any child levels.

Example: A client computer group representing clients for a specific location is disabled for maintenance. By disabling activity at the group level, all clients within the group will automatically be disabled.
Enabling Job Activity

If job activity is enabled at any level within the CommCell tree activity can be disabled at any child level object within the tree.

Example: A specific client has a maintenance window scheduled. By disabling the activity for that client no operations will run. All other clients within the group will operate normally.

Enabling After Delay

If activity is disabled at any level in the CommCell tree the option Enable after a Delay can be used to set a date and time where activity will automatically be re-enabled.

Job Priorities

Commvault software implements a robust method for configuring job priorities. There are three different number values that make up a job priority, the job type, client and agent. The three numbers are combined to form a three-digit priority level. In Commvault software the zero value has the highest priority and the nine value has the lowest priority.

Each job type will have a specific priority value associated with it. CommCell administrative operations such as data aging and the CommServe DR backup have a zero level priority. Restore operations also have a zero level priority. Backup operations have a one level priority. Auxiliary copy jobs have a two level priority.

Client priorities are configured for individual clients in the Job Options tab in the client properties. The default client priority is six.

Agent priorities are configured for each agent type in the Job Management applet in control panel and have a default priority of six.

Operation Rules

Operation windows allow the Commvault administrator to designate black out windows in which designated operations will not run. These rules can be set at the global, client computer group, client, agent, and subclient levels. Different operation windows can be defined for data protection jobs, recovery jobs, copy jobs and administrative jobs. Each defined operation window can have one or more Do not run intervals defined. Different operation rules can be specified for the same operation type to define specific time intervals for different days of the week.

Job starts during an operation window blackout period

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

Job is running and an operation window blackout period become active

If a job is currently running and an operation windows blackout period becomes active, indexed and non-indexed jobs will behave in the following ways:

- Indexed based jobs will finish writing their current chunk then be placed in a waiting state. When the blackout period is lifted, the job will continue from the most successfully written chunk.
- Non-Indexed jobs will continue writing and will ignore the operation windows blackout period.
Overriding operation windows

There are several methods to override operation windows do not run intervals. An optional setting Allow running jobs to complete past operation windows (off by default) can be enabled to allow indexed based running jobs to continue to run. This is a CommCell level setting that will affect all indexed based running jobs. For specific client groups, clients, agents or subclients, operation windows can be configured to ignore operation rules at higher levels. In this case if no rules are defined and the ignore operation rules at higher levels is enabled the jobs will run without interruption.
Data Recovery
Data Recovery Overview

When data needs to be recovered, recovery operations are initiated from the backup set level. This means that if multiple subclients exist within the backup set the, recovery operation will present a view of all data within the backup set, eliminating the need for the administrator to know which subclient the data was backed up through.

Recovery Methods

Commvault software provides several different methods for data recovery. Depending on the situation each of these methods will have their advantages and disadvantages. Recovery methods can be divided into two main categories: Indexed and Non-Indexed recovery.

Indexed Based Recovery Methods

<table>
<thead>
<tr>
<th>Find</th>
<th>Provides the ability to enter search criteria such as myfile.txt or *.docx to search for specific files. This option is useful when you know specifically what file or files need to be restored.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browse</td>
<td>Provides the ability to browse for all protected data using the folder hierarchal structure (like Windows Explorer). This method is useful when multiple files, folders or drives need to be restored.</td>
</tr>
<tr>
<td>Restore</td>
<td>Provides the ability to enter a drive, folder path or file path such as F:\users\jdoe that is required for restore. This option is useful when you know the specific location for data required for restore.</td>
</tr>
<tr>
<td>Full system restore</td>
<td>Provides the ability to restore an entire server in cases of full system crash. This method requires that all data on the server including system state data has been protected. It also requires a base operating system to be installed and the Windows file system IDataAgent. This method is useful when the operating system can be reinstalled or if base images are being deployed to servers.</td>
</tr>
<tr>
<td>1-Touch restore</td>
<td>Provides the ability to restore an entire server in cases of full system crash. This method uses a boot image to boot the system with a temporary operating system. It will then reinstall the operating system using unattended answer files, reinstall the file system IDataAgent and then initiate a full system restore. This method is useful when a system needs to be rebuilt with minimum administrator effort.</td>
</tr>
<tr>
<td>Restore by Job</td>
<td>Provides the ability to perform a non-Indexed restore using one or more streams for one or more jobs. This method is useful in disaster recovery scenarios when the index cache is not available. An indexed based restore would have to restore index files from media before the restore can begin where this method would immediately begin restoring data. This method is also beneficial when backup jobs have been multi-streamed since multiple streams can be used to restore the data. Indexed based restore methods will always be single streamed.</td>
</tr>
</tbody>
</table>
Full system restore

Provides the ability to restore an entire server in cases of full system crash. This method requires that all data on the server including system state data has been protected. It also requires a base operating system to be installed and the Windows file system agent. This method is useful when the operating system can be reinstalled or if base images are being deployed to servers.

