Copyright © 2009, 2010 EMC Corporation. All rights reserved.

Published December, 2010

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

All other trademarks used herein are the property of their respective owners.

Symantec Enterprise Vault and EMC Storage Applied Best Practices

P/N H6790.1
Contents

About this Document .................................................................................................................... 11
Introduction ................................................................................................................................... 12
Audience ....................................................................................................................................... 13
Related documents ........................................................................................................................ 13
  Symantec Enterprise Vault 9.0 manuals ............................................................................... 13
  EMC documentation ............................................................................................................. 14

Chapter 1 Planning .......................................................................................................................... 17
  Solution overview ......................................................................................................................... 18
    Enterprise Vault and EMC Centera data workflow .............................................................. 18
    Enterprise Vault and Celerra data workflow ......................................................................... 20
  Building block ............................................................................................................................... 22
  Sizing considerations ..................................................................................................................... 23
    Exchange .............................................................................................................................. 24
    SQL Server ........................................................................................................................... 26
    Enterprise Vault .................................................................................................................... 29
    EMC Centera ........................................................................................................................ 32
    Network ................................................................................................................................ 33
  Infrastructure / business continuity considerations ........................................................................ 34
    Enterprise Vault backup........................................................................................................ 34
    Enterprise Vault clustering ................................................................................................. 35
    EMC Centera Replication ...................................................................................................... 36
    EMC Centera Restore/tape out ............................................................................................. 39
    Celerra Replicator (V2) ........................................................................................................ 39
    Celerra SnapSure .................................................................................................................. 40
    Celerra backup, recovery, and archive with NDMP ............................................................. 42

Chapter 2 Implementation.................................................................................................................. 43
  Installation requirements and configuration .................................................................................. 44
    Enterprise Vault .................................................................................................................... 44
    SQL Server ........................................................................................................................... 46
    SQLXML .............................................................................................................................. 46
    Hardware / Storage requirements ............................................................................................. 47
    EMC Centera ........................................................................................................................ 52
    Compliance Mode....................................................................................................................... 58
## Contents

- EMC Celerra ................................................................................................................. 61
- FLR Deployment considerations ................................................................................... 67
- Installation process ....................................................................................................... 68
- Licensing ...................................................................................................................... 68
- Installing Enterprise Vault .......................................................................................... 68
- Post-installation tasks .................................................................................................. 69
- Customizing security for the Web Access application ................................................. 70
- Customizing security on the client computers .............................................................. 70
- Configuring Enterprise Vault ....................................................................................... 70
  - Setting up archiving ................................................................................................. 72
- Installation validation .................................................................................................... 73
- Enterprise Vault .......................................................................................................... 73
- EMC Centera ............................................................................................................... 74
- EMC Celerra ................................................................................................................. 74

### Chapter 3

- Configuring Enterprise Vault and EMC Centera for Email Archiving .......................... 75
  - EMC Centera configuration ...................................................................................... 76
  - Enterprise Vault and Centera configuration ............................................................. 77
    - Collections and single instancing ........................................................................ 89
    - Custom configuration of Enterprise Vault and EMC Centera best practices ....... 92
    - Enterprise Vault fine tuning ............................................................................... 96
  - NTFS to EMC Centera migrations .......................................................................... 97
  - Capabilities .............................................................................................................. 97
  - Storage reclamation ................................................................................................. 98

### Chapter 4

- Configuring Enterprise Vault and EMC Celerra for File System Archiving ............... 99
  - EMC Celerra configuration ..................................................................................... 100
  - Setting up EMC Celerra ......................................................................................... 100
  - Adding a volume ..................................................................................................... 109

### Chapter 5

- Operations .................................................................................................................. 113
  - EV updates and upgrades ..................................................................................... 114
  - Day-to-day management tasks ............................................................................... 114
  - EMC Centera upgrades ......................................................................................... 114
    - Added capacity ..................................................................................................... 115
    - CentraStar upgrades ......................................................................................... 115
  - EMC Centera migrations ....................................................................................... 115
  - EMC Celerra upgrades ......................................................................................... 116
    - Added capacity ..................................................................................................... 116
    - Disaster recovery ................................................................................................. 117
    - Disaster recovery for EMC Centera .................................................................... 117
    - EMC Centera primary only disaster recovery ................................................. 118
  - EMC Centera backup .............................................................................................. 121
  - EMC Centera monitoring ....................................................................................... 121
  - Celerra monitoring ................................................................................................. 122
  - High availability ..................................................................................................... 122

### Chapter 6

- Support Model ........................................................................................................... 123
- Cooperative Support .................................................................................................. 124
- Symantec Enterprise Vault troubleshooting considerations ......................................... 124
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Vault logging with DTRACE</td>
<td>124</td>
</tr>
<tr>
<td>EMC Centera troubleshooting considerations</td>
<td>125</td>
</tr>
<tr>
<td>SDK logging</td>
<td>125</td>
</tr>
<tr>
<td>Application Registration</td>
<td>126</td>
</tr>
<tr>
<td>Audit logging (syslog)</td>
<td>126</td>
</tr>
<tr>
<td>Alerts</td>
<td>127</td>
</tr>
<tr>
<td>EMC Celerra troubleshooting considerations</td>
<td>127</td>
</tr>
<tr>
<td>Activity log</td>
<td>127</td>
</tr>
<tr>
<td>Server log</td>
<td>127</td>
</tr>
<tr>
<td>Chapter 7 Conclusion</td>
<td>129</td>
</tr>
<tr>
<td>Appendix A Performance Expectations</td>
<td>131</td>
</tr>
<tr>
<td>Enterprise Vault service level agreement (SLA)</td>
<td>132</td>
</tr>
<tr>
<td>Performance benchmarks</td>
<td>132</td>
</tr>
<tr>
<td>Appendix B Glossary</td>
<td>135</td>
</tr>
<tr>
<td>Terminology</td>
<td>136</td>
</tr>
<tr>
<td>Figure</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Figure 1</td>
<td>Email archiving with EMC Centera building block</td>
</tr>
<tr>
<td>Figure 2</td>
<td>File system archiving with EMC Celerra building block</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Replication failover</td>
</tr>
<tr>
<td>Figure 4</td>
<td>Bidirectional replication with hot standby</td>
</tr>
<tr>
<td>Figure 5</td>
<td>FLR state diagram</td>
</tr>
<tr>
<td>Figure 6</td>
<td>Setting up removal of safety copies during vault store creation</td>
</tr>
<tr>
<td>Figure 7</td>
<td>Setting up removal of safety copies for an existing Vault Store</td>
</tr>
<tr>
<td>Figure 8</td>
<td>Selecting EMC Centera as the storage type</td>
</tr>
<tr>
<td>Figure 9</td>
<td>Entering the EMC Centera access node (AN) IP addresses</td>
</tr>
<tr>
<td>Figure 10</td>
<td>Add Address (DNS Name optional)</td>
</tr>
<tr>
<td>Figure 11</td>
<td>Enabling Centera SiS on the Enterprise Vault partition</td>
</tr>
<tr>
<td>Figure 12</td>
<td>Setting up single instancing (sharing)</td>
</tr>
<tr>
<td>Figure 13</td>
<td>Setting retention policies from Enterprise Vault to EMC Centera</td>
</tr>
<tr>
<td>Figure 14</td>
<td>Defining EMC Centera Replication’s partition scan intervals</td>
</tr>
<tr>
<td>Figure 15</td>
<td>Setting up EMC Centera collections</td>
</tr>
<tr>
<td>Figure 16</td>
<td>Enabling EMC Centera collections on an existing Vault Store partition</td>
</tr>
<tr>
<td>Figure 17</td>
<td>Associating Enterprise Vault Retention Categories and EMC Centera Retention Classes</td>
</tr>
<tr>
<td>Figure 18</td>
<td>Establishing the EMC Centera connection string</td>
</tr>
<tr>
<td>Figure 19</td>
<td>Number of threads</td>
</tr>
<tr>
<td>Figure 20</td>
<td>Assigning retention categories to a provisioning group</td>
</tr>
<tr>
<td>Figure 21</td>
<td>Setting the File Server fully qualified DNS name</td>
</tr>
<tr>
<td>Figure 22</td>
<td>Enabling placeholder shortcuts</td>
</tr>
<tr>
<td>Figure 23</td>
<td>Adding a file server</td>
</tr>
<tr>
<td>Figure 24</td>
<td>Enabling data collection for FSA Reporting</td>
</tr>
</tbody>
</table>
Figures
### Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1</td>
<td>Recommended database storage allocation</td>
<td>29</td>
</tr>
<tr>
<td>Table 2</td>
<td>Supported mailboxes for mailbox archiving based on EV server configuration</td>
<td>30</td>
</tr>
<tr>
<td>Table 3</td>
<td>Index storage requirements</td>
<td>31</td>
</tr>
<tr>
<td>Table 4</td>
<td>Additional storage requirements per Enterprise Vault Server</td>
<td>32</td>
</tr>
<tr>
<td>Table 5</td>
<td>Minimum specification for an Enterprise Vault server</td>
<td>47</td>
</tr>
<tr>
<td>Table 6</td>
<td>Minimum specification for SQL Server</td>
<td>49</td>
</tr>
<tr>
<td>Table 7</td>
<td>Recommended EMC Centera configuration</td>
<td>52</td>
</tr>
<tr>
<td>Table 8</td>
<td>Recommended EMC Celerra configuration</td>
<td>61</td>
</tr>
<tr>
<td>Table 9</td>
<td>Features in FLR-C and FLR-E</td>
<td>63</td>
</tr>
<tr>
<td>Table 10</td>
<td>FLR states</td>
<td>66</td>
</tr>
<tr>
<td>Table 11</td>
<td>Enterprise Vault components – Summary of recommended values for EMC Centera devices</td>
<td>79</td>
</tr>
<tr>
<td>Table 12</td>
<td>Recommended default retention category for EMC Centera</td>
<td>91</td>
</tr>
<tr>
<td>Table 13</td>
<td>Remove Safety Copies setting impact on shortcut creation</td>
<td>107</td>
</tr>
<tr>
<td>Table 14</td>
<td>Required SDK environment variables</td>
<td>126</td>
</tr>
<tr>
<td>Table 15</td>
<td>Expected Enterprise Vault ingest rates for physical CPUs</td>
<td>132</td>
</tr>
<tr>
<td>Table 16</td>
<td>Performance and stress test results</td>
<td>133</td>
</tr>
</tbody>
</table>
Information organizations are faced with an environment that is becoming increasingly subject to external and internal regulations and supervision. The scope and number of requirements and regulations facing businesses today are increasing – along with the costs of ensuring they are complied with.

Even though the cost of compliance can be considerable, the legal and goodwill risks associated with noncompliance can be even higher.

Proper management of unstructured data growth, primarily driven by the use of email as the predominant form of enterprise communications, imposes a greater challenge onto today’s organizations, which are determined to provide their customers – internal and external – with exceptional service and a satisfying experience.

Enterprise Vault is a Windows application that enables companies to automatically apply corporate, legal, and IT policies around the storage, transfer, retention, and disposition of unstructured data such as email, IM, files, or SharePoint documents. This translates into reduced and simplified infrastructure management costs, and controlled data exposure and protection while ensuring a centralized and indexed archive that can be searched on demand.

With all of its storage platforms archive-capable, whether your needs are a multi-purpose storage solution or a pure archive EMC has the solution for your use with Symantec Enterprise Vault.

EMC Centera® is a simple, affordable, power-efficient, and secure repository purpose built for information archiving to keep static and infrequently changing digital information available online for immediate access. EMC Centera enhances business value by preserving original content and ensuring complete, reliable integrity for the life of the archived information.

EMC Centera’s self-healing/self-management/self-configuration capabilities, in addition to nondisruptive repair and phone-home features, enable customers to efficiently manage more archive content at a lower cost.

Supported by unmatched retention and disposition management capabilities, EMC Centera successfully addresses the most rigorous compliance regulations, while minimizing the total cost of ownership. EMC Centera enforces organizational and application policies for information retention and disposition intrinsic in storage—and by doing so completes the information chain of custody. It ensures corporate accountability and reduces the costs of legal discovery and litigation support—and it’s easy to manage.

EMC Celerra® unified storage is a highly efficient multiple-purpose, multi-protocol platform that can be used for information throughout its lifecycle. Robust in storage functionality, Celerra is optimized for file and block access, delivering high-end features in a scalable, easy-to-use package.

For the ultimate flexibility in scale and performance, Celerra delivers innovative best-in-class Flash technology that can be utilized for storage or as an extension of system cache, Fibre Channel disks for transactional workloads, and SATA disks for least cost storage tiering. Automated management features like policy-based tiering and deduplication, automated volume
provisioning, and automated extension of file system and storage pools reduce the amount of an administrator’s time involved in storage management activities.

To address information retention, Celerra’s layered software, FLR (file level retention), provides WORM functionality, ensuring that email and files cannot be modified or deleted before their specific retention date has passed. A retention policy for each email or file is simply controlled as an attribute of the file. For Compliance uses, FLR-C (Compliance) prevents any modification or deletion of locked emails, files, and records by both users and administrators. For stringent compliance environments, FLR-C includes an enhancement for write verification. Celerra with FLR-C ensures the integrity of the stored information by reading back the information written to the file system. This data verification functionality is only available in the Compliance Version of FLR (FLR-C).

All of these capabilities are easily configured in a single storage array, delivering the right level of performance and information protection, at the right cost whether emails and files are newly created or archived.

From application through storage, the unique functionalities offered by EMC storage, in combination with Symantec Enterprise Vault’s flexibility, create an intelligent, complete chain of information custody. This level of information authenticity and the ability to ensure that an organization’s retention and disposition policies are enforced make EMC and Symantec the optimal yet simple email and file system archive solution for businesses and organizations.

Introduction

This white paper addresses the challenges of deploying an email or file system archiving solution by looking at the several phases of any project lifecycle, from planning and architecting to installing, configuring, and fine-tuning of the system, in addition to covering maintenance activities after successful deployment.

Guidelines and recommendations are provided based on lessons learned through several years of successful partnership and tight technical integration between Symantec and EMC.

The paper is not intended to replace the documentation that either Symantec or EMC provide for Symantec Enterprise Vault, EMC Centera, and EMC Celerra, but rather to serve as a reference and complement to the already existing documentation, and to provide stakeholders with a holistic, unified perspective on the topic of email and file system archiving as it pertains to the joint offering.

In this context, the paper discusses not only the specifics of installing and configuring Celerra, EMC Centera, and Enterprise Vault, but also the additional know-how EMC has on deploying Microsoft Exchange and Microsoft SQL Server as the email and database engines, respectively, on the appropriate storage tiers for the enterprise. Similarly, an overview of the expectations around performance and available support mechanisms is provided.

Although EMC Centera configuration is minimal and is performed as part of the installation process, detailed information on each topic is provided in order to minimize ambiguity, and misinterpretation, and to provide a greater understanding of the benefits each feature provides to the organization.

As it is the role of the application to exploit EMC Centera capabilities, careful attention to Enterprise Vault’s archiving configuration is required, and dedicated in the paper. Similarly, details on how to configure Celerra to best perform when used with Enterprise Vault are covered in the document.
The ultimate goal for this document is to trigger an open dialogue between all parties involved and to clarify the most common and critical project/product areas in order to successfully identify, plan, implement, monitor, and maintain the several component parts of the solution.

**Audience**

This white paper is intended for:

- Customers, including IT planners, storage architects, and administrators
- EMC and Symantec technical staff and partners
- Field personnel who are tasked with implementing archiving solutions, using Symantec Enterprise Vault and EMC Centera or EMC Celerra, focused on email and file system archiving for Microsoft Exchange Server environments
- Engineering and product development groups
- Account personnel involved in pre-sales activities

This white paper assumes the reader has a basic knowledge and understanding of Microsoft Windows, Microsoft Exchange, Microsoft SQL Server, Symantec Enterprise Vault, EMC Celerra, and EMC Centera.

**Related documents**

**Symantec Enterprise Vault 9.0 manuals**

<table>
<thead>
<tr>
<th>Doc ID</th>
<th>Document Title/Link</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOC2843</td>
<td>Enterprise Vault 9.0 and later - Backing up Enterprise Vault</td>
<td>Symantec Enterprise Vault 9.0 - Administrators Guide</td>
</tr>
<tr>
<td>DOC2852</td>
<td>Setting up Domino Server Archiving 9.0</td>
<td>Symantec Enterprise Vault 9.0 - Setting up Domino Server Archiving</td>
</tr>
<tr>
<td>DOC2853</td>
<td>Setting up Exchange Server Archiving 9.0</td>
<td>Symantec Enterprise Vault 9.0 - Setting up Exchange Server Archiving</td>
</tr>
<tr>
<td>DOC2854</td>
<td>Setting up File System Archiving (FSA) 9.0</td>
<td>Symantec Enterprise Vault 9.0 - Setting up File System Archiving</td>
</tr>
<tr>
<td>DOC2855</td>
<td>Setting up SharePoint Server Archiving 9.0</td>
<td>Symantec Enterprise Vault 9.0 – Setting up SharePoint Server Archiving</td>
</tr>
<tr>
<td>DOC2856</td>
<td>Setting up SMTP Archiving 9.0</td>
<td>Symantec Enterprise Vault 9.0 – Setting up SMTP Archiving</td>
</tr>
<tr>
<td>DOC2848</td>
<td>Registry Values 9.0</td>
<td>Symantec Enterprise Vault 9.0 - Registry Values</td>
</tr>
<tr>
<td>TECH38537</td>
<td>Symantec Enterprise Vault Compatibility Charts</td>
<td>Enterprise Vault Compatibility List</td>
</tr>
<tr>
<td>N/A</td>
<td>Backing up Enterprise Vault in a clustered environment – For internal distribution only</td>
<td>Backing up Enterprise Vault in a clustered environment.pdf</td>
</tr>
</tbody>
</table>
## Symantec Enterprise Vault and EMC Storage Applied Best Practices

### Install/Upgrade

<table>
<thead>
<tr>
<th>Doc ID</th>
<th>Document Title/Link</th>
<th>File Name</th>
</tr>
</thead>
</table>

### Compliance Accelerator and Discovery Accelerator 9 manuals

<table>
<thead>
<tr>
<th>Doc ID</th>
<th>Document Title/Link</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOC2861</td>
<td>Discovery Accelerator - Installing and Configuring Guide 9.0</td>
<td>Symantec Discovery Accelerator 9.0 – Installation Guide</td>
</tr>
</tbody>
</table>

### EMC documentation

Note: To access EMC documents that are published on Powerlink, a user must have a Powerlink account or contact an EMC representative.

#### EMC Centera

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Document Link</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>REV A12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>069001185</td>
<td>EMC Centera SDK V3.2 API Reference Guide</td>
<td>EMC Centera SDK V3.2 API Reference Guide</td>
</tr>
<tr>
<td>REV A08</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H5553</td>
<td>EMC Centera Replication - A Detailed Review</td>
<td>EMC Centera Replication - A Detailed Review</td>
</tr>
<tr>
<td>H5735.3</td>
<td>EMC Centera CentraStar/SDK Compatibility with Centera ISV Applications - A Detailed Review</td>
<td>EMC Centera CentraStar / SDK Compatibility with Centera ISV Applications - A Detailed Review</td>
</tr>
<tr>
<td>N/A</td>
<td>For internal distribution only</td>
<td>Symantec Partner Kit</td>
</tr>
<tr>
<td>N/A</td>
<td>Centera CentraStar and SDK Release and Interoperability Matrix</td>
<td>Centera CentraStar SDK Interoperability Matrix</td>
</tr>
</tbody>
</table>

#### EMC Celerra

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Document Link</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td><a href="http://celerra.emc.com/docs/DOC-2319">http://celerra.emc.com/docs/DOC-2319</a></td>
<td>Celerra File-Level Retention (FLR) (EDN login required)</td>
</tr>
<tr>
<td>N/A</td>
<td><a href="http://celerra.emc.com/docs/DOC-2088">http://celerra.emc.com/docs/DOC-2088</a></td>
<td>Celerra Data Deduplication (EDN login required)</td>
</tr>
<tr>
<td>N/A</td>
<td><a href="http://celerra.emc.com/docs/DOC-2049">http://celerra.emc.com/docs/DOC-2049</a></td>
<td>Celerra Business Continuity - Celerra Replicator V2 (EDN login required)</td>
</tr>
<tr>
<td>N/A</td>
<td><a href="http://celerra.emc.com/docs/DOC-2440">http://celerra.emc.com/docs/DOC-2440</a></td>
<td>Celerra SnapSure (EDN login required)</td>
</tr>
<tr>
<td>N/A</td>
<td><a href="http://celerra.emc.com/docs/DOC-2368">http://celerra.emc.com/docs/DOC-2368</a></td>
<td>Celerra Backup, Recovery and Archive - NDMP</td>
</tr>
</tbody>
</table>
For Microsoft SQL Server information, refer to the Microsoft websites, including [http://www.microsoft.com/sql](http://www.microsoft.com/sql), or more directly to the documentation page for the various versions.

Microsoft SQL Server Books On Line documentation provides extensive coverage of features and functions and may be installed through the SQL Server installation process, independently of the SQL Server database engine. Updated versions of the Books On Line documentation are available for free download from the Microsoft SQL Server website: [http://www.microsoft.com/sql](http://www.microsoft.com/sql)

Note:  Links listed are functional as of this document’s publication date. Over time, the location of reference material may change. A navigation description is included to assist in those cases. If the user has difficulty locating referenced material, contact your EMC or Symantec representative.
This chapter presents these topics:

- Solution overview ................................................................. 18
- Building block ........................................................................ 22
- Sizing considerations ............................................................. 23
- Infrastructure / business continuity considerations ............. 34
Solution overview

Enterprise Vault provides the framework for organizations to automatically store messaging and file system data from Microsoft Exchange, SharePoint Portal Server, Lotus Domino, SMTP, IM, file server environments, and other collaborative environments into centralized archives.

In particular, automatic email archiving and archive management provide the following important benefits:

- They ensure that messages and documents are retained for the period of time required by compliance regulations or company policy.
- The size of Exchange Server mailboxes and public folders and Domino mail files is easily controlled without the loss of data (.PST or .MSG files).
- Primary disk space usage is reduced.

According to scheduled times, Enterprise Vault archiving processes check target servers for items to archive based on predefined policies. Items meeting the archival criteria are then stored in the archive. Archived items are indexed by Enterprise Vault to enable fast searching and retrieval, based on the level of indexing required by the organization as set up by the administrator.

A retention category, which defines how long an item must be kept, is automatically assigned to each item at archiving time. The administrator can define different retention categories for different data types or subsets of data. EMC storage can be leveraged to host such Enterprise Vault archives – depending on the compliance and advance retention requirements: EMC Centera for the most stringent of the environments and EMC Celerra for environments where automated tiering between primary and secondary storage is required while delivering basic archiving with WORM capabilities.

Enterprise Vault and EMC Centera data workflow

EMC Centera receives archived content from Enterprise Vault and stores this content as individual objects, which are uniquely identified by content addresses (CAs) derived by running a hashing algorithm over the archived content. Archived content is then accessed by Enterprise Vault using these CAs rather than by name or path as with traditional stores.

If an attempt is made to store the same file, regardless of what application it comes from again, EMC Centera will generate exactly the same CA and will detect that there is no need to store this redundant copy. For disaster recovery purposes, data is automatically replicated to the target or replica EMC Centera cluster in an asynchronous fashion.

Once Enterprise Vault verifies that the data is replicated, the original items can be replaced with shortcuts to the archived copy in order to release primary storage on user computers and target application servers. From the end user’s point of view, they will still be able to access the items as before.

As Enterprise Vault monitors the archives, it can then delete items when the retention period expires. Under EMC Centera compliance mode, any application attempt to delete data still under retention will be denied and an event log will be created.

In order to better understand the data flow between Enterprise Vault and EMC Centera, workflows for ingest, retrieval, and delete operations are discussed next.
The following is the workflow for content ingests:

<table>
<thead>
<tr>
<th>Component</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Enterprise Vault| Archiving Services pick up items from target stores (such as Exchange mailboxes, public folders, SharePoint workspaces) and queues them to the Storage Service.  
Storage Service stores them and initiates Indexing Service. 
Indexing Service indexes selected items’ attributes. 
Items are compressed. 
Collections are built, if applicable. 
Items are sent to EMC Centera for archiving (when Enterprise Vault is storing shareable data it sets EMC Centera’s FP_OPTION_CLIENT_CALCID so that data already on the EMC Centera is not sent again) |
| EMC Centera     | Content address is calculated.  
Single instancing is checked.  
Item is stored based on storage policies.  
Item is put in the replication queue. |
| Enterprise Vault| Archiving Services verifies the item exists in replica (scheduled / configurable).  
A shortcut to the item is created once the replica copy is detected.  
Item is removed from the target store (stubbed out). |

The following is the workflow for content retrieval:

<table>
<thead>
<tr>
<th>Component</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Enterprise Vault| 1. End user requests item from the information source (such as Exchange mailboxes, public folders, SharePoint workspaces).  
2. Storage Service uses SavesetId to look up an item in the SQL database, and to get the Clip-id.  
3. The EMC Centera content address (Clip-id) is determined from database lookup. |
| EMC Centera     | 4. Content is read (Partial Read is performed per collection items).          |
| Enterprise Vault| 5. Item is decompressed and re-assembled into a saveset object.  
6. The saveset is validated against SavesetID and clip attributes.  
7. The saveset object is made available for the end user. |
The following is the workflow for content deletion:

<table>
<thead>
<tr>
<th>Component</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Vault</td>
<td>1. Expiry process identifies item to be deleted based on retention policies (alternatively, end user can also request an item to be deleted).</td>
</tr>
<tr>
<td></td>
<td>2. Storage Service uses SavesetId to look up an item in the SQL database, and to get the Clip-Id.</td>
</tr>
<tr>
<td></td>
<td>3. The EMC Centera content address (Clip-id) is determined from database lookup.</td>
</tr>
<tr>
<td>EMC Centera (primary)</td>
<td>4. Content is read on the primary cluster (Partial Read is performed per collection items).</td>
</tr>
<tr>
<td>Enterprise Vault</td>
<td>5. The item is validated against SavesetID and clip attributes.</td>
</tr>
<tr>
<td>EMC Centera (replica)</td>
<td>6. The item is deleted (if collections are used, the counter is decreased – if the counter reaches zero (0), collection is deleted).</td>
</tr>
<tr>
<td>EMC Centera (primary)</td>
<td>7. The item is deleted (if collections are used, the counter is decreased – if the counter reaches zero (0), collection is deleted).</td>
</tr>
<tr>
<td>Enterprise Vault</td>
<td>8. Indexing Service deletes the entry from the AltaVista index file</td>
</tr>
<tr>
<td></td>
<td>9. Storage Service deletes Saveset and SavesetStore records (which includes the Clip-ID) from the SQL Server DB.</td>
</tr>
</tbody>
</table>

**Enterprise Vault and Celerra data workflow**

EMC Celerra receives archived content from Enterprise Vault and stores this content via CIFS interface. Once Enterprise Vault verifies that the data is backed up, the original items can be replaced with shortcuts to the archived copy in order to release primary storage on user computers and target application servers. From the end user’s point of view, they will still be able to access the items as before.

As Enterprise Vault monitors the archives, it can then delete items when the retention period expires. For a Celerra with File Level Retention enabled, any application attempt to delete data still under retention will be denied and an event log will be created.

