



Continuous Data Protector (CDP) Technical Whitepaper

Using FalconStor CDP with Microsoft
Exchange 2007

FalconStor[®]
Software

Using FalconStor CDP with Microsoft Exchange 2007

Continuous Data Protector (CDP) Technical Whitepaper

FalconStor Software, Inc.
2 Huntington Quadrangle, Suite 2S01
Melville, NY 11747
Phone: 631-777-5188
Fax: 631-501-7633
Website: www.falconstor.com

Copyright © 2009 FalconStor Software. All Rights Reserved.

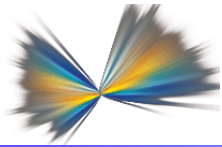
FalconStor Software and FalconStor are registered trademarks of FalconStor Software, Inc. in the United States and other countries.

Windows is a registered trademark of Microsoft Corporation.

All other brand and product names are trademarks or registered trademarks of their respective owners.

FalconStor Software reserves the right to make changes in the information contained in this publication without prior notice. The reader should in all cases consult FalconStor to determine whether any such changes have been made.

10.28.2009



Contents

Contents	iii
Introduction.....	4
Abstract	4
Document Scope.....	4
Audience.....	4
Assumptions	4
Falconstor Continuous Data Protector	6
Overview.....	6
Key features	6
Terminology	8
Integration with Microsoft Exchange environments	9
Overview.....	9
How does it work?	9
A Typical Configuration	11
Architecture.....	11
Estimating the storage size needed for the CDP appliance.....	12
Microsoft Exchange 2007 Server	12
Microsoft Domain Controller server	13
SUN StorageTek ST6140 storage array	13
Step 1 – Protecting the access to the CDP (front end and back end)	14
Step 2 – Protecting the Exchange server and the Microsoft domain controller	14
Step 3 – Protecting the CDP appliance.....	17
Recovery in an Exchange Environment using CDP	21
Scenario 1: One or multiple files on a drive.....	21
Scenario 2: One or multiple emails.....	22
Scenario 3: Recovering from scratch after a system disk failure or a major disaster	26
Conclusion	27
Appendix	28
References	28



Introduction

Abstract

The FalconStor® Continuous Data Protector (CDP) solution provides rapid recovery from system and data center failures caused by natural disasters, hardware failures, and user-induced events such as deletion, corruption, or viruses.

This paper illustrates how to use FalconStor CDP to protect a Microsoft® Exchange 2007 server and its email database(s). It also explains how continuous real-time data journaling and periodic snapshots provide simple, rapid, and granular recovery to any point in time.

Document Scope

This document describes the basic concepts and integration guidelines for FalconStor Continuous Data Protector (CDP) in a Microsoft Exchange 2007 environment. The document is intended to provide an architectural overview of CDP being used with Exchange along with the benefits of a combined solution. The objective is to propose a procedure to protect an Exchange 2007 environment starting from the Operating System (OS) to the Exchange server and associated storage groups. The information in this document is presented in the form of guidelines. This document is not meant to be a technical Best Practices Guide.

Audience

The audience for this document includes storage consultants, pre-sales specialists in charge of projects involving Microsoft environment protection concepts, and partners interested in FalconStor Continuous Data Protector (CDP). This document is especially beneficial for IT directors, storage administrators, backup administrators, Exchange administrators, datacenter managers, architects and others involved in the administration of backup architecture including Exchange. This document can also be valuable to IT staff in charge of disaster recovery (DR) projects.

Assumptions

It is assumed that the reader is familiar with:

- Microsoft Exchange 2007
- Microsoft Windows Operating Systems
- Network-attached storage and protocols (i.e. iSCSI, NFS, CIFS)
- SAN environments
- LAN-based data protection
- Backup challenges
- Recovery Point and Recovery Time Objectives (defined below)
- Service Level Agreements and Objectives (defined below)

Term	Definition
Recovery Point Objective (RPO)	The maximum period of time for which a business is willing to accept data loss. For example, nightly backups have an RPO of 24 hours while synchronous mirroring can have an RPO of zero.
Recovery Time Objective (RTO)	The maximum amount of downtime a business is willing to accept. The time period from incident of failure, to resumption of business operations.
Service Level Agreement (SLA)	A contract which records a common understanding regarding services, priorities, responsibilities, guarantees and warranties. Each area of service scope has the 'level of service' defined. Frequently used to represent the contracted RTO.
Service Level Objective (SLO)	<p>A key element of an SLA between a service provider and a customer. An SLO is a specific quantitative characteristic that is agreed upon as a measure of performance between the service provider and customer. For example, availability, throughput, frequency, response time, or quality.</p> <p>The purpose of an SLO is to eliminate misunderstandings and disputes regarding levels of service provided.</p>

It is assumed that the reader has had limited exposure to CDP, so an introduction to the product is included.



Falconstor Continuous Data Protector

Overview

FalconStor Continuous Data Protector (CDP) is a secondary, backup, storage solution that features *per-write data journaling* for local and remote recovery; two implementation options are available, in-band or out-of band. Continuous protection mode allows organizations to recover data to the last point before a service disruption occurred. FalconStor CDP also integrates periodic mode protection via FalconStor TimeMark[®] technology, which provides point-in-time snapshots with transactional integrity for rapid recovery, data set duplication, backup window elimination, DR validation, and long-term data retention.

Snapshots are created on a pre-set schedule, such as every hour or every few hours, delivering substantially more recovery points than daily tape backup. In addition, FalconStor CDP provides WAN optimized replication for remote data protection and recovery. Its flexible features allow switching between continuous and periodic remote replication modes based upon the availability and capability of the WAN connecting to the DR site.

The traditional tape backup and data archiving focus is on data retention rather than protection of the entire system. If a system disk is damaged or corrupted, administrators are faced with the time-consuming task of re-installing the operating system and application, then reapplying configuration information to fully recover the entire system. This results in an unacceptable amount of downtime for most organizations.

FalconStor CDP provides instant recovery via SAN boot technology without having to copy data back to a disk target. FalconStor CDP allows you to browse any snapshot of the original server, even while the primary volume is still mounted. Using high-speed iSCSI and/or Fibre Channel (FC) SAN connectivity, you can inspect the contents of the snapshot disk, validate the image, and immediately recover an application server operating system by booting from the backup image.

Key features

Fibre Channel support option: Supports Fibre Channel protocols over 2Gb, 4Gb, or 8Gb ports. Supports FC booting using certified HBAs. Integrates with Disk Manager to securely allocate storage.

iSCSI support: Supports iSCSI protocol over built-in Gigabit Ethernet ports. Load balancing and path failover are supported via standard Microsoft iSCSI Initiator driver. Supports iSCSI booting using certified iSCSI HBAs. Integrates with Disk Manager to securely allocate storage without the usual complexity associated with iSCSI authentication.