1-Touch restore

Provides the ability to restore an entire server in cases of full system crash. This method uses a boot image to boot the system with a temporary operating system. It will then reinstall the operating system using unattended answer files, reinstall the file system agent and then initiate a full system restore. This method is useful when a system needs to be rebuilt with minimum administrator effort.

Non-indexed Based Recovery Method

Restore by Job

Provides the ability to perform a non-indexed restore using one or more streams for one or more jobs. This method is useful in disaster recovery scenarios when the index cache is not available. An indexed based restore would have to restore index files from media before the restore can begin where this method would immediately begin restoring data. This method is also beneficial when backup jobs have been multi-streamed since multiple streams can be used to restore the data. Indexed based restore methods will always be single streamed.
Using the Find Feature

Your first and best tool in locating data within protected storage is **Find.** The Find task is available at the backup 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/backup set.
Using Browse

Key Points:

- Browse latest data
- Point-in-time browse
- Relative browse
- Show deleted items

A browse operation allows the administrator the browse through the folder structure to select files and folders to restore. Multiple files and folders can be selected for recovery operations. If a parent object in the folder structure is selected, then all objects within the parent folder will automatically be selected for restore. When selecting a file that was modified multiple times during a cycle, the specific version of the file or all version can be selected to be recovered.

Image and Non-Image Browsing

Each time a backup operation is conducted, an image file is generated which represents a view of the folder structure at the time the backup occurred. By Default, when a browse operation is conducted, an Image Browse is used to present the folder structure as it existed based on the browse date and time. This is done by displaying the folder structure from the most recent image file prior to the point in time being browsed. So, if a browse is being conducted on Wednesday at 2:00 PM and the most recent backup was run on Tuesday at 10:00 PM, the image file from the 10:00 PM backup will be used. This image browse method is used to produce a consistent structure of the data based on the browse time which is important since folder structures may change from day to day during a cycle. When restoring an entire folder structure, it is important that the structure represents a specific point when a backup was conducted and not represent data for the entire cycle. This is best explained by using temporary files as an example. Temporary files and folders can be generated, deleted and regenerated multiple times during a cycle. Each time a backup is run, the file folder structure will be different based on which files existed at the specific point in time. When a restore operation is run, you wouldn't want every temporary file and folder to be restored, just a particular point or day.
Where the image browse option is good for restoring file and folder structures to a particular point in time, it could also result in deleted items not showing up when a browse operation is conducted. For example, if at Wednesday at 2:00 PM a browse operation is run using the Tuesday 10:00 PM image file, and a file or folder was deleted on Tuesday at 2:00 PM, the deleted files will not appear in the browse results. This is because when the 10:00 PM image file was created, the deleted files were not present.

There are two methods to ensure deleted items are displayed during browse operations:

1. **Select the Show Deleted Items check box** - This will run what is referred to as a No-Image browse. In this case the image files are bypassed and the browse operation will return results from the index cache which will show all items backed up from the point the full was run. This method is useful when recovering user data that has been deleted but may not be a good choice when restoring an entire folder structure, especially if the folder structure was modified during the cycle.

2. **Specify date and time to browse** - If you know when the data was deleted, specify that date and time in the browse options. So, if data was deleted at 2:00 PM on Tuesday and you specify Tuesday as the browse date, then the most recent image file prior to the point the browse is being conducted would be Monday at 10:00 PM. Since the day was deleted on Tuesday it would be present in the image file on Monday night and will show up in the browse results.
Pie Chart Browse View

The pie chart view in the browse window provides insight into what data is stored on a client and provides a visual method for browsing data.
Additional Recovery Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore by job</td>
<td>• Job based restore &lt;br&gt;• Does not require indexes &lt;br&gt;• Multi-stream restore</td>
</tr>
<tr>
<td>Full system restore</td>
<td>• Use browse and select entire backup set &lt;br&gt;• Must back up system state data &lt;br&gt;• Requires operating system and file system agent to be installed on client</td>
</tr>
<tr>
<td>1-Touch recovery</td>
<td>• Bare metal restore &lt;br&gt;• Does not require software to be installed on client</td>
</tr>
</tbody>
</table>

**Restore by Job**

Restore by job is a non-indexed restore that can use multiple concurrent streams during the restore operation. Unlike traditional browse and recovery operations which require the index files to be available in the index cache and can only use a single stream during the restore operation, the restore by job option can provide faster restores in DR situations, especially in the case when the production index cache location is not available. Since restore by job does not require indexes, restore operations can be immediately run. The restore by job is a chunk based restore which allows multiple streams to be run simultaneously providing a faster restore speed. One negative aspect of the restore by job is since it does not use indexes, the single pass restore method used with indexed based recoveries where only the proper version of an object is restored based on the point of browse is not used. This means that in order to bring a machine back to its last state, the last full backup job would need to be recovered first and then followed by each subsequent incremental job ending with the most recent.

