CONTENTS

Preface

Chapter 1  Solution Overview

  Executive summary................................................................. 11
  About replication technology.................................................. 12
  Supported products.................................................................... 12
  Key components....................................................................... 12
  SourceOne architecture.......................................................... 13
  Product overview...................................................................... 14
  Data sources............................................................................ 14
  SourceOne services.................................................................. 15
  Native Archive host computers.............................................. 15
  Native Archive storage............................................................ 15
  SQL Server and databases....................................................... 17
  Applications............................................................................ 17

Chapter 2  Solution Configuration Details

  Hot/cold disaster recovery architecture example.......................... 20
  Hot/warm disaster recovery architecture example........................... 20
  Considerations......................................................................... 21
  Component disaster recovery configuration................................... 22
  Console application.................................................................... 22
  Messaging environment............................................................ 22
  Microsoft SharePoint environment.......................................... 24
  File system environment.......................................................... 25
  Master computer....................................................................... 25
  Worker computer..................................................................... 26
  Web server............................................................................... 27
  SQL Server and databases....................................................... 28
  SourceOne Native Archive host computer................................... 29
  Native Archive-Message Center storage.................................... 30
  Native Archive-Index storage.................................................. 30
  Native Archive-Container storage............................................ 30
  File server host or NAS device configuration............................ 34
  Centera.................................................................................. 34

Chapter 3  Failover to the Disaster Recovery site

  Failover procedures..................................................................... 35
  Stopping SourceOne processing at the disaster recovery site........ 36
  Checking that replicated data is accessible.................................. 36
  Verifying the disk health of file servers..................................... 36
  Performing Active Directory changes for SQL and file servers....... 37
  Ensuring dependent systems are online and accessible................ 37
  Recovering the DiskXtender configuration.................................. 37
  Powering on SourceOne computers (hot/cold configuration only)... 40
Ensuring the SourceOne computers can access key resources...... 41
Running the SourceOne Archive Integrity Tool...............................41
Starting SourceOne services..........................................................41
Performing reprocessing............................................................... 42
Rerunning the SourceOne Archive Integrity Tool...........................43
Verifying SourceOne operations.................................................... 43
(Optional) Running the Microsoft SharePoint EBS integrity tool...44

Failback to the Primary Site 45
Failback procedures....................................................................................46
Stopping SourceOne processing at the disaster recovery site......46
Ensure the exported DiskXtender Registry keys are available(Optional) ..........................................................46
Copy data back to the primary site..........................................................46
Re-establishing disaster recovery configuration for SourceOne computers....................................................................................46
Creating a gold copy of replicated data.............................................47
Enabling storage devices at the primary site...........................................47
Performing Active Directory changes for SQL and file servers...... 47
Ensuring dependent systems are online and accessible.....................47
Recovering the DiskXtender configuration........................................ 47
Starting SourceOne services..............................................................47
Verifying that primary site is replicating to the disaster recovery site .......................................................................................................51
Verifying SourceOne operations.........................................................51

Appendix A
SourceOne Archive Integrity Tool Operations 53
Overview.................................................................................................... 54
Command line description........................................................................ 54
Syntax.................................................................................................. 54
Required parameters......................................................................... 55
Optional parameters......................................................................... 56
Examples.......................................................................................... 57
Permissions.......................................................................................... 57
Sequence of operations........................................................................ 57
Parsing command line options.......................................................... 57
Adding volumes to the candidate volume set......................................57
Adding objects found to the candidate object set.............................58
Adding full-text indexes found to the candidate index set.................59
Removing objects from SQL...............................................................59
Verifying operations............................................................................ 59
Query and display results................................................................. 59
Query and retrieve results................................................................. 60
Log file viewing.................................................................................. 60

Appendix B
SourceOne EBS Integrity Tool Operations 61
Overview............................................................................................. 62
Recovery scenarios.............................................................................. 62
BLOB records missing from EBS database, BLOBs exist in Native Archive.......................................................... 62
BLOBs missing from Native Archive, BLOB records exist in EBS database.......................................................... 62
BLOBs missing from Native Archive and EBS database................. 63
Using the EBS Integrity Tool............................................................... 63
Launching the tool................................................................. 63
Reviewing scan results....................................................... 63
Recovering BLOBs.............................................................. 64
Logging................................................................................. 65

Glossary 67
As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC technical support professional if a product does not function correctly or does not function as described in this document.

**Note**

This document was accurate at publication time. Go to EMC Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

**Purpose**

This document describes how to implement a disaster recovery configuration for supported EMC SourceOne products.

**Audience**

This manual is intended for the person implementing the disaster recovery solution and executing the recovery procedures. The person must have good knowledge of EMC SourceOne products, EMC DiskXtender (if used), Microsoft SQL Server, storage and replication technology and practices.

**Revision history**

The following table presents the revision history of this document.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>02</td>
<td>July 31, 2017</td>
<td>Updated technical content.</td>
</tr>
<tr>
<td>01</td>
<td>April 30, 2015</td>
<td>First release of the EMC SourceOne 7.2 Disaster Recovery Solutions Guide.</td>
</tr>
</tbody>
</table>

**Related documentation**

The SourceOne documentation set includes the following publications.

SourceOne Products:
- *SourceOne Products Compatibility Guide*
- *SourceOne Products Security Configuration Guide*

SourceOne Email Management:
- *SourceOne Email Management Installation Guide*
- *SourceOne Email Management Administration Guide*
- *SourceOne Email Management Release Notes*
- *SourceOne Email Management Localized Product Release Notes*
- *SourceOne Auditing and Reporting Installation and Administration Guide*
• SourceOne Management Pack for Microsoft System Center Operations Manager Guide
• SourceOne Search User Guide
• SourceOne Disaster Recovery Solution Guide
• SourceOne 7.0 and later SNMP Trap Monitoring Solution Technical Notes

SourceOne Discovery Manager:
• SourceOne Discovery Manager Installation and Administration Guide
• SourceOne Discovery Manager Desktop User Guide
• SourceOne Discovery Manager Web Application User Guide
• SourceOne Discovery Manager Release Notes
• SourceOne Discovery Manager Localized Product Release Notes
• SourceOne Discovery Manager Desktop Quick Reference Cards

SourceOne for File Systems:
• SourceOne for File Systems Installation Guide
• SourceOne for File Systems Administration Guide
• SourceOne for File Systems Release Notes

SourceOne Offline Access:
• SourceOne Offline Access Installation and Administration Guide
• SourceOne Offline Access User Guide
• SourceOne Offline Access Release Notes

SourceOne Archiving for Microsoft SharePoint:
• SourceOne Archiving for Microsoft SharePoint Installation Guide
• SourceOne Archiving for Microsoft SharePoint Administration Guide
• SourceOne Archiving for Microsoft SharePoint Release Notes
• SourceOne Archiving for Microsoft SharePoint Archive Search Quick Reference Card

SourceOne for Microsoft SharePoint Storage Management:
• SourceOne for Microsoft SharePoint Storage Management Installation Guide
• SourceOne for Microsoft SharePoint Storage Management Administration Guide
• SourceOne for Microsoft SharePoint Storage Management Release Notes

SourceOne Email Supervisor:
• SourceOne Email Supervisor Installation Guide
• SourceOne Email Supervisor Administration Guide
• SourceOne Email Supervisor Web Application (Reviewer and Reports) Guide
• SourceOne Email Supervisor Release Notes

Special notice conventions that are used in this document
EMC uses the following conventions for special notices:

NOTICE
Identifies content that warns of potential business or data loss.
Note
Contains information that is incidental, but not essential, to the topic.

Typographical conventions
EMC uses the following type style conventions in this document:

Table 2 Style conventions

<table>
<thead>
<tr>
<th>Style</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bold</td>
<td>Used for names of interface elements, such as names of buttons, fields, tab names, and menu paths (what the user specifically selects or clicks)</td>
</tr>
<tr>
<td>Italic</td>
<td>Used for full titles of publications that are referenced in text</td>
</tr>
<tr>
<td>Monospace</td>
<td>Used for:</td>
</tr>
<tr>
<td></td>
<td>• System code</td>
</tr>
<tr>
<td></td>
<td>• System output, such as an error message or script</td>
</tr>
<tr>
<td></td>
<td>• Pathnames, file names, prompts, and syntax</td>
</tr>
<tr>
<td></td>
<td>• Commands and options</td>
</tr>
<tr>
<td>Monospace italic</td>
<td>Used for variables</td>
</tr>
<tr>
<td>Monospace bold</td>
<td>Used for user input</td>
</tr>
<tr>
<td>[]</td>
<td>Square brackets enclose optional values</td>
</tr>
<tr>
<td></td>
<td>Vertical bar indicates alternate selections - the bar means “or”</td>
</tr>
<tr>
<td>{}</td>
<td>Braces enclose content that the user must specify, such as x or y or z</td>
</tr>
<tr>
<td>...</td>
<td>Ellipses indicate non-essential information that is omitted from the example</td>
</tr>
</tbody>
</table>

Where to get help
EMC support, product, and licensing information can be obtained as follows:

Product information
For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at https://support.emc.com.

Technical support
Go to EMC Online Support at https://support.emc.com, and click Service Center. Several options for contacting EMC Technical Support appear on the site. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Online communities
Go to the EMC Community Network at https://community.emc.com for peer contacts, conversations, and content on product support and solutions. Interactively engage online with customers, partners, and certified professionals for all EMC products.

Your comments
Your suggestions help to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to DPAD.Doc.Feedback@emc.com.
Preface
CHAPTER 1

Solution Overview

This document describes a reference implementation for a disaster recovery solution that supports SourceOne products that have been qualified with this solution.

This section contains the following topics:

- Executive summary.................................12
- SourceOne architecture.............................13
- Product overview........................................14
Executive summary

This document contains a detailed configuration for a SourceOne deployment that is configured to support disaster recovery. This information has the intent of providing a proven configuration for deployment of a disaster recovery environment.

The information in this document is framed in a timeline-based structure as seen in this section.

1. Procedures to plan and implement the hardware, software, and configuration settings to support disaster recovery.

2. The actions that you must take to fail over to a secondary site following a disaster.

3. The actions that you must take to return processing to the primary site after the disaster situation is resolved.

This document provides best practices for setting up a manageable disaster recovery solution, without specific regard to the replication technology. The assumption is that a consistent replication scenario is established and that with the assistance of utilities and best practices that are provided, the customer can recover from a failure in a reasonable timeframe with minimal data loss.

About replication technology

The solution that is documented in this guide is based on testing conducted using an array-based replication technology.

The use of an array-based solution as described in this document does not preclude the use of other replication technologies from or other vendors, (or even NAS, host-based, software, or backup solutions) to make the key data available at a secondary site.

Review the procedures and practices for configuring, failing over to a secondary site, and failing back to the original site. Although this information is framed in an array-based scenario, the focus of this document is not on how the data important to SourceOne is replicated and presented at the other site, but on how the data is used after a disaster scenario occurs. It is up to the implementation team to determine the specific means of making the data available at the disaster recovery site.

Supported products

This guide provides a disaster recovery solution for the following products.

- SourceOne Email Management (this product provides the core infrastructure that is required for all SourceOne products).
- SourceOne for Microsoft SharePoint.
- SourceOne for File Systems.

Key components

The key components that are considered in this solution include the following list:

- SourceOne computers (Master, Worker, and Native Archive servers).
- SourceOne data storage locations (file servers and storage devices).
- Microsoft SQL Server and databases.
- DiskXtender configuration (if used).
- Centera configuration (if used).
- Data source configuration:
  - Mail server configuration (SourceOne Email Management).
  - Microsoft SharePoint configuration (SourceOne for Microsoft SharePoint).
  - File system configuration (SourceOne for File Systems).

The information in this document has the intent to supplement other documentation and training material such as SourceOne product installation guides and other documents providing guidelines for various reference configurations. This document discusses the hardware configuration, software configuration, infrastructure, and the tools, and methods methods that are used to obtain the results. Where applicable, certain proven practices and other configuration settings are noted which affected the results.