WAN-optimized Thin Replication: Efficient, block-level delta replication to a DR site. A built-in UDP or TCP protocol can be used without the need for additional FC/IP routers. Patented FalconStor MicroScan technology analyzes each replication block on-the-fly during replication and transmits only the changed disk sectors (512 bytes). Encryption options are available for both data-at-rest and data-in-flight.

Synchronous mirroring/zero downtime migration: Protects against hardware failures and enables data migration from one storage array to another with zero downtime for servers, applications, and/or users.

Thin Protection: Allows provisioning of virtual storage that represents a higher capacity than is physically available. Physical storage is automatically allocated only when needed. This enables more efficient storage utilization. Thin Protection may be applied to primary storage, replica storage (at the DR site), and mirrored storage.

TimeMark snapshots: Space-efficient snapshots can be enabled for all iSCSI and FC disks or FalconStor DiskSafe protected disks. Database agents are available for popular databases to ensure 100% transactional integrity.

TimeView™ images: TimeMark technology includes the TimeView feature, which creates an accessible, mountable delta snapshot image that enables administrators to freely create multiple and instantaneous virtual copies of an active data set. The data set and/ or replica copies can then be assigned to multiple application servers with read/write access for concurrent, independent processing, all while the original data set is actively being accessed/updated by the primary application server.

FalconStor DiskSafe Agent: Supports timely transaction monitoring of server disk and synchronous / scheduled disk replication. One DiskSafe agent must be configured for each protected server. Supports Microsoft Windows Vista (32-bit or 64-bit); Windows Server 2003 R2 Standard/Enterprise Edition (32-bit or 64-bit); Windows XP Home/Professional Edition (32-bit); Windows 2000 Professional/Server/Advanced Server; Windows Server 2009 (32-bit or 64-bit).

FalconStor Message Recovery for Microsoft Exchange (MRE) option: FalconStor CDP appliances integrate with Microsoft Exchange 2003/2007 Recovery Storage Group technology. The snapshot disk responds directly to Microsoft Exchange databases and rapidly recovers information in single inboxes. A wizard lets you load information into databases without having to restore and recover databases or consume server disk space.

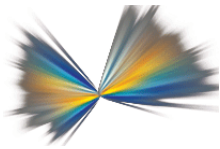
HyperTrac Backup Accelerator option: Supports serverless file backup, enabling the backup server to connect to a FalconStor CDP appliance and assisting with backup by automatically connecting to the snapshot disk. This option completely backs up server files to tape or to a virtual tape library (VTL) such as FalconStor Virtual Tape Library (VTL).

Snapshot Agent suite: Application-aware Snapshot Agents ensure full protection for active databases such as Microsoft SQL Server, Oracle, Sybase, SAP and DB2; messaging applications like Microsoft Exchange and Lotus Notes; and file servers. Complete data and transactional integrity is attained through a robust and automated process that safely and reliably takes snapshots of databases for point-in-time copy purposes and DR.

Terminology

The primary components of the FalconStor Continuous Data Protector (CDP) solution are the CDP appliance, CDP clients, and the console. These components all sit on the same network segment, the *storage network*. The terminology and concepts used in CDP are described here. For additional information, refer to the *FalconStor Continuous Data Protector (CDP) Administrator Guide* and/or the *FalconStor CDP/NSS Reference Guide*.

Component	Definition
Appliance	An industry-standard server that provides a specific computing resource. In this case, the appliance contains FalconStor CDP software. The appliance can function as a standalone appliance with internal storage or as a gateway to storage on an existing network.
Clients	The term to designate all hosts that use the CDP appliance to protect their data. The Exchange server is therefore considered a client.
Console	The administrative tool that allows you to configure your CDP appliance. It is also called the FalconStor Management Console.
Snapshot agent	Snapshot Agents protect databases, messaging systems, and file systems with full point-in-time consistency while allowing full speed, non-stop access to the data.
Journal	The CDP journal tracks data changes before they are committed to the mirror disk(s). It is used for short-term data protection between TimeMarks.
TimeMark	TimeMark technology works with CDP to enable you to create scheduled and on-demand point-in-time delta snapshot copies of data volumes. TimeMark includes the FalconStor TimeView® feature, which creates an accessible, mountable image of any snapshot. This provides a tool to freely create multiple and instantaneous virtual copies of an active data set. The TimeView images can be assigned to multiple application servers with read/write access for concurrent independent processing, while the original data set is actively accessed and updated by the primary application server.
TimeView	An extension of the TimeMark option that allows you to mount a virtual drive as of a specific point in time.
Mirror disk	A full and independent copy of the primary data volume, updated using the journal.
Out-of-band	A solution which is not in the production data path.



Integration with Microsoft Exchange environments

Overview

The FalconStor Continuous Data Protector (CDP) solution integrates tightly with Microsoft Exchange to enable seamless protection, automate and streamline data recovery, and optimize operational efficiency. It allows you to:

- Enable item-level recovery for your Exchange deployment.
- Ease the mail recovery process by using a simple wizard (MRE).
- Satisfy the most demanding Recovery Time Objectives (RTO) - 5 minutes for email files, 10 minutes for systems.
- Achieve the best Recovery Point Objective (RPO) depending on the period you have defined for snapshots with transactional integrity (TimeMarks).
- Slash Exchange disaster recovery costs with WAN-optimized replication.

Note: Exchange integration is also available for other FalconStor products. You can use FalconStor NSS and FalconStor VTL-SIR to:

- Reduce Exchange management costs with storage consolidation.
- Achieve 99.999% availability of Exchange databases with storage virtualization.
- Eliminate redundant data and shrink your backup repository by up to 95% using deduplication technology.

How does it work?

When FalconStor CDP is used to protect a Microsoft Exchange environment, it works just as it would with other applications used to protect ordinary files. Since database files require special treatment in order to preserve transactional integrity, additional software is also used to protect and recover the database files.

The Exchange server is protected by creating a mirror copy for every disk being protected. The mirror copies are maintained by the CDP server using a journal. Consistent snapshots can be scheduled periodically or triggered on demand.

The software needed to achieve this is as follows:

- **CDP (IPStor):** The core of the solution, it is installed on your CDP appliance. Once installed and configured, you do not need to access it again unless you want to manage its storage.
- **DiskSafe:** Installed on each host you want to protect (Centralized management is available), the DiskSafe agent allows you to configure and manage the protection of your local or SAN storage using the CDP appliance. The DiskSafe interface is used the most to manage data protection.
- **Snapshot Agent for Exchange:** DiskSafe coordinates with this application-specific snapshot agent to provide 100% transactionally consistent snapshots, which eliminates

lengthy database and file system consistency checks during recovery. TimeMark snapshots also support consistency groups, ensuring that all interdependent application volume snapshots are created at the exact same point in time. These snapshots can be mounted as a single virtual volume for instant recovery of individual files or as volumes for bare metal recovery.