**Full System Restore**

Full system restore or full agent restore is an indexed based restore where the entire backup set is selected when browsing for data. The backup set selection will include the entire contents of the file system backup including configuration information such as system state. For this to work, a base operating system must first be installed on the system and then the file system agent is installed.
1-Touch Recovery

1-Touch Restore provides a bare metal approach to recovering a server. It works by generating boot images that can be used to boot a crashed server without having to install an operating system. When the system is booted, it will contact the 1-Touch server and initiate a reinstall of the operating system using an answer file that can be customized for each server. Once the OS is reinstalled a file system agent will be installed and a full system recovery will be initiated.
Module 6: Monitoring a CommCell® Environment
CommCell® Monitoring Resources

Monitoring Tools:

- Job controller
  - Job details
- Event viewer
  - Search events
  - Event log settings
- Storage resource view
- Device status view

The CommCell® console provides several different methods for monitoring the CommCell environment:

- Storage usage views
- Resource status views
- Job Controller
- Event Viewer
- Alerts
- Reports

Job Controller

The *Job Controller* in the CommCell console is used to manage all active jobs within the CommCell environment. Regardless of which method is used to initiate a job (schedule, on demand or script), the job will appear in the job controller. The job controller is the most effective tool within the CommCell console for managing and troubleshooting active jobs.

Job Details

*Right-click job | Details or double-click job*

Details for specific jobs can be used to provide information on job status, data path, media usage or job errors.
Event Viewer

The Event Viewer window displays events reported based on conditions within the CommCell® environment. By default, the event viewer will display the most recent 200 events or last 2 days, whichever comes first. This number can be increased up to 1,000 or 30 days. The event log will maintain up to 10,000 events or 7 days of events. These default settings can be modified.

Filtering the Event Viewer

Double-down arrow | Filter | Select field down arrow and select the appropriate filter

The event viewer can be filtered based on the available fields. Although some filters such as Date don’t have a practical application, other fields such as Computer, Program or Event code can be effective in quickly locating specific events.

Searching Event Log

Right-click in event viewer | Search Events

Although only 200 to 1,000 events are displayed in the event viewer, the entire event log can be searched from the event viewer. The default total number of events retained is 10,000.

When right-clicking anywhere in the event viewer, select the option to search events. Events can be searched by time range, severity and job ID. If common searches are frequently conducted, the search criteria can be saved as a query and run at any time.

Setting Event Log Retention

Home tab | Control Panel | Configure | System

By default, the event log will retain 10,000 events or 7 days of events. When the event logs reach their upper limit, the oldest events will be pruned from the event logs.

Storage Resource View

Storage views determine how much disk capacity is being used by protected data.

The Deduplication Engine view, under Storage Resources, determines how much capacity is used based on all Storage Policies associated with the engine.

To view deduplication engine information:

1. Expand the Deduplication Engines entity in Storage Resources.
2. Select the deduplication engine to view.

The Disk Library properties view displays how much capacity has been used on the disk library.

To view disk library capacity usage:

1. Select the library.
2. View capacity charts from the Content / Summary window.
Device Status View

The Resource status view displays view readiness status for storage components within the CommCell® environment.

**Resource status view can be used for the following:**

- MediaAgent status – online or offline (pause)
- Library status – online or offline (pause)
- Tape Drive status for online, offline, and jobs currently running and tape barcode label
Alerts can be configured to provide real-time feedback about conditions in the CommCell® environment as they occur.

- Alerts can be accessed from the Home tab
- The Alert window displays all alerts configured for the CommCell® environment.
- The Alert Summary displays settings for the selected alert and provides the capability to email or save them.

Alerts inform you about certain conditions within the CommCell® environment. They can be triggered based on failures, successes, or changes that may occur during different types of CommCell operations.

Alerts can be:

- Added when configuring a data protection or recovery job
- Configured based on an operation
- Configured to monitor clients or client groups
- Storage alerts can be configured and libraries can be selected and monitored

The Alert Wizard

The Alert Wizard is used to configure the alert type, entities to be monitored, notification criteria and notification method:
You can access the Alert Wizard from the Home tab of the CommCell® Console toolbar:

1. Click the Alert icon and select Configure Alert from the drop-down menu.

Once the wizard opens, you can configure options such as:

- Type of alert
- Entities to be monitored
- Notification criteria
- Notification method

**Console Alerts**

When configuring alerts, console alerts can be selected as a notification method. Once an alert is triggered, it appears in the Console Alerts window within the CommCell® browser. Right-click on an alert to view details, delete, mark as read or unread, or to insert a note. Console alerts can be pinned or deleted using the icons at the bottom of the window.