In order to better understand the data flow between Enterprise Vault and Celerra, workflows for ingest, retrieval, and delete operations are discussed next.
The following is the workflow for content ingests:

<table>
<thead>
<tr>
<th>Component</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Enterprise Vault | 1. Archiving Services pick up items from target stores (such as Exchange mailboxes, public folders, SharePoint workspaces) and queues them to the Storage Service.  
2. Storage Service stores them and initiates Indexing Service.  
3. Indexing Service indexes selected items’ attributes.  
4. Items are compressed.  
5. Items are sent to EMC Celerra for archiving via CIFS interface.  
6. For WORM mode, Enterprise Vault attempts to set retention according to the Enterprise Vault Retention Category. |
| EMC Celerra | 7. For WORM mode, Celerra will enforce the retention requested by Enterprise Vault.                                                   |
9. A shortcut to the item is created once the backup is verified.  
10. Item is removed from the target store.  
11. For non-WORM mode, if collections are configured, items will be collected on the next Collection Run. |

The following is the workflow for content retrieval:

<table>
<thead>
<tr>
<th>Component</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Enterprise Vault | 1. End user requests item from the information source (such as Exchange mailboxes, public folders, SharePoint workspaces).  
2. Storage Service uses SavesetId to look up an item in the SQL database.  
3. Item is requested from EMC Celerra via CIFS interface. |
| EMC Celerra | 4. Item is returned.                                                                                                               |
| Enterprise Vault | 5. Item is decompressed and re-assembled into a saveset object.  
6. The saveset is validated against SavesetID.  
7. The saveset object is made available for the end user. |

The following is the workflow for content deletion:

<table>
<thead>
<tr>
<th>Component</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Enterprise Vault | 1. Expiry process identifies item to be deleted based on retention policies (alternatively, end user can also request an item to be deleted).  
2. Storage Service uses SavesetId to look up an item in the SQL database.  
3. Dependent upon sharing, the entire Saveset object or part of the Saveset will be actioned for deletion. |
| EMC Celerra | 4. For WORM mode, if retention has expired, item will be deleted.  
5. For non-WORM mode, item will be deleted. |
| Enterprise Vault | 6. Indexing Service deletes the entry from the index.  
7. Storage Service deletes relevant records from the SQL Server DB. |
BEST PRACTICE: To facilitate the understanding and deployment of the core system components of the email archival solution, a building block approach is recommended.

A building block is a repeatable unit of Enterprise Vault functionality, hosted on an application server, comprising a full set of Enterprise Vault Services that deliver archiving, indexing, storage, search, and retrieval functions and is both reliable and scalable.

This methodology makes it easy to extend Enterprise Vault capabilities by adding as many blocks/units as needed in order to support business requirements around capacity, performance, and resiliency. This is particularly important for disaster recovery purposes, as an extra building block could serve failover roles. For additional information please refer to the Symantec Enterprise Vault 9.0 - Introduction and Planning Guide.

Figure 1 is a graphical representation of the typical Enterprise Vault and EMC Centera building block to support email archiving for 7,500 mailboxes.
Figure 2 is a graphical representation of the typical Enterprise Vault and EMC Celerra building block to support file system archiving.

**Sizing considerations**

When sizing an email archiving solution, there are several factors to consider such as:

- Mailbox data characterization
- Number of mailboxes
- Number of Exchange servers and their locality
- Type of archiving (journal or email archiving)
- Windows timeframes to perform such activities as:
Network infrastructure upgrades for expansion

Enterprise and divisional policies for archiving, backup, disaster recovery, and high availability

These environmental factors, unique to each organization, have a direct impact on the size of the solution components – mainly the configuration of the Enterprise Vault and SQL servers, and their associated storage requirements. This section will present an overview of each component and guidelines for determining its appropriate sizing and configuration to effectively and efficiently address the business requirements.

**Exchange**

Although Microsoft Exchange is presumed to be installed already, the following are some high-level considerations and recommendations for designing a successful Exchange storage system, based on benchmarks performed by EMC according to the Microsoft Exchange Solution Reviewed Program (ESRP) – Storage program.

The ESRP – Storage program was developed by Microsoft Corporation to provide a common storage testing framework for storage vendors to provide information on their storage solutions for Microsoft Exchange Server. For more details, visit [http://www.microsoftstoragepartners.com](http://www.microsoftstoragepartners.com).

**User information**

This information will help you understand the I/O profile for a set of users, and what their storage requirements are.

**Mailboxes**

- Total number of mailboxes (regular email and journal) and size limits
- Mailbox distribution across multiple Exchange servers/locations
- Daily amount of messages and size
- Anticipated growth over the next few years
- Retention period for deleted items

**User activity**

- Maximum I/O per user
- Average number of log files created per user per day
- Typical working day
- Peak activity periods and number of concurrent users at that time

**Backup/Recovery**

- Backup method
- Backup and maintenance schedules and window timeframes
Recovery service level agreements (recovery point objective and recovery time objective)

Disaster recovery distance from the primary site, network connection links, and available bandwidth

To assist gathering some of these metrics on an existing Exchange environment, the Windows System Monitor tool (PerfMon) can be used on a production server with a user load matching the target community. It is recommended that the run includes a 1-to-2 hour period during peak user activity. In particular, the following sample measurements could be useful:

1. IOPS per user: Use the System Monitor counter Physical Disk\Disk Transfers/sec on the Exchange database drive and the following formula:
   \[
   \text{IOPS per User} = \frac{\text{Disk Transfer/sec}}{\text{Number of Users}}
   \]

2. Read/Write Ratio: During the peak activity period, the ratio is measured on the database drive using the formula:
   \[
   \text{Read/Write Ratio} = \frac{\text{Disk Reads/sec}}{\text{Disk Writes/sec}}
   \]

3. I/O Latency: The read or write latency to the database or log drives can be measured using the counters:
   \[
   \text{PhysicalDisk\ Avg Disk sec/Read and Avg Disk sec/Write}
   \]

**Site-specific constraints**

Any environmental requirements or restrictions where the messaging system is to be implemented must be taken into consideration such as:

- The use of a new or existing array and whether or not it is dedicated to Exchange or shared with other applications
- Type of drives in the array
- Number and location of Exchange servers
- Number of Exchange Storage Groups (ESGs) per server
- Network capacity

An ESG is the fundamental unit for layout planning; the following are considerations/recommendations relevant to ESGs:

- For backup purposes, the elements of an ESG should be treated together.
- For Exchange 2007, it is best to place a single database in each storage group.
- Although determining how many ESGs to have on a server is not as clear, EMC feels that eight or 16 ESGs per server provides a good balance between performance and manageability.
- Database size will vary based on customer requirements but should in general be kept under 210 GB in size.
- Under most circumstances, two LUNs should be allocated for each ESG: one for the database file and one for the transaction logs. These LUNs should not share spindles.
For production Exchange database LUNs, there are two possible RAID type configurations that can be appropriate:

- **RAID 1/0 (mirrored)**, which offers the best performance with high protection, but only 50 percent of the RAID group capacity is usable. It is frequently recommended because it provides sufficient space across the number of spindles required for handling a peak I/O load with today’s larger disk drives. There are two physical I/O operations for each write requested (one to each mirrored disk).

- **RAID 5 (parity)**, which offers a higher usable capacity per RAID group than RAID 1/0. It can be effective for environments with very large mailboxes and/or lower IOPS requirements. There are four physical I/O operations for each write requested (two reads to calculate parity, one write for data and one write for parity).

**BEST PRACTICE:** Regardless of the constraints, the core requirements of providing enough drives to meet peak I/O demand remain, as does the strong recommendation to keep log and database LUNs for the same ESG on separate spindles.

**Building-block design**

It is recommended to create a clean storage layout diagram, using a building block style, assigning meaningful names to LUNs on an organized fashion. This will facilitate the understanding of the diagram, assist in identifying possible weaknesses, and eventually support administration and maintenance of the implementation.

**Design validation**

Techniques such as peer reviews and comparisons against already proven configurations are recommended. Where possible, the configuration should be built and tested with performance tools such as Microsoft JetStress, LoadGen, and Performance Monitor, and EMC Unisphere™ Analyzer.

Further detail on best practices for Exchange 2007 is available at [EMC CLARiiON Storage Solutions: Microsoft Exchange 2007 – Best Practices Planning](#).

Specific technical documentation for Exchange solutions using EMC Symmetrix®, CLARiiON®, and Celerra arrays is available at [Microsoft Exchange Reviewed Program (ESRP)](#).

Detail information for tools available to quantify an Exchange environment and sizing rules of thumb are provided in the [Symantec Enterprise Vault 7.0 - Sizing an Enterprise Vault Solution for Exchange Archiving – Technical White Paper](#).

**SQL Server**

Enterprise Vault leverages SQL Server capabilities as its database engine. Due to the fact that Enterprise Vault performance heavily relies on the performance of the database server, SQL Server needs to be properly specified.

A holistic approach to application, host, and storage configuration planning is required to ensure optimal configuration for a given SQL Server database deployment.
Storage

Eliminating contention, a traditional best practice for database layouts for storage-related resources involves understanding how the database manages the data flow process and ensures that concurrent or near-concurrent storage resource requests are separated on to different physical spindles. Layout recommendations in this regard include:

- Ensuring that partitions, created on LUNs presented from storage arrays, are aligned to 64 KB boundaries during the file system partition creation phase. This partition alignment and the resulting volume alignment should not be confused with the Windows Allocation Unit size specified when formatting the volume. These are two different processes.

- Having transaction logs on separate hypers and spindles, to minimize contention for the logs as new writes come in from the database and any old transaction log information is streamed out during incremental transaction log backups. It also isolates the sequential write and random read activity for these members from other volumes with differing access characteristics.

- Isolating TEMPDB data and log files from other user databases and optionally allocating multiple data files (usually one per processor) for TEMPDB data by hosting them on separate LUNs.

- Implementing only a single file on any given LUN. In general, this provides for the best performance configuration and may not always be possible. Windows Server and HBA configurations create device I/O queues based on LUNs. Ensuring that queue structures are scaled out, and that workloads are optimized for a LUN, will in turn result in performance scaling.

- Utilizing multiple files within a filegroup to distribute I/O load. SQL Server will allow for certain parallel operations when tables have been created on multiple files. Full table scans would represent one such parallel operation.

Note: Although these recommendations may be considered to be best practices, in certain circumstances they may not be possible to implement. In such cases, it is possible to collocate these files in shared locations. However, this will require constant monitoring and management to ensure that the overall performance of the environment is not suffering as a result of these competing workloads.

Other considerations include the organization of the database data files to facilitate recovery when array replication technologies such as EMC TimeFinder® and SRDF® are used. Collocating data and log files or other files on LUNs (viewed as physical disks by Windows servers) will affect functionality. Specifically, an attempt to restore a database located on a LUN may result in the inadvertent and erroneous restoration of other unrelated data.

BEST PRACTICE: It is recommended in a SQL Server environment that separate LUNs only contain volumes that contain database files from the same database, or databases that will be backed up and restored together.

Applications availability and performance requirements determine the appropriate level of RAID to be configured. Although EMC recommends RAID 1 to be the primary choice in RAID configuration for reasons of reliability and availability, SQL Server databases can be deployed on RAID 5-protected disks for many database environments.
Vault Store Group fingerprint database - Enterprise Vault 9.0 introduced this database to support the new storage model. The new database has tables with entries for every single-instanced part, holding fingerprints of the shareable parts of archived items.

**Note:** Although this database is not used when EMC Centera is the archiving storage device, it will be created and will be used in the event that other storage types are added later to the environment.

- Monitoring database - This database holds monitoring information for the Enterprise Vault Site.
- FSA Reporting database (optional) - When FSA Reporting is configured, this database holds the data that the Vault File Collector Service gathers.
- Audit database (optional) - When audit is enabled, this database holds all auditing events for the selected Enterprise Vault servers.

Additional information is provided in the *Symantec Enterprise Vault 9.0 - Installing and Configuring Guide*

### Database capacity requirements

Most of the required databases have predictable growth over time; however, Vault store and Vault store group fingerprint databases’ growth depends on many factors unique to the organization as they will reflect the Exchange environment being archived.

For every item archived (managed) by Enterprise Vault, several attributes – usually referred to as metadata – are added to a vault store database; this is quite predictable once an assessment is performed. Temporary space is used to hold information on items that have not been backed up or indexed. Certain records are held longer for users who have been enabled for Vault Cache. Permanent space is also used to hold data in the Directory database. It is suggested that an extra 5 GB is allowed for this, or 10 GB where millions of items are archived between backups or Vault Cache is enabled for thousands of users. The extra space is added once only.

To calculate the space required for Exchange mailbox and journal archiving:

1. Take the number of items to be archived.
2. Multiply by 1,000 bytes (size of the metadata stored per item).
3. Add 5 GB.

**Note:** Calculations for the storage requirements of the Vault store group databases are more complex and are not part of the scope of this document as they are not relevant for EMC Centera environments.
Table 2 lists the initial database file sizes for both data and transaction logs, as well as the recommended allocated storage per database to allow for temporary growth on a two-year projection.

**Table 1**

<table>
<thead>
<tr>
<th>Database</th>
<th>Recommended storage allocation</th>
<th>Initial database sizes (Data / Log)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Vault Directory database</td>
<td>5 GB</td>
<td>10 MB / 25 MB</td>
</tr>
<tr>
<td>Vault Store databases</td>
<td>5 GB + ((1,000 \text{ bytes} \times \text{number of archived items}))</td>
<td>100 MB / 80 MB</td>
</tr>
<tr>
<td>Vault Store Group fingerprint databases</td>
<td>Not required for EMC Centera</td>
<td>164 MB / 80 MB</td>
</tr>
<tr>
<td>Monitoring database</td>
<td>5 GB</td>
<td>100 MB / 80 MB</td>
</tr>
<tr>
<td>FSA Reporting database</td>
<td>5 GB</td>
<td>100 MB / 80 MB</td>
</tr>
<tr>
<td>Audit database</td>
<td>5 GB</td>
<td>100 MB / 80 MB</td>
</tr>
</tbody>
</table>

Further detail on SQL Server sizing is available in the *Symantec Enterprise Vault 9.0 - Introduction and Planning Guide*.

---

**Enterprise Vault**

**User profile**

This information will help with understanding the profile for a set of users, over time, and what their archiving storage requirements are.

**Mailboxes**

- Total number of mailboxes to be archived (regular email and journal) and size limits
- Mailbox distribution across multiple Exchange servers/locations
- Amount of messages to be archived (from backlog and each day) and size
- Anticipated growth over the next few years
- Retention policies

**Archiving timeframes**

- Expected time to clear the backlog
- Daily window timeframe for email archiving
- Exchange journal schedules

**Midterm considerations**

- Mailbox size growth expectations
- Increased number of mailboxes over time
- How to deal with excess resources after the backlog is archived (if initially required)
Enterprise Vault Consulting and Systems Engineering teams use assessment tools, to be executed on customer premises, to determine the number and size of messages within a certain age band and consequently improve the accuracy of the calculations provided in the *Symantec Enterprise Vault 7.0 - Sizing an Enterprise Vault Solution for Exchange Archiving – Technical white paper*. Of particular interest in this paper are the typical values used in sizing estimates, which have been the guidelines used for all joint performance benchmarks.

A summary of this user profile is:

- Average message size is 75 KB.
- Typical user sends and receives are about 70 messages per workday.
- Typical age-based archiving policy is about 60 days.
- About 20 messages will remain in the users’ mailbox and will be archived.
- About 30 percent of messages reaching archiving age are single instanced.
- Messages, including attachments, will compress between 30 percent and 50 percent.
- Average available archiving window is 6 hours, on a five-nights-per-week scenario.
- Prior to archiving, average backlog size is about 70 percent of a typical Exchange mailbox store.

In general, a dual-processor Enterprise Vault server can support mailbox archiving from up to 7,500 mailboxes (see Table 2).

**Table 2 Supported mailboxes for mailbox archiving based on EV server configuration**

<table>
<thead>
<tr>
<th>Number of Enterprise Vault server - processors</th>
<th>Number for managed mailboxes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4,500</td>
</tr>
<tr>
<td>2</td>
<td>7,500</td>
</tr>
<tr>
<td>4</td>
<td>12,000</td>
</tr>
</tbody>
</table>

Enterprise Vault uses AltaVista’s Search Engine to fulfill end-user search requests, having one index per user or journal archive. As these AltaVista indexes are binary files with very high I/O demands, it is required that the computer hosting the Enterprise Vault Indexing Service has access to adequate storage for such indexes.

Indexes may be placed on local storage, SAN or NAS. However, if fast indexing is required or searches across a large number of archives are to be performed, it is recommended to use SAN devices instead; the same recommendation applies for fast concurrent searches generated by the use of Enterprise Vault Discovery Accelerator or Compliance Accelerator in Enterprise Vault environments.

- Due to the high I/O demands on Enterprise Vault indexes, they should be treated the same way as SQL Server transaction log files, and RAID 1 or RAID 1/0 partitions on 15,000 rpm (15k) drives should be allocated.

**Note:** It is important to exclude the index locations from virus checking applications as anti-virus software can potentially change data.
Note the following about indexes:

- On NAS devices, opportunistic locking must be turned off.
- Indexes become fragmented, whatever the type of device, and this slows down both searching and indexing. It is recommended to regularly defragment indexes, ideally while the Indexing Service is stopped, so that defragmentation does not conflict with updates. This is particularly important when the Accelerator products are being used. Additional information on how to tune the Accelerator products is available in the *Symantec Enterprise Vault 9.0 - Installing and Configuring Guide*.

Index storage requirements are calculated as a percentage of the size of the original data being archived, depending on the Indexing type needed, as listed in Table 3.

### Table 3  Index storage requirements

<table>
<thead>
<tr>
<th>Indexing type</th>
<th>Estimated storage requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brief</td>
<td>3% of original data</td>
</tr>
<tr>
<td>Medium</td>
<td>8% of original data</td>
</tr>
<tr>
<td>Full</td>
<td>12% of original data (recommended)</td>
</tr>
</tbody>
</table>

Note: The percentages for Medium and Full will be less if there is little indexable content. This is often the case where large attachments such as MP3 or JPEG files are part of the environment.

Collections

Enterprise Vault provides two mechanisms for storing items in EMC Centera — with collections and without collections. A collection is up to 100 items or 10 MB of data.

When collections are used, items are first archived to a local staging area until the Enterprise Vault Storage Service process collects files in this area and stores them on EMC Centera. When Centera collections are enabled the Storage Service processes the item in two steps:

1. Item is archived to a temporary saveset file to the staging area (performed by the StorageArchive process).
2. Multiple temporary saveset files are collected and stored in a Collection Clip (performed by the StorageFileWatch process); when complete the temporary saveset files are deleted.

Note: If the primary EMC Centera system is offline when the Storage Service starts, the Storage Archive process does not perform step 1. If, however, the primary EMC Centera system goes offline after the Storage Service starts, the Storage Archive process performs step 1.

A particular Enterprise Vault server can manage multiple Vault Stores; a Vault Store may have multiple collections, but only one opened at any given time.

**BEST PRACTICE:** For performance purposes, enabling EMC Centera collections is the recommended choice.

Note: EMC Centera collections should not be confused with NTFS collections used when archiving to NT file systems.
BEST PRACTICE: Due to the high I/O demands required for collections, RAID 1/0 is the recommended RAID type configuration.

BEST PRACTICE: The recommended size for staging collections is 5 GB for normal operations; however, for contingency / disaster recovery purposes, it is recommended to allocate 50 GB per Enterprise Vault server.

Other Enterprise Vault storage requirements

Table 4 presents two items to be hosted on each Enterprise Vault Server local disk. Although the amount of local storage is small, I/O performance is critical to avoid any impact on the application.

<table>
<thead>
<tr>
<th>Item</th>
<th>Purpose</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temporary files</td>
<td>Used by Enterprise Vault archiving processes, in particular the Storage Service during archiving and conversion</td>
<td>100 MB</td>
</tr>
<tr>
<td>MSMQ files</td>
<td>Used during Exchange archiving and journaling</td>
<td>10 MB</td>
</tr>
</tbody>
</table>

Note: It is recommended to place these items on disks separate from the system disk, having RAID 1/0 as the RAID type configuration.

Note: It is recommended to reassign the TEMP system variable to a drive other than the C: drive.

Note: During installation, Enterprise Vault requires 70 MB of disk space to install all the Enterprise Vault components.

EMC Centera

Properly sizing the EMC Centera for optimal capacity and performance involves several factors. Some major factors would include:

♦ Estimated thread consumption
♦ Average object size
♦ Bandwidth
♦ Daily ingest rates
♦ Protection scheme
Retention policies

Capacity growth

Node object count threshold

Read write requirements.

During the Enterprise Vault archiving process, an item is first compressed and then metadata is added to it. As a general rule, the item is compressed to half its original size and the metadata compresses to approximately 5 KB.

Note: Compression ratios may vary considerably depending on the type of file. Office 2003 documents tend to compress well. Other document types, such as ZIP files or JPG files, are already compressed and cannot be compressed further.

Note: When archiving to EMC Centera, Vault Store Partitions, which are actually the only things stored on the EMC Centera, still use the pre-EV9.0 OSI5 format, as Enterprise Vault relies solely on EMC Centera single-instancing capabilities.

As a rough rule of thumb, it is recommended to assume that the storage required on the EMC Centera (not including the protection mechanism – CPM recommended) will be approximately 50 percent of the original unarchived size. See the Symantec Enterprise Vault 9.0 Performance Guide for more details on the EMC Centera sharing (single instancing) model.

**BEST PRACTICE:** In addition to data growth, protection schema, potential single instancing, retention policies, and other legal requirements greatly impact the size of the archive. These factors should be carefully considered.

Note: EMC Centera single instancing is achieved across all Enterprise Vault’s store partitions, regardless of the Vault Store Group they belong to. This background task, transparent to the application, provides further storage savings, and minimizes the network planning requirements.

Network

Although the network infrastructure seldom is the limiting factor on performance, in order to support the considerable volume of network traffic potentially generated by Enterprise Vault, it is recommended to provide an environment in which the connections support the expected response time of at least 100 Mb/s switched Ethernet LAN. Usually, a 100BaseT is sufficient, but unique requirements and constraints require more precise calculations on network usage for the various archiving components.

Note: For guidelines on the network traffic expected between the various components under different conditions, it is recommended to contact the Symantec supplier responsible for the deployment. The Symantec Enterprise Vault 9.0 - Installing and Configuring Guide has more information.

EMC Centera network segmentation allows for the filtering of network traffic by use case (application data access, Centera Replication, Centera management). This provides not only extra flexibility during the implementation of the solution but also room for network traffic optimization and fine tuning.

**BEST PRACTICE:** Although optional, for environments with high network traffic, it is recommended to implement EMC Centera network segmentation.
Infrastructure / business continuity considerations

During the planning phase, it is recommended to identify the critical activities or functions that are part of the archiving solution and determine their recovery point objective (RPO) and recovery time objective (RTO) in order to ensure that business or technical requirements are met in case of a disaster recovery event.

Enterprise Vault and the EMC storage devices provide several mechanisms that assist enterprises in minimizing the risks associated with these events and properly recover when they do occur.

Enterprise Vault backup

Given Enterprise Vault’s flexibility and scalability, its components can be distributed across multiple computers, requiring an effective backup strategy to prevent data loss, and to provide a means for recovery in the event of a system failure. In particular, Enterprise Vault Services and tasks may be remote to the resources that Enterprise Vault depends on.

To facilitate backup activities and minimize impact on end users, Enterprise Vault provides a backup mode setting for Vault Stores and index locations. When set up, Enterprise Vault backup mode places the Vault Store/index location in read-only mode while the backup is taken, ensuring that users are serviced for searches and retrievals from the archive while the data is in a steady state.

The *Symantec Enterprise Vault 9.0 - Administrators Guide* has additional information on how to set/clear the Vault Store and index locations’ backup mode, including examples for typical use cases.

Data to be backed up

A complete system and file backup, including the registry – because all Enterprise Vault Services store information in the registry – is required. It is recommended to take this system and file backup at the same time the following Enterprise Vault system databases are being backed up:

- EnterpriseVaultDirectory
- EnterpriseVaultMonitoring
- EnterpriseVaultAudit
- EnterpriseVaultFSAResults

Finally, each vault store database must be backed up, as well as all the index locations for that particular Vault Store.

*Note: When archiving to EMC Centera, as opposed to any other storage device, it is not required to back up the vault store partitions.*

The *Symantec Enterprise Vault 9.0 - Administrators Guide* provides additional information on the following topics:

- Enterprise Vault backup requirements, and procedures to determine the locations of the several components
- Enterprise Vault failover configuration
- Enterprise Vault recovery procedures
Note: It is recommended to use a building block approach to setting failover, as it is the practice of backing up the complete Enterprise Vault environment, as listed here.

The Enterprise Vault 9.0 and later - Backing up Enterprise Vault document contains detailed information about backing up Enterprise Vault, including details on how to create a view and store procedures to automatically back up all Enterprise Vault databases, using backup scripts.

Additional information on performing backups of Enterprise Vault systems that are clustered, using Veritas Cluster Server (VCS) or Microsoft server clusters, is available in the Backing up Enterprise Vault in a clustered environment technical note.

Enterprise Vault clustering

As with any other application critical to the business, clustering of an Enterprise Vault environment provides a means for a high-availability solution. Another alternative is to implement Enterprise Vault building blocks.

For clustering purposes, Enterprise Vault can be integrated with Veritas Cluster Server (VCS) or in Microsoft server clusters.

Note: Active/Active clustering configurations are not permitted by Enterprise Vault.

On a VCS environment, active/passive and N+1 configurations are supported. The VCS GenericService agent leverages the information contained in the Enterprise Vault Directory database to manage the following resources:

- Admin Service
- Directory Service
- Indexing Service
- Shopping Service
- Storage Service
- Task Controller Service

Additional information on VCS configuration is available in the Symantec Enterprise Vault 9.0 - Installing and Configuring Guide.

On a Microsoft server cluster environment, the following operation modes are supported:

- An active/passive failover pair - A primary node with a dedicated failover node.
- N+1 (hot standby server) - Two or more primary nodes share a single failover node. Only one node failure can be accommodated at any one time.
- N+M - An extension of the hot standby concept with N primary nodes and M failover nodes. Only M node failures can be accommodated at one time.
- N+M "any-to-any" - Identical to N+M, except that there is no need to fail back to the original node after a failover. When the original node becomes available again, it can operate as a failover node.
The Symantec Enterprise Vault 9.0 - Installing and Configuring Guide has additional information on how to configure Enterprise Vault with Microsoft server clusters.

For failover capabilities, configuring Enterprise Vault following a building block approach is a feasible alternative as it provides a means for having a solution that is both reliable and scalable. Each building block comprises a full set of Enterprise Vault Services that deliver archiving, indexing, storage, search, and retrieval functions.

**Note:** Building blocks in a clustered configuration are not currently supported by Enterprise Vault.

The Symantec Enterprise Vault 9.0 - Introduction and Planning Guide has additional information on possible configurations.

**EMC Centera Replication**

EMC Centera Replication provides a disaster recovery mechanism for content written to EMC Centera clusters. Replication can be used to create multiple protected copies of content written to a primary Centera cluster by copying the content to a replica Centera cluster. Replication runs as an asynchronous background task and can be configured in a number of topologies, to best fit customer requirements.

EMC Centera Replication provides functionality that allows the recovery of content that is either missing or simply unavailable. Applications will fail over automatically to retrieve missing or unavailable content on the primary cluster from the replica cluster.

The main characteristics of Centera Replication are:

- The process automatically copies new content to another EMC Centera cluster. No backups of archived data are necessary.

- The EMC Centera Replication mechanism ensures that new content from a local application is automatically and transparently transferred across a WAN to a designated EMC Centera cluster, presumably in another location.