- **Snapshot Agent for File Systems:** This agent functions similarly to the Exchange snapshot agent except that it interfaces with the Windows file system. Prior to starting the snapshot process, all disk cache and buffers are flushed to disk. Once you install the version corresponding to your Microsoft Windows operating system, it is automatically triggered by DiskSafe when requesting a new snapshot (TimeMark).
- **Message Recovery for Microsoft Exchange (MRE):** This wizard-driven tool is used to easily restore an individual mailbox or all mailboxes for a local or remote message store. MRE can be used to recover mailbox stores on multiple partitions of the same disk as well as partitions that do not include the first partition of a disk. Further filtering can be specified for recovering a certain date range of emails or by specific subject, content or entire email levels.
- **HyperTrac:** An optional tool, HyperTrac allows you to automate the mounting of an image (TimeView) made from a consistent snapshot. This enables you to access or backup your data from any server while operations are running.
- **IntegrityTrac:** An optional tool, IntegrityTrac allows you to automate the mounting of an image (TimeView) made from a consistent Microsoft Exchange snapshot and to control the consistency of the Exchange data.
- **DiskSafe Recovery CD:** Complete server failure can be quickly overcome by booting a new server using the DiskSafe Recovery CD. This tool allows you to restore both your system disk and data disks, and restore them to the original hard disk or another disk. You can restore either the mirror itself or a snapshot (i.e. a point-in-time image) of the data..
- **DynaPath:** This is a load balancing/path redundancy application that ensures constant data availability and peak performance across the SAN by performing Fibre Channel HBA load-balancing, transparent failover, and fail-back services. DynaPath creates parallel active storage paths that transparently reroute server traffic without interruption, in the event of a storage network problem.

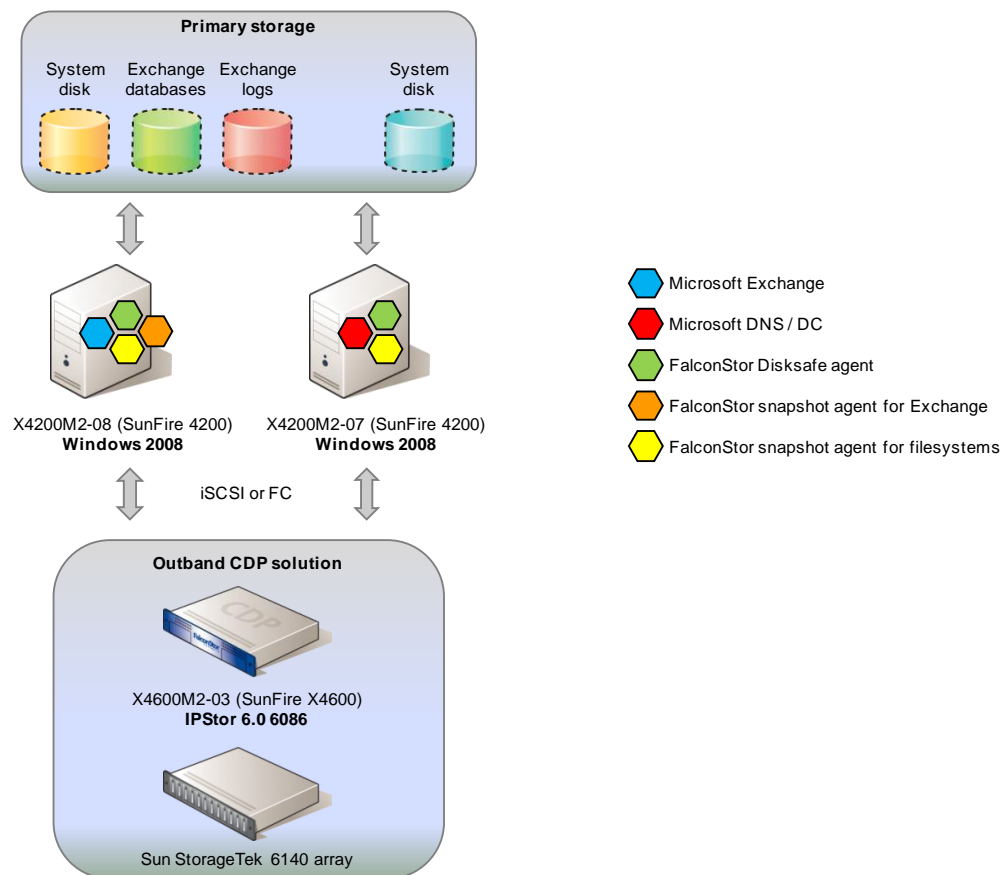


A Typical Configuration

This section illustrates a simple example of how to protect an Exchange environment along with its Domain Controller.

Architecture

Both servers have an internal SATA disk as system disk. The Exchange server uses Fibre Channel protocol to access the storage for its databases and system/log files.



Estimating the storage size needed for the CDP appliance

The amount of storage required to implement the protection of a Microsoft Exchange environment depends on multiple factors. FalconStor can provide guidelines to estimate the sizing needs of a CDP solution. In order to calculate the size of the CDP journal, the following information must be determined:

Item	Value
Number of Windows hosts (physical or virtual)	2
Total storage capacity (# TB) to be protected by CDP Include disk capacity, not only current data size)	2.0TB
Number of days to hold the delta snapshots online	30
Estimated average daily block change rate (%)	4%
Use FC SAN to mirror data from host(s) to CDP appliance(s)	Yes
Use HyperTrac for tape backup; eliminate backup window	No
Replicate local data to a remote site	No
Replicate remote data to a local site	No
Total storage capacity (# TB) replicated from remote site(s)	0.0TB
Number of days to hold the delta snapshots of replica on line	60
Estimated average daily block change rate of replicas (%)	4%