SourceOne architecture

SourceOne is a distributed set of applications which can run on a single physical computer, or across many computers, as shown in the following figure.

**Figure 1  SourceOne architecture**
Product overview

SourceOne products provide an enterprise solution that you can use to reduce the space that is required for the email, Microsoft SharePoint servers, and file servers, and to aid in complying with legal requirements for archiving content and maintain efficient storage.

A high-level overview of components comprising the SourceOne system include the following.

- Data sources. Can include email, Microsoft SharePoint, and SourceOne for File Systems.
- SourceOne services. Includes Master, Worker, Native Archive, and Web Services computers.
- SQL Server and databases. Includes Microsoft SQL Server and SourceOne databases.
- Content archives and storage. Includes the Native Archive and associated storage locations that are used by SourceOne.
- Applications. Includes the console application that is used to administer SourceOne.

Data sources

SourceOne archives, retains, and organizes content from Microsoft Exchange, IBM Domino, SMTP mail servers, Microsoft SharePoint, and file servers. Archived content is stored in the SourceOne Native Archive, and administrators and users can search the content with permission.

SourceOne Email Management environments

SourceOne Email Management supports the archiving of messaging content to enable companies to meet storage management, compliance, and legal discovery requirements.

In Microsoft Exchange environments, SourceOne Email Management supports real-time archiving of messages from Exchange mail servers using native journaling functionality that is provided in Microsoft Exchange. You can also perform historical archiving and shortcutting of messages from Microsoft Exchange mailboxes and historical archiving of Outlook PST files.

In IBM Domino environments, SourceOne Email Management supports real-time archiving and shortcutting of messages from IBM Domino mail servers by installing SourceOne Domino Extensions on IBM Domino mail servers. You can also perform historical archiving and shortcutting of messages from IBM Domino mailboxes and Notes NSF files.

SourceOne for Microsoft SharePoint environments

SourceOne for Microsoft SharePoint addresses long-term or specialized content archiving strategies while leveraging the SourceOne architecture to provide access to archived content using search user interfaces.

SourceOne for File Systems environments

SourceOne for File Systems enables the organization to gain control over unmanaged information residing on file share systems. By archiving content from file servers across the organization, administrators and users can leverage content indexing and
search capabilities that are provided by SourceOne to support information governance, compliance discovery, and data protection.

SourceOne services

The SourceOne services software includes Master Services, Worker Services, Web Services, and Mobile Services software running on one or more computers.

The SourceOne services architecture is scalable, supporting the installation of all components on a single physical computer or allowing you to distribute them across multiple physical computers depending on the requirements of the environment.

Master computers

The SourceOne Master computer schedules and distributes jobs that are processed by Workers.

Worker computers

SourceOne Worker computers perform archiving activities from various data sources. Each Worker computer can be configured to process only specific activities.

- SourceOne Web Services. This software can be installed on one or more Worker Services computers to support underlying Web functions such as fielding search requests and performing shortcut resolution.
- SourceOne Mobile Services. This software provides Universal URL support for the following SourceOne Email Management users:
  - Mobile users.
  - Outlook Web Access users.
  - Outlook users who do not have the SourceOne Offline Access installed. For SourceOne for File Systems users, the Universal URL also supports resolution of links to files in the Native Archive which were archived from a file server.

Native Archive host computers

The SourceOne Native Archive software uses an architecture which can be configured to perform the roles that are listed in this section:

- Archive
- Index
- Search
- Retrieve

The SourceOne Native Archive software can be installed on a single host computer or multiple host computers, enabling you to dedicate hardware to specific roles (archive, index, search, and retrieve) to match the organization’s archiving policies.

Native Archive storage

Storage locations include the following list.

- Message Center storage.
- Index Area storage.
- Container file storage.
• Work (unpack area) storage.

Message Center storage
A location where content is stored and built into volumes before they are written to a container file.

Index Area storage
A location where full-text indexes are stored.

Container Storage
Location for long-term storage of containers. This section lists the supported storage containers.

Network-accessible storage
You can store containers directly on network-accessible storage, such as shareable drives or network-attached storage devices (NAS devices).

Direct storage on Centera
The SourceOne configuration may require the long-term storage of SourceOne container files on an Centera content-addressed storage (CAS) system.
SourceOne Email Management can directly access containers on Centera devices.

Storage on Centera using DiskXtender
If you have existing archive folders that are configured to store containers on Centera using DiskXtender, then you must continue to use this solution for those folders.
You can configure any new archive folders that you create to use direct storage on Centera.

Note
The scenario of using DiskXtender connected to other long-term storage such as optical devices or tape, while valid, is not considered for the purposes of this document. DiskXtender is only described as a means of connecting SourceOne to Centera.

Additional storage options
SourceOne Email Management versions 6.6 SP1 and later support direct storage on the following NAS devices.
• Celerra
• Data Domain
• NetApp
For details, refer to the SourceOne Email Management Administration Guide.

Work (unpack area) storage
A temporary location in which content ready for indexing is stored.

Microsoft SharePoint External BLOB storage
SourceOne for Microsoft SharePoint also provides External binary large object (BLOB) storage, offloading the storage of binary large objects from the Microsoft
SharePoint SQL Server and storing them using SourceOne. EBS is configured at the farm level.

This feature includes an EBS Provider database which is installed on the Microsoft SharePoint SQL Server to maintain identification information for BLOBs stored externally in the SourceOneNative Archive by SourceOne for Microsoft SharePoint.

EBS uses the SourceOneNative Archive to access storage. EBS content is not archived. EBS content is not subject to indexing, retention, or available for search using SourceOne Search. It is available for search using Microsoft SharePoint-side search interfaces.

**SQL Server and databases**

A database server running Microsoft SQL Server supports the following SourceOne databases.

- Activity database. This database maintains data that are associated with SourceOne system processing.
- Search database. This database maintains data that are associated with the SourceOne Search application.
- SourceOneNative Archive database. This database manages data that are associated with the SourceOne Native Archive.

**Applications**

The SourceOne console enables administrators to configure and manage the product. User applications include SourceOne Search and SourceOne Offline Access.
CHAPTER 2

Solution Configuration Details

The components which comprise the SourceOne environment are described in the previous section. This section expands on this configuration to include the addition of a second site which provides a supportable disaster recovery configuration.

This section contains the following topics:

- Hot/cold disaster recovery architecture example ............................................. 20
- Hot/warm disaster recovery architecture example ............................................ 20
- Component disaster recovery configuration ....................................................... 22
Hot/cold disaster recovery architecture example

The following figure depicts an SourceOne Email Management scenario which uses array-based replication for SourceOne data and SQL databases, vendor-recommended replication for the mail environment, and Centera replication. In this configuration, a subset of systems at the secondary site are not active.

Note

Although the mail server in the following figure appears as active at both sites, its status depends on the specific disaster recovery configuration used.

Hot/warm disaster recovery architecture example

The hot/warm configuration is similar to the hot/cold configuration in terms of replication. However, SourceOne Native Archive computers and Workers are active at the secondary site to provide additional processing capabilities in support of the primary site over the WAN.

This is termed a hot/warm configuration because some failover steps must be performed to make the secondary site fully operational. Differences in the configuration, failover, and failback steps for hot/warm and hot/cold architectures are elaborated throughout this document.

The following figure describes the Disaster Recovery hot/warm configuration...
Considerations

Specific best practices for using Workers and SourceOneNative Archive computers at the disaster recovery site in a hot/warm configuration.

- During operation, you can limit the roles on the secondary SourceOne Native Archive and Worker computers to ones which would generate the least WAN traffic. The SourceOne console application configures the roles.
- Deciding whether to limit certain processing on computers at the disaster recovery site depends on the speed and technology that is used for the WAN. A larger WAN “pipe” may accommodate the large amount of traffic that is generated by certain SourceOne activities while a WAN connection with limited bandwidth cannot.
- Examples of activities that you may want to limit from processing across the WAN include indexing, journaling, and large-scale historical archiving activities.
- Examples of activities which can be processed across the WAN include search and limited historical archiving activities.

**Note**

To determine the best configuration for a hot/warm configuration is up to the implementation team, as dependencies and considerations exist which must be evaluated on a site-specific basis.

Disaster recovery of the mail system environment itself is beyond the scope of this document.
Although the mail server in Figure 3 appears as active at both sites, its status depends on the specific disaster recovery configuration used.

Disaster recovery of the Microsoft SharePoint or SourceOne for File Systems is beyond the scope of this document.

Though not depicted in the preceding diagrams, SourceOne for Microsoft SharePoint and SourceOne for File Systems installations use the same underlying structure (for example, Master computer, Worker computers, Native Archive computers, SQL Server and databases, and data storage).

### Component disaster recovery configuration

The following sections provide details about the disaster recovery configuration for each component in the SourceOne environment.

#### Console application

The SourceOne console enables administrators to configure and manage the product.

**Disaster recovery configuration**

Install the console application on at least one computer with access to other computers at the disaster recovery site.

If you use the Microsoft SharePoint or SourceOne for File Systems products, you must also install the corresponding Business Component Extensions (BCE) software:

- SourceOne Business Component Extensions (BCE) for Microsoft SharePoint
- SourceOne Business Component Extensions (BCE) for SourceOne for File Systems

#### Messaging environment

The messaging systems that are supported by SourceOne Email Management consist of one or more Microsoft Exchange or IBM Domino servers.

**Disaster recovery configuration**

This document assumes that the site has employed a solution that is recommended by the mail system vendor for replicating the mail system and data. If a failover to the disaster recovery site is necessary, it is assumed that the mail system can be brought back online and be made accessible to the SourceOne system at the disaster recovery site so that processing can resume.

The benefit of replicating the messaging environment is the ability to run additional archiving tasks at the disaster recovery site after a failover. This improves the recovery point objective (RPO) for the SourceOne environment following a failover.
Note
For Exchange, install SourceOne Extensions for OWA software on Microsoft Exchange servers at the disaster recovery site. Maintain this system in concert with the primary Microsoft Exchange servers (for example, performing software upgrades, and patches of SourceOne software).
For IBM Domino, install SourceOne IBM Domino Extensions software on IBM Domino servers at the disaster recovery site. Maintain this system in concert with the primary IBM Domino servers. Ensure that the SourceOne system is connected to journaling databases in both the primary and disaster recovery sites. If a journaling database in an IBM Domino cluster switches to the disaster recovery site during normal operation, this ensures that the messages are still journaled.

SMTP mail considerations
SourceOne archives SMTP mail from a drop directory. If you configure SourceOne to archive messages directly from this location, and the computer hosting this location is one of the components that are involved in a disaster, those messages are subject to becoming permanently lost. To support a disaster recovery configuration, configure a mechanism that periodically copies the SMTP messages from one location to the location against which the archiving task is directed. Although this may result in some duplicate message processing, it provides a backup of the SMTP message data that can be recovered in a disaster.

Deleted retention/soft delete recommendations
Configure deleted item retention times in Microsoft Exchange, or soft delete retention times in IBM Domino, for a period that at least doubles the estimated RPO for failover and recovery for journal mailboxes or databases.
For example, if the expected RPO is one day, configure deleted retention (Microsoft Exchange) or soft deletes (IBM Domino) to occur for two days. This configuration ensures that the messages on the mail server can be "undeleted and replayed" to more accurately represent the mail server's state at the time of failover. This also furthers the goal of achieving an RPO with as close to zero data loss as possible.

Shortcutting policy recommendations
Configure the shortcutting policy to support disaster recovery. Configure shortcutting to occur at an interval to provide a short period for archived messages to be replicated before a shortcut is created. Set this period to several days that is slightly greater than the amount of time you would expect for the RPO.
For example, if you configure the system to archive messages older than 30 days and shortcut messages older than 32 days, this would provide at least 2 days for archived messages to be replicated before a shortcut is created.

Note
By default, the volume idle time before a volume closes to an archive container is two days. Generally, using a difference of two days or slightly more between archive and shortcut policies can help ensure that shortcuts are always pointing to closed volumes.