- Provides a disaster recovery mechanism for content written to EMC Centera clusters.

- Can be used to create multiple protected copies of content written to a primary EMC Centera cluster by copying the content to a replica Centera cluster.

- Provides functionality that allows the recovery of content that is either missing or simply unavailable. Applications will fail over automatically to retrieve missing or unavailable content on the primary cluster from the replica cluster.

- Replication runs as an asynchronous background task and can be configured in a number of topologies. These combinations provide the replication topology that best fits customer requirements:

  - Unidirectional
  - Bidirectional
  - Chain
  - Star
Note: Enterprise Vault indexes and SQL databases are not held on EMC Centera and still require backups.

In a typical replication setup the EMC Centera clusters are geographically separate to ensure disaster recovery or to distribute the content for access from another location. For example, a company may replicate to a second EMC Centera cluster to enable recovery from the loss of the primary Centera or to avoid multiple requests for the same content across a WAN connection.

Unidirectional replication

The most basic form of replication is unidirectional replication between two EMC Centera clusters. The application writes data to cluster A and that data is automatically copied to cluster B (active passive configuration).

In case of a disaster or when the primary EMC Centera cluster becomes unavailable, the application may fail over to the replica cluster B. Automatic read failover is a feature of the EMC Centera SDK and is enabled by default, but other failover options may be configured (see Figure 3).

Note: Data written to cluster B during a disaster needs to be restored to cluster A, once it is back online. If cluster A was lost during the disaster, all lost data needs to be restored from cluster B, using the EMC Centera Restore feature. To avoid having to restore the content back, it is recommended that bidirectional replication be set up to capture all new content.

![Figure 3  Replication failover](image-url)
Bidirectional replication

The bidirectional replication topology allows applications to write to either of the EMC Centera clusters and have data copied to the other Centera cluster. Data written to cluster A will be replicated to cluster B and vice-versa.

This allows for establishing a complete DR solution whereby the application servers are also redundant. When the complete site A is lost, site B can take over immediately. This is called hot standby and is shown in Figure 4. Data written to cluster B by application 2 or application 1, if it was cut over to site B during a disaster, will be held in a replication queue and replicated to site A as soon as this site comes back online. If site A was lost during the disaster, all lost data must be restored from cluster B, using the EMC Centera Restore capability.

![Bidirectional replication with hot standby](image)

**Figure 4** Bidirectional replication with hot standby

Rather than using site 2 as a hot standby, both sites can be used for production. This is useful when both sites have users who work on the local application server. All data will be kept available at both sites using the bidirectional application.

**Note:** Although from an EMC Centera perspective all data can be shared between sites, each local application may not be aware of data created by the other application. Enterprise Vault databases may need to be synchronized.

Additional information on EMC Centera Replication, including other topologies available, and Restore operations, is available in the *EMC Centera Replication – A Detailed Review* white paper.

**BEST PRACTICE:** Content on the primary (source) cluster that was not yet replicated to the secondary (target) cluster may not be recoverable. Ensuring that the Enterprise Vault Remove safety copy feature is enabled will seamlessly allow the re-archival of the data, preventing any potential data loss.
EMC Centera Restore/tape out

To copy data from one cluster to another, EMC Centera offers restore in addition to replication. Replication is an ongoing process that starts after it has been set up and continues unless it is paused by the system administrator or by the system. Restore is a single operation that copies data from a source cluster to a target cluster and is only performed as needed by the system administrator. A restore operation can be performed from any source cluster to any target cluster. There is no need for a replication setup between the two clusters.

The main characteristics of the Restore capabilities are the following:

- Restore is a functionality of EMC Centera which, when enabled, copies data (clips, BLOBs and mutable metadata) from a source cluster to a target cluster. The set of data to copy can be narrowed down according to the use case at hand, full or partial.

- Restore is a process complementary to replication, whereby an EMC Centera cluster copies some set of its content or the entire Centera to another Centera cluster.

- Replication is used on an ongoing basis to keep two EMC Centera clusters synchronized with new content, whereas restore is used only as needed to populate one EMC Centera cluster with the content of another Centera.

- Restore is capable of restoring content at the cluster or pool level.

Note: When business requirements determine that a copy of EMC Centera data on tape or Virtual Tape Library (VTL) is needed, alternatives to perform such activities are available with or without the use of NDMP technologies. Additional information on available products to support these activities is available through Symantec or EMC.

Celerra Replicator (V2)

Celerra Replicator™ provides the functionality to replicate file systems asynchronously. Celerra Replicator (V2) represents a new generation of replication technology, utilizing adaptive replication technology to optimize replication performance and quality of service in accordance with set RPO levels, which can be set for each replication session. A replication session is made up of a source file system replicating data to a destination file system. This adaptive replication approach empowers the business to focus on deciding how many minutes of data loss is acceptable in a disaster recovery event (the RPO), while Celerra Replicator (V2) automatically attempts to achieve that RPO by intelligently taking into account changes in network transfer rates.

Further highlights include:

- Scalability
  - Up to 1,024 replication sessions, up to 256 active (transferring) replication sessions, and up to 16 initialization replication sessions per Data Mover.
  - Replication from a single storage object to up to four different destinations, and the ability to cascade the replication from each of the four destination objects to as many as three additional destinations – yielding a net 16 replicas per source object while enabling each replica to be governed by its own RPO.
**Chapter 1 Planning**

- **Performance**
  - Adaptive, RPO-based replication scheduling: Set your desired RPO and Celerra Replicator (V2) optimizes your replication sessions continually.
  - Administrative operations (create session, delete session, failover session, and others) are extremely fast.
  - One-click switchover and reverse: This new operation provides a simple method to turn the destination object into production with no data loss, with optional reversal of the replication direction.
  - Failover commands may be issued in parallel.
  - Loopback replication is extremely fast and bypasses the network for a purely disk-to-disk copy.

- **Ease of use**
  - A new graphical wizard to further streamline the replication creation process.
  - Automatic creation of destination file systems and VDMs.
  - New alerting mechanisms to help notify the administrator when network or other problems are interfering with replication.

- **Functionality**
  - Multiple replication modes: Remote, Local (intra-cabinet), and Loopback (intra-Data Mover) replicas.
  - One-time copy tool.
  - New Data Mover interconnects carry data as well as control information.
  - Flexible bandwidth throttling: Reduces network usage during times of peak demand by slowing replication according to configurable policies.

- **Disaster Recovery Auditing (Testing):** Disaster recovery auditing/testing with Celerra Replicator (V2) can be easily performed using a variety of methods that cater to different test objectives including switchover, failover, and copy operations and the ability to create a read-write checkpoint on the destination file system.

In summary, Celerra Replicator (V2) represents a leap forward in the area of information protection. It delivers more value to storage administrators and helps them attain their ultimate goal of service level delivery by easing administration and working to meet their RPOs automatically. At the same time, it delivers groundbreaking scalability and flexibility to help the storage administrator do more with less.

**Celerra SnapSure**

A checkpoint is a file system that represents a point-in-time view of the primary file system (PFS), which is where the files are stored on. A checkpoint often requires far less disk space than a full copy, which makes it a very powerful and cost-saving feature. From an end-user...
perspective, a checkpoint is similar to an accessible file system when viewed over a Common Internet File System (CIFS) or a Network File System (NFS) client.

A read-only checkpoint is a read-only point-in-time view of its associated PFS. A read-only checkpoint can be shared with network clients by using traditional network file sharing protocols such as CIFS, NFS, or File Transfer Protocol (FTP). It provides a snapshot of the PFS at the time the checkpoint was created. Business applications that require access to point-in-time PFS data, but not real-time data, can take advantage of a read-only checkpoint file system.

A writeable checkpoint is a read/write point-in-time view of its associated PFS. Similar to read-only checkpoints, the PFS view in a writeable checkpoint can be shared with network clients by using traditional network file sharing protocols. However, unlike a read-only checkpoint, a writeable checkpoint can be modified (written to) by network clients so that it no longer reflects a point-in-time view of the PFS. Software patch testing and configuration changes to the production environment will benefit from writeable checkpoints. After the updates are stabilized, the changes can be propagated to the PFS.

There are several reasons to deploy SnapSure™ checkpoints:

- **Restore individual files quickly and easily** — SnapSure read-only checkpoints help administrators to process user file recovery requests without the overhead of a file recovery from backup media. Requiring only a nominal amount of disk space, read-only checkpoints are efficient and can be created on a regular basis. Thus, it enables multiple point-in-time views of a PFS. This flexibility enables storage administrators to respond to user requests on time.

- **Restore confidently with roll-back protection** — An administrator can seamlessly restore a point-in-time view of the checkpoint back to the PFS. This feature also enables an administrator to undo a restore and return or roll back to a last known state effectively. SnapSure requires the administrator to create a checkpoint prior to restore operation, thus enabling a rollback option to the last known state.

- **Create true point-in-time backup copies** — Backing up live production data introduces the risk of distorting the versions of files that are backed up. While taking a backup of a PFS, some of its files may be accessed and modified before they are backed up. In such cases, the backup will not reflect the point-in-time state of when the backup was initiated. By backing up from the checkpoint of the PFS, administrators can be confident in their ability to recall the point-in-time state of a file or file system, thereby serving the needs of their users effectively and efficiently.

- **Test production changes offline** — Reduces the risk of rolling out production changes, such as software patches, by first testing those changes on a writeable checkpoint copy of the target file system. After the desired changes are proven stable, they can be rolled out into the production environment confidently, thereby reducing potential downtime and business level impact.

- **Improve efficiency of the PFS** — Copies of a PFS can be created using checkpoints. These copies can be made available to support business units or activities (for example, reporting, data mining) that do not require real-time data that the PFS provides. This segmentation of the workload can improve the efficiency of the PFS by diverting traffic it would otherwise see over to a SnapSure checkpoint.
Celerra backup, recovery, and archive with NDMP

Network Data Management Protocol (NDMP) backups and restores perform over the SAN and provide faster file system backup and recovery times than if backed up or restored over the LAN. NDMP backups and restores are managed from the backup software application, such as Symantec NetBackup and EMC NetWorker®. Another advantage of NDMP is that it has multi-protocol support, which allows files with CIFS and NFS attributes to be retained in the backup.

NDMP is an open protocol used to control data backup and recovery communications between the primary (that is, file system) and secondary (that is, tape library) storage in a heterogeneous network environment. NDMP provides a common architecture for network file servers, like Celerra, to communicate with backup devices without backup software on the file server. Because NDMP backup and recovery do not require the file server to have the backup software, a network client loaded with the backup application can be designated as the management host for the backup environment that can be made up of multiple file servers and tape libraries.
Chapter 2 Implementation

This chapter presents these topics:

- Installation requirements and configuration ................................................................. 44
- Installation process .......................................................................................................... 68
- Configuring Enterprise Vault .......................................................................................... 70
- Installation validation ....................................................................................................... 73
Installation requirements and configuration

Enterprise Vault

Before installing or upgrading Enterprise Vault, it is strongly recommended to run the Enterprise Vault Deployment Scanner to check prerequisite software and settings to review the configuration of a computer and to report on any issues that may stop Enterprise Vault from running on it. The *Symantec Enterprise Vault 9.0 - Deployment Scanner Guide* provides a list describing the tests that Enterprise Vault Deployment Scanner performs, as well as directions on installing the tool.

Enterprise Vault Deployment Scanner is a separate wizard that is supplied on the Enterprise Vault media. When the tool runs, it creates a Reports folder in the folder in which it is run, and places a report file in the Reports folder.

Deployment Scanner and accompanying documentation may be found in the Enterprise Vault 9.0\Deployment Scanner folder on the Enterprise Vault media.

**Note:** Windows Installer 3.1 must be installed on your Enterprise Vault servers in order to install Enterprise Vault Deployment Scanner and the Enterprise Vault server components.

Software requirements

This section describes the operating system and software requirements for the core Enterprise Vault Services.

**Note:** There may be additional requirements for the different types of archiving. The requirements for Exchange are described in the *Exchange Archiving with Enterprise Vault* section of this document.

Operating system

Enterprise Vault server components can be installed on the following operating systems:

- Windows Server 2003 with Service Pack 2 or later
- Windows Server 2008 with Service Pack 1 or later
- Windows Server 2008 R2 x64 edition (using WOW64)

If Windows Server 2008 with Service Pack 1 is installed, the following mandatory hotfix for IIS must also be installed, as indicated by Microsoft at [http://support.microsoft.com/kb/949516](http://support.microsoft.com/kb/949516).

For additional details of supported versions, see the *Symantec Enterprise Vault Compatibility Charts*.

Install Windows with the following options and components; additional information is listed in the pages that follow, as well as in the *Symantec Enterprise Vault 9.0 - Installing and Configuring Guide*

- NTFS file system
- Microsoft Message Queuing (MSMQ) Services
- .NET Framework 3.5 SP1 or SP2
Internet Information Services (IIS) 6.0 or later

Internet Explorer 7.0 or later

MSXML

**MSMQ**

Enterprise Vault tasks use MSMQ to communicate with the Storage Service. To install Enterprise Vault Services on more than one computer in the network, MSMQ must be configured on each computer.

The steps for installing MSMQ on Windows 2003 and 2008 are different. Note that Active Directory Integration should not be enabled when installing MSMQ.

Additional info on how to install MSMQ on different platforms is available in the *Symantec Enterprise Vault 9.0 - Installing and Configuring Guide* according to the operating system of use.

**.NET Framework**

It is required to install Microsoft .NET Framework 3.5 SP1 or SP2 on Enterprise Vault servers.

If necessary, it can be downloaded using the link in the Links to related software folder on the Enterprise Vault media or directly from the Microsoft .NET Framework Version 2.0 Redistributable Package (x86).

**Note:** .NET Framework 3.0 SP1 or later is required for Compliance Accelerator (version 8.0 and later) and Discovery Accelerator (version 9.0 and later). See the *Symantec Enterprise Vault Compatibility Charts* for more details.

**IIS**

It is required to install IIS 6.0 or later on each Enterprise Vault server.

In IIS, it is possible to configure the level of isolation for particular Web applications. For shopping baskets in the Enterprise Vault Web Access application to be created correctly, the application needs to run under the predefined Local System account.

The configuration wizard will automatically set the correct isolation and account settings; consequently, there is no need to configure this.

If IIS 6.0 or later is already installed, the configuration wizard will create a new Application Pool, EnterpriseVaultAppPool, for the Web Access application and assign the Local System account to that pool.

**Note:** Active Server Pages and ASP.NET must be enabled. On Windows Server 2003, it is required to enable Active Server Pages and ASP.NET manually. The *Symantec Enterprise Vault 9.0 - Installing and Configuring Guide* has more information.

In Windows Server 2008, if the Add Roles wizard is used to install IIS, the wizard will provide the default installation, which has a minimum set of role services. Minimum IIS-related roles services required for Enterprise Vault are listed in the *Symantec Enterprise Vault 9.0 - Installing and Configuring Guide*
Internet Explorer

Internet Explorer 7.0 or later is recommended.

MSXML

All Enterprise Vault server computers require MSXML. This is installed automatically with Internet Explorer 7.0 and later.

If MSXML 6.0 is not present when installing the Enterprise Vault Services component, the Enterprise Vault installer installs it without asking for confirmation.

Roles-based administration

Roles-based administration uses Microsoft Windows Authorization Manager. Creating and managing roles using the Administration Console requires the Authorization Manager MMC snap-in, which is only available on the following:

- Windows Server 2003
- Windows Server 2008

The Administration Tools Pack can be downloaded from the following location:

http://www.microsoft.com/downloads/details.aspx?FamilyID=c16ae515-c8f4-47ef-a1e4-a8dcbacf8e3&DisplayLang=en

SQL Server

Enterprise Vault supports SQL Server 2005 SP2 and 2008 as database engines. Additionally, both Windows Authentication mode and Mixed Mode Authentication are supported.

**Note:** The SQL installation must be case-insensitive, as case-sensitive SQL installations are not supported.

Microsoft Data Access Components (MDAC)

To enable access to the SQL databases, MDAC 2.6 or later must be installed on Enterprise Vault servers. A suitable version is installed automatically with both Windows Server 2003 and Windows Server 2008 (which changes the name of MDAC to Windows Data Access Component or Windows DAC).

If necessary, the software can be installed using the link supplied in the **Links to related software** folder on the Enterprise Vault media. The *Symantec Enterprise Vault 9.0 - Installing and Configuring Guide* has additional information.

SQLXML

SQLXML 4.0 is required on computers on which the Enterprise Vault Services component is installed.
If SQLXML 4.0 is not present when installing the Enterprise Vault Services component, the Enterprise Vault installer automatically installs it without asking for confirmation.

**Hardware / Storage requirements**

The most critical factor in the performance of Enterprise Vault is the specification of the system that is used—the servers, disk systems, memory, and network.

**Application server**

In general, the more powerful the processor is, the higher the ingest and retrieval rates are. The other components of the system—the disks, memory, network, and archiving source—need to match this power. The following represents general considerations on server selection and configuration:

- Enterprise Vault must be installed on a computer member of a domain.
- Enterprise Vault makes good use of multi-core processors, and quad-core processors are recommended.
- Four GB of memory is recommended. The operating system boot flag /3GB must not be used as this does not provide any benefit and can result in running out of system page table entries. For a fuller explanation, see “32-bit and 64-bit platforms” in the Symantec Enterprise Vault 9.0 Performance Guide.
- Turning hyperthreading on or off makes no noticeable difference to the overall performance of Enterprise Vault, so it is recommended that the manufacturer’s default setting is not changed.
- There is no performance difference when running Enterprise Vault on 64-bit Windows (WOW 64) when compared with 32-bit Windows. For a fuller explanation, see “32-bit and 64-bit platforms” in the Symantec Enterprise Vault 9.0 Performance Guide.
- There is no performance difference when running Enterprise Vault on a Windows 2008 operating system when compared with Windows 2003 or when archiving from an Exchange Server on a Windows 2008 system.

Table 5 shows the recommended minimum specifications for a production Enterprise Vault system supporting 7,500 user mailboxes.

<table>
<thead>
<tr>
<th>Item</th>
<th>Recommended minimum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of CPUs</td>
<td>2</td>
</tr>
<tr>
<td>Power of CPUs</td>
<td>2.8 GHz</td>
</tr>
<tr>
<td>Memory</td>
<td>4 GB</td>
</tr>
</tbody>
</table>

It is possible to run Enterprise Vault on a computer with less memory, but this is not recommended for a production system, as it does not allow for any growth in archiving requirements. The extra memory is particularly important if users will be performing large, simultaneous archive searches.

Enterprise Vault can be run on a multi-processor system with four or eight CPUs, but in order to take advantage of the extra CPU power, the disk system used must be able to cope with the increased throughput.
In a small to medium Enterprise Vault environment, the core Enterprise Vault Services will typically all be installed on the same computer. In larger installations, services such as the Storage and Indexing Services can be installed on a separate computer.


**Additional processing capacity for initial archiving**

If a large backlog of data needs to be archived quickly, when Enterprise Vault is installed, additional Enterprise Vault servers may be configured for the initial archiving run. When archiving reaches a steady state, the additional Enterprise Vault servers can be redeployed for other purposes.

**Database server**

The recommended specification for best performance is a standard SQL server with four physical CPUs and a minimum of 4 GB of RAM; for medium or large environments, 8 GB of RAM is recommended. It is also recommended to fine-tune the performance of the SQL server using standard methods, such as the ones described in the *Symantec Enterprise Vault 9.0 Performance Guide*.

- Using an x64-based 64-bit platform provides more efficient memory utilization and brings performance benefits. The appropriate editions of Windows Server 2003 and SQL Server 2005 must be installed to support the capacity of memory installed, but no other tuning options need to be set.
- If a 32-bit database server will be used then the server should be carefully tuned to make best use of available memory. These tuning options depend upon using the appropriate edition of Windows and SQL Server for the installed capacity of memory. If the database server has more than 4 GB of physical RAM:
  - Enable the operating system Physical Address Extensions boot flag (/PAE).
  - Enable Address Windowing Extensions (AWE) memory in SQL Server using the following script:
    ```sql
    sp_configure 'show advanced options', 1
    RECONFIGURE
    GO
    sp_configure 'awe enabled', 1
    RECONFIGURE
    GO
    ```
  - Hyperthreading may not be beneficial to SQL Server environments and should be carefully tested before enabling.

Enterprise Vault requires a number of SQL databases:

- The Enterprise Vault Directory database holds the configuration information for an Enterprise Vault Site.
- Each Vault Store has a Vault Store database, which holds configuration information for the Vault Store and details of the items stored in its archives.
Each Vault Store Group has a fingerprint database, which holds the fingerprints and other information related to the single-instance storage parts that are created for Enterprise Vault single-instance storage.

The Monitoring database holds monitoring information for the Enterprise Vault Site.

If FSA Reporting is configured, Enterprise Vault creates an FSA Reporting database to hold the FSA Reporting data.

The SQL server that manages these databases will typically reside on a different computer from the Enterprise Vault server.

In general, the specification of the SQL Server computer should match that of the Enterprise Vault server. The performance of the SQL Server will also benefit from extra memory; a minimum of 4 GB is recommended. The amount of memory that the SQL server can use depends on the Windows and SQL Server versions. Table 6 shows the recommended minimum specifications for a production SQL server.

<table>
<thead>
<tr>
<th>Item</th>
<th>Recommended minimum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of CPUs</td>
<td>2</td>
</tr>
<tr>
<td>Power of CPUs</td>
<td>2.8 GHz</td>
</tr>
<tr>
<td>Memory</td>
<td>4 GB</td>
</tr>
</tbody>
</table>

Note: There is no need to have a separate SQL server for every Enterprise Vault server. As a general rule, one SQL server can manage four to eight Enterprise Vault servers. For additional information, see the Symantec Enterprise Vault 9.0 - Installing and Configuring Guide.

Indexes

Note the following points:

- It is required that the default index storage location is on an accessible device and that the Vault Service account can write to it.

- With Exchange Server archiving, Enterprise Vault adds information about the index storage location to the Directory database once the mailboxes are enabled. It is recommended to perform any changes to the index storage location, or add further locations before any mailboxes are enabled via the Administration Console. Changing the index storage location for mailboxes after they have been enabled cannot be done easily.

- As anti-virus software can potentially change data, it is important to exclude the cache and index locations in the virus checking application. The Symantec Enterprise Vault 9.0 - Installing and Configuring Guide has more information.

Exchange archiving with Enterprise Vault

This section covers additional requirements and considerations for Microsoft Exchange archiving using Enterprise Vault.

The following target Exchange servers are supported for archiving items from mailboxes and public folders:
For Exchange Server archiving, one of the following must be installed on the Enterprise Vault server:

- Outlook 2003 SP2
- Outlook 2007 SP2 with Microsoft hotfix KB968858 (required to archive from Exchange Server 2010).

In addition to the previous requirements, the following pre-installation tasks are required prior to installing and configuring Exchange Server archiving components. The Symantec Enterprise Vault 9.0 - Installing and Configuring Guide has detailed information.

### The Enterprise Vault system mailbox

A system mailbox is required on each Exchange server that Enterprise Vault is to archive; this Enterprise Vault system mailbox will be used by the Exchange mailbox, Exchange journaling, and Exchange public folder tasks when connecting to the Exchange server.

**Note:** If database availability groups (DAGs) are used in your Exchange Server 2010 environment, the Enterprise Vault system mailbox in a database that is replicated across the DAG must be created.

This mailbox name is required by the Administration Console whenever an Exchange Server archiving task is created. The following restrictions apply to this mailbox:

- The Enterprise Vault tasks require exclusive use of this mailbox, so the mailbox must not be used for any other purpose.
- The mailbox must not be hidden from address lists.
- The account must not be disabled

Note that after creating the Enterprise Vault system mailbox, it may take some time for the mailbox to be available. The amount of time depends on configuration options in Exchange System Manager. The mailbox must be available before an Exchange Server archiving task is added. Additional information on how to manually force a mailbox update on Exchange Server 2000 or 2003 is available in the Symantec Enterprise Vault 9.0 - Installing and Configuring Guide

### Additional pre-installation tasks for Microsoft Exchange Server

Depending on the Microsoft Exchange Server version used, there are several prerequisites to be considered prior to installing Enterprise Vault.

Among other considerations, for Exchange Server 2010 it is required to re-configure the default throttling restriction policies; it is also required to grant the Vault Service account Send As permission on the system mailboxes, as well as to assign Exchange Server proper permissions to the Vault Service account.
Detailed information on these processes is provided in the Symantec Enterprise Vault 9.0 - Installing and Configuring Guide.

Create an Outlook profile on the Enterprise Vault server computer

When Outlook is installed on the Enterprise Vault server, a profile must be created and a connection to an Exchange Server mailbox must have been established before installing Enterprise Vault.

**Note:** Outlook must be the default mail client on the Enterprise Vault server. On startup, the Enterprise Vault Admin service checks that Outlook is configured as the default mail client and, if it is not, configures it as such.

Configure Internet Explorer

Microsoft Office Outlook must be set as the default email application for Internet services in Internet Explorer on the Enterprise Vault server.

Other Enterprise Vault components

- Stand-alone Vault Administration Console
- Operations Manager
- Discovery Accelerator
- Compliance Accelerator
- EMC Centera Checker
- EVR

File System Archiving with Enterprise Vault

Enterprise Vault File System Archiving can be set up to archive files from network shares (volumes). Users can then access the archived files using shortcuts in the original locations, Archive Explorer, or the browser search page. When configuring archiving for a volume, an archive point is placed to control which folders are archived and which archive is used to store files from a particular folder and its subfolders.

When a file is archived, Enterprise Vault can, optionally, leave one of the following types of shortcut in its place:

- **A placeholder.** This is a special file that appears exactly as the original file but, when opened, forces Enterprise Vault to fetch the archived file. If placeholders on a Windows file server are to be used, the FSA Agent must be installed on the file server.

- **An internet (URL) shortcut.** This is a .url text file containing a hypertext link to the archived file.

The FSA Agent

Installing the FSA Agent on a Windows file server is required to:

- Replace archived files with placeholder shortcuts, or to:
Gather data for FSA Reporting.

**Note:** Do not install the FSA Agent on EMC Celerra devices, or on Enterprise Vault servers.

- For details of the prerequisite versions and service packs of the Windows operating system on the file server, see the Enterprise Vault Compatibility Charts at http://entsupport.symantec.com/docs/276547.

To configure FSA Reporting for a NetApp or EMC Celerra device an FSA Reporting proxy server must be configured to perform the data collection. For more details, see the Reporting guide.

The FSA Agent can be installed on Windows file servers from the Administration Console, or manually. See Installing the FSA Agent on a Windows file server from Setting up File System Archiving (FSA) 9.0.

**Note:** In an environment where Windows file servers are grouped in a cluster, the FSA Agent must be installed on each cluster node. See Adding the target virtual file server in Setting up File System Archiving (FSA) 9.0 for additional information.

---

### EMC Centera

This section presents an overview of the features offered by EMC Centera applicable to an environment where Enterprise Vault is to be deployed, and the recommendations to configure EMC Centera to best perform in such setting.

The recommended EMC Centera configuration for Enterprise Vault is listed in Table 7.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Protection</td>
<td>Mirrored (CPM) (default)</td>
</tr>
<tr>
<td>Storage Strategy</td>
<td>Performance Full (default)</td>
</tr>
<tr>
<td>Pool/Profile</td>
<td>Enterprise Vault requires a profile to have Read, Write, Delete and Exist capabilities</td>
</tr>
<tr>
<td>PEA File</td>
<td>Use of a Pool Entry Authorization (PEA) file is recommended</td>
</tr>
<tr>
<td>Replication</td>
<td>At least Unidirectional is recommended; other topology depending on business requirements</td>
</tr>
<tr>
<td>Compliance Mode</td>
<td>At least Governance Edition; Compliance Edition recommended based on business requirements</td>
</tr>
</tbody>
</table>

**Note:** Content Protection and Storage Strategy are values set at the time of EMC Centera installation; it is recommended to verify that the EMC Change Control Request Form accompanying the box has the appropriate values.