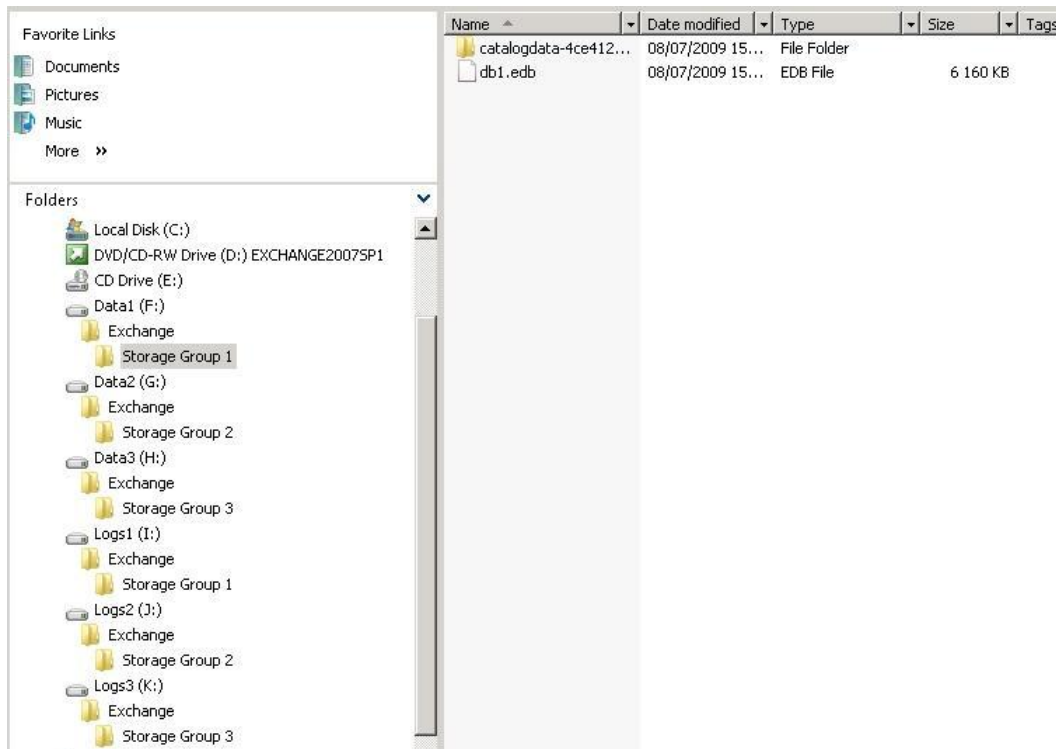
Gathering the above information is essential and the first step in estimating the size of the CDP configuration needed. The next step is an assessment of the Exchange environment. Because the objective of the CDP integration is not just to calculate the amount of data to be protected by the CDP, but also to explain and propose the best methodology to integrate the CDP into the existing Exchange environment. This might include the modification of the existing backup procedures as well as the way disaster recovery is managed and performed.

Microsoft Exchange 2007 Server

In order to demonstrate the CDP solution, the Microsoft Exchange 2007 software has been installed on one server running Windows 2008. In this example, the Exchange 2007 server is connected to the CDP via one dual port 4Gb/s QLogic HBA.

Note: This is not a cluster configuration. However, the CDP solution is also applicable in a clustered solution. CDP provides a Microsoft Cluster agent that is able to consistently protect Microsoft Cluster environments.

The Exchange server has been configured with three storage groups. Each storage group contains one database along with its system and log files. Each database is stored on a different partition. This applies to the system as well as to log files.



Microsoft Domain Controller server

The Microsoft Domain Controller has been installed on a second server using the standard installation procedure. This server is running Windows 2008 and is connected to the CDP appliance via a dual port 4Gb/s QLogic HBA.

SUN StorageTek ST6140 storage array

Disk layout can dramatically affect the performance of the CDP solution. For optimal performance, the following guidelines have been applied:

- If possible, segregate the CDP resources and repository LUNs on two separate RAID groups.
- Use RAID 5 or 6 with a large number of disks (spindles). The more drives, the faster the performance. Use RAID 6 for optimal protection from disk failure for the CDP repository (RAID 6 puts a 20% performance penalty on SATA). Use RAID 5 for FalconStor CDP resources in order to improve the overall performance.
- Do not span LUNs across multiple RAID groups. SATA performance is best when the RAID group has a single write or read activity. The FalconStor CDP resources and repository LUNs are best suited for this configuration.
Note: Storage configuration plans should be aligned with the business' best practice methodology.
- Set the stripe size to 128 KB or greater (multiple of 128) for the FalconStor CDP repository. Generally any stripe size greater than 128 KB (256, 512, etc...) will improve performance. The optimal stripe size ultimately depends on the storage hardware.
- Allocate all LUNs for a RAID group to a single default controller.

Step 1 – Protecting the access to the CDP (front end and back end)

In order to ensure protection of the entire Exchange solution, both the CDP front end and back end data paths must be protected. By connecting the Exchange server to the CDP via multiple paths, you can secure the access to the CDP front end. CDP is able to manage multiple paths by using the FalconStor DynaPath feature (multi-pathing, auto path failover).

In addition, you can connect the storage disk array to the CDP appliance via two independent paths connected to two separate fabrics. This avoids any single point of failure that might negatively affect the protection of the Exchange solution. By doing this, you can ensure the access to the CDP via the preferred path. If a path fails, the CDP automatically moves the disk workflow to the alternate path.

Step 2 – Protecting the Exchange server and the Microsoft domain controller

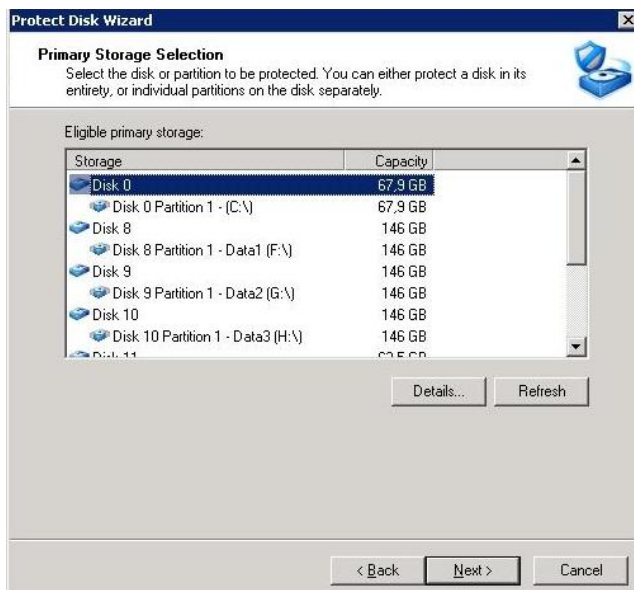
Protecting the Exchange server and the domain controller is the foundation of the proposed solution. Both servers need to be protected by the CDP as they are strongly linked.

Once all of the required software mentioned in the previous chapter has been installed on the servers, some simple configuration steps will allow you to use DiskSafe to protect each disk on each server.

- **Domain Controller server:** DiskSafe + Snapshot Agent for File systems.
- **Exchange server:** DiskSafe + Snapshot Agent for File systems + Snapshot Agent for Exchange + Message Recovery for Exchange.