Consistency groups
You can replicate the messaging system components along with the other SourceOne components using a consistency group (or similar functionality supported by your replication solution). Replicating all SourceOne components as a group can normalize
the recovery time objective (RTO), minimize data lag, and simplify replication management.

**Replication timing**

If the use of a consistency group is not possible (for example, in cases where the messaging system replication is occurring on an already established or different replication technology), configure the replication timing to be the same or as close as possible as the replication timing configured for other SourceOne components. This furthers the goal of achieving an RPO with as close to zero data loss as possible.

**Microsoft SharePoint environment**

The systems that are supported by SourceOne for Microsoft SharePoint consist of one or more Microsoft SharePoint servers.

**Disaster recovery configuration**

This document assumes that the site has employed a solution that is recommended by Microsoft for replicating the Microsoft SharePoint system, databases, and data. If a failover to the disaster recovery site is necessary, it is assumed that Microsoft SharePoint environment can be brought back online and be made accessible to the SourceOne system at the disaster recovery site so that processing can resume.

**Best practice recommendations**

To minimize the chance of data loss, it is recommended that administrators that configure Microsoft SharePoint archiving activities observe the best practices that are described in this section.

When archiving content from a Microsoft SharePoint system with the intent of removing the content from Microsoft SharePoint, always configure two activities:

- Configure the first activity to copy the content from Microsoft SharePoint to the archive using the “Copy items to archive” Archive Action. After archiving, the content will exist in both the archive and in Microsoft SharePoint.

- Configure a second activity to move the content from Microsoft SharePoint to the archive using the “Copy items to archive and Delete them from SharePoint” Archive Action. After archiving, the content exists only in the archive and is deleted from Microsoft SharePoint.

Configure this second activity to occur after a period equal to the expected Recovery Point Objective (RPO). Following this practice ensures that content in Microsoft SharePoint is not deleted until the archived content has been successfully stored and replicated. If a disaster scenario occurs before this process is complete, the Microsoft SharePoint activities can be “replayed” against the Microsoft SharePoint systems.

**External BLOB Storage integrity utility**

If the organization is using the optional External BLOB Storage (EBS) feature, an EBS integrity utility (installed with the EBS provider software) is used to compare data in
the EBS database on the SharePoint SQL Server with the BLOBs stored in the Native Archive.

**Microsoft SharePoint SQL Server**

The use of this utility assumes that the EBS database is protected from a disaster along with other databases on the Microsoft SharePoint SQL Server, and is available for query after a disaster occurs.

**SourceOneNative Archive storage and EBS content**

EBS uses the SourceOneNative Archive to access storage. EBS content is not archived. EBS content is not subject to indexing, retention, or available for search using SourceOne Search. It is available for search using Microsoft SharePoint-side search interfaces.

The utility requires that the SourceOneNative Archive and storage is available for comparison with the EBS database after a disaster occurs.

**File system environment**

The systems that are supported by SourceOne for File Systems consist of one or more supported file systems.

**Disaster recovery configuration**

There is no specific disaster recovery configuration that is required for the file systems from which SourceOne for File Systems archives content.

**Best practice recommendations**

To minimize the chance of data loss, recommends that administrators configuring file system activities observe the best practices that are described in this section.

When archiving file content from a file system with the intent of removing the files from the file system (or shortcutting which replaces each file with a link to the archived file), always configure two activities. Configure the first activity to copy the files from the file system to the archive. You can then configure a second activity in one of the following two ways.

- Move the files from the file system to the archive (the files are removed from the file system).
- Move the files from the file system to the archive and replace them with a link to each archived file.

In either case, the second activity must be configured to occur after a period equal to the expected Recovery Point Objective (RPO). Following this practice ensures that content on file systems is not deleted until the archived content has been successfully stored and replicated. If a disaster scenario occurs before this process is completed, the file archiving activities can be “replayed” against the file systems.

**Master computer**

The SourceOne Master schedules and distributes jobs that are processed by Workers.

- The Master host computer is stateless and does not require replication.
- There only can be one *active* Master computer in a SourceOne configuration.
- You can cluster the Master computer at the disaster recovery site for high availability during a failover using the Microsoft Cluster Service.
• Install and configure an identical standby Master computer at the disaster recovery site. Use the following guidelines when installing the SourceOne Master Services software on the disaster recovery Master computer.
  
  ▪ Before installing the Master Services software on the disaster recovery computer, temporarily stop the SourceOne services (ExJobScheduler and ExAddressCacheService) on the primary Master computer.
  
  ▪ Install the software on the disaster recovery computer and restart the system.
  
  ▪ If clustering the Master computer at the disaster recovery site, follow the procedure in the SourceOne Installation Guide to configure the cluster.
  
  ▪ Disable the SourceOne services on the disaster recovery computer. The services must remain disabled during normal operation. Never have more than one Master Server running at a time.
  
  ▪ Restart the SourceOne services on the primary Master computer. This process registers the second Master computer in the SourceOne Activity database so that it is recognized in a failover scenario, but remains inactive until it is needed during a failover.
  
• Maintain this system in concert with the primary Master computer. For example, by performing software upgrades, and hotfixes.

Worker computer

SourceOne Worker computers perform message archiving activities from various messaging data sources. Each Worker computer can be configured to process only specific activities.

• Worker host computers are stateless and do not require replication.

Note

There is a work directory for the Worker in which temporary data is stored. This temporary data is not needed in a failover scenario.

• Install and configure at least one Worker computer at the disaster recovery site.

• If you use the Microsoft SharePoint or SourceOne for File Systems products, you must also install the corresponding Business Component Extensions (BCE) software to enable the Workers to process the types of activities that are listed in this section.
  
  ▪ SourceOne Business Component Extensions (BCE) for Microsoft SharePoint
  
  ▪ SourceOne Business Component Extensions (BCE) for SourceOne for File Systems

• Ideally the number of Workers at the disaster recovery site matches the number of Workers at the primary site to maintain a consistent level of service during a failover. If there are fewer Workers at the disaster recovery site, consider the following.
  
  ▪ Until the failback occurs and both sites return to usual operation, the level of service may be limited to the number of Workers at the secondary site.
  
  ▪ If dealing with an extended failover, you can consider adding Workers at the secondary site to maintain a high level of service.
  
• During a failover, you can adjust the roles of the Workers to assume the primary site's processing tasks.
• In a hot/warm configuration, Workers can be operational at the disaster recovery site and configured to work over the WAN with devices at the primary site.

• In a hot/cold configuration, Workers at the disaster recovery site are one of the following.
  • Powered off
  • Running with SourceOne services set to “disabled”

  **Note**
  Do not pause or stop the Worker using the SourceOne administration console as a substitute for powering off or disabling services. If the Worker is restarted, the Worker does not remain in this state (and is listed as available in the console).

• Ensure that SourceOne applications such as web Services and Mobile Services are installed and configured on Workers at the disaster recovery site.

• Maintain this system in concert with the primary Worker computers (for example, performing software upgrades, and hotfixes).

**Web server**

The SourceOne Search application provides a web client interface to end users and passes query and results data to and from the SourceOne Web Services software that is installed on one or more Workers. One of the following scenarios may occur.

• Scenario 1: You can install the SourceOne Search application on a single SourceOne Web Services computer.

• Scenario 2: You can install the SourceOne Search application on two or more SourceOne Web Services computers and configure a network load balancing using an appliance or software solution such as Microsoft Network Load Balancing Service (NLBS).

• Scenario 3: You can install the SourceOne Search application in an IIS web server farm accessible to end users. SourceOne Search then communicates through the load balancer address to the web Services application on the Worker Services computer. You can optionally use a Secure Sockets Layer (SSL) connection between the SourceOne Search application and the web Services application.

The disaster recovery configuration information in this section applies only to Scenario 3. If you are using Scenario 1 or Scenario 2, the Search application is installed on a Worker computer and that disaster recovery configuration applies.

**Disaster recovery configuration**

When configuring a disaster recovery operation, consider the following.

• Web servers are stateless and do not require replication.

• Install and configure at least one web server (including the SourceOne Search application) at the disaster recovery site.

• As with Worker computers, the number of web servers at the disaster recovery site is based on SLA requirements.

• Maintain this system in concert with the primary web servers (for example, performing software upgrades, and hotfixes).
SQL Server and databases

A database server running Microsoft SQL Server supports the following SourceOne databases.

- Activity database-This database maintains data that is associated with SourceOne system processing.
- Search database-This database maintains data that is associated with the SourceOne Search application.
- Native Archive database-This database manages data that is associated with the SourceOne Native Archive, a role-based architecture that manages the archiving, indexing, searching, and retrieving of content.

**Note**

Detailing a specific disaster recovery solution for Microsoft SQL Server is beyond the scope of this document.

SourceOne requirements

Before recovering from a disaster recovery scenario, consider the following:

- An available copy of the SourceOne databases, SQL system and temporary databases, and logs at the disaster recovery site.
- A SQL Server host at the disaster recovery site on which the databases can be mounted.
- An alias configuration in DNS to support redirecting SourceOne servers to the database server at the disaster recovery site during failover.
- This solution requires the use of existing Microsoft best practices which provide frequent replication of the databases that are listed in this section.
  - All SourceOne databases (Activity, Native Archive, Search)
  - SQL system databases. See the following MSDN information for a list of SQL system databases: [http://msdn.microsoft.com/en-us/library/ms190190%28SQL.90%29.aspx](http://msdn.microsoft.com/en-us/library/ms190190%28SQL.90%29.aspx)
- Alternatively, you can replicate SQL Server and the databases along with the other SourceOne components using a consistency group (or similar functionality as supported by the replication solution). Replicating all SourceOne components as a group can normalize the RTO time, minimize data lag, and simplify replication management.
  
  If the use of a consistency group is not possible (for example, in cases where the messaging system replication is occurring on an already established or different replication technology), configure the replication timing to be the same or as close as possible as the replication timing configured for other SourceOne components.

SQL Server host configuration

Before recovering from a disaster recovery scenario, consider the following.

- Use a CNAME alias in DNS which, during typical operations, points to the SQL Server host computer (or virtual host if clustering) at the primary site. When using a CNAME alias, follow standard best practices that are provided by Microsoft.
  - Register the Kerberos service principal names (SPNs), the hostname, and the fully qualified domain name (FQDN) for all the new DNS alias (CNAME)
records. If you do not perform this, a Kerberos ticket request for a DNS alias (CNAME) record may fail and return the following error code: KDC_ERR_S_PRINCIPAL_UNKNOWN

- You must be a domain administrator to run this command.
- For more information, refer to the following Microsoft KB article: http://support.microsoft.com/kb/870911

- Connection issues can occur when using a CNAME to address a server by another name other than the one it recognizes as itself. The server is not "listening" on the alias, and is not accepting connections to that name. To resolve this issue, add a Registry value (DisableStrictNameChecking) as described in the following Microsoft KB article: http://support.microsoft.com/kb/281308
- Maintain the SQL Server host in concert with the primary SQL Server host (for example, performing software upgrades, and hotfixes).

SourceOneNative Archive host computer

The SourceOne Native Archive software uses an architecture which can be configured to perform the roles that are listed in this section.

- Archive
- Index
- Search
- Retrieve

The SourceOneNative Archive software can be installed on a single host computer or multiple host computers, which enables you to dedicate hardware to specific roles to match the organization's policies and requirements.

This section describes the high availability and disaster recovery strategy for the SourceOneNative Archive host computers. The storage locations that are associated with the SourceOneNative Archive are hosted on hardware.

Disaster recovery configuration

Before recovering from a disaster recovery scenario, consider the following.

- SourceOneNative Archive computers are stateless and do not require replication.
- Install and configure at least one SourceOneNative Archive computer at the disaster recovery site.
- Ideally the number of SourceOneNative Archive computers at the disaster recovery site matches the number of computers at the primary site to maintain a consistent level of service during a failover. If there are fewer computers at the disaster recovery site, consider the following options that are listed in this section.