---

### Content Protection

EMC Centera provides two protection schemes for storing data objects redundantly:

- Content Protection Parity (CPP)
Content Protection Mirrored (CPM)

For additional information, see the *EMC Centera V2.1 Programmer’s Guide.*

Content Protection Parity (CPP)

CPP or parity is the process whereby each stored object is split into six fragments. Each fragment will be stored on a different node in the same cluster. CPP calculates a parity fragment from the stored fragments and stores that as the 7th data fragment on yet another node. This provides the ability to reconstruct the object in the event of data loss of any one of the seven fragments.

CPP is a more space-efficient way to store data at the cost of lower performance.

CPP segments a data object into six parts and stores each one on a different node in the same cluster. CPP calculates a parity fragment from the stored fragments and stores that as the 7th data segment on yet another node. This mechanism is a derivative of RAID 3 (mostly used in single-user systems with large record applications). If seven nodes are not available, data is stored with CPM only.

When CPP is enabled, not all files will be using CPP. CDFs are always written in CPM as well as small files. EMC recommends using CPP only for files greater than 250 KB.

The threshold that is set for CPP can impact the overall storage capacity expectations. If the majority of the stored files fall below this threshold then they will not be stored in CPP and the capacity benefits of CPP will be lost.

Content Protection Mirrored (CPM)

CPM or mirroring is the process whereby each stored object is copied to another node in an EMC Centera cluster. There is a dual power supply to each node, helping to ensure that at least one copy of the data will always be available in the event of a disk, node, or power failure.

CPM stores a complete copy of the data object on a mirror node. CPM enhances faster data regeneration and improves performance during normal operation. Object retrieval is improved because the access node with the access role can select the least loaded node with the storage role from which to retrieve a specific object.

CPM is the default protection scheme for storing C-Clips that are 250 KB or less.

---

Note: Additional information on EMC Centera content protection mechanisms, regeneration, and self-healing is available the EMC Centera online help.

---

Note: When CPP is enabled, a fallback can be configured for when there are not enough nodes available in any cube for writing the fragments on seven different nodes. The default fallback is to return an error to the application and disallow further ingest to the cluster. The system can also be configured to fall back to CPM in such a case.

Additional information for data protection and self-healing EMC Centera capabilities is available in the Centera online help.

**BEST PRACTICE:** Content Protection Mirroring is the default Centera protection scheme and is recommended when used with Enterprise Vault.
Storage strategy

EMC Centera provides two storage strategy mechanisms:

- **Storage Strategy Capacity**
- **Storage Strategy Performance Full**

Storage Strategy Capacity ensures single instancing – the archival of a single copy of an item, regardless of the number of references (instances) of the content in the original data source – and thus optimizes capacity.

Storage Strategy Performance Full improves the speed of write operations at the cost of single-instance storage. When Storage Strategy Performance Full is enabled, identical content may be stored multiple times.

Note that setting the Storage Strategy to Performance Full does not improve performance substantially for large files (> 1 MB). When setting the Storage Strategy to Performance Full the default threshold (maximum file size) is 250 KB. Objects larger than this threshold will automatically revert to Storage Strategy Capacity in order to benefit from single-instance storage. The threshold can be adjusted to optimize the balance between performance and capacity.

For CPM the threshold of 250 KB equals the file size. For CPP the threshold corresponds to a file size of 6*250 KB = 1.5 MB.

**BEST PRACTICE:** The Storage Strategy is set to Performance by default and is the recommended setting when used with Enterprise Vault, as it enhances Enterprise Vault Sharing capabilities for large objects, which usually represent the bulk of the archive.

Storage optimizations – Embedded BLOBs and containers

In addition to these storage strategies, EMC Centera provides other programmatic mechanisms to allow applications to further improve their integration and performance when archiving small items to EMC Centera:

- **BLOB Embedding**

  Very small data BLOBs (less than 100 KB) can be converted to a Base64 string and stored in the CDF, either as an embedded Data BLOB or in a Tag string attribute, as opposed to a BLOB object, hence non-impacting the object count and allowing access to the data without incurring in the extra overhead of reading the data from EMC Centera.

- **Containerization**

  Another approach for managing small objects is to aggregate them into a single BLOB. This technique is called containerization. For example, many Call Detail Records (CDRs) can be taken from a telecom switch and stored as a single EMC Centera object. The offset and length for each component object can be stored as an attribute associated with the BLOB tag. Specific API calls (FPTag_BlobReadPartial) can then be used to retrieve the individual component objects from the container.

The following considerations are relevant to data containerization:

- In general, aggregated data does not benefit from single-instance storage. However, Enterprise Vault does archive attachments and other large objects individually (outside the
container) in order to favor SiS. The retention period applies to the aggregated data, as all data archived in the container follows the same retention policies.

♦ Individual data objects cannot be deleted without rewriting the container object.

Note: If the requirement is to store many small files (< 50K), EMC recommends that the application embeds the file directly in the CDF or combines multiple small files in one C-Clip™. Refer to the EMC Centera API Reference Guide for more information on embedding data.

Enterprise Vault fully leverages both BLOB embedding and containerization capabilities. Small items are stored in the CLIP directly. Items that are smaller than 15 KB will be stored in the CLIP and since this is “relational” it tends to be faster. Enterprise Vault “knows” how to store the item in the CLIP and retrieve it. Collections (or EMC Centera containers) are done differently to NTFS. Taking email as the example, only collected items will be sent to EMC Centera.

Emails are split into three parts, per user, body, and attachments. If an item is over the 15 KB threshold it will be passed to the Enterprise Vault Collector Service – if collections are enabled in Enterprise Vault. The per-user and bodies are collected into larger collections, while the attachments (greater than 50 KB) are stored separately. For additional information see the Sharing section in this document. Using collections, Enterprise Vault not only improves its SiS efficiency but also improves the performance of EMC Centera, by sending fewer, larger files.

The body and per-user details are always going to fail SiS checking as they are by their nature unique. By sending them as part of the collection, it is ensured that Centera SiS testing is kept to a minimum, thus improving EMC Centera throughput. This is another reason why setting the storage strategy to Performance Full (SSP) perfectly fits the model.

The details of the actual items that are stored in EMC Centera (header, body and attachments) are then referenced in the original CLIP. Enterprise Vault will then read the CLIP content to see how to recover any piece of content based on the offset and size of the message, without having to retrieve the whole container. Along with all the information stored in the CLIP are Enterprise Vault generated checksums. These checksums help Enterprise Vault guarantee that the content committed to Centera is valid when recalled.

In general, these are the two primary factors in archiving with Enterprise Vault and EMC Centera:

♦ Saveset collection limit is 10 MB or 100 savesets.

♦ Anything larger than 50 MB is not compressed.

Note: As opposed to email, NTFS or CIFS files being archived by Enterprise Vault FSA (File System Archiving) are handled differently. If the file is less than 50 MB it is handled like an email message. If the file is larger than 50 MB it is stored in a different way. The file is not compressed, the contents are not indexed, and the saveset is always stored in an individual Saveset Clip (never as part of a Collection Clip).

BEST PRACTICE: Containerization is a storage technique strongly recommended by Centera which can be enabled or disabled (default) in Enterprise Vault. It is a best practice to enable Enterprise Vault Sharing (Centera containers) while setting up archiving in Enterprise Vault.
Security and data segregation

**Virtual pools and profiles**

Virtual pools (VP) allow storage administrators the ability to logically segregate application data stored on EMC Centera. In pre-CentraStar™ 3.0 incarnations, CentraStar presented a single, communal pool that housed all data stored on a cluster. The value of the VP model is that it presents a highly abstracted method of operation that protects applications from details of the underlying storage mechanics. VPs represent a natural evolution of the pool model. The advantages of subdividing the communal pool are substantial and include:

- The ability to perform CentraStar operations on select subsets of data
- The ability to replicate on a pool basis
- Segregation of application data on the cluster
- The ability to set up hard pool capacity quotas
- Capacity reporting by pool
- The ability to restrict what IP can access a virtual pool

The exposed use of VPs is in data segregation and the ability to change the scope of the CentraStar Replication/Restore functions from the cluster at large to a set of discrete VPs. VPs allow changing the scope of most cluster functions away from the global cluster to individual pools and they also make it transparent to the application accessing the EMC Centera storage. For additional information, see the *EMC Centera SDK V3.2 API Reference Guide*.

An EMC Centera profile specifies what capabilities (or operations) can be performed on a connection established with that profile. The capabilities are Read, Write, Purge, Delete, Exist and Query.

A profile can have access to one or more pools, each pool/profile pair having a separate set of granted capabilities; consequently, it is possible for an application to establish a connection to EMC Centera for which there are Read, Write and Delete capabilities to one pool, but only Read privileges are given to another. This characteristic is particularly relevant for EMC Centera migrations.

Enterprise Vault requires a profile to have Read, Write, Delete, and Exist capabilities in order to perform all its operations. Enterprise Vault version 5.0 or later checks that a connection has the Read, Write, Delete, and Exist capabilities it needs.

**Pool Entry Authorization (PEA) files**

The use of Pool Entry Authorization (PEA) files – files containing authentication credentials for a given profile – is a best practice for applications when connecting to EMC Centera during the Centera Application Authentication process. The following are the Enterprise Vault requirements for this PEA File:

- A profile with Read, Write, Delete, and Exist capabilities.
- The PEA file must be accessible to the Enterprise Vault Storage Service that manages the Vault Store Centera partition that will use the profile.
Chapter 2 Implementation

- The Storage Service runs under the Vault Service account and therefore the PEA file must allow read access by this account.
- For greater security, access to the PEA file by any other account could be disabled.

**BEST PRACTICE:** Usage of Pool Entry Authorization files is strongly recommended.

**Note:** If Application Authentication is not used – which is not recommended – an application is granted access to EMC Centera using the Anonymous profile; to prevent this, the Anonymous profile is disabled by default. Enabling this profile is only available to the EMC Centera system administrator.

**Replication**

For disaster recovery and high availability purposes, it is recommended to have at least EMC Centera unidirectional replication enabled; ideally, bidirectional replication should be set up.

**Note:** Failure to follow the standard procedures for pools and profiles creation and PEA files generation on replicated environments may lead to Enterprise Vault not being able to successfully establish an EMC Centera connection.

Details for these procedures are available at the EMC Centera online help.

**Network segmentation**

The concept of network segmentation – the use of multiple physical networks allowing each type of traffic to be segregated, monitored, and managed according to the appropriate per-site policies – for different types of traffic going to the EMC Centera system adds additional security for end users. Any management interaction with the system can be segregated from application input/output, ensuring the utmost security for data integrity.

**Note:** For environments where such separation of traffic is not necessary, a single physical network may still be used for all network traffic.

The main characteristics of the different network traffic types going to and from EMC Centera are:

**Application traffic**

- Input/Output requests are defined as standard input/output operations to the EMC Centera (read, write, delete, exists, and query).
- Replication requests are defined as requests to a secondary or disaster recovery EMC Centera to store data.

**Management traffic**

- EMC Centera Viewer/CLI connections are administrative tools for system administrators and end users.
- Email home mails are reports from the EMC Centera that show system health, failure alerts, and sensors.
- SNMP traps are additional monitoring mechanisms of system health.
Node roles

The roles that can be assigned to each individual node are either external or internal:

- **External node roles**: Nodes with an external node role have an external IP address configured and use their Eth2 port for communication with the customer's network.

The external node roles are:

- **Access**: For all application transactions. A node configured with the access role controls all input/output operations to and from the EMC Centera. The access node also serves as the staging area for all content that is archived and retrieved. The access nodes control all requests that come from application servers to store, retrieve, or dispose content.

- **Replication**: For all replication and restore traffic between clusters.

- **Management**: For all manageability connections to the cluster (CV, CLI, and Centera Console) and the E-mail Home, Syslog, and SNMP services.

- **Internal node roles**: Nodes with an internal node role do not allow for any communication with the customer network.

The internal node roles are:

- **Storage role**: The storage role is an internal node role. Nodes with the storage role store data. It is possible to combine the storage role with one or more external node roles (not on Gen2 nodes).

- **Spare nodes**: Nodes without any node role are spare nodes.

**Note: Additional information for spare nodes is available in the EMC Centera online help.**

It is recommended that a thorough assessment is done both of the cluster when deciding which nodes should be assigned which roles and of the traffic expectations. The access and replication roles require the most system resources to complete their tasks. It is recommended that newer hardware (Gen4 and Gen4LP, if available) be used for these roles. Management traffic requires far less system resources and can be assigned to older generations of hardware (Gen2 and Gen3).

Application failover

Application failover is affected by network segmentation. The EMC Centera SDK has internal capabilities to retrieve data from multiple EMC Centera systems. This is achieved by leveraging the replicated configuration on the EMC Centera. When the application interacts with EMC Centera, the replication settings are stored by the SDK for purposes of failover. If a primary EMC Centera in a traditional failover environment becomes unavailable, the application still has the capability to retrieve data from the replicated environment.

**Note: In a purely segregated environment of application and replication data traffic, built-in failover functionality will not function as expected. It is recommended that the access role is added to the nodes with replication role in the replica Centera.**

Compliance Mode

EMC Centera compliance models

EMC Centera offers three compliance models or editions: Basic, Governance Edition (GE), and Compliance Edition Plus (CE+).
Chapter 2 Implementation

Note: EMC Centera relies solely on the application to perform any disposition actions, as data will never be deleted automatically/proactively; depending on the compliance model, EMC Centera will prevent the deletion of data still under retention.

Basic model

In its Basic edition, EMC Centera delivers the full power of content addressed storage (CAS). Self-configuring, self-managing, and self-healing, it captures and preserves original content, protecting the context and structure of electronic records. However, data retention is not enforced and advanced features such as shredding and advanced retention management are not available. Data can be deleted at any time, provided the application has the appropriate access rights, regardless of the retention period initially set.

Governance Edition (GE) model

Governance Edition provides the retention capabilities required by organizations to responsibly manage electronic records, on top of the features provided by EMC Centera Basic. Deploying Governance Edition enforces organizational and application policies for information retention and disposition. Original content can be captured and preserved — and ensure complete, reliable integrity for the life of the archived information.

Compliance Edition Plus (CE+) model

Compliance Edition Plus exploits the core strengths of the EMC Centera platform while adding extensive compliance capabilities to the Governance Edition model. CE+ is designed to meet the requirements of the most stringent of regulated business environments for electronic storage media as established by regulations from the U.S. Securities and Exchange Commission (SEC), the Australian AS 3806 Compliance Programs, or other national and international regulatory groups.

Note: Upgrading from Basic to either the GE or CE+ compliance model will have an immediate effect on retention reinforcement for all legacy data already archived.

The following hierarchical retention period setting applies to each data object stored on EMC Centera:

- **Application setting**: The application can assign a fixed retention period or a retention class to the CDF during its creation. The application setting of the retention period overrules the pool and cluster retention setting. Note that a CDF can be deleted only if the retention class to which it is assigned to is defined on the cluster.

- **Pool setting**: If a CDF does not have a retention period or class assigned by the application, the default retention period of the pool applies to the CDF. The pool setting of the retention period overrules the cluster retention setting.

- **Cluster setting**: If the CDF does not have a retention period or class assigned by the application and if the pool has no default retention period, the default retention period of the cluster applies to the CDF.

RetentionPolicy

Retention periods

An EMC Centera retention period provides a simple mechanism for defining retention periods for items archived in Centera. Retention periods are fixed numeric values part of the metadata (CDF) that cannot be changed; if a new retention period is required, a new metadata file (CDF) must be created for that piece of content. The data will be eligible for deletion only after all retention periods associated to it have expired.
Retention classes

Retention classes provide a way to manage and change retention periods for a set of data objects. Contrary to fixed retention periods given by the application or the pool, the retention periods assigned to a retention class can be changed by the system administrator. A retention class exists as a symbolic representation of a retention period.

A retention class name—not the period itself—is associated with a CDF. A retention class acts as a retention policy that governs all CDFs cluster-wide for those CDFs assigned to that retention class. If the time period of a retention class is changed, it likewise immediately affects the retention period of all CDFs referring to that class, without changing the individual CDFs. EMC Centera supports up to 1,000 retention classes, which can be defined only via the CLI. The SDK allows the setting up and removal of retention class assignments on CDFs. A retention class period can be increased and decreased at GE and only increased at CE+

Note: Retention periods in EMC Centera are calculated from the date that the CDF was created (archival or creation date) and not from the item’s last modification date.

Enterprise Vault supports both EMC Centera retention periods and retention classes, referred to as retention categories. It is possible to establish Enterprise Vault’s retention behavior based on one of the following options:

♦ Only for the EMC Centera Compliance Edition Plus model: When selecting this option, Enterprise Vault sets a retention period on Centera Compliance Plus (CE+) models that corresponds to the Enterprise Vault retention period (defined in each item's retention category). On other EMC Centera models, Enterprise Vault sets a retention period of zero, which means that the items can be deleted immediately.

Note: If this option is set before the EMC Centera Compliance Edition Plus model is installed, Enterprise Vault begins setting the retention period only for all newly archived items that correspond to the Enterprise Vault retention period (all legacy data has a zero retention period).

♦ For all Centera models: When selecting this option, Enterprise Vault sets a retention period on all EMC Centera models that corresponds to the Enterprise Vault retention period (defined in each item's retention category).

♦ Never: Select this to make Enterprise Vault set a retention period of zero on all EMC Centera models (items can be deleted immediately).

When configuring retention policies in Enterprise Vault, it is recommended to follow the guidelines below, depending on the nature of the data to be archived:

♦ Retention classes: for any new data eligible for archival

♦ Retention periods: for any legacy or backlog data to be archived

Note: Enterprise Vault retention categories should be mapped to EMC Centera retention classes during the setting of the Vault Store retention policies.

It is the role of the application to set the retention periods that EMC Centera enforces, and to store, retrieve, and dispose of (delete) content as required. Once the retention period of a content object has expired, the application must dispose of the content by way of the Centera API; normal delete operations will fail on GE and CE+ models when attempting to dispose objects still under retention. A cluster will never proactively dispose of content managed by an application.

Although Enterprise Vault does not explicitly recommend data deletion for content still under retention (commonly known as privileged deletes), users with enough access rights are allowed to
Chapter 2 Implementation

Symantec Enterprise Vault and EMC Storage Applied Best Practices

perform such activities. For implementations where EMC Centera has been deployed using GE or CE+ compliance modes, these actions might result in warning or error messages reported in the Administration Console, as EMC Centera will deny such requests until the retention period is expired.

As Enterprise Vault does not leverage EMC Centera Privileged Deletes, when the delete request is submitted, Enterprise Vault will attempt and fail the delete operation, and the end user will be notified. However, if the Expiry Service attempted to delete the item, Enterprise Vault will try again the next time the service runs; this operation will be retried each time the Expiry Service runs until the retention period expires and Centera grants the delete request.

It is recommended to carefully review all business cases before defining Enterprise Vault retention policies and the roles/access rights that users will have, in order to prevent such temporary processing overheads and data inconsistencies. (For additional information, see the white paper *EMC Centera Compliance Models Governance Edition and Compliance Edition Plus*).

**EMC Celerra**

This section presents an overview of the features offered by EMC Celerra applicable to an environment where Enterprise Vault is to be deployed, and the recommendations to configure EMC Celerra to best perform in such setting.

The recommended EMC Celerra configuration for Enterprise Vault is listed in Table 8.

<table>
<thead>
<tr>
<th>Table 8</th>
<th>Recommended EMC Celerra configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature</td>
<td>Recommendation</td>
</tr>
<tr>
<td>Software</td>
<td>EMC Celerra Network Server version 5.6 or later</td>
</tr>
<tr>
<td>Hardware</td>
<td>Celerra Network Server with 510 or later model Data Movers having 3 GB RAM</td>
</tr>
<tr>
<td>Network</td>
<td>No specific network requirements</td>
</tr>
<tr>
<td>System resources</td>
<td>Sufficient Data Mover blockmap memory, system space, and disk storage must be available to support SnapSure operations.</td>
</tr>
</tbody>
</table>

To ensure that the tests suggested in this document can be executed, the following are required:

- A Celerra running version 5.6.43 or later of DART – This provides the FLR functionality.
- Celerra File-Level Retention documentation – “Using File-Level Retention on Celerra,” P/N 300-004-163, Version 5.6, available on EMC Powerlink and the Celerra user documentation CD.

**Celerra File-Level Retention**

This section provides an overview of Celerra File-Level Retention (FLR) and its features. Deployment considerations are also included for additional information on implementation.

To understand how Celerra FLR works, a retention policy for each file is simply controlled by an attribute. The attribute is an additional characteristic to the file. It lets the system know that the file is an FLR file. If the attribute shows that it is an FLR file, the metadata provides the associated data such as the retention period and the state (for example, not locked, locked,
append-only, or expired), which is necessary for the Data Mover to process the file. The FLR attribute protects the file, but the storage environment in which the file is stored plays an important role in determining the level of protection. If an administrator can manipulate the environment by changing the system clock or circumvent the protection by deleting the container (for example, file system) in which the file is stored to modify a locked file, the required protection solution is defeated.

Celerra FLR secures the environment in which FLR files are stored, and strengthens the integrity and protection of FLR files.

Celerra provides two FLR configurations to accommodate various business requirements: FLR-E (Enterprise) for basic retention capabilities and FLR-C (Compliance), for more robust and secured environments.

FLR-C protects data from changes made by users through NAS protocols such as CIFS, NFS, and FTP along with administrators’ actions, and it also meets the requirement of the SEC Rule 17a-4(f). FLR-C file system that has files in the locked state cannot be deleted.

Note: EMC engaged Cohasset Associates Inc., widely recognized as one of the foremost consulting firms that specialize in document-based information management, to validate that FLR-C meets the SEC rule 17a-4(f) requirements. A validation paper by Cohasset Associates that discusses Celerra FLR and the SEC rule 17a-4(f) requirements is available at http://Powerlink.EMC.com. For additional information on Cohasset Associates, visit their website at www.cohasset.com.

FLR-E protects data from changes made by users through NAS. However, a Celerra administrator with the appropriate authorization can delete an FLR-E file system even if it has protected files.

In both FLR-C and FLR-E file systems, files that are in the locked state cannot be modified or deleted. Additionally, the path to a file in the locked state is also protected from modification, which means that a directory on a FLR file system cannot be deleted or renamed if it contains protected files.

Functionalities part of FLR-C and FLR-E include:

♦ Protection of locked files in case of activity by malicious administrators. That is against regulatory policies.

♦ Logging of activities related to FLR.

♦ A new state called append-only that allows users to modify empty WORM files.

There are additional features on FLR-C to meet SEC compliance.

♦ Data verification

♦ Default "hard" infinite retention period
Table 9 shows the features that are available in both FLR-C and FLR-E file systems.

<table>
<thead>
<tr>
<th>Feature</th>
<th>FLR-C</th>
<th>FLR-E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tamper-proof Clock</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>File system protection</td>
<td>Cannot delete with protected files</td>
<td>Can delete with protected files</td>
</tr>
<tr>
<td>Data verification</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Default “hard” infinite retention</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Activity log</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Append-only files</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Detailed FLR feature review

This section describes the features implemented in Celerra FLR to meet data protection and auditing objectives, and regulatory requirements.

**Tamper-proof clock**

In the FLR options, Enterprise and Compliance, a software clock is used to track the retention period that is set. Thus, it addresses the issue of malicious administrators attempting to delete WORM content before its expiry date by tampering with the system clock.

The software clock mechanism implements a tamper-proof clock set once for each file system. The value of the FLR clock is initialized by synchronizing it with the current Data Mover system time when the FLR file system is first mounted. For a Data Mover that is upgrading to NAS code that supports this mechanism, the clocks for these FLR file systems are initialized with the system clock of the Data Mover, when the file systems are first mounted after the NAS code is upgraded.

The FLR clock has some flexibility for file system downtime, movement of file systems between Data Movers, and so on. The FLR clock is periodically stored in the file system. When an FLR file system is unmounted or mounted as read-only, the FLR clock does not advance. After the file system is remounted as read/write, the FLR clock continues to advance. This prevents locked files from being deleted prematurely though it would cause locked files to expire later than initially planned.

The FLR clock can adjust itself to changes in the Data Mover system clock. If the Data Mover clock is turned back such that the FLR clock is ahead of the system clock, the FLR clock resets back to the current time. If the Data Mover clock is ahead of the FLR clock, the FLR clock gradually adjusts to that change. The FLR clock is allowed to advance only 138 seconds per hour if it is behind the current value of the system clock. The FLR clock can catch up at the maximum of two weeks per year if necessary. This implementation is meant to prevent attacks by malicious administrators from deleting locked files early because the slow rate of change makes attacks of this nature impractical.

**Note:** FLR allows authorized administrators to restore from previous point-in-time views for FLR-E file systems. The FLR clock adjusts accordingly. Point-in-time restores are prohibited for FLR-C file systems.
Chapter 2 Implementation

File system protection

An authorized administrator could destroy protected content on an FLR file system at any time by deleting it or by restoring it to a previous point-in-time view or overwriting protected files.

To meet the SEC Rule 17a-4(f) requirement, FLR-C prohibits destructive operations to an FLR-C file system that contains protected files. If there are no protected files, the file system can be deleted.

FLR-E treats this scenario differently. Celerra alerts the administrator about the presence of protected content on the FLR-E file system. The system requires a confirmation from the administrator. Though this implementation prevents destructive actions against protected content at the file system level for FLR-C file systems, it does not protect committed content at the disk level. An authorized administrator can destroy the LUNs that the file system resides on by using management tools such as Unisphere and Unisphere CLI. However, referring to the SEC Rule 17a-4(f) ruling, the intent of the requirement is to prevent modification of individual records without trace or record. Celerra FLR-C meets this requirement because an administrator cannot target individual files for deletion.

Additionally, the Multi-Path File System (MPFS) and Parallel Network File System (pNFS) on an FLR-C file system cannot be enabled. This is to prohibit malicious MPFS clients from writing to the array.

Data verification

FLR-C includes an enhancement for write verification. SEC Rule 17a-4(f) requires that the storage system ensure the integrity of the stored data by reading back the data written to the file system. This data verification functionality is available only on FLR-C file systems.

If the data that is read back from the storage system does not match the data in memory, the Data Mover attempts to write and read back two more times. If a mismatch still occurs, the Data Mover logs a message in the Data Mover server log and generates an event on Celerra Manager to inform the administrator before panicking the Data Mover. This event is meant to explain the reason why the Data Mover panicked.

A server parameter controls the data verification feature. By default, data verification is disabled. Changes to the parameter take effect immediately without the need for a system reboot.

Default “hard” infinite retention period

When a file is committed to a locked state and the retention period is not defined, the file is given a “soft” infinite retention period. Therefore, the file is protected for an indefinite length of time. However, the file owner or administrator can change the retention period to an explicit time (less than infinite).

Based on the intent of the SEC 17a-4(f) ruling, it is prudent for files without a set expiry date to retain a permanent retention period.

FLR-C adheres to this ruling by issuing a “hard” infinite retention period for committed files with no explicit retention date and time set. The retention period is permanent and cannot be decreased.