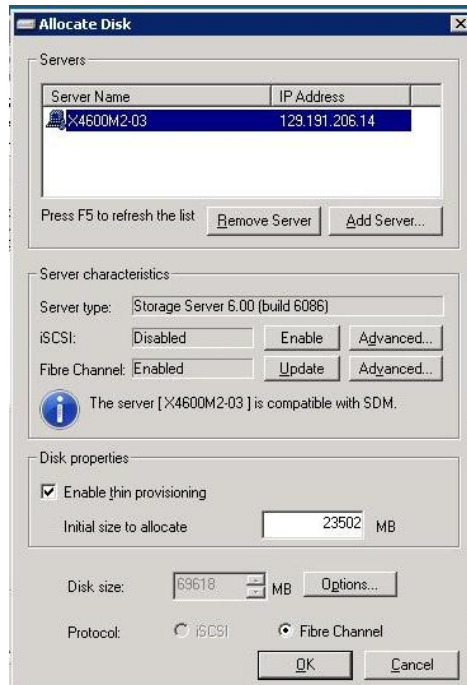
The following steps describe how to protect your data using DiskSafe.

1. Select a disk to protect:

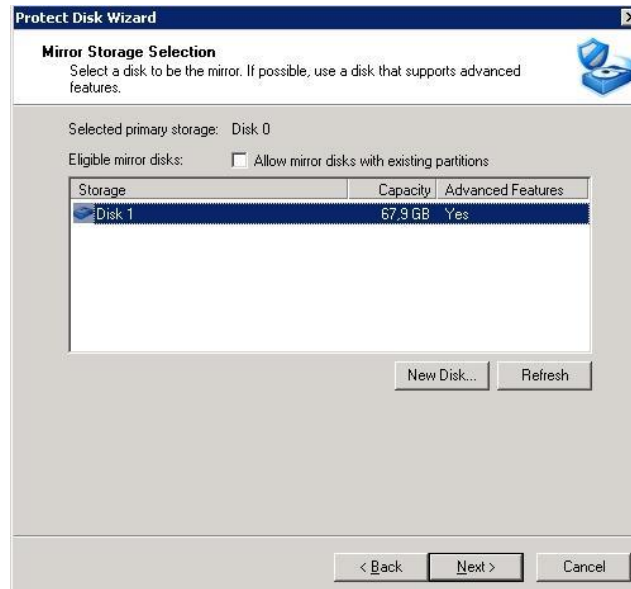


The DiskSafe interface displays the protection as a mirroring operation.

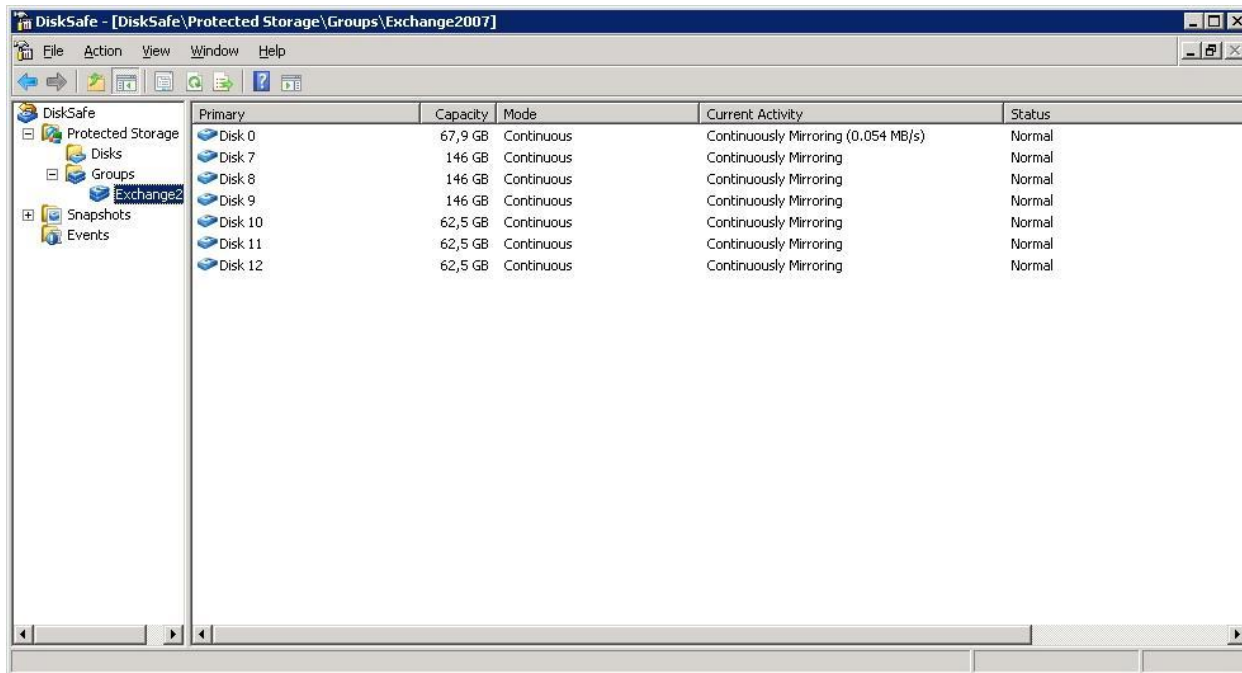
2. Create one virtual disk on the CDP server per data disk to protect:



Once the virtual disk has been created, you can use it to protect your data disk:

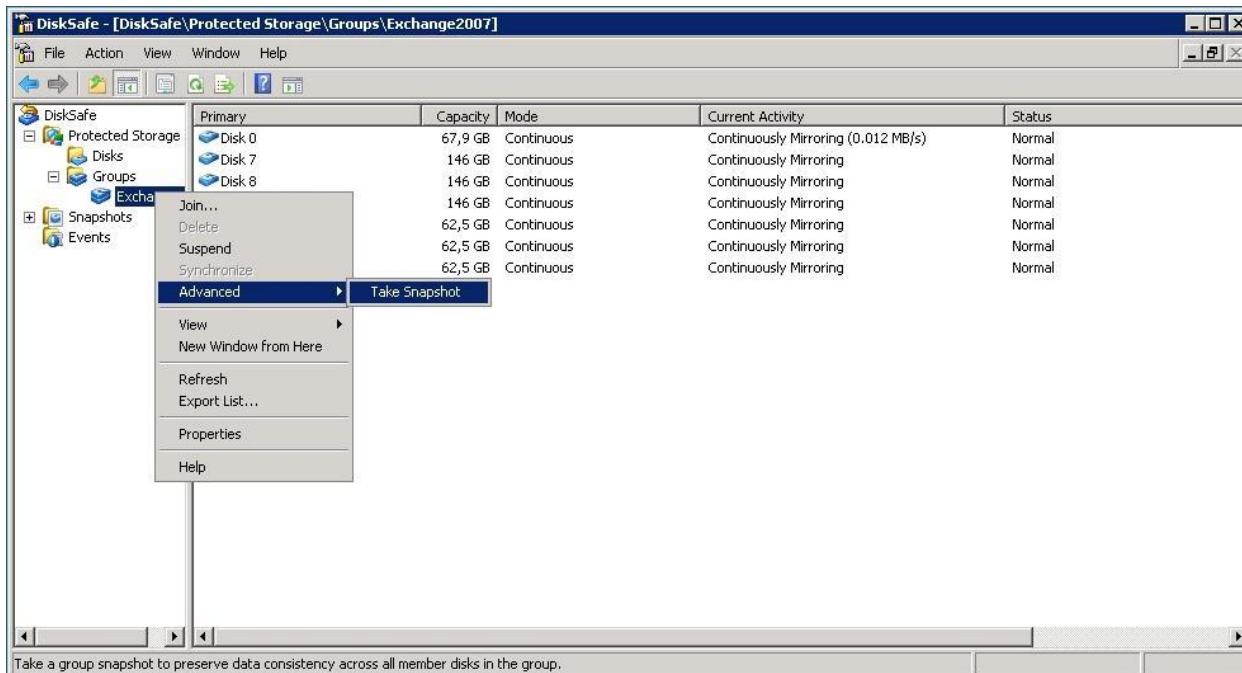


When all of the drives are protected, DiskSafe displays the status of the disks. The screen below illustrates that all of the drives (The system disk + the three database file disks + the three logs file disks) are continuously mirrored. The screen also shows you that the write operations on system disk (Disk 0) are currently generating traffic:

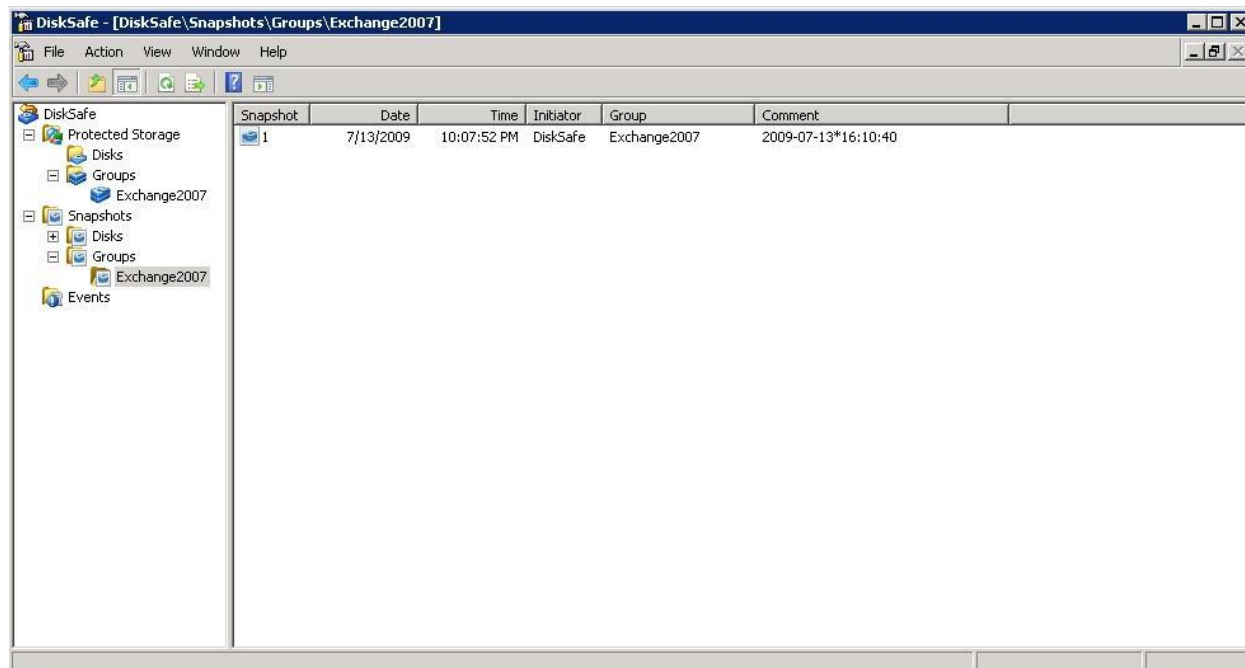


3. Take a Snapshot.

If you want to generate a snapshot, you can schedule one or manually request one by right-clicking on the server and select Advanced → Take Snapshot (as shown below):



Once the snapshot is taken, you can view your consistent snapshot (TimeMark) from the Disk Safe console.



At this stage of the configuration, the Exchanger server and the Microsoft Domain controller are fully protected. This includes both Windows System and Microsoft Exchange application.

Step 3 – Protecting the CDP appliance

1. Autosave option

Once the CDP appliance is installed and configured, you can use the *autosave* option via the FalconStor Management Console to automatically save the CDP configuration to a safe location from where it can be restored.. Thus, all storage configurations are preserved. This includes all of the CDP entities previously created.

In order to protect CDP data (journal, snapshots, and mirrors), read the sections below:

2. CDP Mirror

The basic way to protect a disk or data volume is to mirror its storage onto CDP. The mirror can be defined using disks that are not necessarily identical to each other in terms of vendor, type, or even interface (SCSI, FC, iSCSI). In addition the destination LUNs can be physically located in a local or remote site. Mirroring the protected data ensures instant local access to the CDP data, but it does not protect from localized data center disasters.

3. CDP Replication

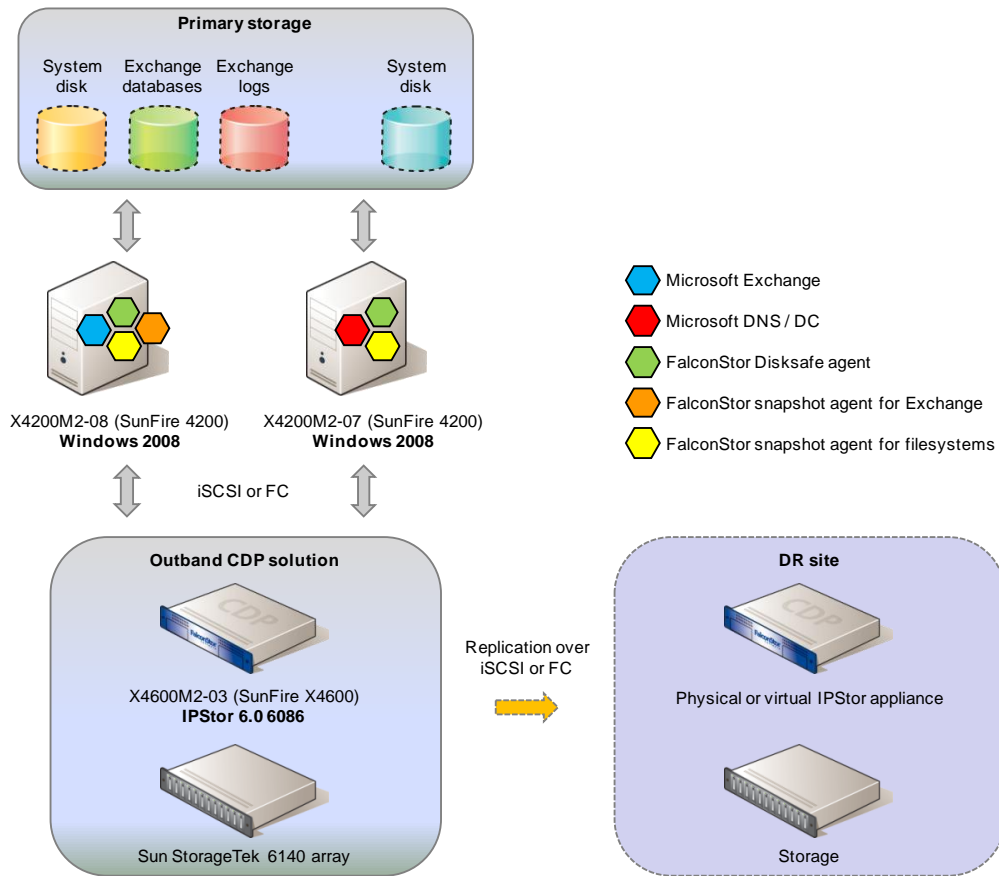
In order to secure the actual CDP appliance and data volumes, another way to protect CDP data is to use FalconStor® Replication. This option allows you to replicate data over any distance and existing networking infrastructure. This can be done locally, using the CDP server, or remotely, using another FalconStor physical or virtual appliance (CDP-VA). The implementation of virtual appliances allows the consolidation of multiple replicas on a single