  - Until the failback occurs and both sites return to normal operation, the level of service may be limited to the number of SourceOneNative Archive computers at the secondary site.
  - If dealing with an extended failover, you can consider adding SourceOneNative Archive computers at the secondary site to maintain a high level of service.
  - During a failover, you can adjust the roles of the SourceOneNative Archive computers to assume the primary site's processing tasks.
In a hot/warm configuration, this computer is operational at the disaster recovery site and configured to work over the WAN with devices at the primary site.

In a hot/cold configuration, SourceOneNative Archive computers at the disaster recovery site are one of the following options.

- Powered off
- Running with SourceOne services set to disabled

Maintain the SourceOneNative Archive server at the disaster recovery site in concert with the primary SourceOneNative Archive servers (for example, performing software upgrades, and hotfixes).

Native Archive-Message Center storage

When you define one or more archive folders within a SourceOneNative Archive to contain content, you configure a Message Center storage location in which content is stored and built into volumes before it is written to a container file.

- This storage location is defined in the SourceOne console as a UNC path (\computer_name\shared_folder).
- Data can be stored on a storage array that is connected using a Storage Area Network (SAN). Alternatively, the data can be stored directly on the NAS device.
- Replicate this storage location. If the storage solution supports the concept of consistency groups, replicate this data consistently with other SourceOne data.

Native Archive-Index storage

When you define one or more archive folders within a SourceOneNative Archive to contain content, you also configure an index storage location in which full-text indexes are stored.

- This storage location is defined in the SourceOne console as a UNC path (\computer_name\shared_folder).
- Data can be stored on a storage array that is connected using a Storage Area Network (SAN). Alternatively, the data can be stored directly on the NAS device.
- Replicate this storage location. If the storage solution supports the concept of consistency groups, replicate this data consistently with other SourceOne data.

Native Archive-Container storage

Depending on the requirements and the version of SourceOne you are using, you have the following options for storing containers.

Network-accessible storage

You can store containers directly on network-accessible storage, such as shareable drives or network-attached storage devices (NAS devices).

- This storage location is defined in the SourceOne console as a UNC path (\computer_name\shared_folder).
- Data can be stored on a storage array that is connected using a Storage Area Network (SAN). Alternatively, the data can be stored directly on the NAS device.
- Replicate this storage location. If the storage solution supports the concept of consistency groups, replicate this data consistently with other SourceOne data.
Direct storage on Centera

The SourceOne configuration may require the long-term storage of SourceOne container files on an Centera content-addressed storage (CAS) system.

Existing archive folders
If you have existing archive folders that are configured to store containers on Centera using DiskXtender, you must continue to use this solution for those folders.

New archive folders
SourceOne Email Management can directly access containers on Centera devices.

Pool address configuration
You configure Centera pool addresses using the SourceOne console. To support the redirection to alternative Centera access nodes in a disaster recovery scenario, configure the Centera pool addresses as symbolic access node addresses \((node1,node2,node3, \text{and so on})\) in the connection string instead of IP addresses. You can then perform the redirection by changing DNS entries.

For information on configuring this storage option, refer to the SourceOne Administration Guide.

Note
IP addresses and node names are valid entries in the Pool Address field.

Storage on Centera using DiskXtender

This section includes information about storage on Centera using DiskXtender.

Existing archive folders
If you have existing archive folders that are configured to store containers on Centera using DiskXtender, you must continue to use this solution for those folders.

New archive folders
You can configure new archive folders to use direct storage on Centera.

DiskXtender and other storage media
The scenario of using DiskXtender connected to other long-term storage such as optical devices or tape, while valid, is not considered for the purposes of this document. DiskXtender is only described as a means of connecting SourceOne to Centera.

Base configuration
You install DiskXtender on a Microsoft Windows file server and provide a Windows NT File System (NTFS) volume (called an extended drive) to which SourceOne container files are written.

- This location is then specified when configuring an archive folder using the SourceOne console.
- The container files are systematically moved to Centera using a policy-based configuration.
The containers are deleted from the extended drive and replaced with pointers to the content stored in Centera.

Disaster recovery configuration

This solution requires the configuration for disaster recovery that is described in the DiskXtender Microsoft Windows Version Installation Guide for the supported version of DiskXtender. Current information on the version of DiskXtender supported with SourceOne is provided in the EMC SourceOne Email Products Compatibility Guide.

General considerations

- Replicate the extended drive storage location. If the storage solution supports the concept of consistency groups, replicate this data consistently with other SourceOne data.
- DiskXtender does not support a hot/hot configuration. Disaster recovery is provided by replicating the extended drive data to the disaster recovery site so that it is available to a corresponding passive DiskXtender host and extended drive at the disaster recovery site.

Host computer configuration

This solution requires that you setup DiskXtender replication using the configuration information that is provided in the DiskXtender Microsoft Windows Version Installation Guide.

- DiskXtender is installed and managing files on the server at the primary site.
- DiskXtender is also installed on the server at the disaster recovery site. The DiskXtender service is stopped (set to manual or disabled) or is passive at the disaster recovery site.
- Ensure that the DiskXtender servers at the primary and disaster recovery site have the same hostname and extended drive letter designation (for example, H:).
- Also ensure that the extended drive at the disaster recovery site has the same Microsoft volume serial number as the extended drive on the primary site. This can be set using the `volumeid.exe` utility from Microsoft.
- Maintain the DiskXtender host computer at the disaster recovery site in concert with the DiskXtender host at the primary site (for example, performing software upgrades, and hotfixes). Refer to the DiskXtender documentation set for information on maintaining systems in this configuration.
- DiskXtender can be installed in a high-availability configuration at each site using Microsoft Windows cluster configuration. For details on implementing this configuration at the primary and disaster recovery site, refer to the DiskXtender Microsoft Windows Version Installation Guide.

Refer to the DiskXtender Microsoft Windows Version Installation Guide for more information host computer configuration in a replicated environment.

Exporting and replicating Registry keys

In addition to replicating the DiskXtender extended drive itself, you must also configure a script to frequently export the DiskXtender Registry keys to one of the replicated storage locations. This configuration enables you, during a failover, to
import the replicated Registry keys to the DiskXtender server at the disaster recovery site. Export and replicate the following Registry keys:

HKEY_LOCAL_MACHINE\SOFTWARE\DiskXtender
HKEY_LOCAL_MACHINE\SOFTWARE\EMC\XMS

The script looks similar to the following:

regedit /E \STORAGE\SourceOne_Recovery\DX.reg HKEY_LOCAL_MACHINE\SOFTWARE\DiskXtender
regedit /E G:\Xtender_Recovery\XMS.reg HKEY_LOCAL_MACHINE\SOFTWARE\EMC\XMS

Consider the following:

- If you are configuring a stand-alone DiskXtender server, the script can be run using a Windows scheduled task, which you configure to run frequently (for example, every two minutes).

- If you are configuring a clustered DiskXtender server, configure the script to be run as a Generic Application. Ensure that the script is written to loop frequently (for example, every two minutes). Replicate the Registry keys to a location other than the DiskXtender extended drive. For example, in a clustered DiskXtender configuration, use another replicated disk in the cluster group.

**DiskXtender media service configuration options for Centera**

Best practices for configuring the media service options for DiskXtender for Windows and Centera are beyond the scope of this document. For specific guidance on this configuration, including considerations for an environment which includes Centera replication, refer to the following white paper.

Connecting DiskXtender for Windows to Centera: Best Practices Planning

This white paper can be found on Online Support in the DiskXtender for Windows white paper location.

Additional resources are listed in this section.

- For detailed information and best practices for configuring a media service for Centera, refer to information on media management for configuring Centera in the DiskXtender Microsoft Windows Version Best Practices Guide.


**Delete configuration options**

Optionally, you can delay the clearing of volumes until they have been replicated by Centera. This can prevent a situation in which a stub exists on the extended drive, but the associated clip does not exist on the disaster recovery Centera. Because of current software limitations, you must logically determine when volumes have likely been replicated by Centera and then configure a corresponding delete rule in DiskXtender. For example, if Centera replication generally takes less than a few hours, then you configure the delete delay of volumes from the extended drive to the lowest granularity (one day).
To support a disaster recovery configuration in which you want to support Direct Read for all files, yet enable data to be replicated by Centera before deleting files from the extended drive, consider the following when configuring move rule settings.

- In the SourceOne console (which allows you to configure some DiskXtender options in the Storage Options page of the New Archive Folder wizard), clear the delete after move and Direct read options.
- Use the Force Direct Read for all files option on the Options tab of the Extended Drive Properties dialog box. This will automatically perform Direct Read for any deleted file, but will not change the attribute.
- Configure a default rule to delete files based on high and low drive size watermarks.

**Note**

Refer to the Media Management section of the *EMC DiskXtender Microsoft Windows Version Best Practices Guide* for best practices and other considerations for using Centera.

### File server host or NAS device configuration

File servers or NAS devices that are associated with Native Archive storage require a disaster recovery configuration.

**Disaster recovery configuration**

Use a CNAME alias in DNS which, during typical operations, points to the host computer (or virtual host if clustering) or NAS device at the primary site. When using a CNAME alias, follow standard best practices that are provided by Microsoft.

- You must register the Kerberos service principal names (SPNs), the hostname, and the fully qualified domain name (FQDN) for all the new DNS alias (CNAME) records. If you do not perform this, a Kerberos ticket request for a DNS alias (CNAME) record may fail and return the following error code: KDC_ERR_S_SPRINCIPAL_UNKNOWN

**Note**

you must be a domain administrator to run this command.

- Connection issues can occur when using a CNAME to address a server or device by another name other than the one it recognizes as itself. The server or device is not listening on the alias, and is not accepting connections to that name. Ensure that the host computer is not running at the disaster recovery site.
- Maintain the host computer in concert with the primary host (for example, performing software upgrades, and hotfixes).

### Centera

Centera provides for long-term storage for SourceOne container files.

For information on configuring Centera replication, refer to the Centera documentation set.
CHAPTER 3

Failover to the Disaster Recovery site

This section provides a detailed procedure for performing a failover from the primary site to the disaster recovery site.

This section contains the following topics:

- Failover procedures

[36]
Failover procedures

This procedure describes the manual steps that are required when an outage occurs and communication is lost at the primary site, requiring a failover to the environment set up at the disaster recovery site.

Stopping SourceOne processing at the disaster recovery site

To perform the failover procedures, the SourceOne system must remain in a quiesced state. Ensure that all computers in the SourceOne configuration (Master, Workers, Native Archive servers) are stopped and no data is moving through the system.

- In a hot/warm configuration in which Workers and Native Archive computers are already operational at the disaster recovery site, stop all the SourceOne services on each of these computers.
- In a hot/cold configuration, ensure that the SourceOne computers remain powered off or the SourceOne services are disabled at the disaster recovery site.

Checking that replicated data is accessible

Ensure that the latest good copy of replicated data is available at the disaster recovery site. For detailed information, refer to the storage solution documentation.

- Message Center data
- Indexes
- Container files

Note

This can also include SQL and mail system databases, logs, and data if replicated using the same solution as SourceOne data. However, the expectation is that you make these systems and data available through existing practices that are used at your site.

Verifying the disk health of file servers

Check the SourceOne file server systems hosting the Message Center, index, and container shares for errors by running `chkdsk`. Proactively running this command enables you to review and repair file system errors.

Use the following procedure to verify the disk health of file servers,

Procedure

1. Run `chkdsk` in read-only mode (default). This displays a status report of the findings.
2. If you have corruptions, back up that disk before you correct it.
3. To fix the errors, run `chkdsk -f`.

For more information about `chkdsk`, including usage, command syntax and parameters, refer to the Microsoft Windows Server TechCenter and search for `chkdsk` or access the following URL:

Performing Active Directory changes for SQL and file servers

Redirect the CNAME aliases to SQL and file server host computers (or virtual host) names at the disaster recovery site. Use the following procedure to perform Active Directory changes for SQL and file servers.

**Procedure**

1. From Active Directory, repoint the CNAME to SQL and file servers to the servers or virtual hosts (if clustered) at the disaster recovery site.
2. Flush the DNS Resolver Cache:

   
   ipconfig /flushdns

3. Ping each server/virtual host by hostname and confirm that the ping resolves to the correct IP address for each computer at the disaster recovery site.