FLR-E retains the “soft” infinite retention period in this scenario.
Activity log

Because an FLR file system is used in environments that are subject to strict law enforcements, both FLR-C and FLR-E record events of actions that pertain to successful changes or attempts to change protected data on the file system. The activity log records the user, time of event, and the type of action taken against FLR files.

The FLR log has a fixed naming convention, flr.log [timestamp], and is stored in the root directory of each FLR file system. The FLR log has a maximum size limit of 10 MB. Logs that meet the limit are converted to WORM files, and subsequent events are written to another file with the same naming convention. A converted log file is set with the longest retention period that exists for the files referred to in this particular FLR log.

The administrator is responsible for deleting old log files. If there is insufficient space in the file system to update the activity log, the operations are not allowed to proceed and warnings are logged in the Data Mover server log, the sys_log, and posted as an alert to the administrator.

The activity log captures the following events:

- Create append-only file
- Set file to a locked (WORM) state
- Extend retention period on a WORM or expired file
- Attempt to make a WORM or expired file writeable
- Delete or attempt deletion of a protected (WORM, expired, append-only) file

The following information accompanies a recorded event:

- Time of event (software clock maintained by the file system)
- Action (events described above)
- Inode number of the file
- Unique identifier (UID) or security identifier (SID) of the user who performed or attempted the action
- Event-specific information:
  - The retention date and time if a WORM file is committed
  - Success or failure if a WORM file is deleted or if there is an attempt to delete it

Append-only files

An append-only feature provides users the capability to append data to a WORM file without changing existing data. Some applications interpret appending a file as extending a new file to the desired size and then appending new data afterwards. To a file server, it is creating empty space on a file followed by modification of the empty space. This is not allowed.

Append-only is a new type of FLR file protection; it is a state that can be set only on an empty file in the locked state. An append-only file does not have a retention period, but it cannot be deleted. After modifying an append-only file, it can be converted back to a traditional WORM
file or can remain in an append-only state forever. Transitioning back to the locked state also requires a retention period either specifically set by the user or set to an infinite retention period. After data is written to an append-only file and converted back to a traditional WORM file, the file cannot be changed back to the append-only state.

Append-only files are supported in both FLR-C and FLR-E file systems.

**FLR states**

![FLR state diagram](image)

Figure 5  FLR state diagram

Figure 5 shows the four possible states in the FLR-C and FLR-E file systems — Locked, Not Locked, Append-only, and Expired.

<table>
<thead>
<tr>
<th>FLR File State</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Locked</td>
<td>All files start in the Not Locked file state. A Not Locked file is an uncommitted file that is treated as a regular file in a file system. In an FLR file system, the state of an uncommitted file can change to Locked or remain as Not Locked.</td>
</tr>
<tr>
<td>Locked</td>
<td>A Locked file has a set retention period that prevents users from modifying, deleting, renaming, or appending to a file. A Locked file remains in this state until the retention period expires. Locking a file also causes a bit in the inode to be flipped in the background. This is the indicator that a file is locked. When migrating read-only files from a non-FLR-enabled file system to a file system that has FLR enabled, the read-only files are not locked even though they are read-only. An administrator can perform two actions on a committed file: Increase the file retention date to extend the existing retention period. If the Locked file is initially empty, move the file to the Append-only state.</td>
</tr>
<tr>
<td>Append-Only</td>
<td>Existing data in an Append-only file cannot be deleted, renamed, and modified, but data can be added to it. The file can remain in the Append-only state forever. However, it can be transitioned to the Locked state by setting the file status to read-only with a retention period. An empty append-only file can be deleted.</td>
</tr>
<tr>
<td>Expired</td>
<td>When the retention period ends, the file transitions from the Locked to the Expired state. A file in the Expired state cannot be modified or renamed, but it can be deleted. An expired file can have its retention period extended such that the file transitions back to the Locked state. An empty expired file can also transition to the append-only state by first extending the retention period.</td>
</tr>
</tbody>
</table>
FLR Deployment considerations

- Non-FLR, FLR-C, and FLR-E file systems can exist on the same system.
- When creating the file system, the required FLR setting (Off, Enterprise or Compliance) must be selected. The setting cannot be changed after the file system is created.
- Celerra Data Deduplication can be enabled on an FLR-enabled file system. It does not affect the integrity of the data.
- FLR-E is intended for self-regulated archiving. FLR-C is intended to assist companies that have to comply with regulations such as the United States Securities and Exchange (SEC) ruling 17a-4.
- CAVA’s scan-on-first-read functionality does not detect a virus in a protected file. A subsequent scan of the file system is necessary to detect viruses on protected files.
- For Celerra Replicator (V1), a replication session cannot be created or restarted unless both the source and destination file systems have the FLR type set to either Off or Enterprise.
- Celerra Replicator (V1) cannot be used to replicate FLR-C file systems.
- For Celerra Replicator (V2):
  - A replication session or a copy of a session cannot be created unless both the source and destination file systems have the same FLR type. Also, when creating a file system replication, an FLR-C destination file system that contains protected files cannot be used.
  - A replication session cannot be started if an FLR-C destination file system contains protected files and updates have been made to the files in the destination file system.
  - A switched-over replication session cannot be started in the reverse direction when an FLR-C original source file system contains protected files and updates have been made to the original source since the switchover.
- It is possible to create a file system with FLR enabled as secondary storage for a FileMover environment. It is not possible to enable the FileMover functionality with an FLR-enabled file system as primary storage.
- Although FLR supports all backup functionality, the FLR attribute is not preserved in the NDMP backup. Therefore, the Celerra administrator must ensure that the file system is restored to a Celerra file system with FLR enabled. If a file is restored from an NDMP backup where the retention date has expired, the file has an infinite retention date after it is restored. To protect the file, without having an infinite retention date, restore the file to a non-FLR file system and then copy it back to an FLR file system.
- FLR cannot be enabled on the root file system of the nested mount.
- The FLR features of NFSv4 cannot be used to manage the FLR state of files in an FLR-enabled file system. NFSv4 clients must use the same mechanisms as NFSv3 clients.
- A writeable checkpoint of an FLR-C file system cannot be created. However, a writeable checkpoint of an FLR-E file system can be created.
- Upgrades from an FLR-E type file system to an FLR-C type file system cannot be done.
Upgrades from the old FLR-E type file system to the new FLR-E type file system can be done.

### Installation process

#### Licensing

Enterprise Vault uses the Enterprise Licensing System (ELS). To run the associated Enterprise Vault Services, a license key file that covers the Enterprise Vault features that the user wants to implement must be installed.

The following types of Enterprise Vault license are available:

- **Production license.** This license comprises a product base license and any additional feature licenses. When the license file is installed, the functionality of Enterprise Vault depends on the feature licenses that were purchased. Production licenses generally do not have an expiry date.

- **Trialware license.** With this 30-day license, the full functionality of Enterprise Vault is available, but the functionality is time-limited, as defined by the key. When the license expires, the software continues to run in restricted, read-only mode, which allows archived items to be viewed and retrieved, but no items can be archived. Enterprise Vault tasks will not start, and the contents of personal folder (PST) files cannot be migrated to Enterprise Vault.

- **Temporary licenses.** Temporary licenses are available for 10-day to 90-day duration.

When the license expires, the software continues to run in restricted, read-only mode, which allows archived items to be viewed and retrieved, but no items can be archived. Enterprise Vault tasks will not start, and the contents of PST files cannot be migrated to Enterprise Vault. For additional information, see the [Symantec Enterprise Vault 9.0 - Installing and Configuring Guide](#).

### Installing Enterprise Vault

The following are the steps needed to install the required Enterprise Vault components:

1. Log in to the Vault Service account to install Enterprise Vault.
2. Load the Enterprise Vault media.
3. Open the Symantec Enterprise Vault 9.0 folder.
4. Double-click the ReadMeFirst file to display the ReadMe text and read it before continuing with the installation.
5. Open the Server folder.
6. Double-click SETUP.EXE to start the installation.
7. Install the required Enterprise Vault components for this computer.

The core components for an Enterprise Vault server are as follows:

- Enterprise Vault Services - Installs the entire core Enterprise Vault Services. After the installation, the services must be configured before using them. This is done when the Enterprise Vault configuration wizard is run. (Additional information is available in the “About configuring Enterprise Vault” section of the [Symantec Enterprise Vault 9.0 - Installing and Configuring Guide](#).)
Chapter 2 Implementation

Symantec Enterprise Vault and EMC Storage Applied Best Practices

69

- Administration Console - Installs the Administration Console. This is a snap-in to the Microsoft Management Console (MMC) that enables the user to manage Enterprise Vault.

This component also installs the Enterprise Vault configuration wizard, PST Migrator, and NSF Migrator wizards.

To install a standalone Administration Console on a remote system, select this component only.

A number of other components can be installed as required, if their prerequisites are met. Some of these components are listed only if certain software is present:

- SMTP Archiving Components, Exchange Server Extensions, and Microsoft SharePoint components are usually installed on computers other than the Enterprise Vault server. For details, see the appropriate section of the Symantec Enterprise Vault 9.0 - Installing and Configuring Guide

- Enterprise Vault Operations Manager must be installed on at least one Enterprise Vault server if the desire is to use it to monitor the Enterprise Vault servers at that site.

- Enterprise Vault Reporting is listed for selection only if Microsoft SQL Server Reporting Services (SSRS) are installed on the computer. Enterprise Vault Reporting can be installed on an Enterprise Vault server, but is more typically installed on a separate server running SSRS.

8. At the end of installation, a computer restart might be required.

Post-installation tasks

Default security for the Web Access application

The default security settings for the Web Access application configure automatically, during the Enterprise Vault installation, and set access to the Web Access application using HTTP over TCP port 80; both Basic authentication and Integrated Windows authentication are configured automatically.

These settings affect the way users log in to the Web Access application, as follows:

- For Internet browsers supporting Integrated Windows Authentication (for example, Internet Explorer)

  The user must supply the domain name and username separately:

  - Username: username
  - Password: password
  - Domain: domain (This domain can never be defaulted)

Note: An Internet Explorer user with suitably customized browser settings does not need to supply login details manually because the login is automatic; Internet Explorer automatically uses the details of the account to which the user is currently logged in.

See —Customizing security on the client computers” in the Symantec Enterprise Vault 9.0 - Installing and Configuring Guide

- For Internet browsers that do not support Integrated Windows Authentication the user must supply both the domain name and username in response to a single username prompt:
Chapter 2 Implementation

- Username: domain\username
- Password: password

It is possible to set up a default domain. See the *Symantec Enterprise Vault 9.0 - Installing and Configuring Guide* in the section “Customizing authentication and Customizing security for Web Access.”

**Note:** If a message was received during the installation saying that setup could not set alias security, please refer to the *Symantec Enterprise Vault 9.0 - Installing and Configuring Guide* “Setting up the default authentication” section, for detailed instructions on how to perform the default authentication.

Customizing security for the Web Access application

In addition to customizing the amount of information that users need to provide when logging in to the Web Access application, it is also possible to change the port or protocol that is used to access the Web Access application, if for instance it is required that connections to the application be made using HTTPS.

The *Symantec Enterprise Vault 9.0 - Installing and Configuring Guide* has additional information on how to perform these activities.

Customizing security on the client computers

It is possible to configure Internet Explorer on user computers so that users are automatically logged in to the Web Access application, without receiving a login prompt. Essentially, Internet Explorer must be configured so that it trusts the Web Access application computer.

For this to work, the Integrated Windows Authentication is a requirement, as described in “Setting up the default authentication” in the *Symantec Enterprise Vault 9.0 - Installing and Configuring Guide*.

To make Internet Explorer log in automatically, it may be required to modify the Internet Explorer Internet Options on each client computer. As the settings are saved in the Windows registry, it is possible to save them for en-mass rollout purposes.

Out of the many ways available to configure Internet Explorer security, the methods listed are detailed in the *Symantec Enterprise Vault 9.0 - Installing and Configuring Guide*

- Using the proxy bypass list
- Explicitly naming the Web Access application computer

**Configuring Enterprise Vault**

The Enterprise Vault configuration wizard can be executed either immediately after installation (after restarting the computer if prompted), or after performing the post-installation tasks for the Web Access application, as described in the previous section.

Note the following:

- If the configuration wizard is run immediately after the installation, remember that there are some additional tasks that need to be done before users can use Enterprise Vault.
If the user exits from the configuration wizard before configuration is complete, the configuration wizard can be run again and have the option to delete the Directory database. Once the configuration wizard has been successfully completed, it cannot be run again on the same computer.

Using the Enterprise Vault configuration wizard it is possible to:

* Select which SQL server to use for the Enterprise Vault Directory database
* Create the Enterprise Vault Directory database (*)
* Create the Enterprise Vault Monitoring database
* Create an Enterprise Vault Site (*)
* Add the computer to the site (*)
* Select the Enterprise Vault Services that are desired to run on the computer
* Choose the storage areas to use for Enterprise Vault data

Note: Tasks identified with (*) can only be performed using the configuration wizard; however, other tasks such as adding a service or assigning storage areas for the data can also be done using the Enterprise Vault Administration Console.

The main activities during the configuration process are:

* Registering the Enterprise Vault Service account on the local computer
* Creating the Directory Database (for the first Enterprise Vault server only)
* Creating the Enterprise Vault Site and registering the local computer
* Selecting the Enterprise Vault Services to be added to the computer
* Defining the storage locations for the Indexing and Shopping Services
* Configuring the Service mailbox
* Starting the selected services on the local computer
* (Optional) Launching the Getting Started wizard or the Vault Administration Console (VAC) to set up archiving.

Note: These instructions apply to a non-clustered environment. If Enterprise Vault is being configured in a Veritas Cluster Server or Microsoft Server Cluster environment, see the appropriate clustering section in the Symantec Enterprise Vault 9.0 - Installing and Configuring Guide.

Complete details on the Configuration wizard are available in the Symantec Enterprise Vault 9.0 - Installing and Configuring Guide and a summary of these tasks is presented elsewhere in this document.
The configuration wizard may be launched after completing the Installation Program or after restarting the computer, if it was initially required.

The first task to be executed is to register the Enterprise Vault Service account to the Local Administrators Group with the following advance User Rights:

- Log On As a Service and Act as Part of the Operating System
- Debug programs
- Replace a process-level token

When running the configuration wizard on the site’s first Enterprise Vault server, a Directory database will be created on the specified SQL server (or instance); the location of the SQL server, as well as the path for the transaction log and database files, can be specified/modified at this time.

With the Directory database created, the configuration wizard will then create an Enterprise Vault Site and will add the local computer to the site using an unqualified DNS alias, as fully-qualified DNS aliases are not recommended.

Once the Enterprise Vault Services to be executed in the computer are selected and added to the computer, the default storage locations for the Indexing and Storage Services are defined; it is recommended to ensure that these locations are on an accessible device and the Enterprise Vault Service account has Write access to them. For Exchange archiving, special attention must be placed to these locations as they cannot be easily modified after they have been enabled. Before mailboxes are enabled, the Administration Console can be used to change the index storage location, or add further locations. Then, the Service mailbox is configured, the selected services are started and their status are presented; selecting Next on the configuration wizard will refresh the status, until all of them are successfully started. It is recommended to check the licenses keys to ensure the selected services are properly licensed.

The final screen of the wizard presents the following options:

- Run the Enterprise Vault Getting Started wizard - It is recommended to select this option, as it allows setting up archiving as quickly as possible. The wizard provides both express and custom options for maximum flexibility (for additional information, see Setting up archiving).
- Run the Enterprise Vault Administration Console - This option is only recommended for users already familiar with the Administration Console and familiar with setting up archiving.
- Just close the wizard - This option will close the Configuration wizard. Access to the Enterprise Vault Getting Started wizard or the Administration Console is available via the Enterprise Vault Start menu options.

It is also recommended to refer to the Enterprise Vault online help when using the configuration wizard to configure Enterprise Vault on subsequent computers.

Setting up archiving

The Configuring Enterprise Vault and EMC Centera for Email Archiving and Configuring Enterprise Vault and EMC Celerra for File System Archiving chapters provide detailed
information on how to configure and fine-tune the application for these particular devices. Performing a validation immediately after will ensure the environment is up and ready.

**Installation validation**

Once Enterprise Vault has been configured, it is recommended to validate that all settings and configurations initially planned have been taken into consideration. The following are the Enterprise Vault and EMC Centera tools and procedures that are available.

**Enterprise Vault**

Enterprise Vault Deployment Scanner reviews the configuration of a computer and reports on any issues that may stop Enterprise Vault from running on it. In particular, the test named **EMC Centera Connectivity** checks the connectivity to EMC Centera access nodes.

To run Enterprise Vault Deployment Scanner, the following steps must be performed:

1. Log in using the Vault Service account.
2. Use one of the following methods to start Deployment Scanner:
   - On the Windows Start menu, click All Programs > Enterprise Vault > Deployment Scanner.
   - On the Tools menu of the Vault Administration Console, ensure that **Advanced Features** is selected. Then, in the left pane of the Vault Administration Console, right-click the Enterprise Vault server and click **Deployment Scanner**.
3. In the Welcome page, select **Do not set configuration options for Deployment Scanner** if the Deployment Scanner was previously run and you want to rerun it without entering the configuration options again.
4. Click Next and then, if **Do not set configuration options for Deployment Scanner** was selected, go to step 6. Otherwise, complete the fields in the two Server Configuration pages.

   Identify the machines on which SQL Server has been installed. Enterprise Vault uses SQL Server to store configuration data and information about the archives.

   If the default database instance is not being used on SQL Server, the instance name must also be entered here, in addition to the name of the database server, in the format `sql_server\database_instance`. An example is `sql\vault`. The SQL server(s) identify the Microsoft Exchange servers from which the user wants to archive the items in user mailboxes, journal mailboxes, or public folders.

   - **Microsoft Exchange Server(s)** - Specify the addresses of the Microsoft SharePoint servers that hold the documents to be archived.
   - **Microsoft SharePoint Server(s)** - Identify the file servers that contain files for archiving.
   - **File Server(s)** - Specify the paths to the network shares that contain files for archiving.
   - **File Share(s)** - Specify the IP addresses of access nodes in an EMC Centera cluster.
   - **EMC Centera Access Node(s)** - Specify the IP addresses of access nodes in an EMC Centera cluster.

   In each case, a new item can be added by typing its name or address and then clicking Add. To remove an item from a list, click it and then click Remove.
5. When all the options have been set, click Next to proceed with the tests.
6. Wait a few moments for the utility to perform the tests and display the results.
7. Click the blue links to display more information on each test result. As well as displaying the test results on-screen, Enterprise Vault Deployment Scanner saves the report to an HTML file in the Reports subfolder. The name of the report file identifies the date and time at which it was created.
8. Click Finish to exit the Enterprise Vault Deployment Scanner.

EMC Centera

The EMC Technical Solutions Test and Acceptance procedure is performed against the EMC Centera to ensure all configuration parameters are configured and functioning properly. The test and acceptance procedure validates:

- The application can make a successful connection to the virtual pool.
- Retention is set properly by viewing the metadata of a file written by the application.
- EMC and the administrators are receiving daily health reports, alerts, and SNMP traps.
- External network ports on EMC Centera are negotiating correctly.
- Replication is working by testing it with JCentverify.

EMC Celerra

Besides the EMC Technical Solutions Test and Acceptance procedure, there are several test cases specific to FLR that might be tested to ensure proper configuration. Verifying FLR is enabled would allow for further testing on the following capabilities, which Enterprise Vault has already qualified for:

- Apply retention (finite and infinite)
- Manage append-only files
- Identify lock (retained) and expired files
- Delete expired files
- Gracefully handle the inability to modify retained files and associated folders
This chapter presents these topics:

- EMC Centera configuration ................................................................. 76
- Enterprise Vault and Centera configuration ........................................ 77
- NTFS to EMC Centera migrations ....................................................... 97
Up to this point, all information provided in this document has been generic to the installation and configuration of Enterprise Vault. It is here when the best practices for archiving to EMC Centera come into play, as the storage device is selected while setting up archiving.

**EMC Centera configuration**

Prior to performing the Enterprise Vault archiving setup, EMC Centera is expected to be fully configured; in order to ensure Enterprise Vault access to Centera, at the end of this process, the following items must be available to the Enterprise Vault system administrator:

- Generated PEA file
- Source (primary) Centera access node(s) IP address(es)
- If replication is enabled on a network segmented environment, target (replica) Centera access node(s) IP address(es)
- Name of default Centera retention class (optional)

**Note:** If replication is enabled on an environment being replicated without leveraging Centera network segmentation capabilities, the IP addresses of the replica cluster are not required.

The main activities during the Centera configuration process are:

- Setting the initial configuration according to the EMC Change Control Request Form (CCRF) (factory defaults CPM and SSP recommended)
- Creating the Enterprise Vault application pool
- Creating the Enterprise Vault application profile
- (Optional) Setting IP restrictions on the application profile
- Generating the associated PEA file on the primary Centera cluster
- Creating the default retention class
- Setting up replication
- Generating the associated PEA file on the replica Centera cluster
- Merging primary and replica PEA files

Complete details on these procedures are available in the EMC Centera online help, and all of them are performed by certified EMC Implementation Specialists using the Centera Viewer / Command Line Interface (CV/CLI).

The first task to be executed is the configuration of the cluster according to the guidelines laid out on the CCRF; the particular importance are the settings for Content Protection, which should be set to Mirroring (CPM) and the Storage Strategy, to be set to Performance Full (SSP).

When creating the application pool, the **Write, Read, Delete**, and **Exist** capabilities must be defined as the Pool Mask; any rights omitted will deny that particular capability. Any requirements for pool quota management are specified at this time.
Next, an application profile with Data Access Capabilities must be created, having the application pool created as the home pool. Answering "Yes" when prompted to establish a Pool Entry Authorization will allow the definition of the location of the PEA file in the local machine where the CV/CLI utility is installed.

**Note:** This location is temporary and only used to generate the file; once created, the file must be located on a shared path accessible to the Enterprise Vault Storage Service. Generation of the PEA file is possible at any other time by use of the “update profile” CLI command.

Optionally, IP restrictions on the profile to only allow the application and the management servers access to the pool can be specified.

To finish the setup on the primary cluster, the creation of the necessary retention classes is performed. An EMC Centera retention class must be created to be used as a default, and should mirror the retention policy of the Enterprise Vault default retention category.

**Note:** For security reasons, retention classes in EMC Centera can only be created by an EMC Centera system administrator; it is recommended that mapping and consistency between Centera retention classes and Enterprise Vault retention categories are ensured by the appropriate system administrators.

**Note:** New retention classes can be defined at any time, based on business requirements. Updates to existing retention classes are possible, depending on the Centera Compliance mode in use.

If replication is being leveraged for disaster recovery and high availability purposes, the pool and profile configurations must be exported from the primary EMC Centera cluster and imported into the replica cluster; similarly, all retention categories must be created. If network segmentation has been implemented, the Access Role must be added to the nodes with the Replication Role on the target cluster.

Once the replica cluster is set up, its PEA file must be generated, and both PEA files are merged into a unique file to be used for any and all connection purposes. Detailed information on merging PEA files is available in the EMC Centera online help.

**Enterprise Vault and Centera configuration**

**Note:** Prior to setting archiving, access to the Centera PEA file, and the IP addresses of the access nodes on the primary and replica addresses (if replication is enabled), is required. See *EMC Centera configuration* for additional information.

Although archiving can be manually set up using the Vault Administration Console (VAC), it is recommended to use the Getting Started wizard in order to set up archiving as quickly as possible.

The wizard can be executed immediately after the Configuration wizard as part of a new Enterprise Vault deployment, or from the Enterprise Vault Start menu options. The Getting Started wizard cannot be executed in the same computer once it has successfully finished; however, it can be used on other computers in the site, or restarted in the same computer if it was interrupted before the end.

The Enterprise Vault Getting Started wizard assists in the following tasks, as appropriate:

- Set up storage locations
- Create retention categories
- Create archiving policies for Exchange Server, Domino, and File System Archiving
It is possible to run sections of the wizard in express mode or in custom mode, as follows:

- In express mode, the wizard does not ask many questions. Instead, it applies as many default settings as possible. Later, the Administration Console can be used to make changes to the settings, if required.

- In custom mode, the wizard provides the flexibility to change the default settings.

Note: It is required to run the wizard in custom mode for the storage configuration section in order to configure EMC Centera as the remote storage location – which by default is set to a local NTFS volume that cannot be modified after the fact – for the Vault Store Partition’s Device type (EMC Centera).

It is required that the Enterprise Vault license keys be installed as the Getting Started wizard checks them to determine which options to present. It is recommended to run the Enterprise Vault Deployment Scanner to determine whether the Enterprise Vault prerequisite configuration is correct.

Additional information is available in the Symantec Enterprise Vault 9.0 - Deployment Scanner Guide in the Documentation folder of the Enterprise Vault media.

Storage configuration

Storage in Enterprise Vault is logically allocated to each Vault Store Partition; a Vault Store Partition is part of the Site hierarchy, set as the lower level within the Vault Store Group/Vault Store branch. For EMC Centera, the Getting Started wizard will set up the Enterprise Vault components listed in the next table.

Note: Refer to the “Planning for the Getting Started Wizard” chapter in the Symantec Enterprise Vault 9.0 - Installing and Configuring Guide for a complete planning sheet listing the Getting Started wizard’s Express-mode choices:
### Table 11 Enterprise Vault components – Summary of recommended values for EMC Centera devices

<table>
<thead>
<tr>
<th>Component</th>
<th>Item</th>
<th>Recommended EMC Centera value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vault Store Group</strong></td>
<td>Not Applicable</td>
<td>Although the creation of a Vault Store Group and a Fingerprint database is required for Enterprise Vault 9.0, if only EMC Centera partitions are used, none of the settings on the Vault Store Group are relevant; therefore, all values can be left at their default, for example, Sharing. The Fingerprint database is created but not used; no special care needs to be taken when deciding where to place the database and log files on disk.</td>
</tr>
<tr>
<td><strong>Vault Store</strong></td>
<td>Sharing</td>
<td>Not applicable. For EMC Centera the setting is defined at the Vault Store Partition level.</td>
</tr>
<tr>
<td><strong>Vault Store Partition</strong></td>
<td>Remove Safety Copy</td>
<td>After backup</td>
</tr>
<tr>
<td><strong>Vault Store Partition</strong></td>
<td>Storage Type</td>
<td>EMC Centera</td>
</tr>
<tr>
<td><strong>Vault Store Partition</strong></td>
<td>Access Nodes Addresses</td>
<td>The network fixed IP addresses assigned to the EMC Centera access nodes</td>
</tr>
<tr>
<td><strong>Vault Store Partition</strong></td>
<td>Sharing</td>
<td>“Enable device-level sharing” ON</td>
</tr>
<tr>
<td><strong>Vault Store Partition</strong></td>
<td>Retention Period</td>
<td>For all EMC Centera models</td>
</tr>
<tr>
<td><strong>Vault Store Partition</strong></td>
<td>Check Centera Replication (interval)</td>
<td>60 minutes</td>
</tr>
<tr>
<td><strong>Vault Store Partition</strong></td>
<td>Enable collections</td>
<td>“Enable collections” ON</td>
</tr>
<tr>
<td><strong>Vault Store Partition</strong></td>
<td>Location for Temporary Files</td>
<td>For collections, the temporary location where the collections will be created (at least 1% of estimated Centera capacity; 50 GB recommended)</td>
</tr>
<tr>
<td><strong>Vault Store Partition</strong></td>
<td>Security ACLs</td>
<td>Checked</td>
</tr>
</tbody>
</table>

**Note:** The wizard will first go through the process of creating a Vault Store Group, as a requirement for Enterprise Vault 9.0, although it is not relevant when EMC Centera is the only type of partition used. Similarly, when creating a new Vault Store, the Sharing tab is not relevant and is ignored for Centera partitions, as this will be defined at the Vault Store Partition level instead.