physical machine. This can significantly reduce the cost of the Disaster Recovery solution by allowing multiple virtual appliances to run on a single consolidated server.

With CDP remote replication, data is copied on a continuous or periodic basis to designated remote CDP DR volumes. These DR volumes can reside on any storage system, including economical SATA or MAID disks. In the event of a primary site disaster, CDP remote replica volumes can be promoted to primary status and used by standby servers or virtual machines.

FalconStor® Remote Replication uses a patented data de-duplication technology called Microscan™, which minimizes the amount of data transferred during replication. Data changes are replicated at the smallest possible level of granularity (512 bytes – disk sectors); reducing transmitted data traffic by as much as 95%, and associated bandwidth costs.

Snapshots of replica volumes can also be mounted during normal operations, allowing the DR site to be used for offsite backup or testing with zero impact on the host server or application. The replication process itself is tunable on a per-volume basis to match the available bandwidth. Data can also be compressed or encrypted.



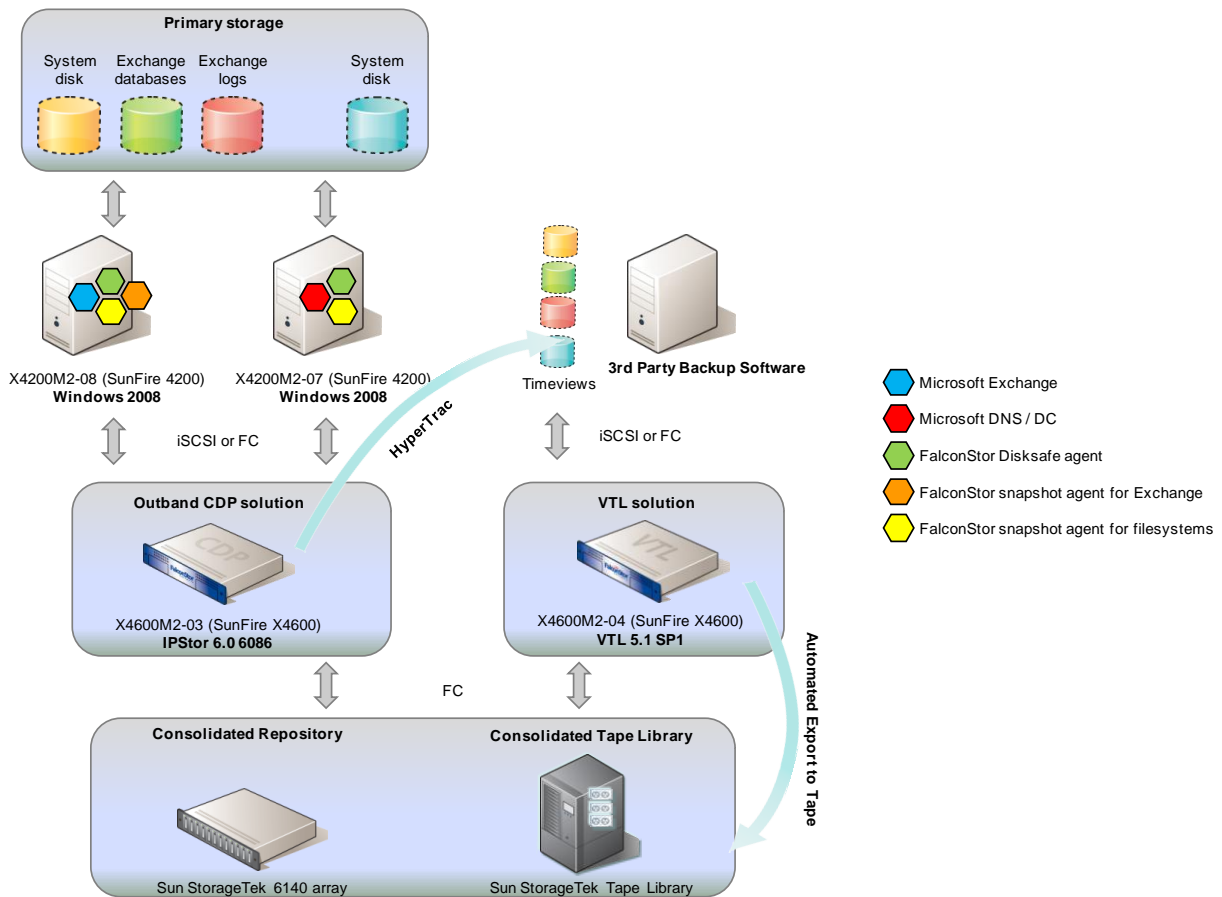
4. CDP and HyperTrac™ : ZerolImpact™ Backup

Legal or regulatory compliance issues often mandate some type of long-term, or permanent, archiving of business data; such as tape backups. FalconStor CDP can complement or minimize tape backups, and their associated costs. FalconStor HyperTrac is a solution that automates and accelerates the process of creating tape backups from CDP TimeMark snapshot volumes.

With HyperTrac, customers can back up data at any time without disruption of business applications or production data volumes, even during peak production hours. HyperTrac resides on the backup server, automatically initiating and mounting FalconStor TimeMark snapshots when backup jobs are performed. This allows the instant recovery of data to any point in time and makes it an ideal software option for organizations that require tape backup for long-term archiving or regulatory compliance.