Ensuring dependent systems are online and accessible

Ensure that disaster recovery has been performed so that the following systems on which SourceOne depends are online and accessible.

- Data sources (Mail servers, Microsoft SharePoint servers, and file systems)
- SQL Server, databases (SQL system and SourceOne) and logs
- File servers hosting SourceOne storage shares

Follow your organization’s procedures for restoring these systems.

Recovering the DiskXtender configuration

If you are not using DiskXtender in the environment, continue to Powering on SourceOne computers (hot/cold configuration only) on page 38. If you are using DiskXtender in the environment, follow the sub-procedures in this step (in the order presented) to recover the DiskXtender configuration at the disaster recovery site.

Verifying DiskXtender connectivity to Centera

Verify DiskXtender connectivity to Centera using best practices that are described in the documents that are listed in this section.

- Connecting DiskXtender for Windows to EMC Centera: Best Practices Planning. This white paper can be found on the Online Support site.
- DiskXtender Microsoft Windows Version Installation Guide.
- DiskXtender Microsoft Windows Version Administration Guide.

Importing the DiskXtender Registry keys to the DiskXtender host computer

As part of the disaster recovery solution configuration, the DiskXtender Registry key is continuously exported to a designated storage location at the disaster recovery site.
This enables you to update the DiskXtender host computer at the disaster recovery site with the last known configuration from the primary site.

Import the DiskXtender Registry key to the DiskXtender host computer at the disaster recovery site by completing the following steps.

- Deleting the existing DiskXtender key
- Merging the replicated key to the DiskXtender server at the disaster recovery site

Perform the following steps to replace the Registry keys at the disaster recovery site with the replicated keys from the primary site.

**Procedure**

1. If using clustered DiskXtender, bring the cluster group online using Cluster Administrator.
2. Go the replicated location that contains the replicated DiskXtender Registry keys.
3. Delete keys to remove old data during the merge.
   
   For example:
   
   ```
   regedit /S G:\del.reg
   REM Example of the del.reg file
   REM [HKEY_LOCAL_MACHINE\SOFTWARE\DiskXtender]
   REM [HKEY_LOCAL_MACHINE\SOFTWARE\XMS]
   ```
4. Merge the key that was replicated from the primary site.
   
   For example:
   
   ```
   regedit /S G:\ SourceOne_Recovery\DX.reg
   regedit /S G:\ SourceOne_Recovery\XMS.reg
   ```
5. If using clustered DiskXtender, take the cluster group offline using Cluster Administrator.

Configuring export of DiskXtender Registry keys back to primary site

Ensure the DiskXtender Registry keys are configured for export to one of the replicated drives and ensure that the keys are replicated back to the primary site for later use during the failback process.

Adding the Reset Disk Resources Registry key for Clustered DiskXtender only

This step may not be necessary always, but if DiskXtender disk resources do not appear in the Extended Drive Resource Groups in Cluster Administrator, a Registry key can be configured to re-create it.

**Note**

This procedure is described in the Knowledgebase article esg92158.

Perform the following steps to re-create the DiskXtender Disk resource.

**Procedure**

1. Stop the DiskXtender Service resource in Cluster Administrator.
2. Create a STRING value in the following location:
   
   ```
   KEY NAME: HKEY_LOCAL_MACHINE\Software\Emc\DiskXtender\Setup
   VALUE NAME: ResetDiskResource
   VALUE: YES
   ```
• The DiskXtender Disk resource is only re-created for extended drives that have already been configured in the DiskXtender Administrator.

• After performing this procedure, the DiskXtender Disk resource appears in the Cluster Administrator.

• The Registry key deletes itself.

Restarting the DiskXtender host computer or cluster nodes

Restart the DiskXtender host computer or cluster nodes.

Verifying data consistency between DiskXtender and Centera

Use the following procedure to verify that the data in the DiskXtender extended drive is consistent with data on Centera and, if required, rewrite data that was not replicated to Centera at the disaster recovery site.

Procedure

1. Obtain the DXCenVerify utility. Download the version for the release of DiskXtender you are using. Registered customers can download software from the Online Support site.

2. Run the DXCenVerify utility to determine which volumes are on the extended drive but did not replicate to the disaster recovery (now local) Centera.

Results

The DXCenVerify utility outputs a text file indicating the missing volumes (MisFileRep_DateTime.log). After you run the utility and determine that there is a missing volumes issue, you have two options to ensure data consistency.

Option 1 - Manually remove DiskXtender attributes from volumes

Once you identify the missing volumes from the output log generated by DXCenVerify, use the following procedure to remove DiskXtender attributes from files to enable DiskXtender to recognize the files that must be moved to the Centera.

Procedure

1. Copy all files indicated as missing to a temporary directory other than an extended drive (for example, c:\DX_Temp). Copying the files removes any DiskXtender attributes.

2. On the extended drive on which the copied files reside, perform a privileged delete.

   Note

   You must start the DiskXtender service to perform this step.

3. With the DiskXtender service now running, copy the files from the temporary directory back to the extended drive location.

4. Because the Fetched attribute has been removed, DiskXtender moves these files to the Centera based on existing move rules.

5. Run the DXCenVerify utility again to validate the files have been moved to the remote (now local) Centera.

6. Force a DiskXtender background scan. Background scans enable DiskXtender to verify that all files on the extended drive that must be managed are being
managed. Refer to the *EMC DiskXtender Microsoft Windows Version Administration Guide* for more information about background scans.

**Starting the DiskXtender service**

Start the DiskXtender service (if not already started when performing the previous step).

**Option 2 - Remove DiskXtender attributes from volumes using the DxDmChk utility**

Alternatively, you can remove the DiskXtender attributes using the DiskXtender Data Manager Check (DxDmChk) utility. This utility can be used to remove the extended drive attributes from a file so that it can be moved to the Centera using the existing move rules:

- Download the version for the release of DiskXtender you are using. Registered customers can download software from Online Support.
- You can run the utility to generate a report to determine if there are issues. To remove extended drive attributes, you must obtain an activation key from DiskXtender Support and receive assistance with using the utility.

**Inspecting DiskXtender**

Use the DiskXtender File System Manager interface to review the DiskXtender configuration and verify that media is present and online.

**Running a DiskXtender file report**

Use the following procedure to run a DiskXtender file report to view the status of SourceOne containers on the extended drive.

**Procedure**

1. Right-click the SourceOne container folder on the extended drive and select DiskXtenderFile Report.
2. Accept the report defaults.
3. Verify that all containers have a status of fetched or deleted.

**Tips:**

- Search for the word NOT to quickly find volumes that are not fetched or deleted.
- Search for the word “offline” to find media which is not online.

**Powering on SourceOne computers (hot/cold configuration only)**

Assuming the correct steps were taken during the disaster recovery configuration, when you start the computers at the disaster recovery site, all SourceOne services are in a Manual or Disabled state.

**Note**

Do not start the SourceOne services yet.
Ensuring the SourceOne computers can access key resources

Ensure that SourceOne computers can access SQL Server, the data sources (mail servers, Microsoft SharePoint servers, file systems), and shares. Perform another check to ensure that all computers and resources are accessible.

- On each SourceOne computer (Master, Workers, Native Archive), flush the DNS Resolver Cache:
  
  ```
  ipconfig /flushdns
  ```

- Ping each server/virtual host by hostname and confirm that the ping resolves to the correct IP address for each host at the disaster recovery site.

- Use ODBC tools to check database connectivity.

Running the SourceOne Archive Integrity Tool

Ensure that you run the version of the SourceOne Archive Integrity Tool for the version of SourceOne Email Management you are running.

Log in to a SourceOne Native Archive server at the disaster recovery site using the SourceOne primary service account.

Use the following procedure to run the SourceOne Archive Integrity Tool and ensure that it successfully completes its operations.

Procedure

1. (Optional) Run the tool in simulation mode (default) to assess the situation.
2. Run the tool using the `nosim` option.

Results

After completing this process, the tool will identify and correct consistency issues and generate a log file which is used later in the failover process.

The remaining steps of the failover procedure include starting the SourceOne services at the disaster recovery site, performing some reprocessing activities, and rerunning the tool.

Starting SourceOne services

Start the SourceOne services on each computer in the configuration at the disaster recovery site in the following order.

Procedure

1. Master
2. Native Archive servers
3. Workers

Note

For environments in which the system was in the midst of a backup (and is in a suspended state which was likely persisted through replication), run the resume scripts that have the SourceOne backup utilities. For details, refer to the backup information provided in the *EMC SourceOne Administration Guide.*
Performing reprocessing

Before returning SourceOne to full operation at the disaster recovery site, you must perform the reprocessing steps that are listed in this section.

Starting the SourceOne management console

Log in to a computer on which the SourceOne management console is installed using a valid SourceOne administrator account. Start the console.

Adjusting Worker and SourceOneNative Archive computer roles

To maintain expected service levels while operating the SourceOne system from the disaster recovery site, adjust the roles for the Workers and Native Archive servers to pick up the primary site’s processing tasks.

In environments in which the number of SourceOne Worker and Native Archive computers is less than the number of computers at the disaster recovery site, define a processing strategy applicable for the period you expect to be operating SourceOne from the disaster recovery site. For example, you may want to dedicate the computers to journaling, indexing and searching activities while limiting historical archiving activities until the primary site is re-established.

Reprocessing deleted retention (Microsoft Exchange) or soft deleted (Microsoft Domino) messages

In SourceOne Email Management environments, perform manual procedure to reprocess deleted retention (Microsoft Exchange) or soft deleted (IBM Domino) items.

**Microsoft Exchange**

All deleted email messages are restored to the journal mailbox and available for archive again.

All soft deleted email messages are restored to the journal database and are available for archive again.

Use the following procedure to reprocess deleted retention.

**Procedure**

1. Log in to a Worker computer using an account which has rights to all journaling mailboxes (for example, the SourceOne primary service account).
2. Mount each journal mailbox to this account so you can see all of them.
3. For each journal mailbox, click the Inbox and select **Tools > Recover Deleted Items**.

**Domino**

All soft deleted email messages are restored to the journal database and are available for archive again. Use the following procedure to reprocess soft deleted messages.

**Procedure**

1. Log in to a Worker computer using an account which has rights to all journaling mailboxes (for example, the SourceOne primary service account).
2. Open each SourceOne journal database (for example, **ExJournal1.nsf**, **ExJournal2.nsf**, and so on) on the IBM Domino server.
3. Click **Soft Deletions**.
4. Click **Restore All** at the top of the view.

**Rerunning historical archiving activities**

Rerun any historical archiving activities that were within the RPO window. Refer to the *EMC SourceOne Administration Guide* for specific procedures.

**Rerunning SourceOne for File Systems activities**

Rerun any SourceOne for File Systems activities that were within the RPO window. Refer to the *EMC SourceOne Administration Guide* for information about configuring activities.

**Rerunning Microsoft SharePoint activities**

Rerun any SourceOne for Microsoft SharePoint activities that were within the RPO window. Refer to the *EMC SourceOne Administration Guide* for information about configuring activities. If the activity is recursive, you must delete the previous record from the activity list which is located in the SourceOne sub-site of the Microsoft SharePoint Central Administration site and then run the activity again.

**Rerunning the SourceOne Archive Integrity Tool**

Use the Archive Integrity Tool to identify inconsistencies in the SourceOne index.

---

**Note**

Ensure all historical archiving and indexing activities (started automatically as a result of running the tool earlier) have successfully completed before performing this step.

Use the following procedure to rerun the Archive Integrity Tool.

**Procedure**

1. Ensure that you run the version of the SourceOne Archive Integrity Tool for the version of SourceOne Email Management you are running.
2. Log in to a SourceOneNative Archive server at the disaster recovery site using the SourceOne primary service account.
3. Run the SourceOne Archive Integrity Tool.
4. Rerun the tool using the `-FullMsgVerify` option (using the log file that was generated when you previously ran the tool).
5. Observe the results to ensure that all possible inconsistencies are identified and corrected. A log is output indicating any remaining inconsistencies which were not possible to correct.