**Remove safety copy**

Enterprise Vault can be configured to retain archived items until the Vault Store partition in which they are archived has been backed up. During the time between archiving and removal, the original items are treated as safety copies by Enterprise Vault.

This feature favors compliance requirements around the need for keeping two copies of the same content available at all times; similarly, this could be leveraged during disaster recovery procedures.

When the Vault Store partition has been backed up, Enterprise Vault can remove the safety copies. It also creates shortcuts and placeholders at this time if it is configured to do so. See the “Managing Safety Copies” section in the “Day-to-day Administration” chapter of the *Symantec Enterprise Vault 9.0 - Administrators Guide* for additional information.

When deployed on an EMC Centera replicated environment, Enterprise Vault’s archived data is replicated instead of backed up, significantly reducing the backup window requirements, as well as providing for a high availability environment.
It is recommended to set the removal of the safety copies **After backup**, so that Enterprise Vault ensures the existence of the replicated data before removing the safety copies from primary storage (for example, MS Exchange) (see Figure 6).

![New Vault Store](image)

*Figure 6  Setting up removal of safety copies during vault store creation*
The removal of safety copies can also be configured, using the Vault Store Properties page (see Figure 7).

To configure the removal of safety copies for an existing Vault Store, go to the General tab of the Vault Store Properties page, and choose the **After backup** option.

**Note:** For fine-tuning purposes, the Remove Safety Copies option could be set to After Backup (Immediate for Journaling); for journaling, this means that the existence of the items in the replica Centera is not verified, to save on the performance hit in EV of post-processing the items.

---

**Figure 7** Setting up removal of safety copies for an existing Vault Store
Storage type

The wizard will then go through the process of creating a partition. Selecting EMC Centera as the storage type will start a configuration path different from other partition types (Figure 8).

Figure 8 Selecting EMC Centera as the storage type

Note: Additional information regarding Symantec’s compatibility and support for EMC Centera and other devices can be found on the Symantec Enterprise Vault Compatibility Charts.
Access node addresses

Next, access node IP addresses are entered (Figure 9) by clicking **Add** to add a new IP address, until all access node (AN) IP addresses are registered (see Figure 10).

Figure 9  Entering the EMC Centera access node (AN) IP addresses

Note: Optionally, defining a DNS Name for each access node will help minimize any impact related to future infrastructure network changes on Enterprise Vault’s access to EMC Centera.
Sharing

EMC Centera single instancing (SiS) is enabled when setting the Enterprise Vault sharing feature by selecting the **Enable device-level sharing** checkbox (Figure 11).

![New Partition]

**Figure 11  Enabling Centera SiS on the Enterprise Vault partition**

The way that items are shared or single-instanced with EMC Centera differs from other devices. On EMC Centera, attachments are detached from the message and stored in Centera, where Centera identifies them as candidates for sharing. The rules are as follows:

- A saveset with an uncompressed size of 100 KB is stored unshared.
- A saveset with a compressed size of over 100 KB is examined for "streams"—indexable items or XML streams such as recipient lists—and attachments.

**Note:** In EV 8.0 and later the single “Indexable item” stream has been replaced with one or more “Convertible Content” streams.

- If there are no streams or attachments, the saveset is stored unshared.
- If there are no streams or attachments with an uncompressed size of over 50 KB, the saveset is stored unshared.
- Any stream or attachment with an uncompressed size of over 50 KB is stored separately and is eligible for sharing.

This model has the advantage that attachments are shared even if they are attached to different messages or archived separately by File System Archiving. It also means that there is sharing across Vault Stores. Small messages are not shared. However, even though small messages make
up the bulk of messages, messages with large shareable attachments usually make up the bulk of the size. For example, a large report might be sent or forwarded to all members of a company. Just one copy of this report is held on EMC Centera, although there will be many copies held on the Exchange Stores or Lotus mail files in the company.

Enterprise Vault can optimize the use of storage space by storing a single instance of items that have copies in multiple places; for example, a large PowerPoint presentation sent to multiple recipients. To enable single-instance storage, **Enable device-level sharing** must be enabled on the partition properties; this will ensure that EMC Centera single instancing is possible for multiple Vault Stores, Vault Store Groups, and even Vault Sites.

It is also possible to enable device-level sharing from the General tab of the partition properties (Figure 12).

![Figure 12](image.png)

**Figure 12** Setting up single instancing (sharing)

The Vault Store Partition Properties dialog box is displayed for the partition clicked. The General tab allows the user to turn on sharing and set the state of the partition.

**Note:** Enabling Enterprise Vault device-level sharing is how attachments are written as single-instanced BLOBs on EMC Centera. Failure to select this option will result in no SiS savings from EMC Centera.

**Note:** It is recommended to always have this checked in order to achieve EMC Centera SiS.
Chapter 3 Configuring Enterprise Vault and EMC Centera for Email Archiving

Note: For storage other than EMC Centera, Enterprise Vault SISO capabilities must be carefully assessed as there are additional considerations on network traffic and extra complexity to the solution, such as fingerprint databases, policies, and limitations on data moves/migrations. See “Developing a suitable sharing regime” in the *Symantec Enterprise Vault 9.0 - Installing and Configuring Guide*.

Note: Partitions for EMC Centera do not take part in Enterprise Vault single-instance storage sharing. If a partition is created for EMC Centera in a Vault Store that is configured for sharing, the partition is ignored for the purposes of Enterprise Vault single-instance storage sharing.

RetentionPolicy

To determine how the Enterprise Vault retention policy settings should be reflected in EMC Centera, the wizard (Figure 13) presents three alternatives (see the Compliance Mode section). To have the system apply, at minimum, the default Enterprise Vault retention period for all data archived to EMC Centera, select the **For all Centera models** option.

![New Partition](image)

**Figure 13** Setting retention policies from Enterprise Vault to EMC Centera

Symantec Enterprise Vault and EMC Storage Applied Best Practices
Check EMC Centera Replication

Setting up how often replication is checked (see Figure 14) supplements the Safety Copy configuration defined at the Vault Store level. This step is performed to determine the maximum time elapsed before verifying they have been replicated to the secondary Centera and thus becoming eligible for deletion from the Exchange server. It is recommended to take the default 60 minutes value as a fair compromise/balance between application performance and disaster recovery capabilities.

![New Partition](image)

Enterprise Vault checks that Centera partition replication has taken place, when the vault store is taken out of backup mode, and when the storage service starts. Click Help for more information.

Additionally you can set a partition scan interval to check for replication, if required.

- **Scan partition every** : 60 minutes

---

**Figure 14** Defining EMC Centera Replication’s partition scan intervals
Enable collections

Enable collection is the recommended value; the wizard will also prompt for the location of the staging area used to create/host the containers prior to sending to EMC Centera for archival (see Figure 15).

**Figure 15 Setting up EMC Centera collections**

Enterprise Vault offers two methods of storing items in EMC Centera — with collections and without collections. EMC Centera collections are completely different from NT File System (NTFS) collections that can be used when storing to NTFS storage.

With collections, items are first archived to a local staging area. Another Enterprise Vault process collects files in this area and stores them on EMC Centera. There is some extra processing involved and CPU usage increases on the Enterprise Vault server. Despite this, similar archiving rates are usually achieved as when collections are turned off and there is no difference in retrieval rates.

A collection is up to 100 items or 10 MB of data. Collections are recommended because they result in fewer objects on EMC Centera. This has several advantages:

- No fall-off in performance as the EMC Centera gets fuller
- Fewer resources are used on the EMC Centera, allowing an overall greater throughput
- Faster replication
- Faster deletion of expired items
Chapter 3 Configuring Enterprise Vault and EMC Centera for Email Archiving

- Faster self-healing in the event of a failed disk
- Very fast retrieval of items because only the item is retrieved from EMC Centera and not the whole collection (Centera partial read)
- No impact on EMC Centera single instancing abilities

Additional information is available in the *Symantec Enterprise Vault 9.0 Performance Guide*.

**Note:** It is possible to see the collection configuration for existing Centera Vault Store Partitions, by selecting the Collection tab on the Properties dialog box (see Figure 16).

---

**Figure 16**  Enabling EMC Centera collections on an existing Vault Store partition

Collections and single instancing

Collections and single-instance storage are handled differently on EMC Centera devices:

- Temporary saveset files are used instead of CAB files (used for other storage platforms).
- Files are collected as soon as they are archived (not according to a schedule).
Note: If Enterprise Vault Sharing (collections) is enabled, EMC Centera single-instancing capabilities are not impacted.

When EV creates a collection, one data BLOB contains multiple objects. For each object an Attributes Tag and one or more Tags with data BLOBs for the separately stored Indexable Item Stream, XML Stream, and Attachments are created.

Note: In EV 8.0 and later the single “Indexable item” stream has been replaced with one or more “Convertible Content” streams.

These data BLOBs are capable of being shared and all other data BLOBs contain single attachments (or other streams) so that the attachments or streams can be shared (single instanced).

Note: Although archiving without collections is not recommended, if it has been decided to archive without using collections, then the number of processes writing to EMC Centera must be increased. Writes to EMC Centera take longer than to other devices, but many writes can take place in parallel.

Examples of increasing the number of processes are:

♦ To increase the number of Storage Archive processes, for Exchange Server mailbox and Exchange Server journal mailbox archiving, change the number of Archive Processes. Do this in the Administration Console by editing the properties of the Enterprise Vault Storage Service. Increase the number of Archive Processes to 10.

♦ To increase the number of Domino threads, from the Administration console, edit the properties of the Lotus Domino Task. Increase the number of concurrent connections to the Domino Server to 15.

♦ For File System Archiving and SharePoint the number of threads writing to EMC Centera should be 10. Change the value, if necessary, by editing the configuration files. There are examples of configuration files in the Enterprise Vault program folder, usually C:\Program Files\Enterprise Vault. These files are:

   • Example EvFileArcSvr.exe.config
   • Example EvSharePointArchiveTask.exe.config

♦ To change the number of threads, rename the file so that the name does not begin with Example, then edit the file, changing the value of NoItemProcessorThreads to 10.

   • Find the following line: <add key="NoItemProcessorThreads" value = "10"/>

   • Change the number to the new value as required.

Note: For additional information, see the “Threading” section.

Location of temporary files

Items for collection are stored on a local disk before they are archived to EMC Centera. This needs to be a fast disk but not large (See Other Enterprise Vault storage requirements.)

The temporary folder is where the collections are to be temporarily staged.
Security ACLs

It is recommended to use access control lists (ACLs) to further secure access to the collections.

Exchange Server archiving policies

When configuring Exchange Server targets, the Getting Started wizard searches the network for instances of Exchange Server. It is possible to select the Exchange Server computers for which archiving are to be configured.

For the selected Exchange Server the following must be determined:

- Specify whether to configure mailbox archiving or journal archiving, or both.
- For mailbox archiving, a system mailbox on that server that Enterprise Vault can use to log in must be specified.
- For journal archiving, the journal mailboxes to archive and the journal archive to use for each mailbox must be specified.

The wizard enables the creation of new archives, if required.

The wizard will set up the Enterprise Vault components. Table 12 lists the items related to EMC Centera.

<table>
<thead>
<tr>
<th>Table 12</th>
<th>Recommended default retention category for EMC Centera</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>Item</td>
</tr>
<tr>
<td>Exchange Provisioning Group</td>
<td>Default retention category</td>
</tr>
</tbody>
</table>

BEST PRACTICE: It is recommended to create an EMC Centera retention class to map the Enterprise Vault default retention category.

If Enterprise Vault is configured to archive from the Exchange managed folders, it can automatically synchronize managed content settings to managed folder retention categories. Enterprise Vault creates managed folder retention categories automatically. For more information, see the Symantec Enterprise Vault 9.0 - Administrators Guide
When setting the retention policies, the user is required to associate the Enterprise Vault retention categories to the EMC Centera retention classes (Figure 17).

![Retention Category Properties - Default Retention Category](image)

**Figure 17**  Associating Enterprise Vault Retention Categories and EMC Centera Retention Classes

**Policy definition**

A policy defines which documents are to be archived and how they are to be archived.

Enterprise Vault creates policies automatically. The Getting Started wizard uses the default Enterprise Vault policies. The default policies in Express mode and Custom mode are the same and, if required, can be modified at a later time, using the Administration Console.

**Custom configuration of Enterprise Vault and EMC Centera best practices**

Once the Getting Started wizard has finished, there are still some particular settings pending configuration.

**EMC Centera connection string**

EMC Centera Application Authentication is the process whereby an application (in this case Enterprise Vault) has to provide authentication information to EMC Centera before access is granted. The connection string is a parameter that is used by applications when they connect and
authenticate to a cluster. In its most basic form, it consists of a number of IP addresses all belonging to the same cluster plus credential information.

Although one IP address will be enough for the SDK to discover all available IP addresses in the primary and replica clusters, it is recommended to provide the IP addresses of all access nodes in the primary cluster to ensure that a connection can be made even if some access nodes are not available (offline). The credential information is contained in the PEA file.

**Note:** The Enterprise Vault VAC does not require that the IP addresses of the replica Centera are entered; these are always obtained from the primary Centera.

Additional information on connection strings, authentication, and probing mechanisms is available in the EMC Centera online help, the *EMC Centera V2.1 Programmer’s Guide* and the *EMC Centera SDK V3.2 API Reference Guide*.

The PEA file must be accessible to the Enterprise Vault Storage Service that manages the Vault Store Centera partition that will use the profile.

The Storage Service runs under the Vault Service account and therefore the PEA file must allow read access by this account. For greater security access to the PEA file by any other account could be disabled.

The Vault Store Partition’s Connection tab allows the user to establish the IP Address(es) for the primary Centera. In addition, a PEA file must be specified; using the Browse button instead of entering the path location will further ensure that the PEA file is accessible (see Figure 18).

Use the Test Settings button to verify the connection to the primary Centera.

![Figure 18 Establishing the EMC Centera connection string](image-url)
Enterprise Vault version 6.0 or later supports setting EMC Centera PEA files in the Vault Administration Console. The process is documented in the VAC help as well as in the EMC Centera Global Services Documentation online help.

Network segmentation

In a purely segregated environment of application and replication data traffic, where network segmentation has been established, built-in read failover functionality will not function as expected. For any application that requires read failover capabilities to a secondary EMC Centera, under these circumstances, it is recommended that these failover IP addresses are explicitly specified by adding the access role to the replication nodes in the replica cluster. Reviewing the application settings and ensuring that the application traffic network has access to the secondary EMC Centera is strongly recommended.

Threading

**BEST PRACTICE:** A thread is a part of a program that can execute independently of other parts. CentraStar supports multi-threading, thus enabling threads to run at the same time without impacting each other. A single thread cannot take advantage of this parallelism.

**BEST PRACTICE:** In EMC Centera, threads are distributed evenly over the available nodes and the number of nodes influences the number of threads that can be supported.

**BEST PRACTICE:** It is recommended not to have more than 20 concurrent threads per access node.

Enterprise Vault uses multi-threading to increase the maximum transfer rate by leveraging EMC Centera parallelism capabilities. When archiving with collections, this is not relevant because it is only collections that are written to EMC Centera and not individual items. However, when archiving to EMC Centera without collections, optimum performance is reached when the number of processes is increased. For example:

<table>
<thead>
<tr>
<th>Number of storage archive processes</th>
<th>Number of PST migrators</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>20</td>
</tr>
</tbody>
</table>

Expanding the Enterprise Vault Servers branch and selecting the Advanced tab, on the Storage Service properties, allows the configuration of the number of threads for writing (used by the Archive processes) and reading (used by the Restore processes) purposes.

When collections are not enabled, the rate at which items are expired and deleted from EMC Centera can be improved by increasing the number of Expiry threads to its maximum value of 10. This is done by changing the value of the following registry key:

Key name: HKEY_LOCAL_MACHINE\SOFTWARE\KVS\Enterprise Vault\Storage

REG_DWORD value: EMCCenteraExpiryThreads

**Note:** The default value is 5. The maximum number of threads is 10.

**BEST PRACTICE:** The number of archive processes should be 10 when collections are not used - and the default (5) when collections are used. For Restore it should be set to 1 Restore process and 10 threads, regardless of whether or not collections are used.

The settings displayed in Figure 19 are per Vault Store server.
Chapter 3 Configuring Enterprise Vault and EMC Centera for Email Archiving

Note: If there are multiple servers deployed, these settings must be checked for consistency in all of them.

![Service Properties - Enterprise Vault Storage Service](image)

*Figure 19 Number of threads*
Enterprise Vault retention categories

Figure 20 shows how to assign a retention category to a provisioning group.

![Figure 20 - Assigning retention categories to a provisioning group](image)

Enterprise Vault fine tuning

Additional information for customizations and best practices around mailbox archiving, public folder archiving, File System Archiving and placeholder shortcuts, and performance tuning is available in the *Symantec Enterprise Vault 9.0 - Administrators Guide*.

In particular, the following sections are presented in greater detail for mailbox archiving:

- Archiving based on age
- Archiving based on quota or age and quota
- Archiving items from Exchange managed folders
- Archiving items only if they have attachments
- Customizing the Enterprise Vault settings for a journal mailbox
- Disabling archiving for mailboxes
NTFS to EMC Centera migrations

Customers that have initially deployed Symantec Enterprise Vault in their environment, and later decide to introduce EMC Centera as the archiving storage component of the solution, need to migrate the pre-existing NTFS archive into EMC Centera.

Enterprise Vault has a utility delivered as part of the installation kit, specifically designed to automate this process, while providing the flexibility and granularity to prioritize and project manage the migration process based on specific business requirements including date ranges.

Symantec’s NTFS to Centera Migration utility copies Enterprise Vault savesets from an NTFS source partition to an EMC Centera destination partition. The source partition and destination partition are always in the same vault store, so performing a migration does not have an impact on existing archives and indexes.

The NTFS to Centera Migrator tool does not recall data back to Exchange. It retrieves Saveset files from the NTFS partition into a Saveset object, which is then stored in the Centera partition. The information in the Vault Store database is updated to record that the savesets are stored in the Centera partition.

Note: The source partition files are not deleted. Data in the source folders may be shared with other partitions.

**BEST PRACTICE:** It is recommended to delete the files from the source folders only once it has been verified that there are no additional references pointing to such files from other partitions.

One of the factors that will most influence performance is if the NTFS partition has collections disabled or enabled. If enabled, the files have to be extracted from CAB files, which adds to the processing.

**BEST PRACTICE:** The NTFS to Centera Migration tool is multi-threaded. The number of threads and thread priority can be set. It is recommended that multiple threads at low priority are used, and that the migration is always running. The low thread priority reduces the impact on other EV operations, but when the EV servers are quiet the multiple threads will maximize the migration rate.

Capabilities

The NTFS to Centera Migration utility provides a command line interface (CLI) enabling the following tasks:

- Create migration jobs: There will be prompts to customize the job in regards to:
  - Source and destination stores
  - Date ranges (default is all)
  - Number of threads and priorities
  - Sharing (single instancing)
  - Log file location

Symantec Enterprise Vault and EMC Storage Applied Best Practices
• Error handling
  ♦ List migration jobs: monitor current jobs
  ♦ Delete migration jobs: delete unfinished or undesired jobs.

Additional information is provided in the “NTFS to Centera Migration” chapter in the *Symantec Enterprise Vault 9.0 - Utilities Guide*, available from the Utilities folder within the Enterprise Vault installation path.

**Storage reclamation**

Once the migration has finished and there are no further references to the files in the source store, it is possible to delete these files in order to reclaim the storage capacity consumed.

To delete the source partition and data:
1. In the Administration Console, expand **Vault Store Groups**. Expand the vault store that contains the partition to be deleted.
2. Right-click the partition and, on the shortcut menu, click **Delete**. The Administration Console prompts to confirm the delete operation.
3. Click **Yes**.
4. If the Administration Console allows the deletion of the partition, Windows Explorer can be used to delete the partition's files.

**Note:** If the Administration Console does not allow the deletion of the partition, then it is not safe to delete the partition's files.
This chapter presents this topic:

EMC Celerra configuration ........................................................................................................ 100
EMC Celerra configuration

Prior to performing the Enterprise Vault archiving setup, EMC Celerra is expected to be fully configured; in order to ensure Enterprise Vault access to Celerra, at the end of this process, the following items must be available to the Enterprise Vault system administrator:

- The fully-qualified DNS name of the file server that is being added
- An account on the Celerra Data Mover that has the Celerra dhsm permission (Optional, when using placeholder shortcuts)

In particular, EMC Celerra must be configured to support alternate data streams (ADS). Enterprise Vault uses ADS to indicate archive points.

To support the use of placeholder shortcuts, the FileMover functionality on the Celerra must be enabled and an HTTP connection must be created.

Note: Unwanted placeholder recalls can occur if the Windows Explorer preview pane that is provided with Windows Vista and Windows Server 2008 is used. When a placeholder is selected, Windows recalls the file to display the preview. This restriction is due to a limitation with the previewing of offline files.

Note: To configure the pass-through behavior on placeholder recall, it is recommended to read about the read_policy_override parameter before proceeding. Additional information is available in the “Configuring Celerra pass-through behavior for placeholder shortcuts” section in Setting up File System Archiving (FSA) 9.0.

Note: The technical note How to configure an EMC Celerra device on the Symantec Support Website provides additional troubleshooting information (http://www.symantec.com/business/support/index?page=content&id=TECH52430).

Setting up EMC Celerra

To set up EMC Celerra, the following information must be available to the Celerra administrator.

- Data Mover name
- Data Mover user account to be used for Enterprise Vault authentication
- File System name on Celerra
- IP address of the computer running the FSA Agent (policy agent)
- URL of the Enterprise Vault Web Access application

Note: If the Celerra fails to find a connection with the server name specified in the URL, the files are archived but no placeholders are created. The File System Archiving task report's "Shortcut status" column then shows the error “NO_MATCHING_CONNECTION”. Additional information is available in the “Specifying the correct URL for the Web Access application” section of the Setting up File System Archiving (FSA) 9.0 guide.

- Vault Service account that will have access to all the archives from which files are restored
- Password to the Vault Service account
Detailed information on the following procedure is provided in the “Preparing an EMC Celerra device” section on the Setting_up_File_System_Archiving (FSA) 9.0 guide:

1. Log in to the Celerra Control Station.
2. Ensure that the Celerra device is configured to support alternate data streams (ADS), which Enterprise Vault uses to indicate archive points.

   The Celerra shadow stream parameter controls support for ADS:
   - If the shadow stream parameter is set to 1, ADS support is enabled. 1 is the default value.
   - If the shadow stream parameter is set to 0, ADS is disabled.
3. Add a Celerra account for Enterprise Vault to use for authentication on the Celerra device.
4. Enable the file system for Celerra FileMover <command line interface>.
5. Configure the HTTP server on the Data Mover to accept Celerra FileMover API connections <command line interface>.
6. Configure the HTTP connection to use for recall requests <command line interface>.
7. Add the Vault Service account as a member of the Administrators group of the Celerra CIFS server.

Configuring Celerra pass-through behavior for placeholder shortcuts

Pass-through recall can be useful in the following circumstances:

- With placeholders on read-only file systems. A normal placeholder recall to a read-only file system fails because Enterprise Vault cannot write the recalled file to the file system.
- With Windows file servers when there is limited space on the file server, or when users have strict quotas for space usage. Recalled files normally occupy space on the target file system, and therefore count toward a user’s space quota.

If required EMC Celerra's read policy override with placeholder recalls can be used. The Celerra's -read_policy_override parameter determines how a read request is handled for a file in secondary storage. An example would be enabling to pass a file directly through to the client without recalling it to the Celerra. Celerra Network Server then recalls the file only if a write request is received. For pass-through, the Celerra uses the same cache on the Enterprise Vault server that was set up for Enterprise Vault to use when retrieving files for the Celerra.

**BEST PRACTICE:** If Celerra pass-through is configured, do not configure the Enterprise Vault option to delete archived files on placeholder deletion, as this combination can lead to data loss.

Detailed information on this option is available on Setting_up_File_System_Archiving (FSA) 9.0.

Enterprise Vault and Celerra configuration

Once the Celerra is configured, the Administration Console can be used to add the device as an archiving target.

1. In the Administration Console, expand the Enterprise Vault site until the Targets container is visible.
2. Expand the Targets container.
3. Right-click the File Servers container and, on the shortcut menu, click **New** and then **File Server**. The New File Server wizard starts.

4. Work through the wizard to finish adding the file server:
   - On the first screen, click **Next**.
   - On the second screen (Figure 21), enter the DNS name of the Celerra device. Do not select the option to install the FSA Agent. Click **Next**.

![New File Server](image)

**Figure 21** Setting the File Server fully qualified DNS name
On the third screen (Figure 22), choose whether to use placeholder shortcuts. If placeholder shortcuts are to be used, enter the details of the account that was configured on the Celerra that has permission to use the dhsm feature.

Figure 22  Enabling placeholder shortcuts

The account details can be changed later, if required, by editing the properties of the Celerra.

Click Next to continue.
On the summary screen (Figure 23), click **Next** to add the Celerra device.

![Figure 23  Adding a file server](image)

On the following screen (Figure 24), choose whether to enable data collection for FSA Reporting.

![Figure 24  Enabling data collection for FSA Reporting](image)
Additional information on FSA reporting is available in Setting_up_File_System_Archiving (FSA) 9.0.

- On the final screen, click **Close** to exit from the wizard.

When the file server has been added, it is possible to start adding the volumes that File System Archiving should process.

Creating FSA archiving policies

Enterprise Vault provides two levels of archiving policies: volume policies and folder policies, which override volume policies.

**Volume policies**

A volume policy's settings are applied to a complete volume, unless overridden by a folder policy. The volume policy determines the following:

- Which retention category to apply to the files that are archived with this policy.
- The archiving rules to apply for the volume. Each archiving rule specifies the file criteria to match, such as the file type, the time that the file was last modified or last accessed, the file size, and file attributes.
  
  **Note:** Additional information is available in the “Tips on archiving policy rules” section in Setting_up_File_System_Archiving (FSA) 9.0.

- The action to take on the files that match the criteria specified.
- Whether and when to create shortcuts for the matching files. Shortcuts can be created immediately or some time later, according to criteria specified.
  
  **Note:** Additional information is available in the “Shortcut creation options” section in Setting_up_File_System_Archiving (FSA) 9.0.

- The type of shortcut to leave to an archived file, if the archiving rules specify that a shortcut is created. The option to leave a placeholder shortcut or an Internet link is available.
  
  If a placeholder shortcut is left, select one of the following:

- Delete placeholders for the items that have been deleted from archives.
- Delete archived files when placeholders are deleted.
  
  **Note:** Additional information is available in the “Deleting archived files on placeholder deletion” section in Setting_up_File_System_Archiving (FSA) 9.0.

- Whether to archive the files that have explicit permissions set on them. When Enterprise Vault archives files, it gives the archived version the same permissions as the folder that contained the original file.
  
  **Note:** Additional information is available in the “Files with explicit permissions” section in Setting_up_File_System_Archiving (FSA) 9.0.
Folder policies

A folder policy contains settings that are to be applied to specific folders.

Note: Folder policy settings override volume policy settings.

To make for easier management, it is strongly recommended not to apply folder policies to folders that have a short life, such as temporary folders. It is better to create folder policies for folders that will have a long life, such as a user's root folder.

Shortcut creation options

The Enterprise Vault archiving task creates shortcuts during normal archiving runs. The task creates the shortcuts according to rules defined in the archiving policy. Running the archiving task’s Run Now option creates shortcuts at any other time.