**Common Alerts**

<table>
<thead>
<tr>
<th>Category</th>
<th>Type</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Updates</td>
<td>Download, Install</td>
<td>Job Failed</td>
</tr>
<tr>
<td>Job Management</td>
<td>Data Protection, Data Recovery</td>
<td>Job Failed, Phase or network errors</td>
</tr>
<tr>
<td>Job Management</td>
<td>Dedupe DDB Reconstruct</td>
<td>All alert criteria</td>
</tr>
<tr>
<td>Job Management</td>
<td>Disaster Recovery Backup</td>
<td>Job Failed</td>
</tr>
<tr>
<td>Media Management</td>
<td>Device Status</td>
<td>Drive / Library offline</td>
</tr>
<tr>
<td>Media Management</td>
<td>Library Management</td>
<td>Insufficient storage, Maintenance alerts</td>
</tr>
</tbody>
</table>
Reports

Using Reports:

- Schedule
- Save as script
- Report templates
- Recommended reports

Common CommCell® reports:

- The **Job Summary** report, which can be used to view data protection, data recovery and administrative jobs.
- The **CommCell® Readiness** report, which can be used as a status report for CommCell components such as clients, MediaAgents, library storage capacity and index caches.
- The **CommCell® Configuration** report, which provides CommCell configuration, license usage and update status of CommCell components.
- The **Job Schedule** report, which can be used to view schedules for client computer groups, clients and administrative jobs.
- The **Data Retention Forecast and Compliance** report, which can be used to view jobs in storage, the media it is located on, and the estimated time the data will age.

CommCell® reports can be configured from the Reports tab in the CommCell toolbar. The most common report types are listed in the toolbar, such as:

  - Job Summary
  - Job Schedule
  - CommCell Readiness reports

When the report type is selected it will be the default report in the report window. Note that any other report type can be accessed from the window.

Reports can be:

  - Scheduled
  - Saved to a specific location
  - Saved as report templates

Depending on the report type selected, various report criteria can be configured from the tabs on the Report Selection window.

Use the tabs to set which resources will be included in the report, such as clients, MediaAgents, libraries, or Storage Policies.

You can also select the information to be included in the report, such as failed items, storage usage, job information, or resource configuration.
Use the Time Range tab to set the scope of the report and use the Output tab to select the output format:

- HTML
- PDF
- Text file - which is saved as a CSV file for spreadsheet import.

You can also choose the Output method. Choices include scheduling, save as script, save as template or save to a disk location.

The following lists some common CommCell® reports:

- The Job Summary report, which can be used to view data protection, data recovery and administrative jobs.
- The CommCell® Readiness report, which can be used as a status report for CommCell components such as clients, MediaAgents, library storage capacity and index caches.
- The CommCell® Configuration report, which provides CommCell configuration, license usage and update status of CommCell components.
- The Job Schedule report, which can be used to view schedules for client computer groups, clients and administrative jobs.
- Data Retention Forecast and Compliance report, which can be used to view jobs in storage, the media it is located on, and the estimated time the data will age.
Thank You

Three tiered survey:

- **Learning experience survey** at conclusion of class
- **Learning effectiveness survey** approximately six weeks following class
- **Education value survey** 3-6 months following class

At Commvault, we have a strong focus on providing quality education. We use a 3-tier student survey process to assess your learning experience, how the training affected your ability to be more productive using Commvault products, and finally how the training impacted your ability to enhance and improve the impact Commvault products have in your data management environment.

2. The initial ‘Learning Experience’ or course survey can be done as soon as your course is complete via Education Advantage. We’ll show how to launch the survey on the next slide and take 10-15 minutes for all to complete it.

3. The ‘Learning Effectiveness’ follow-up survey is sent to all students about 6 weeks after your course via email. We are looking for your input on how you were able to apply the skills learned in your environment and whether there is content we need to add to our courses to better address your skills needs (something that may not be evident at course completion).

4. 3-6 months after completing your course you will receive the Education Value Survey via email from Techvalidate. We use a third party to collect, audit, and validate these survey responses. This survey is used to assess the impact training has had on your business and data management environment. Were you better able to leverage Commvault products, with better performance, better resource usage? Were you better skilled, reducing reliance on customer support for product usage queries over time? Finally, we ask based on your Commvault learning experience, how likely you would be to recommend Commvault training to a friend or colleague. This one question produces an overall learner satisfaction (or Net Promotor) score. This metric is used to measure (at a high level) how we are doing overall.
We strive to meet your highest expectations and highest survey marks. If we fail to meet your expectations with the learning experience, please provide specific comments on how we can improve. We take all comments seriously and will adjust our offerings to better support your needs.