**Verifying SourceOne operations**

At this point, the SourceOne system is recovered and operational at the disaster recovery site. Run SourceOne applications and ensure normal operation.

- Performing a full-text index search of archived content between the RPO and current time.
Testing that email shortcuts can be resolved through the SourceOneOffline Access client and that email and file shortcuts can be resolved using the universal URL.

(Optional) Running the Microsoft SharePoint EBS integrity tool

If the organization is using the optional SourceOne for Microsoft SharePoint External BLOB Storage (EBS) feature, an EBS integrity tool (installed with the EBS provider software) is used to compare data in the EBS database on the Microsoft SharePoint SQL Server with the BLOBs stored in the SourceOneNative Archive.
CHAPTER 4

Failback to the Primary Site

This section provides a detailed procedure for performing a controlled failback of an operational disaster recovery site to the primary site.

This section contains the following topics:

- **Failback procedures**........................................................................................................ 46
Failback procedures

This procedure describes the manual steps that are required to re-establish operations at the primary site.

Stopping SourceOne processing at the disaster recovery site

Stop all SourceOne processing at the disaster recovery site. Refer to the procedure described in the *EMC SourceOne Release Notes* for quiescing the system before an upgrade.

**Note**

Ensure that the Master computer at the disaster recovery site is disabled. There can only be one *active* Master computer in a SourceOne configuration.

Ensure the exported DiskXtender Registry keys are available (Optional)

Ensure the DiskXtender Registry keys are configured for export to one of the replicated drives and ensure that the keys are replicated back to the primary site.

Copying data back to the primary site

Start the process to copy data from the disaster recovery site back to the primary site.

Examples of copy back options for array-based storage include the following.

- Incremental copy back. If the original storage array hardware is back online at the primary site, perform an incremental copy back.
- Full copy back. If the original Symmetrix or CLARiiON hardware is no longer physically available at the site and is being replaced by another Symmetrix or CLARiiON, a full copy back is required.

If using another storage solution (such as NAS), ensure that the data is available at the primary site.

Re-establishing disaster recovery configuration for SourceOne computers

At the disaster recovery site, return the configuration to the hot/cold or hot/warm configuration that was in place before the disaster occurred.

- In a hot/warm configuration, Worker and SourceOneNative Archive computers are operational at the disaster recovery site and configured to work over the WAN with devices at the primary site. Review the information described in “Considerations” on page 23 which describes the types of activities that can be processed across a WAN connection.
- This section lists the Workers and SourceOneNative Archive computers at the disaster recovery site in a hot/cold configuration.
  - Powered off
  - Running with SourceOne services set to disabled
Creating a gold copy of replicated data

To prevent any issues from being carried during replication from the primary site to the disaster recovery site, create a gold copy of the replicated data that can be used if issues occur when you bring the primary site back online.

Enabling storage devices at the primary site

After all SourceOne processing is stopped and the data between the primary and disaster recovery sites is synchronized, suspend replication and enable the storage array at the primary site.

Performing Active Directory changes for SQL and file servers

Use the following procedure to redirect the CNAME aliases to SQL and file server host computers (or virtual host) names at the primary site.

Procedure

1. From Active Directory, repoint the CNAME to SQL and file servers to the servers or virtual hosts (if clustered) at the primary site.
2. Flush the DNS Resolver Cache:
   ipconfig /flushdns
3. Ping each server/virtual host by hostname and confirm that the ping resolves to the correct IP address for each host at the primary site.

Ensuring dependent systems are online and accessible

Ensure that disaster recovery has been performed so that the systems listed in this section, on which SourceOne depends are online and accessible.

- Data sources (Mail servers, Microsoft SharePoint servers, and file systems)
- SQL Server, databases (SQL system and SourceOne) and logs
- File servers hosting SourceOne storage shares

Follow your organization’s procedures for restoring these systems.

Recovering the DiskXtender configuration

If you are using DiskXtender in the environment, follow the sub-procedures in this step (in the order presented) to recover the DiskXtender configuration at the primary site.

Verifying DiskXtender connectivity to Centera

Verify DiskXtender connectivity to Centera using best practices that are described in the documents that are listed in this section.

- Connecting EMC DiskXtender for Windows to EMC Centera: Best Practices Planning. This white paper can be found on the Online Support site.
- DiskXtender Microsoft Windows Version Installation Guide.
- DiskXtender Microsoft Windows Version Administration Guide.
Importing the DiskXtender Registry keys to the DiskXtender host computer

As part of the disaster recovery solution configuration, the DiskXtender Registry key is continuously exported to a designated storage location at the primary site. This enables you to update the DiskXtender host computer at the primary site with the last known configuration from the disaster recovery site.

Import the DiskXtender Registry key to the DiskXtender host computer at the primary site by following the steps that are listed in this section.

- Deleting the existing DiskXtender key
- Merging the replicated key to the DiskXtender server at the primary site

Follow the procedure that is listed in this section to replace the Registry keys at the primary site with the replicated keys from the disaster recovery site.

Procedure

1. If using clustered DiskXtender, bring the cluster group online using Cluster Administrator.
2. Go the replicated location that contains the replicated DiskXtender Registry keys.
3. Delete keys to remove old data during the merge.
   
   ```regedit /S G:\del.reg REM Example of the del.reg file REM [HKEY_LOCAL_MACHINE\SOFTWARE\DiskXtender] REM [HKEY_LOCAL_MACHINE\SOFTWARE\XMS]```
4. Merge the key that was replicated from the disaster recovery site.
   
   ```regedit /S G:\ SourceOne_Recovery\DX.reg regedit /S G:\ SourceOne_Recovery\XMS.reg```
5. If using clustered DiskXtender, take the cluster group offline using Cluster Administrator.

Configuring export of DiskXtender Registry keys back to disaster recovery site

Ensure the DiskXtender Registry keys are configured for export to one of the replicated drives and ensure that the keys are replicated back to the disaster recovery site.

Adding the Reset Disk Resources Registry key to the Clustered DiskXtender.

This step may not be necessary always, but if DiskXtender disk resources do not appear in the Extended Drive Resource Groups in Cluster Administrator, a Registry key can be configured to re-create it.

---

**Note**

This procedure is described in the Knowledgebase article esg92158.

Perform the following steps to re-create the DiskXtender Disk resource.

**Procedure**

1. Stop the DiskXtender Service resource in Cluster Administrator.
2. Create a STRING value in the following location:

   ```KEY NAME: HKEY_LOCAL_MACHINE\Software\DiskXtender\Setup VALUE NAME: ResetDiskResource VALUE: YES```

**Note**

The DiskXtender Disk resource will only be re-created for extended drives that have already been configured in the DiskXtender Administrator. After performing this procedure, the DiskXtender Disk resource appears in the Cluster Administrator. The Registry key deletes itself.

**Restarting the DiskXtender host computer or cluster nodes**

Restart the DiskXtender host computer or cluster nodes.

**Verifying data consistency between DiskXtender and Centera**

You must verify that the data in the DiskXtender extended drive is consistent with data on the Centera and, if required, rewrite data that was not replicated to the Centera at the primary site.

To verify that the data consistency between DiskXtender and Centera:

1. a. Obtain the **DXCenVerify** utility.
   b. Download the version for the release of DiskXtender you are using. Registered customers can download software from Online Support.
   c. Run the **DXCenVerify** utility to determine which volumes are on the extended drive but did not replicate to the primary (now local) Centera.

   The **DXCenVerify** utility outputs a text file that indicates the missing volumes (MisFileRep_DateTime.log).

   After you run the utility and determine that there is a missing volumes issue, you have two options to ensure data consistency.

**Option 1-Manually remove DiskXtender attributes from volumes**

Once you identify the missing volumes from the output log generated by **DXCenVerify**, use the following procedure to remove DiskXtender attributes from files to enable DiskXtender to recognize the files that must be moved to the Centera.

**Procedure**

1. Copy all files indicated as missing to a temporary directory other than an extended drive (for example, c:\DX_Temp). Copying the files removes any DiskXtender attributes.
2. On the extended drive on which the copied files reside, perform a privileged delete.

   **Note**
   
   You must start the DiskXtender service to perform this step.
3. With the DiskXtender service now running, copy the files from the temporary directory back to the extended drive location.
4. Because the "Fetched" attribute has been removed, DiskXtender moves these files to the Centera based on existing move rules.
5. Run the DXCenVerify utility again to validate the files have been moved to the remote (now local) Centera.

**Option 2-Remove DiskXtender attributes from volumes using the DxDmChk utility**

Alternatively, you can remove the DiskXtender attributes using the DiskXtender Data Manager Check (DxDmChk) utility. This utility can be used to remove the extended drive attributes from a file so that it can be moved to the Centera using the existing move rules.

- Download the version for the release of DiskXtender you are using. Registered customers can download software from Online Support.
- You can run the utility to generate a report to determine if there are issues. To remove extended drive attributes that you must obtain an activation key from DiskXtender Support and receive assistance with using the utility.

**Starting the DiskXtender service**

Start the DiskXtender service (if not already started when performing the previous step).

**Inspecting DiskXtender**

Use the following procedure in the DiskXtender File System Manager interface to review the DiskXtender configuration and verify that media is present and online.

It may also be useful to run a DiskXtender file report to view the status of SourceOne containers on the extended drive.

**Procedure**

1. Right-click the SourceOne container folder on the extended drive and select the DiskXtenderFile Report.
2. Accept the report defaults.
3. Verify that all containers have a status of fetched or purged.
   - Search for the word “not” to quickly find volumes that are not fetched or purged.
   - Search for the word “offline” to find media which is not online.

**Starting SourceOne services**

Start the SourceOne services on each computer in the configuration at the primary site in the following order.

**Procedure**

1. Master
2. Native Archive servers
3. Workers
Verifying that primary site is replicating to the disaster recovery site

Validate the data at the primary site. Once you have validated the data at the primary site, you can begin replication from the primary site back to the disaster recovery site.

Verifying SourceOne operations

At this point, the SourceOne system is recovered and operational at the primary site. Run SourceOne applications and ensure normal operation.

- Performing a full-text index search of archived content between the RPO and current time.
- Testing that email shortcuts can be resolved through the SourceOneOffline Access client and that email and file shortcuts can be resolved using the universal URL.
Failback to the Primary Site
This appendix describes how to use the SourceOne Archive Integrity Tool.

This section contains the following topics:

- **Overview** ................................................................. 54
- **Command line description** ........................................ 54
- **Permissions** ............................................................... 57
- **Sequence of operations** ............................................ 57
- **Verifying operations** ................................................ 59
- **Log file viewing** ........................................................ 60
Overview

The SourceOne Archive Integrity Tool, version 6.6 supports the environments that are listed in this section.

- SourceOne Email Management version 6.6 and higher
- SourceOne for Microsoft SharePoint version 6.6
- SourceOne for File Systems version 6.6

The SourceOne Archive Integrity Tool performs an extensive number of operations to ensure that a consistent environment exists at the disaster recovery site, with as close to zero data loss as possible, before normal SourceOne operations are resumed.

You run the utility (twice) along with the failover procedure described in Failover to the Disaster Recovery site on page 35.

After a consistent environment is up and running at the disaster recovery site, you can perform a proactive failover to the primary site and continue normal processing. When performing a controlled failback, you do not need to run the SourceOne Archive Integrity Tool again at the primary site, as the failback is planned and run with the system quiesced.

Command line description

This section describes the command line syntax and optional parameters for the SourceOne Archive Integrity Tool.

Syntax

This section describes the syntax and command line options.