The shortcut creation options are as follows:

- Shortcut creation. There are three possible settings:
  - None. Archive and delete file. Do not create any shortcuts to archived files. Enterprise Vault archives the files that meet the archiving criteria and then deletes the files.
  - Create shortcut immediately. Archive the files that meet the archiving criteria and then create shortcuts to the archived files.
  - Create shortcut later. Archive the files that meet the archiving criteria but do not delete the files. Enterprise Vault leaves the files until they meet the date criteria defined on this tab. This option enables the archiving of the files as well as leaves the original files in place until they are no longer needed. This means that a user can read or edit the files without them being recalled from the archive.

- Last archive time is. Enterprise Vault creates shortcuts when the specified time has elapsed since the last time the file was archived. This option ensures that shortcuts are not created for frequently modified files.

- Last access time is. Enterprise Vault creates shortcuts when the specified time has elapsed since the last time the file was accessed. This option ensures that shortcuts are not created for frequently accessed files.

- Last modified time is. Enterprise Vault creates shortcuts after the specified time has elapsed since the last time the file was archived. This option ensures that shortcuts are not created for frequently modified files.

- Created time is. Specifies that Enterprise Vault must create shortcuts when the specified time has elapsed since the file was created.
Note: Specifying more than one of the time conditions, Enterprise Vault does not create shortcuts until all the conditions are satisfied.

Note: Enterprise Vault checks the vault store setting for Remove safety copies before creating shortcuts. If safety copies cannot be removed because of this setting, Enterprise Vault does not create shortcuts. Table 13 shows how the Remove safety copies settings can affect shortcut creation.

Table 13  Remove Safety Copies setting impact on shortcut creation

<table>
<thead>
<tr>
<th>Remove Safety Copies Setting</th>
<th>Shortcut Creation Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>None. Archive and delete file</td>
<td>Create shortcut immediately</td>
</tr>
<tr>
<td>Immediately after archive</td>
<td>Delete original file</td>
</tr>
<tr>
<td>Never</td>
<td>Leave the original file</td>
</tr>
<tr>
<td>After Backup</td>
<td>Delete original file after backup</td>
</tr>
</tbody>
</table>

Deleting archived files on placeholder deletion

When using placeholder shortcuts, Enterprise Vault can be configured to delete archived files when their placeholders are deleted. Additional information on this feature is available in Setting_up_File_System_Archiving (FSA) 9.0.

How the 'Delete archived file when placeholder is deleted' feature works

Enterprise Vault uses the following mechanism with EMC Celerra file server placeholders, as follows:

- To configure archived file deletion with Celerra a target volume whose share points to the root of the file system must be configured. The “Delete archived file when placeholder is deleted” policy setting that applies to this root volume determines this policy setting for all of the file system’s archived files.

Note: The root volume’s policy setting overrides any “Delete archived file when placeholder is deleted” policy setting that is applied to any other target volumes or target folders in the same file system.

- For Celerra placeholders, Enterprise Vault does not use a DOD cache. When a Celerra placeholder is deleted, Enterprise Vault examines the value of the "Delete archived file when placeholder is deleted" setting for the policy that applies to the Celerra target root volume.

BEST PRACTICE: FileMover logging on the Celerra device must be enabled. Enterprise Vault uses the Celerra FileMover log’s records of deleted placeholders to determine which archived files to delete.
The deletion of the archived Celerra files does not occur immediately upon placeholder deletion. Deletion from the Celerra takes place daily according to the schedule that is specified in the properties of the File System Archiving task.

**Configuring the deletion of archived files on placeholder deletion**

To configure the deletion of archived files on placeholder deletion, it is recommended to follow the procedure that is appropriate for the type of file server.

**Note:** Enterprise Vault does not delete archived files in the following circumstances:
A. For NTFS volumes on which pass-through recall is enabled. This combination of settings can result in data loss.
B. If the archiving policy applies a retention category with "Prevent deletion of archived items in this category" set. The retention category setting takes precedence.

**BEST PRACTICE:** If Celerra pass-through is configured, the Enterprise Vault option to delete archived files on placeholder deletion must not be configured, as this combination can lead to data loss.

The following procedure describes how to configure deletion of archived files on placeholder deletion for EMC Celerra file servers:

1. Configure a target volume under the target Celerra file server whose share points to the root of the file system.
2. Apply an archiving policy to the root volume in which the setting "Delete archived file when placeholder is deleted" is selected on the Shortcuts tab.
3. This root volume policy setting controls the deletion of archived files on placeholder deletion for all of the Celerra file system:
   - Enterprise Vault ignores the policy setting that applies to the folder volume, when any additional target volumes that point to specific folders in the same Celerra file system are configured.
   - Enterprise Vault ignores the "Delete archived file when placeholder is deleted" policy setting in any folder policies that apply to target folders.
4. Enable FileMover logging on the Celerra device. Logging must be enabled for file deletion to work. Testing whether logging is enabled may be done from the EMC Celerra tab in the properties of the Celerra target volume.

**Note:** Enterprise Vault performs archived file deletion for all of the placeholder deletions that are listed in the log. The file deletion occurs even if the placeholder deletion took place before the "Delete archived file when placeholder is deleted" policy setting is applied. If possible, do not enable FileMover logging before applying the policy setting.

   
   Set the value as follows:
   - Start the Windows registry editor regedit on the Enterprise Vault server.
   - Find the following registry key:
     - HKEY_LOCAL_MACHINE\Software\KVS\Enterprise Vault\FSA\ ArchivedFilesFlags
   
   The ArchivedFilesFlags key must be created if it does not exist.
Chapter 4 Configuring Enterprise Vault and EMC Celerra for File System Archiving

- Create a DWORD registry value named DeleteOnDelete under the ArchivedFilesFlags key, if this registry value does not already exist.

- Give DeleteOnDelete a value of 1. This value means "Delete an archived Celerra file when its placeholder is deleted". Alternatively, Celerra archived file deletion can be turned off on placeholder deletion by setting this value to 0.

- Save the changes and quit the registry editor

6. Restart the Enterprise Vault Admin service on the Enterprise Vault server to activate the registry change.

7. Configure the daily deletion schedule for the archived files whose placeholders were deleted. See Scheduling the deletion of archived files for EMC Celerra information.

Adding a volume

Enterprise Vault File System Archiving processes volumes added when using the New Volume wizard.

The New Volume wizard asks the following:

- Which volume to add
- Which vault store to use for the files that are archived from this volume
- Which File System Archiving task to use to process this volume
- Which volume policy to apply when files are archived from this volume

If FSA Reporting is configured, the wizard also provides the option to choose whether to enable FSA Reporting for this volume.

When adding an EMC Celerra volume, the following must be considered:

- Before adding the first volume for a Celerra device a cache location for Enterprise Vault to use for temporary files must be specified. See Specifying a cache location for EMC Celerra for details.

- When using the archiving policy setting "Delete archived file when placeholder is deleted", certain restrictions and requirements apply. See Deleting archived files on placeholder deletion for details.

Additional information is available in Setting_up_File_System_Archiving (FSA) 9.0.

Specifying a cache location for EMC Celerra

In order to improve performance, an Enterprise Vault server that retrieves files from an EMC Celerra device requires a location to use for temporary files. Before adding the first volume on a Celerra device specify a folder that is local to the Enterprise Vault server that can be used for caching temporary files.

To specify a cache location

1. In the Administration Console, expand the Enterprise Vault site until the Enterprise Vault Servers container is visible.

2. Expand the Enterprise Vault Servers container.
Chapter 4 Configuring Enterprise Vault and EMC Celerra for File System Archiving

3. Right-click the server that will archive from the Celerra and, on the shortcut menu, click Properties.
4. Click the Cache tab.
5. Under Cache Location, enter an existing path on the server that can be used to cache files retrieved from the Celerra.

Scheduling

Scheduling File System Archiving

A File System Archiving task processes its target servers according to the schedule defined for that task. It is possible to define an individual schedule for each File System Archiving task, or to use the site schedule. The File System Archiving task checkpoints its progress. If the task is stopped before it has completely processed a volume, then when the task next starts it continues from the point of interruption.

Scheduling the deletion of archived files for EMC Celerra

If File System Archiving has been configured, to delete archived files when their placeholders are deleted, the deletion of the archived EMC Celerra files takes place, according to the schedule that the user defines on the properties of the File System Archiving task (once or twice daily).

To schedule the deletion of archived files for EMC Celerra
1. In the Administration Console, expand the Enterprise Vault site until the Enterprise Vault Servers container is visible.
2. Expand Enterprise Vault Servers.
3. Expand the Enterprise Vault server that runs the File System Archiving task to archive from the Celerra device.
4. Click Tasks.
5. Right-click the File System Archiving task and, on the shortcut menu, click Properties.
6. Click the Celerra tab.
7. Set the AM and PM deletion times that is required.
8. Click OK.

Virus-checking a file server

Enterprise Vault placeholder shortcuts appear to the operating system as markers for offline files. Some antivirus programs can be configured to ignore offline files, but others cannot. If the antivirus program cannot be configured to ignore offline files, every placeholder that the program checks results in an offline file being recalled.

**BEST PRACTICE:** It is strongly recommended to configure the antivirus program to ignore offline files, before running virus scans on disks with Enterprise Vault placeholder shortcuts.

EMC Celerra provides additional capabilities when the antivirus program cannot be configured to ignore offline files. In this case, it is possible to use before running virus scans on disks with Enterprise Vault placeholder shortcuts.

EMC Celerra provides additional capabilities when the antivirus program cannot be configured to ignore offline files. In this case, it is possible to use the Celerra's backup options to exclude the
appropriate Active Directory account from triggering placeholder recalls. Additional information
is available in the “Preventing file recalls on EMC Celerra” section of
Setting up File System Archiving (FSA) 9.0

Preventing file recalls on EMC Celerra

The Celerra backup options can be leveraged to prohibit Active Directory groups or Active
Directory accounts such as a service account from triggering placeholder recalls from the Celerra
file systems. For instance, the service account for a backup program or antivirus program can be
excluded.

To prevent members of a group or an individual account from triggering placeholder recalls
through the CIFS interface, it is possible to add the appropriate group or account to the Celerra
Backup Operators group. Then executing the following command will prevent those accounts
from recalling placeholders:

```
fs_dhsm -m fs_name -backup offline
```

where `fs_name` is the name of the file system on the Celerra. Additional information is available
from the EMC Celerra documentation.
Chapter 5  Operations

This chapter presents these topics:

EV updates and upgrades................................................................. 114
EMC Centera upgrades........................................................................ 114
EMC Celerra upgrades....................................................................... 116
Disaster recovery .............................................................................. 117
EMC Centera backup.......................................................................... 121
EMC Centera monitoring................................................................. 121
Celerra monitoring ......................................................................... 122
High availability .............................................................................. 122
EV updates and upgrades

Day-to-day management tasks

The following provides a checklist of the main day-to-day administration tasks required to maintain optimal performance of the Enterprise Vault system:

- Monitoring Enterprise Vault Services and tasks
- Starting or stopping tasks or services
- Checking logs
- Monitoring Exchange Server journal mailboxes and Domino journal databases
- Monitoring disk usage
- Monitoring MSMQ queues
- Maintaining SQL databases
- Backing up Vault Stores
- Enable archiving for new Microsoft Exchange Server mailboxes or Domino mail files
- Importing PST files (Personal Folder files)
- Importing NSF files
- Changing disks for journal archives
- Monitoring licenses
- Modifying the list of who has access to an archive that is being shared by a number of users

Full details of how to perform these tasks are given in the *Symantec Enterprise Vault 9.0 - Administrators Guide*. There are a number of utilities available for performing a variety of tasks, such as re-creating FSA Placeholder shortcuts on a file server, moving archived data from an NTFS device to an EMC Centera device, and managing FSA archive points. For additional information, see the *Symantec Enterprise Vault 9.0 - Utilities Guide*.

EMC Centera upgrades

Customers should not face any compatibility issues when upgrading any of the EMC Centera components of their archiving solution.

EMC strongly recommends upgrading to the latest hardware and software versions available. Based on the EMC Centera SDK backward compatibility with CentraStar, there should not be any issues upgrading CentraStar to a newer version. All ISV applications communicating with an upgraded EMC Centera cluster should still be able to function as expected.

**Note:** Upgrading to a new CentraStar version does not imply or require customers to upgrade their applications.
EMC Centera partners release their products with the particular EMC Centera SDK version with which the application was developed. Upgrading to a newer ISV application version most likely means upgrading the EMC Centera SDK version it ships with.

Based on the SDK forward- and backward-compatibility statements from EMC, there should not be any EMC Centera SDK/CentraStar compatibility issues when upgrading an application to a newer version.

**Note:** Upgrading an application version does not imply or require customers to upgrade their Centera CentraStar version. For additional information, see the white paper *EMC Centera CentraStar/SDK Compatibility with Centera ISV Applications - A Detailed Review*. In addition to this, as part of their regular business practices, Symantec performs additional testing when major CentraStar releases are available; see the *Symantec Enterprise Vault Compatibility Charts* for detailed information.

### Added capacity

*Capacity* is added to the EMC Centera at the cube level. A cube can consist of up to 16 nodes. A cluster can contain up to eight cubes or 128 nodes. Cubes are connected through an interconnection switch. Nodes are added to a cube in two-node expansion increments when using CPM, and eight-node expansion increments when using CPP. The capacity add is automated and is transparent to the application.

### CentraStar upgrades

CentraStar upgrades can be performed online. One node is upgraded and rebooted at a time, making an upgrade seamless to the application.

### EMC Centera migrations

In EV 6.0 or later multiple EMC Centera partitions can exist in a single Vault Store, which can be useful during EMC Centera hardware migrations.

In this case, using the Vault Administration Console (VAC), all existing partitions pointing to the old EMC Centera will be closed, and new partitions will be created to archive against the new EMC Centera for all on-going data. With this configuration, archiving activities will not be impacted and users will be able to read from both closed and open vaults.

**BEST PRACTICE:** How to migrate EV data from older to newer Centera hardware is as follows:

1. "Close" all current vaults, so that they are in read-only mode. Consequently, no extra data is added to the old cluster, making this environment stable.
2. Create as many vaults as currently exist, but pointing to the new cluster. All new writes/reads go there; the user should implement the virtual pools, and all other security configurations at this time (pools/profiles/PEA files, and so on). Now that the new environment is up and running, it is possible to start the migration process, one vault at a time. This allows the company more control over the process, prioritizing the vaults to migrate first. For each Vault:
   - Obtain the list of clips (savesets) to migrate (by vault). There are two ways for doing this:
     - EV support tells the customer the list of clips or the SQL script to run against EV SQL database
Chapter 5 Operations

- The customer generates the list using the EVSVR Utility for Enterprise Vault, included in EV 8.0 SP1 or later.

4. The customer provides a clip list to EMC Centera (Support or Professional Services) to perform the migration.

5. Once migrated and a reconciliation has been completed, the old vault, which was closed, is reconfigured to point to the new EMC Centera (connection string).

6. Repeat steps 3 - 5 as needed.

7. Once all vaults are migrated, the old cluster can be disposed.

EMC Celerra upgrades

EMC strongly recommends upgrading to the latest software version that Symantec Enterprise Vault supports. Also, upgrading an ISV application may involve upgrading the Celerra software version as well. However, the solution should function as expected due to the compatibility testing Symantec conducts with Celerra software releases. See the Symantec Enterprise Vault Compatibility Charts (same link from the Centera upgrade section) for detailed information on the testing Symantec has performed with Celerra software versions.

The upgrade can be performed online. Celerra upgrades for minor software releases (that is, 5.6.43 to 5.6.44) are nondisruptive, meaning that file system access is not lost during the upgrade. An upgrade to the next major software release (that is, 5.6.44 to 6.0.36) results in temporary loss of access to the file systems on the Celerra.

Added capacity

Capacity is added at the disk device level for the Celerra. Additional storage is provisioned from the storage arrays (CLARiiON or Symmetrix) to the Celerra as disk devices, from which file systems can be created for the Symantec EV solution. Allocating more space from the storage array to Celerra and creating new file systems or extending new file systems would require storage administrative privileges in order to perform these tasks.

For existing file systems used in the Symantec EV solutions, a file system auto-extend policy can be configured in advance such that if the used capacity of the file system reaches a certain percentage of the total capacity, the file system will automatically extend by using available capacity in the storage pool on the Celerra. The auto-extend policy can be configured during the setup of the Symantec EV solution so that file system storage capacity can extend without administrator interaction. If the storage pool does run out of space, provisioning more space to the storage pool will require administrator interaction.
**Disaster recovery**

There are different procedures and considerations for disaster recovery purposes depending on the storage device used to hold the archive. This section provides detailed information for both EMC Centera and EMC Celerra.

**Disaster recovery for EMC Centera**

EMC Centera Replication provides a disaster recovery mechanism for content written to EMC Centera clusters. EMC Centera Replication can be used to create multiple protected copies of content written to a primary Centera cluster by automatically copying the content to a replica Centera cluster. Replication runs as an asynchronous background task and can be configured in a number of topologies, namely unidirectional, bidirectional, chain, star, and star and chain. For detailed information on disaster recovery, refer to the *Symantec Enterprise Vault 9.0 - Administrators Guide*.

EMC Centera Replication provides functionality that allows the recovery of the content that is either missing or simply unavailable. Applications will fail over automatically to retrieve missing or unavailable data content on the primary cluster from the replica cluster.

Additional information for EMC Centera Replication is available in the white paper *EMC Centera Replication - A Detailed Review.*

The following sections describe the DR procedures for events impacting either Enterprise Vault or EMC Centera. If the event impacted both components of the environment, follow both procedures.

**Enterprise Vault only disaster recovery**

If a disaster event impacted only the Enterprise Vault portion of the archival infrastructure, following the methodology and procedures described in the “Recovery” section of the *Symantec Enterprise Vault 9.0 - Administrators Guide* as it applies to the strategy chosen (for example, full system backup, data-only backup) should get the application up and running.

Regardless of the strategy used, it is necessary to ensure that the Pool Entry Authorization (PEA) file(s) is part of the backup content checklist plan, as it grants access to the EMC Centera cluster (for additional information see *EMC Centera connection string*).

The following is the list of activities that needed to perform to re-establish normal operations:

1. For a full system backup strategy, the user may want to Test the connection from the Vault Partition Properties Connection tab (Figure 18).

2. In the case that a full system backup strategy is not used, while following the recovery procedures described in the *Symantec Enterprise Vault 9.0 - Administrators Guide* restore the PEA file and provide its new location path at the time of executing the Enterprise Vault Configuration, and follow the best practices laid out in this document.

3. Due to changes made since the last set of backups were done and because certain operations may not have completed before the system failure occurred, revert all pending shortcuts in order to re-archive them (See Step 6 “Repeat Operations” in the “Recovery” section of the *Symantec Enterprise Vault 9.0 - Administrators Guide* for more details):
   
   - Repeat archive operations done since the last set of daily backups were made.
Chapter 5 Operations

1. Cancel all archive pending items from mailboxes. Symantec’s tech note 35618 describes "How to cancel items in an "archive pending" state in Enterprise Vault (EV) for Microsoft Exchange"; Solution 3 - using the VAC to change the Pending Shortcut Timeout to 0 – is the recommended method.

4. Optional: To further verify the integrity between the Enterprise Vault database(s) and the EMC Centera archive, use the EVSVR Utility provided with the Enterprise Vault 9.0 Installation kit. Additional information on the use of the tool is available in the Symantec Enterprise Vault 9.0 - Utilities Guide.

Note: Enterprise Vault 9.0 SP2 is the first version that includes repair operations as part of EVSVR. Corrective actions are available to Symantec Support in previous versions of Enterprise Vault, via platform specific tools; EVCentera Checker could be used by Symantec support if inconsistencies are found.

EMC Centera primary only disaster recovery

If a disaster event impacted only the Centera primary cluster, Enterprise Vault will automatically fail over for reads.

Due to the asynchronous nature of the EMC Centera Replication mechanism, any data written to the primary Centera still resides on primary storage (Exchange Server) as part of the About this Document Safety Copy functionality, until its replication has been confirmed. Since the data written to the primary EMC Centera might not have been replicated prior to the occurrence of the disaster event, it is necessary to re-archive any data still identified as “Shortcut Pending” by the Safety Copy, in order to sync up the system.

To allow full recovery, it is necessary to reconfigure the EV server(s) to point to the new (former replica) EMC Centera as the primary cluster, and then re-archive the data:

1. Look at the Connection tab properties of the Vault Store and add the –Saved Replica IP address List” as the –IP Address List” (Figure 18).

2. Because certain operations may not have completed before the system failure occurred, revert all pending shortcuts in order to rearchive them (See Step 6 –Repeat Operations” in the –Recovery” section of the Symantec Enterprise Vault 9.0 - Administrators Guide for more details):

   • Repeat archive operations done since the last set of daily backups were made.

   • Cancel all archive pending items from mailboxes. Symantec’s tech note 35618 describes "How to cancel items in an "archive pending" state in Enterprise Vault (EV) for Microsoft Exchange"; Solution 3 - using the VAC to change the Pending Shortcut Timeout to 0 – is the recommended method.

3. Optional: To further verify the integrity between the Enterprise Vault database(s) and the Centera archive, use the EVSVR Utility provided with the Enterprise Vault 9.0 Installation kit. Additional information on the use of the tool is available in the Symantec Enterprise Vault 9.0 Utilities Guide.

Note: Enterprise Vault 9.0 SP2 is the first version that includes repair operations as part of EVSVR. Corrective actions are available to Symantec Support in previous versions of Enterprise Vault, via platform specific tools; EVCentera Checker could be used by Symantec support if inconsistencies are found.
Disaster recovery for EMC Celerra

If the DR event brought down the entire cabinet, the storage administrator needs to ensure the system in the cabinet was powered on correctly once the power was restored on the cabinet.

1. Check for system faults. Acknowledge the known faults (that is, power failure) and address the existing faults (that is, LUN trespassed to a different storage processor). The faults are displayed on Celerra Manager and Unisphere, the management interface for the CLARiiON. If the Celerra is running version 6.0, then the administrator can use Unisphere™ to manage the Celerra and CLARiiON.

2. Check that all Data Movers are ready for I/O, by checking the status of each Data Mover. Check that the network connectivity is restored.

**Recovering from a DR event using Celerra Replicator**

In a DR event, some data that was not yet transferred from the source file system to the destination file system will be lost due to the asynchronous nature of Celerra Replicator. However, the file systems are in sync as of the last transfer. When a DR event does happen, Celerra Replicator will automatically fail over and allow the destination file system to act as the primary file system so that reads and writes can continue. When the primary site is back up and ready for I/O, a storage administrator can do the following to transfer the production I/O back to the primary site:

1. Log in to Celerra Manager or Unisphere on your destination Celerra.
2. Go to the Celerra Replicator section and look for the replication sessions for the file systems used in the Symantec EV solution. The status should say “Failed Over”.

![Celerra Manager Interface](image-url)
3. Now that the primary site is back up, restart the replication session again. Highlight the replication session entry and click the **Start** button.

4. Then fail back the replication session so that the primary site can assume production I/O for the file system and the DR site can reassume the role as the destination, or replica, in the replication session. Highlight the entry for the replication session and click the **Reverse** button.
Recovering from an NDMP backup

A full recovery from an NDMP backup is a point-in-time recovery. The recovery will bring the file system data back to the point in time at which the backup took place for the file system. Any data that was modified or created after that point will be erased. An NDMP backup requires a third-party software application that manages the data backed up and the backup/restore operations. Recovering a file system involves locating the right backup data set and pointing to the target to which the data should be restored to (that is, file system path). Each third-party software application has its own instructions. Please refer to the instructions manuals to perform an NDMP restore:

- Symantec NetBackup (http://www.symantec.com/business/netbackup)
- EMC NetWorker (http://www.emc.com/products/detail/software/networker.htm)

EMC Centera backup

Tape out (Seven10 StorFirst Altus)

- Altus is a complete tape library and VTL management solution and manages tape and VTL data in all possible locations: in the drive, in the library slot, and offline (on-shelf or in-vault).
- Altus is designed specifically to back up an EMC Centera to tape or a virtual tape library.
- Altus builds a single, complete, and always synchronized copy of all the information in EMC Centera by incrementally capturing new C-Clips.
- Altus can perform a full, partial, or a single clip restore.

EMC Centera monitoring

EMC Centera Console

EMC Centera Console is a Web-based user interface that enables system administrators to view detailed information concerning the health, capacity, and performance of one or more clusters in their EMC Centera environment.

CV/CLI

CV/CLI is a Java-based tool used to monitor and manage an EMC Centera.

Health report

A daily HTML report is emailed to system administrators reporting the state of the EMC Centera.

Alerts

An XML report is emailed to system administrators reporting on an alert that had occurred on the EMC Centera.
Audit logging

EMC Centera automatically logs information that allows the system administrator to see who logged in to the EMC Centera and which actions were performed.

Celerra monitoring

Unisphere daily management

Unisphere makes daily management easier. The features that simplify daily management of Unisphere are:

- **Dashboards**: When customers log in to a system, they are immediately brought to a dashboard. This dashboard is customizable and it displays information such as domain wide alerts, and Celerra and CLARiiON capacity as well as a listing of all systems in the domain. If customers have a large environment to manage and need to address multiple alerts across multiple systems, they can simply view the domain-wide alerts page and easily identify which system is generating which alert.

- **Tables**: Customers have complete control over reporting with Unisphere. Any table within Unisphere can be customized to show specific fields, and then exported to a csv file. Filtering is now available within these tables as well. If customers have environments with hundreds of file systems, they can easily filter to see specific names, sizes, and other parameters.

- **Cross-linking**: For advanced users, Unisphere introduces cross-linking. A customer can view a specific file system’s properties, see which volumes comprise it, and even see which CLARiiON LUNs it is built from.

High availability

For detailed information on configuring a working building blocks solution and recovery, refer to the *Symantec Enterprise Vault 9.0 - Administrators Guide*.
This chapter presents these topics:

Cooperative Support ....................................................................................................................124
Symantec Enterprise Vault troubleshooting considerations ........................................................124
EMC Centera troubleshooting considerations .............................................................................125
EMC Celerra troubleshooting considerations ..............................................................................127
Chapter 6 Support Model

Cooperative Support

EMC and Symantec manage its collaborative support in two different ways, through Cooperative Support Agreements (CSAs) and through TSANet, a web-based customer support consortium. EMC is a member of TSANet, and holds a seat on its board of directors, along with more than 100 other technology companies. Symantec and EMC use TSANet to collaborate on interoperability issues. As part of TSANet, companies are members of a Mission Critical Community that enables its members to triage and collaborate on issues on a 24/7 basis until a call owner for problem resolution is determined. EMC and Symantec, in conjunction with Oracle, have also created a Multi-Vendor Escalation Center (MVEC) for the purposes of providing seamless backline technical support. The center provides another level of collaboration between the support organizations that ultimately results in a better customer experience. (For additional information, see the Symantec Enterprise Vault 9.0 Performance Guide.)

Symantec Enterprise Vault troubleshooting considerations

If you are an existing Enterprise Vault user who is experiencing problems because of environmental factors, use Deployment Scanner to collect and export configuration information in a form that Symantec Technical Support can analyze.

To export information about the environment:
1. On the Welcome page of Deployment Scanner, select Gather information about the environment, and then click Next.
2. Select the environment checks to perform, and then click Next.
3. On the Support Case page, enter the support number if one exists, and choose where to save the exported data.
4. Click Next to collect and export the information about the environment.

Enterprise Vault logging with DTRACE

DTRACE is a command-line utility that logs what an Enterprise Vault Service, process, or task is doing at the code level and provides a way to diagnose what is going wrong. With DTrace, it is possible to monitor multiple services simultaneously, filtering for specific words and writing the trace to a log file.

The use of this tool is commonly one of the first steps required when logging a support call with the Symantec Enterprise Vault support team.

To use DTRACE to diagnose an EMC Centera-specific problem, it is necessary to run DTRACE manually from Start > Programs > Enterprise Vault > Dtrace.

Typing View from the command line will display the components that can be traced; EMC Centera calls may be made from several of these components. Depending on the nature of the problem, the following may need to be traced:
- ArchiveTask - Exchange archiving
- EvLotusDominoArchivingTask - Domino archiving
- EvSharePointArchiveTask - SharePoint archiving
- EvFsaArchivingTask - FSA archiving
Chapter 6 Support Model

- StorageArchive - Any archiving without collections
- StorageFileWatch - Any archiving with collections
- StorageRetrieval - Retrieval of items
- StorageOnlineOpsns - Retrieval of items by end-user "on-demand" requests
- StorageCrawler - Retrieval of items for indexing
- StorageDelete - Expiry of items, deletion of archives and Vault Stores, and NTFS to EMC Centera migrations

Note: Additional information on the processes involved when Centera Collections are enabled is available in the "Collections" section of the document.

To set the components to be traced, the following commands are recommended:

- **Set nn verbose** - Where nn is the component id returned from the View command.

To set the trace to log only EMC Centera commands:

- Filter clear both
- Filter set Centera

To start monitoring and direct output to a log file:

- **Log Centera.log** - Will create a log file in the Enterprise Vault program folder called Centera.log and will start logging.

While DTRACE is running, the components that are enabled will run slower. The log file may grow rapidly. Normally DTRACE should not run for more than 10 minutes (but may need to run longer to catch a more infrequent error).

The log file may be mailed to the support team handling the problem.

**EMC Centera troubleshooting considerations**

**SDK logging**

SDK logging is the process of capturing SDK activity between the application and EMC Centera. This log is used for SDK troubleshooting and development. For application debugging of supported platforms, the SDK provides thread-safe logging of all its activities via log API functions or logging environment variables. Logging does not create new threads.

Note: When using environment variables, an application server restart is required before and after the log file is collected. Enterprise Vault does not use API functions and relies solely on the environment variables mechanism to enable SDK logging.

When checking for log state settings, the FPLogging mechanism observes the following order of priority, from highest to lowest:

1. FPLogState settings applied by FPLogging_Start() calls
2. FPLogState.cfg in the working directory
3. FP_LOG_STATE_PATH environment variable
4. Logging environment variables
For example, during application startup, FPLogging first checks for the presence of the FPLogState.cfg properties file in the working directory. If this file exists, the SDK automatically reads and uses the settings contained in that file, including the log path for the logging output. No attempt is made to read any logging environment variables unless FPLogState.cfg is absent from the working directory.

If this is the case and environment variables are to be used, the log state settings of the configuration file defined in FP_LOG_STATE_PATH (if specified) take precedence. That is, the SDK ignores the log path specified in the FP_LOGPATH environment variable.

Note: To avoid any confusion, it is recommended to verify that the FPLogState.cfg file is not present in the working directory. Table 14 lists the required environment variables.

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Recommended value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FP_LOGPATH</td>
<td>Example: C:\mylog.txt</td>
<td>The full path and file name of the file to receive the log data and restart the application</td>
</tr>
</tbody>
</table>

The following are the steps to enable and collect SDK logging using enterprise variables:

1. Create the FP_LOGPATH environment variable with the valid path.
2. Restart the Enterprise Vault server.
3. Reproduce the issue.
4. Remove the environment variable.
5. Restart the application.

Once the SDK log file is collected, it must be sent to EMC Customer Support for analysis.

Additional information on available logging mechanisms and environment variables is available in the EMC Centera SDK V3.2 API Reference Guide.

Application Registration

Application Registration is an automated collection of application information. This information provides instant data for all applications connected to the EMC Centera. Information includes application make, version, hostname, hardware version, operating system, profile used to connect, SDK version, date of first connect, date of most recent connection, and number of successful connections OS.

Audit logging (syslog)

Audit logging provides audit trail security information for all management actions. These actions include:

- Changes made with Centera Viewer (CV), Centera CLI, Management API (MaPi), and Centera Platform commands
- Failed and successful management logins
- Failed and successful SDK logins
All management actions that result in a configuration change

Audit logs are stored safely in a system pool on the EMC Centera called AuditArchive. Each log entry can be sent out through the syslog industry-standard logging protocol through UDP port 514. The administrator can define how long this log information is kept before it is automatically purged. A human readable audit trail is available via the CV/CLI and via a syslog interface.

Alerts

EMC Centera actively monitors its health, capacity, and performance using sensors. Each sensor has a value that it periodically records by monitoring EMC Centera hardware and software components such as nodes, disks, replication queues, and so on. Fixed rules and thresholds are defined that decide if and when an alert has to be generated. An alert is a message with information on the cluster's state to notify the system administrator and EMC using SMTP and SNMP of a potential problem.

EMC Celerra troubleshooting considerations

Activity log

Celerra records events on actions on a FLR file system that pertain to successful changes or attempts to change protected data on the file system. The activity log records the user, time of event, and the type of action taken against files on an FLR file system.

The activity log has a fixed naming convention, flr.log [timestamp], and is stored in the root directory of each FLR file system. The FLR log has a maximum size limit of 10 MB. Logs that meet the limit are converted to a protected file, and subsequent events are written to another file with the same naming convention. A converted log file is set with the longest retention period that exists for the files referred to in this particular activity log.

The administrator is responsible for deleting old log files. If there is insufficient space in the file system to update the activity log, the operations are not allowed to proceed and warnings are logged in the Data Mover server log, the sys_log, and posted as an alert to the administrator.

Server log

Celerra records events on actions on the Data Mover. The log can be retrieved from the Control Station. Data Mover events are organized chronologically and prefaced by which facility performed the operation. In particular, an administrator may be interested in looking at events pertaining to FLR activity performed on a particular file system. For FLR activity, look for events that start with FLR at the beginning of the log entry. The server log is a file of set size; therefore older entries will be overwritten as space is required for newer events to be recorded. Unlike the activity log, the older entries are not protected from deletion.
Chapter 7 Conclusion

With all of its storage platforms archive capable, whether your need is a multi-purpose storage solution or a pure archive, EMC has the solution for your use with Symantec Enterprise Vault.

EMC Celerra provides the system flexibility, performance, high availability, ease of use, and advance protection to make it the ideal storage platform for the entire lifecycle of your emails and files. As your primary information store, archive or both, Celerra’s robust features, automated storage tiering and file level retention capabilities provide the right level of information protection, at the right cost whether emails and files are newly created or archived.

Maintaining its factory defaults, EMC Centera provides a quick and simple storage configuration requiring only a custom pool/profile setup to exactly match Enterprise Vault access, and security requirements. This, combined with Enterprise Vault’s convenient wizard-like graphical user interface to easily fine-tune the behavior and performance of the archive policy engine when archiving to EMC Centera, makes the joint Symantec/EMC offering an almost “turn-key” alternative for email and other unstructured data type archiving.

Given the robustness, flexibility, and maturity of the solution, it is not the installation and configuration of the Enterprise Vault and EMC Centera or EMC Celerra that is most critical to the successful implementation of archiving initiatives in the enterprise, but rather the careful planning and design of the architecture. This initial phase must be driven by a clear understanding of the short-, mid-, and long-term stakeholder’s needs, wants, and expectations, along with environmental and organizational constraints.

Together, Enterprise Vault and EMC Centera or EMC Celerra can comfortably scale to satisfy the most demanding and challenging of the environments, as benchmarks and existing deployments alike have proven over time. At the same time, the solutions provide a secure yet simple framework for companies to achieve increased operational efficiencies by dramatically reducing the size of email stores and optimizing storage utilization in the face of data growth and longer retention periods. Furthermore, the offerings enable companies to obtain risk mitigation associated with growing regulatory and corporate governance requirements for data permanence, security, and confidentiality, and to maintain assured authenticity and easy accessibility to archived records.
This appendix presents these topics:

Enterprise Vault service level agreement (SLA) .......................................................... 132
Performance benchmarks............................................................................................... 132
The performance of Enterprise Vault with EMC storage has been extensively tested both at Symantec performance test laboratories and at EMC performance test laboratories.

The conclusion of the testing is that EMC storage is very scalable and well suited to large enterprises.

Enterprise Vault service level agreement (SLA)

Table 15 lists Symantec’s expected throughput for different numbers of physical CPUs per server, having an average message size of 70 KB, including attachments.

<table>
<thead>
<tr>
<th>Number of CPUs</th>
<th>Hourly ingest rate (70 KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>25,000</td>
</tr>
<tr>
<td>4 single or 2 dual processors</td>
<td>40,000</td>
</tr>
<tr>
<td>2 quad-core processors</td>
<td>60,000</td>
</tr>
</tbody>
</table>

The average size of mail messages has an effect on the throughput. The observed effect is that when the average message size is doubled, throughput is reduced by one-third.

Performance benchmarks

A series of joint performance and stress tests have been conducted by Symantec and EMC in order to verify that the joint solution meets the Enterprise Vault Service level agreements.

Archival (tasks including file system archiving, journal email archiving, regular email archiving, and the migration of PST files), retrieval, and storage expiry, as well as exception tasks such as AltaVista re-indexing and application isolated stress tests, have been covered, showing that the performance is mostly limited by the number of Enterprise Vault servers available for testing. EMC storage absolute maximum is much higher than the rates observed, but it is not possible to speculate what this may be. The following table shows the results from the latest tests, for which dual-processor computers hosted the Enterprise Vault servers.
Table 16  Performance and stress test results

<table>
<thead>
<tr>
<th>Enterprise Vault task</th>
<th>Enterprise Vault SLA</th>
<th>EMC Centera benchmark</th>
<th>Delta</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Normal Tests</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email archiving (msg/hour)</td>
<td>40,000</td>
<td>50,000</td>
<td>25%</td>
</tr>
<tr>
<td>Journal archiving (msg/hour)</td>
<td>40,000</td>
<td>40,000</td>
<td>0%</td>
</tr>
<tr>
<td>Journal and archive (msg/hour)</td>
<td>N/A</td>
<td>48,000</td>
<td>N/A</td>
</tr>
<tr>
<td>File System Archive</td>
<td>40,000</td>
<td>47,000</td>
<td>17%</td>
</tr>
<tr>
<td>PST migrations</td>
<td>40,000</td>
<td>56,000</td>
<td>40%</td>
</tr>
<tr>
<td>Online viewing</td>
<td>40,000</td>
<td>100,000</td>
<td>150%</td>
</tr>
<tr>
<td>PST exports</td>
<td>30,000</td>
<td>50,000</td>
<td>60%</td>
</tr>
<tr>
<td>Storage Expire</td>
<td>100,000</td>
<td>160,000</td>
<td>60%</td>
</tr>
<tr>
<td>Re-indexing</td>
<td>100,000</td>
<td>100,000</td>
<td>0%</td>
</tr>
<tr>
<td><strong>Stress Tests</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Vault Storage API</td>
<td>N/A</td>
<td>1,000,000</td>
<td>N/A</td>
</tr>
</tbody>
</table>

In this test, a business use case to be able to archive and back up the content from 50,000 mailboxes, each of them having 20 messages eligible for archive was proposed; this translated to 1 million messages to be archived on a daily archiving window timeframe.

The testing proved that enterprises using Enterprise Vault and EMC Centera as a joint email archiving solution will be able to comfortably archive 50,000 user mailboxes in less than three hours (8 Enterprise Vault servers used); further savings on the operational overhead required for unnecessary backup of the archive was reinforced, as replication was implemented. In the case of extraordinary events that force the execution of both journal archiving and email archiving simultaneously, customers will be able to do so in less than 4 hours.

**Note:** The best practices mentioned in this paper were followed.

Over the years, these benchmarks have demonstrated repeatedly that the combination of Enterprise Vault as the enterprise archive engine along with EMC storage as the archive repository meets or exceeds such SLAs and provides a resilient infrastructure against failures in either component of the solution.
This appendix presents this topic:

Terminology ................................................................................................................................ . 136
### Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Profile</strong></td>
<td>Access profiles are used by applications and users of management tools to authenticate to a cluster, and by clusters to authenticate to another cluster for replication or restore connections. System administrators can create access profiles using the CLI. Each access profile consists of a profile name, a secret (password), and a set of capabilities and roles.</td>
</tr>
<tr>
<td><strong>Automatic Volume Management (AVM)</strong></td>
<td>A feature of the Celerra Network Server that creates and manages volumes automatically without manual volume management by an administrator. AVM organizes volumes into storage pools that can be allocated to file systems.</td>
</tr>
<tr>
<td><strong>BLOB</strong></td>
<td>A BLOB is a series of bytes that represents a fixed content object stored in EMC Centera. The format and structure of the BLOB are wholly owned by the client application, and neither the SDK nor the cluster attempts to interpret the binary object.</td>
</tr>
<tr>
<td><strong>Building block</strong></td>
<td>Represents the required amount of resources required to support a specific number of Exchange 2007 users on a single VM. The amount of required resources is derived from a specific user profile type.</td>
</tr>
<tr>
<td><strong>Call detail record (CDR)</strong></td>
<td>CDR is the computer record produced by a telephone exchange containing details of a call that passed through it. It is the automated equivalent of the paper toll tickets that were written and timed by operators for long-distance calls in a manual telephone exchange.</td>
</tr>
<tr>
<td><strong>C-Clip (Clip)</strong></td>
<td>A C-Clip is an application object that represents a bundle of fixed content data and metadata.</td>
</tr>
<tr>
<td><strong>C-Clip Descriptor File (CDF)</strong></td>
<td>The C-Clip Descriptor File (CDF) is the physical object stored to the cluster that represents an application-defined C-Clip. The CDF contains all of the metadata specified by the client application, and the links to all associated BLOBs. The CDF-to-BLOB relationship can have a cardinality of one-to-one, one-to-many, or many-to-many.</td>
</tr>
<tr>
<td><strong>Centera API / Centera SDK</strong></td>
<td>The EMC Centera SDK is a set of cross-platform application programming interfaces (API) that make it simple for customer applications to perform functions such as store, retrieve, delete, and query for data objects in a variety of flexible and powerful ways. All applications must use this API to read and write to EMC Centera.</td>
</tr>
<tr>
<td><strong>Centera Capabilities</strong></td>
<td>Pool-bound content access rights granted by the system administrator to an access profile. They determine which operations an application can perform on the pool data. Possible capabilities are write (w), read (r), delete (d), exist (e), privileged delete (D), query (q), clip copy (c), Purge (p), and Litigation hold (h).</td>
</tr>
<tr>
<td><strong>Centera CLI</strong></td>
<td>The EMC Centera Command Line Interface (CLI) is a tool for system administrators to manage and monitor EMC Centera.</td>
</tr>
<tr>
<td><strong>Centera Cluster</strong></td>
<td>A cluster is a single logical CAS archive that is accessible to an SDK-based client application. Client applications can store, retrieve, and delete fixed content objects from a cluster. A single cluster can be accessed by one or more applications via a set of node IP addresses and access profiles. Clustered nodes are automatically aware of nodes that attach to and detach from the cluster.</td>
</tr>
<tr>
<td><strong>Centera Independent Software Vendor (ISV)</strong></td>
<td>Independent software vendor (ISV) is a business term for companies specializing in making or selling software, usually for vertical markets, such as medical imaging or email archiving. An ISV makes and sells software products that run on one or more computer hardware or operating system platforms. In this case, an EMC Centera ISV is a software company that integrates its archiving solution to EMC Centera.</td>
</tr>
<tr>
<td><strong>Centera Partner/ISV</strong></td>
<td>An EMC Centera partner is an independent software vendor (ISV) that integrates to EMC Centera. These two terms are used interchangeably throughout this paper.</td>
</tr>
<tr>
<td><strong>Centera Software Development Kit (SDK)</strong></td>
<td>The EMC Centera SDK is a set of cross-platform application programming interfaces (API) that make it simple for customer applications to perform functions such as store, retrieve, delete, and query for data objects in a variety of flexible and powerful ways. All applications must use this API to read and write to EMC Centera.</td>
</tr>
<tr>
<td><strong>CentraStar</strong></td>
<td>EMC firmware used by EMC Centera.</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Checkpoint</strong></td>
<td>A read-only, logical, point-in-time image of a file system (PFS). A</td>
</tr>
<tr>
<td></td>
<td>checkpoint is sometimes referred to as a checkpoint file system, a</td>
</tr>
<tr>
<td></td>
<td>snap, or a SnapSure™ file system.</td>
</tr>
<tr>
<td><strong>Cluster Mask</strong></td>
<td>Defines the EMC Centera capabilities that access profiles can enable.</td>
</tr>
<tr>
<td></td>
<td>At the cluster level, the cluster (authorization) mask is used to</td>
</tr>
<tr>
<td></td>
<td>override other profiles.</td>
</tr>
<tr>
<td><strong>Content Address</strong></td>
<td>A data object’s unique identifier. A Content Address is the claim</td>
</tr>
<tr>
<td></td>
<td>ticket that is returned to the client application when an object is</td>
</tr>
<tr>
<td></td>
<td>stored to the archive.</td>
</tr>
<tr>
<td>**Data Access in Real</td>
<td>On a Celerra system, the operating system software that runs on the</td>
</tr>
<tr>
<td>Time (DART)</td>
<td>Data Mover. It is a real-time, multithreaded operating system</td>
</tr>
<tr>
<td></td>
<td>optimized for file access, while providing service for standard</td>
</tr>
<tr>
<td></td>
<td>protocols.</td>
</tr>
<tr>
<td><strong>Data Mover</strong></td>
<td>A Celerra Network Server cabinet component running its own operating</td>
</tr>
<tr>
<td></td>
<td>system that retrieves files from a storage device and makes them</td>
</tr>
<tr>
<td></td>
<td>available to a network client. This is also referred to as a blade.</td>
</tr>
<tr>
<td></td>
<td>A Data Mover is sometimes internally referred to as “DART” because</td>
</tr>
<tr>
<td></td>
<td>DART is the software running on the platform.</td>
</tr>
<tr>
<td>**Destination File</td>
<td>A destination object that is of the file system type.</td>
</tr>
<tr>
<td>System (DFS)</td>
<td></td>
</tr>
<tr>
<td>**Destination Object</td>
<td>The target (possibly remote) Celerra Network Server object in a</td>
</tr>
<tr>
<td>(DO)</td>
<td>Celerra Replicator (V2) session. It may be a file system, VDM, or iSCSI</td>
</tr>
<tr>
<td></td>
<td>LUN depending upon the type of the source object. The destination</td>
</tr>
<tr>
<td></td>
<td>object is typically the “standby” side of a disaster recovery</td>
</tr>
<tr>
<td></td>
<td>configuration.</td>
</tr>
<tr>
<td>**File System archiving</td>
<td>FSA manages rapidly growing data such as office documents, web pages,</td>
</tr>
<tr>
<td>(FSA)</td>
<td>images, and audio and video files by automatically migrating inactive</td>
</tr>
<tr>
<td></td>
<td>data to more cost-effective, self-managed archive storage. The result</td>
</tr>
<tr>
<td></td>
<td>is improved productivity and compliance, plus faster, more reliable</td>
</tr>
<tr>
<td></td>
<td>recovery.</td>
</tr>
<tr>
<td><strong>Initialization</strong></td>
<td>The process of performing a full copy from a point-in-time view of</td>
</tr>
<tr>
<td></td>
<td>the production object to the destination object. This full copy,</td>
</tr>
<tr>
<td></td>
<td>sometimes referred to as “silvering,” enables Celerra Replicator to</td>
</tr>
<tr>
<td></td>
<td>keep the destination object within the RPO by performing subsequent</td>
</tr>
<tr>
<td></td>
<td>differential copies as needed.</td>
</tr>
<tr>
<td><strong>Metadata</strong></td>
<td>Data about data. Metadata is information about an informational</td>
</tr>
<tr>
<td></td>
<td>resource, be that a document (such as a webpage), image, dataset, or</td>
</tr>
<tr>
<td></td>
<td>other resource. Metadata is valuable in the storage and retrieval of</td>
</tr>
<tr>
<td></td>
<td>information. Resources supported by good quality, structured</td>
</tr>
<tr>
<td></td>
<td>metadata are more easily discoverable.</td>
</tr>
<tr>
<td>**MS Exchange Solution</td>
<td>The ESRP - Storage program was developed by Microsoft Corporation to</td>
</tr>
<tr>
<td>Reviewed Program (ESRP)</td>
<td>provide a common storage testing framework for storage vendors to</td>
</tr>
<tr>
<td></td>
<td>provide information on their storage solutions for Microsoft</td>
</tr>
<tr>
<td></td>
<td>Exchange Server.</td>
</tr>
<tr>
<td><strong>Node</strong></td>
<td>Logically, a network entity that is uniquely identified through a</td>
</tr>
<tr>
<td></td>
<td>system ID, IP address, and port. Physically, a node is a computer</td>
</tr>
<tr>
<td></td>
<td>system that is part of the EMC Centera cluster.</td>
</tr>
<tr>
<td><strong>Node Role</strong></td>
<td>The roles that can be assigned to each individual node are either</td>
</tr>
<tr>
<td></td>
<td>external or internal. Nodes with an external node role have an</td>
</tr>
<tr>
<td></td>
<td>external IP address configured and use their Eth2 port for</td>
</tr>
<tr>
<td></td>
<td>communication with the customer’s network; external roles are access,</td>
</tr>
<tr>
<td></td>
<td>management, and replication. Storage role is the only internal role.</td>
</tr>
<tr>
<td></td>
<td>Refer to the online help for additional information.</td>
</tr>
<tr>
<td><strong>Pool Mask</strong></td>
<td>Defines the EMC Centera capabilities granted to a particular virtual</td>
</tr>
<tr>
<td></td>
<td>pool.</td>
</tr>
<tr>
<td><strong>Production Archive</strong></td>
<td>Production Archives is a term that customers have dubbed for the use</td>
</tr>
<tr>
<td></td>
<td>of an archive as an extension of primary storage.</td>
</tr>
<tr>
<td>**Production File</td>
<td>A production object that is of the file system type.</td>
</tr>
<tr>
<td>System, or Primary File</td>
<td></td>
</tr>
<tr>
<td>System (PFS)</td>
<td></td>
</tr>
<tr>
<td>**Production Logical</td>
<td>An iSCSI LUN that serves as a primary (production) storage device. A</td>
</tr>
<tr>
<td>Unit, or Production</td>
<td>PLU can be configured as a disk device through an iSCSI initiator.</td>
</tr>
<tr>
<td>LUN (PLU)</td>
<td></td>
</tr>
<tr>
<td>**Production Object,</td>
<td>A Celerra object where production data is stored and the source</td>
</tr>
<tr>
<td>or Primary Object (PO)</td>
<td>object in a replication session. It may be a file system, VDM, or</td>
</tr>
<tr>
<td></td>
<td>iSCSI LUN.</td>
</tr>
<tr>
<td>**Recovery Point</td>
<td>The amount of data, measured in units of time, which may be lost in</td>
</tr>
<tr>
<td>Objective (RPO)</td>
<td>a failure. This value represents a target, and it may be influenced</td>
</tr>
<tr>
<td></td>
<td>by the RTO, SLA, and business impact analysis.</td>
</tr>
<tr>
<td><strong>Recovery Time Objective (RTO)</strong></td>
<td>The length of time a business process can be unavailable before the consequences are unacceptable. This value represents a target and is typically the result of a business impact analysis.</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Refresh</strong></td>
<td>A checkpoint operation that discards the checkpoint’s previous point-in-time view and replaces it with the current point-in-time view of the PFS. In the context of Celerra Replicator (V2), it also includes a subsequent transmission of the data that changed since the last refresh operation.</td>
</tr>
<tr>
<td><strong>Replica</strong></td>
<td>An exact point-in-time copy of a production object.</td>
</tr>
<tr>
<td><strong>SDK backward compatibility</strong></td>
<td>In technology, especially computing (irrespective of platform), a product is said to be backward-compatible when it is able to take the place of an older product, by interoperating with products that were designed for the older product versions. In this particular case, it refers to the compatibility between older SDK versions and newer CentraStar versions.</td>
</tr>
<tr>
<td><strong>SDK binary compatibility</strong></td>
<td>The use of a stable application binary interface (ABI) – the low-level interface between an application program and its libraries, or that between component parts of an application – that enables partners to dynamically replace older SDK versions with newer ones without having to recompile their application.</td>
</tr>
<tr>
<td><strong>SDK forward compatibility</strong></td>
<td>Forward compatibility is the ability of a system to gracefully accept input intended for later versions of itself. In this particular case, it refers to the compatibility between newer SDK versions and older CentraStar versions. <strong>NOTE:</strong> The <em>EMC Centera CentraStar and SDK Release and Interoperability Matrix</em> has additional information.</td>
</tr>
<tr>
<td><strong>Secondary File System (SFS)</strong></td>
<td>See Destination File System. This term was used in Celerra Replicator V1, and is now deprecated.</td>
</tr>
<tr>
<td><strong>Service Level Agreement (SLA)</strong></td>
<td>A contract or agreement that formally defines the level of service expected or required along various lines of attributes. It may include the maximum acceptable downtime and the maximum acceptable disaster recovery parameters (RTO and RPO).</td>
</tr>
<tr>
<td><strong>Snapshot</strong></td>
<td>A generic term for a point-in-time copy of data. In Celerra, a point in time of an iSCSI LUN is called a snap or snapshot, and a point-in-time copy of a file system is typically called a checkpoint although the generic term of snap or snapshot can also be used.</td>
</tr>
<tr>
<td><strong>SnapSure</strong></td>
<td>A feature that provides read-only point-in-time views, known as checkpoints, of a PFS.</td>
</tr>
<tr>
<td><strong>SnapSure for iSCSI</strong></td>
<td>A feature that provides read-only point-in-time views, known as snapshots, of an iSCSI PLU.</td>
</tr>
<tr>
<td><strong>SnapSure SavVol</strong></td>
<td>As used in SnapSure Checkpoints and Celerra Replicator (V2), a Celerra volume to which SnapSure copies original point-in-time data blocks from the PFS before the blocks are altered by a transaction. SnapSure uses the contents of the SavVol and the unchanged PFS blocks to maintain a checkpoint of the PFS. As used in Celerra Replicator (V1), it is a Celerra volume, required by replication, used to store modified data blocks from the source file system. A dedicated replication SavVol is no longer used with Celerra Replicator (V2) which uses the SnapSure checkpoint SavVol.</td>
</tr>
<tr>
<td><strong>Source Object</strong></td>
<td>See Production Object.</td>
</tr>
<tr>
<td><strong>TCO</strong></td>
<td>Total cost of ownership (TCO) is a financial estimate. Its purpose is to help enterprise managers determine direct and indirect costs of a product or system.</td>
</tr>
<tr>
<td><strong>Virtual Data Mover (VDM)</strong></td>
<td>A Celerra software feature enabling users to administratively separate CIFS servers, replicate their CIFS environments, and move servers from Data Mover to Data Mover.</td>
</tr>
<tr>
<td><strong>WORM</strong></td>
<td>WORM (write once, read many) is a data storage technology that allows information to be written to a disc a single time and prevents the drive from erasing the data. The discs are intentionally not rewritable, because they are especially intended to store data that the user does not want to erase accidentally. Because of this feature, WORM devices have long been used for the archival purposes.</td>
</tr>
</tbody>
</table>