```
ES1IntegrityTool -d Log File Path -t Temp Directory [options]
```

The following table describes the command options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s</td>
<td>Process all content greater than or equal to this date.</td>
</tr>
<tr>
<td>-d</td>
<td>Destination path to store log file.</td>
</tr>
<tr>
<td>-t</td>
<td>Temporary disk directory for utility. Contents of this directory are deleted each time that the tool is run, so take care in defining this location.</td>
</tr>
<tr>
<td>-e</td>
<td>Optional end date to process all objects less than or equal to this date.</td>
</tr>
<tr>
<td>-DBServer</td>
<td>Required. Name of the SourceOne SQL Server computer hosting the Archive database.</td>
</tr>
</tbody>
</table>
### Table 3  SourceOne Archive Integrity Tool command syntax (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-ArchiveDB</code></td>
<td>Optional. Name of the SourceOne Archive database (default is <code>ES1Archive</code> if not specified).</td>
</tr>
<tr>
<td><code>-nosim</code></td>
<td>Turn off simulation mode</td>
</tr>
<tr>
<td><code>-FullMsgVerify</code></td>
<td>After SourceOne reprocessing occurs, perform full verification of all objects.</td>
</tr>
<tr>
<td><code>-MissMsgVerify</code></td>
<td>After SourceOne reprocessing occurs, perform missing object verification.</td>
</tr>
</tbody>
</table>

### Required parameters

The SourceOne Archive Integrity Tool requires at least three parameters to operate in a disaster recovery scenario.

**Note**

By default the utility operates in simulation mode, meaning that it operates as read-only and generates a log file. Simulation mode allows you to review the log before performing the disaster recovery operation. After running in simulation mode, you can add the optional `-nosim` parameter to perform the disaster recovery operation.

**-d parameter**

Specifies the directory where a log file is generated. Each execution of the SourceOne Archive Integrity Tool produces an output log file detailing its findings. This log file name includes a date and timestamp, as shown in the following example.

```plaintext
ES1IntegrityTool_2009-08-01T18-15-40.txt
```

**-t parameter**

Defines a temporary disk directory that is used as a scratch location for the utility.

**Note**

All contents of this directory are removed by this utility so take care in defining it. Do not use this directory for anything else except a “scratch” area for running the tool (for example, log file storage). If the path does not exist, it is created.

**-s parameter**

Denotes the starting date of objects to be verified, also referred to as the RPO.

**Note**

The time between the `-s` parameter (start date) and the `-e` parameter (end date) cannot exceed 7 days. The time between the `-s` parameter (start date) and the present date (where the `-e` parameter is not specified) cannot exceed 7 days. An error appears if the time between parameters exceeds 7 days.
This parameter uses the following form in GMT:

```
yyyy-mm-ddTh:mm:ss
```

For example, August 8, 2009 at 2:00 P.M. would be expressed as follows:

```
2009-08-07T14:00:00
```

SourceOne writes real-time data to several different areas, like different devices, or different replication schedules. The RPO date is the last known date where it can be assured that replication has completed successfully for all replication schedules. Usually this date does not exceed a few days. The closer the RPO date is to the current date, the quicker the RTO is for SourceOne to be operational at the disaster recovery site.

**Note**

When identifying candidate objects, the tool views the file date on disk (last accessed).

- **DBServer**

  Required parameter specifying the name of the computer hosting the SourceOne Archive database.

### Optional parameters

This section describes the optional parameters, or parameters that can be used in other scenarios.

- **-e parameter**

  Used to verify objects between certain date ranges. Not to be used during disaster recovery.

- **-ArchiveDB**

  Optional. Used only if the name of the SourceOne Archive database is not the default name (*ES1Archive*).

- **-nosim parameter**

  Instructs the SourceOne Archive Integrity Tool to perform its functions. Unless this parameter is specified, the operation of the SourceOne Archive Integrity Tool is read-only (except for generating a log file). Simulation mode allows you to review the log before performing the disaster recovery operation.

- **-FullMsgVerify parameter**

  Used after reprocessing has occurred during the failover process. This option is followed by the log file path that was generated during the initial run of the SourceOne Archive Integrity Tool. All objects that are processed after the RPO date are queried against SourceOne. This allows the operator to discover possible lost objects during the recovery process.
-MissMsgVerify parameter

Used after reprocessing has occurred during the failover process. This option is followed by the log file path that was generated during the initial run of the SourceOne Archive Integrity Tool. Only the objects that were flagged as possibly lost are queried. This is a faster verification than –FullMsgVerify.

Examples

The following table provides usage examples for the SourceOne Archive Integrity Tool.

<table>
<thead>
<tr>
<th>Example Syntax</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s 2009-09-20T17:00:00 -d C:Utils \ES1IntegrityTool\Logs -t C:Utils \ES1IntegrityTool\Temp</td>
<td>Provides a simulated recovery from 9/20/2009 at 5:00 PM to the current date.</td>
</tr>
<tr>
<td>-s 2009-09-20T17:00:00 -d C:Utils \ES1IntegrityTool\Logs -t C:Utils \ES1IntegrityTool\Temp -nosim</td>
<td>Provides a recovery from 9/20/2009 at 5:00 PM to the current date.</td>
</tr>
<tr>
<td>-fullmsgverify C:Utils \ES1IntegrityTool\Logs \ES1IntegrityTool\Logs 2-13.txt -d C:Utils \ES1IntegrityTool\Logs</td>
<td>Verify content after a recovery. This command is run after SourceOne services are started and the system has fully recovered.</td>
</tr>
</tbody>
</table>

Permissions

You run the SourceOne Archive Integrity Tool on a SourceOneNative Archive server. Ensure that you log in to the server using the SourceOne primary service account.

Sequence of operations

This section describes in detail the sequential operations that the SourceOne Archive Integrity Tool performs when recovering from a failover. Each step includes details about the operation being performed and prescriptive information that you can use to troubleshoot issues you may encounter when running the utility.

Parsing command line options

The utility parses the command line options that are entered by the user to determine the scope of operations.

Adding volumes to the candidate volume set

Add volumes as candidates for reprocessing by identifying volumes that have a date (from which the volume name is comprised in the format YYYYMMDDHHMMSS) greater than the RPO.

- SQL volumes—A table that is named Volume in the SourceOneSQL database contains all the volumes that are archived by SourceOne. This table is scanned for
all volume names > the RPO date. Each matching entry is added to the candidate volume set.

- Container drive volumes—During the recording process, volumes are written as container files to one of the following locations, depending on the configuration.
  - Network-accessible storage
  - The DiskXtender extended drive (if used). This drive is scanned for all container files that are created on or after the RPO data and added to the candidate volume set.
  - The Centera (if storing containers directly on Centera without DiskXtender). The Centera is scanned for all container files that are created on or after the RPO data and added to the candidate volume set.

At this point, the candidate set contains all volumes that are found in SourceOne that were created after the RPO date. The utility has captured information on which volumes are in SQL or closed container files. Ideally, every volume exists in both places.

---

**Note**

Volume information can also exist in a full-text index. This information is identified during the full-text index scan, which is described later in this document.

---

**Adding objects found to the candidate object set**

Add objects as candidates for reprocessing. The utility does this by identifying objects that have a receive date greater than the RPO date and objects that are orphaned, or objects that are in containers but not in the SQL database. Candidate objects are added from the sources that are listed in this section.

- **SQL objects.** A table that is named Messages in the SourceOne SQL database is scanned for all objects with a receive date greater than the RPO date. All matching objects are added to the candidate object set.

- **Objects in Candidate Volumes.** If a historical archive task was run after the RPO date, objects could exist in which the receive date is earlier than the RPO date, but were archived after the RPO date. To ensure that this situation is accounted for, all candidate volumes are scanned, and every object that is contained in each candidate volume is in the candidate object set.

- **Message Center.** During the archive process, SourceOne writes objects to a Message Center directory. These objects remain in the Message Center until a volume reaches a certain size or a certain amount of time passes. The utility scans the Message Center and places any objects that it finds into the candidate object set.
  
  For email messages, each message is validated for integrity. If the message has large attachment (in the large content, or LC, subdirectory) it is loaded into the message object. The message ID is then calculated and compared to the ID used for the file name. If the ID's do not match, the message is considered corrupt.

- **Archive location.** The archive location holds closed container files. The share is enumerated and each container that is created after the RPO time is opened and validated. Each object is added to the candidate object set.

At this point SourceOne Archive Integrity Tool has a comprehensive set of objects that it identifies as processed after the RPO date. It also contains any possible orphaned objects that are found on the disk.

The candidate object set is stored in a SQL table that is called MsgMap which resides in the SourceOne Archive SQL database. Every time SourceOne Archive Integrity Tool
is run, it removes the previous MsgMap table from SQL and re-creates a new one. This means that after successful operation the MsgMap table is left in the SourceOne database. This allows interrogation by the user of possible offending objects. This table can be removed after the disaster recovery site is operational.

Adding full-text indexes found to the candidate index set

Add full-text indexes as candidates for reprocessing by identifying indexes whose last modified date is greater than the RPO date. To identify indexes that may have been in a pending state (not written to an index yet) when the outage occurred, the utility also scans all indexes for candidate volumes and includes them in the candidate index set. This is done because it is possible for objects to be in an index pending state during disaster recovery, and the index may not have been written to yet.

The utility also automatically schedules full-text indexes for re-indexing.

Note

Although there can be an RTO impact to performing the re-indexing of all candidate indexes, it is the best method to guarantee the consistency and integrity of the SourceOne environment.

Removing objects from SQL

The candidate object set is traversed and all objects that exist in SQL without having been assigned to a volume are removed from SQL. This prevents duplication detection during the reprocessing of objects.

Verifying operations

After successful operation of the SourceOne Archive Integrity Tool, a log file is generated which lists the entire candidate object set and a possible missing object set (which is always smaller than the candidate object set). The tool can be run using optional parameters to “replay” the log file against one of the object sets.

Query and display results

You can use the following command line options when running the tool and specifying the log file that is created from a previous run.

- \-FullMsgVerify - This command line option selects the entire candidate object set
- \-MissMsgVerify - This command line option selects only the possible missing object set

During verification, each object in the selected set is queried for from SourceOne and the results are displayed. These results can be cross-referenced with the SQL MsgMap table to help find any possible lost objects.

Examples of the SourceOne Archive Integrity Tool command using each of these options include:

\-MissMsgVerify D:\ES1\IntegrityTool_2009-07-24T16-42-13.txt -d D:\Logs
Query and retrieve results

You can also specify an option that is called `GetMsgDuringVerify` which, when used with either the `FullMsgVerify` or `MissMsgVerify` option, retrieves the object from SourceOne and verifies its integrity.

Examples of the ES1IntegrityTool command using this option include:

```
-MissMsgVerify D:\ES1IntegrityTool_2009-07-24T16-42-13.txt -d D:\Logs -GetMsgDuringVerify
```

Log file viewing

Log files that are written by the utility are in binary Unicode format, and do not display well using a basic text viewer such as Notepad. Use a viewer such as Microsoft Internet Explorer.
This appendix describes how to use the SourceOne for Microsoft SharePoint External BLOB Storage (EBS) Integrity Tool.

This section contains the following topics:

- **Overview** ................................................................. 62
- **Recovery scenarios** .................................................. 62
- **Using the EBS Integrity Tool** .................................... 63
Overview

SourceOne for Microsoft SharePoint also provides External binary large object (BLOB) storage, offloading the storage of binary large objects from the Microsoft SharePoint SQL Server and storing them using SourceOne. EBS is configured at the farm level.

This feature includes an EBS Provider database which is installed on the Microsoft SharePoint SQL Server to maintain identification information for BLOBs stored externally in the SourceOneNative Archive by SourceOne for Microsoft SharePoint.

EBS uses the SourceOneNative Archive to access storage. EBS content is not archived. EBS content is not subject to indexing, retention, or available for search using SourceOne Search. It is available for search using Microsoft SharePoint-side search interfaces.

If your organization is using the optional SourceOne for Microsoft SharePoint External BLOB Storage (EBS) feature, the EBS Integrity Tool (installed with the EBS provider software) is used to compare data in the EBS database on the Microsoft SharePoint SQL Server with the BLOBs stored in the SourceOneNative Archive.

Recovery scenarios

The EBS Integrity Tool can accommodate several recovery scenarios.

BLOB records missing from EBS database, BLOBs exist in Native Archive

In this scenario, one or more BLOB records are missing from EBS database, but the BLOBs exist in the Native Archive.

- The missing BLOBs are in the same archive folder that is configured for EBS.
- Some missing BLOBs are located in different archive folders than the configured folder because of the configuration change. In this case, the tool searches for the BLOBs in all valid archive folders on the Native Archive server and restore the correct database records.

BLOBs missing from Native Archive, BLOB records exist in EBS database

In this scenario, one or more BLOBs are missing from Native Archive but BLOB records still exist in the EBS database.

- The missing BLOBs are located in the cache folder that was configured for EBS.
- Some missing BLOBs are located in some other folders that were previously used as a cache folder.

In this case, the tool searches for BLOBs in the cache folder.

- You can optionally instruct the tool to add additional folders to search for missing BLOBs.
- The tool provides an option to manually disable the local cache garbage collection function so that files in the cache will not be automatically deleted.

Note

If you run out of disk space, the garbage collection is run regardless of the setting you configure.
BLOBs missing from Native Archive and EBS database

In this scenario, one or more BLOBs are missing from both the Native Archive and EBS database, and cannot be found in the local cache or additional folders. It is not possible to recover them in this case.

Using the EBS Integrity Tool

This section describes how to use the EBS Integrity Tool.

Launching the tool

The EBS Integrity Tool is installed with the EBS Provider software and can be launched from the following location:

%Program Files%\ SourceOne\EBS Provider\Emc. SourceOne.ES1EBSIntegrityChk.exe

When you launch the tool, a dialog box appears that enables you to:

- Automatically scan the entire farm.
- Skip the automatic scan and manually scan individual site collections.

Depending on the environment, perform one of the options that is listed in this section.

- For a small farm with fewer BLOBs and site collections, use the automatic scan option to scan the entire farm.
- For larger farm, you can perform a manual scan of individual site collections to better control the duration of the scan.

Reviewing scan results

Once an automatic or manual scan is performed, the SourceOne EBS Integrity Check Results page appears.

The following figure displays scan results.
If site collections are scanned, they are sorted by the status of the scan results. There are three possible icons that display the status.

- **Critical**—The tool failed to verify some or all BLOBs because of errors.
- **Warning**—There are some BLOBs missing.
- **OK**—The site collection is intact with no BLOBs missing.

### Recovering BLOBs

To recover missing blobs, select the SharePoint site and click one of the following buttons.

- **Recover BLOB From**. This option recovers missing BLOBs that are in the same archive folder that was configured for EBS. It will also recover missing BLOBs in all valid archive folders in the Native Archive and restore the correct database records.

- **Recover BLOB From Cache**. This option recovers missing BLOBs which are located in the cache folder that was configured for EBS. It will also recover BLOBs located in other folder which were previously used as a cache folder. You can also manually add additional folders to search for missing BLOB files.

- **Garbage Collect**. The tool provides an option to manually disable the local cache garbage collection function so that files in the cache will not be automatically deleted.

In each recovery situation, the tool provides a progress window for the recovery operation. When processing is complete, the progress window is automatically closed.
Logging

The tool logs its operations using standard .NET trace logging. You can modify the configuration file for the tool to turn on the logging (and log levels) and configure to a specific log file location.

The configuration file is provided in the following location:

%Program Files%\SourceOne\EBS Provider\Emc.
SourceOne.ESIEBSSignatureChk.exe.config
This glossary contains terms related to replication, storage systems, EMC SourceOne, and disaster recovery. Many of these terms are used in this manual.

Symbols

.emx files  Flat, portable files of a configurable size containing messages archived by EMC SourceOne organized by month. Also called volumes or container files.

Access (node) role  An EMC Centera node with the access role. These nodes serve as the connection points for an EMC Centera device, and are identified by IP addresses that enable applications like DiskXtender to communicate with and transfer data to the device through the TCP/IP protocol. For best practices purposes, you should configure node name aliases for the node IP addresses before you configure the media service connection in DiskXtender.

Access profile  A profile used by an application, such as DiskXtender, to access an EMC Centera device.

Activity  An activity defines a specific type of work to be performed by EMC SourceOne, including the environment it will be performed in and when it will be performed. For example, Journal Email, Shortcut Email, and Archive Email are all activities. An activity component uses the information defined by the activity to create one or more jobs that perform the work. Activities are grouped in the EMC SourceOne console using policies. See policy

Archive folder  Contains volumes and indexes in the message archive. Archive folders are organized using automatically created monthly folders.

SourceOne Archive Integrity Tool  The SourceOne Archive Integrity Tool performs an extensive number of operations to ensure that a consistent environment exists at the disaster recovery site, with as close to zero data loss as possible, before normal SourceOne operations are resumed.

Centera  A line of disk-based storage devices deployed on a Redundant Array of Independent Nodes (RAIN). Centera devices use unique, permanent content addresses to store and retrieve data.

Consistency group  A logical entity that defines a set of data to be replicated. The implementation and use of consistency groups varies among replication products, but the basic principle is the same.
container files  Flat, portable files of a configurable size containing archived messages organized by month. Also called volumes or .emx files.

Database Source Name (DSN)  A named connection to a database. Typically used with ODBC.

data source  The location from which EMC SourceOne collects messages or to which EMC SourceOne archives messages. A journaling mailbox on an Exchange mail server is an example of a data source.

Dependent Write-Consistent  A data state where data integrity is guaranteed by dependent write I/Os.

Dependent Write I/O  An I/O that cannot be issued until an associated predecessor I/O has completed. Most applications, and in particular database management systems (DBMSs), have imbedded dependent write logic to ensure data integrity if a failure occurs in the host or server processor, software, storage subsystem, or if an environmental power failure occurs.

Direct Read  A DiskXtender setting whereby files that have been purged from the extended drive are read directly from the media rather than being copied back to the extended drive when requested.

disaster recovery  The process of restoring a previous copy of the data and applying logs or other necessary processes to that copy to bring it to a known point of consistency.

DiskXtender  An EMC product that allows you to "extend" the capacity of the EMC SourceOne storage drive by automatically writing .emx files to other storage media.

extended drive  In DiskXtender, an NTFS volume (such as a hard drive or the EMC SourceOne storage drive) or partitioned part of a hard drive for which DiskXtender provides file migration services by moving files to media and fetching files from media according to the parameters you set.

External BLOB Storage (EBS)  A feature of EMC SourceOne for Microsoft SharePoint which is used to store binary large object content externally from the SharePoint database.

fetch  DiskXtender term for retrieving purged file data from media back to the extended drive.

folder  Contains all volumes and indexes. Folders can be archive folders in a message archive or mapped folders that are virtual folders which map to archive folders.

full-text indexing  An index of all available text within the header, message, or attachment of an email. Indexes are created to enable fast searching of the Native Archive.
index server One or more servers, called Native Archive servers, performing the indexing role within the Native Archive. This server is used to index archived messages. This includes content scraping, creating content caches, distributing content to indexes, indexing, re-indexing, and disposing of indexes.

job The scheduled instance of an activity. For example, a user of the EMC SourceOne console creates a Domino shortcut activity to run every night of the week at 11:00 PM. At the end of 7 days, there would have been 7 jobs created and executed by this activity, assuming only one job was created for each run.

job dispatcher A process on the Worker computer that registers the Worker computer with the activity database and scans the Job table in the activity database for work. The job dispatcher compares the job types of scheduled jobs against all registered activity components to determine if there is an activity component capable of executing the jobs. If a registered activity component is found, the job dispatcher locks the job and transfers execution to the activity component.

job scheduler Service that creates and schedules jobs from activities. The job scheduler is responsible for checking the status of Worker servers and rescheduling jobs if a Worker or job fail.

journaling Is the ability to copy, in real-time, messages received, and delivered by a mail server. EMC SourceOne allows you to use the Journal activity to journal messages from an Exchange mail server, a Domino mail server, or both. Once the messages have been journaled they can then be archived, shortcut, or searched.

journaling mailbox The holding place on the mail server for messages before they are transferred to the SourceOne Message Center.

logical unit (LUN) Hosts access storage using logical unit numbers, which are exported by a SCSI target. The actual storage object is a logical unit, which is often referred to as a LUN.

mail server A mail server is an application that receives incoming email from local users and remote senders and forwards outgoing email for delivery. A computer dedicated to such an application can also be called a mail server. Microsoft Exchange, IBM Lotus Domino, and sendmail are mail server applications.

mapped folder Virtual folders which are associated with archive folders.

media or virtual media EMC Centera media is considered virtual media because it does not physically hold the files migrated to it. Instead, the virtual media act as logical interface points for DiskXtender. They function as a logical partition of the whole EMC Centera repository.
| **message archive server** | One or more servers performing the message archive role within the Native Archive. These servers, called Native Archive servers, are used to archive messages. This includes journaling, historical archiving (mailboxes, PST files, and NSF files) and user-directed archiving. |
| **Message Center** | Native Archive storage location in which messages are processed before being written to the archive. |
| **Microsoft Management Console (MMC)** | Extensible common presentation service for managing applications used by administrators to manage Workers, activities, and so on. The EMC SourceOne console is implemented as an MMC snap-in. |
| **monthly folder** | Subfolders within the archive folders. Monthly folders are created by the archiving process to organize the archived content and associated full-text indexes by month. |
| **move rule** | DiskXtender term describing a rule or policy that defines the criteria identifying which files should be moved to media. Move rules also identify the target media to receive the files (media group) and the retention period that should be applied to the files. |
| **Native Archive** | A horizontally scalable archive that includes the data store, message database, and full-text indexes. The Native Archive can be configured to allow separate roles to be performed on one or more separate computers. These roles are: message archive server, index server, search server, and retrieval server. These computers are referred to as Native Archive servers. |
| **Native Archive server** | A computer used to perform a computing role within the Native Archive. |
| **point of consistency** | A point in time to which data can be restored and recovered or restarted and maintain integrity for all data and applications. |
| **policy** | A logical grouping of one or more related activities in the EMC SourceOne console. |
| **purge** | DiskXtender term which refers to when data for files that have been copied to media is removed from the extended drive and a file tag is left behind. The file tag allows a purged file to appear to be resident on the extended drive so that client computers can access it. |
| **Recovery Point Objective (RPO)** | The amount of acceptable data loss after the recovery or restart processes are complete. This is the difference between the point of the disaster and the time of the last known point of consistency. |
| **Recovery Time Objective (RTO)** | The amount of time allowed for performing a restore and recovery or restart to a specified point of consistency. |
| **restore** | A process that reinstates a prior copy of the data. |
retention/file retention  The act of restricting the modification or deletion of a file for some time.

retention period  A folder-level setting that allows you to track how long volumes exist in the EMC SourceOne system. They are designed to help you to meet legal retention requirements by preventing you from deleting volumes before the specified amount of time has passed.

retrieval server  One or more servers, called Native Archive servers, performing the retrieval role within the Native Archive. This server is used to retrieve archived messages.

rolling disaster  A series of events that lead up to a complete disaster. For example, the loss of a communication link occurs before a site failure.

rules  Criteria you configure to organize email archives and to control which messages EMC SourceOne archives. Rules are hierarchical, and can be nested up to three levels deep. Once defined, rules can be shared by multiple activities.

search server  One or more servers, called Native Archive servers, performing the search role within the Native Archive. This server is used to search archived messages.

shortcut  Pointers that are placed on the mail server to copies of messages that are archived in EMC SourceOne.

SourceOne Console  A graphical user interface that allows an SourceOne administrator to configure and manage an SourceOne system. The SourceOne Console is implemented as a Microsoft Management Console (MMC) snap-in.

storage (node) role  An EMC Centera node with the storage role. These nodes store data.

task  A task is used by the activity component to specify configuration information for a job, such as the schedule, based on a specific activity. A task generates one or more jobs. A task is not configurable from the user interface.

Transactional Consistency  A DBMS state where all transactions are committed or rolled back.

user-directed archiving  A type of archiving that allows a mail user or mail application to direct messages to a specific folder in EMC SourceOne for archiving.

volume  Flat, portable files of a configurable size containing archived messages organized by month. Also called container files or .emx files.
W

Worker  A networked computer that can perform one or more SourceOne jobs. There can be any number of Workers. A Worker can also be configured to run specific jobs.