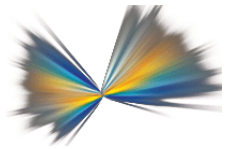
FalconStor HyperTrac Backup Accelerator (HyperTrac) also works in conjunction with FalconStor VTL, allowing faster backup and restore. In this context, you can share the same disk storage pool as VTL (no need to invest in another set of controllers). This type of architecture essentially eliminates the backup window, the host backup agent license fees, management overhead, and removes the backup agent's performance impact on the host.

A typical HyperTrac configuration can look like this:



This solution is ideal for customers that are running VTL in production.

As illustrated, the protection of the CDP appliance is possible via different methods. It is important to keep in mind that all of these methods are not mandatory. The adoption of one of the methods depends on the business requirements and the level of protection expected.



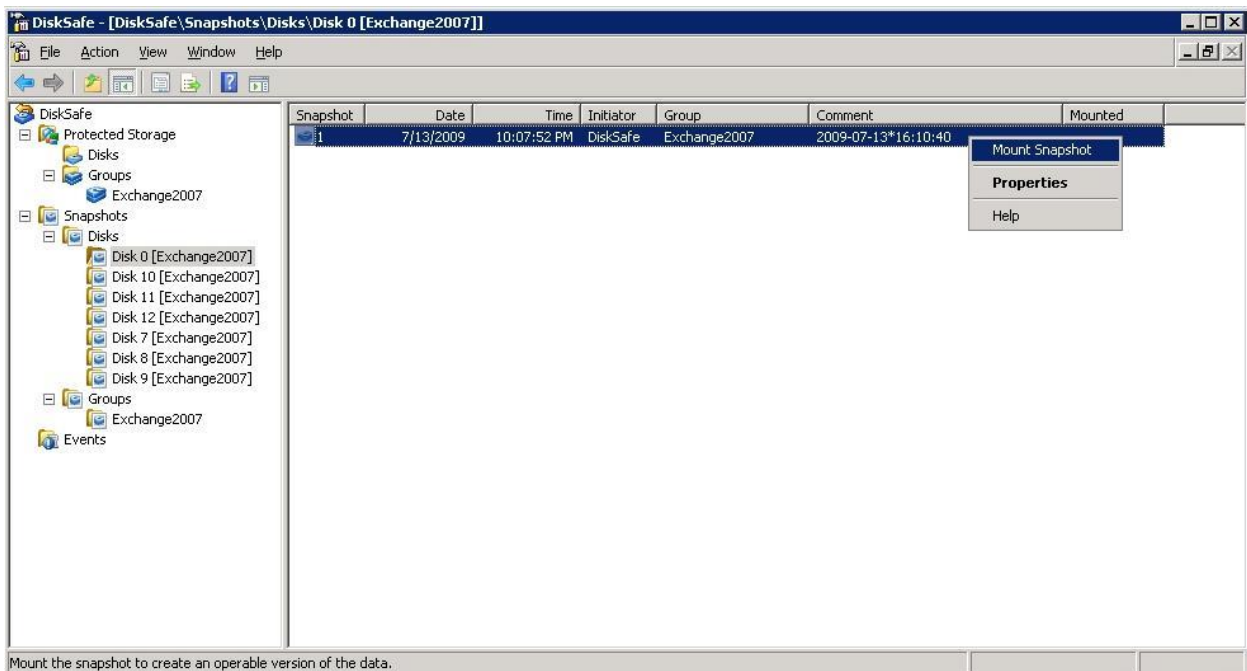
Recovery in an Exchange Environment using CDP

This section contains some examples of data recovery using FalconStor CDP.

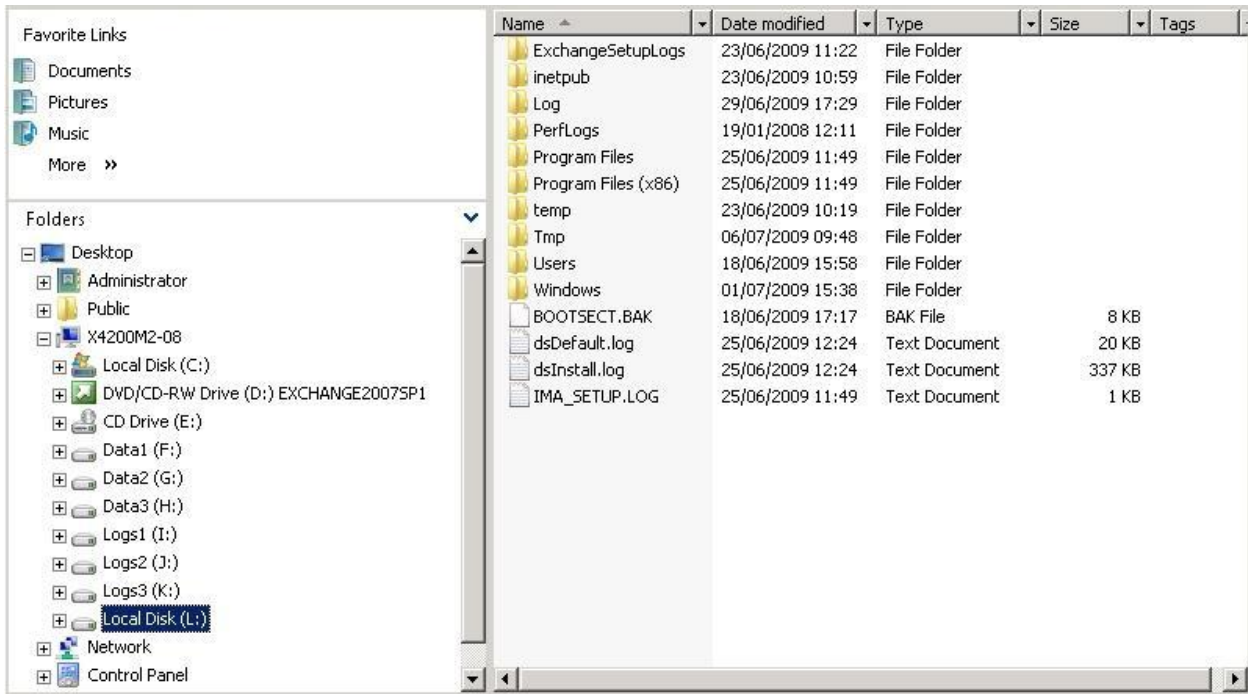
Scenario 1: One or multiple files on a drive

If you have accidentally deleted a file on a disk, the easiest way to recover it is to mount an image of a snapshot containing the missing file. That means a snapshot that was generated prior to the time of the file deletion. Once the snapshot image is mounted, navigate the directory structure, find the previously deleted file and simply copy the file its original location.

See the example below with the system disk (C:), running DiskSafe and mounting the image :



The new partition (L:) displays with the image of system disk (C:):



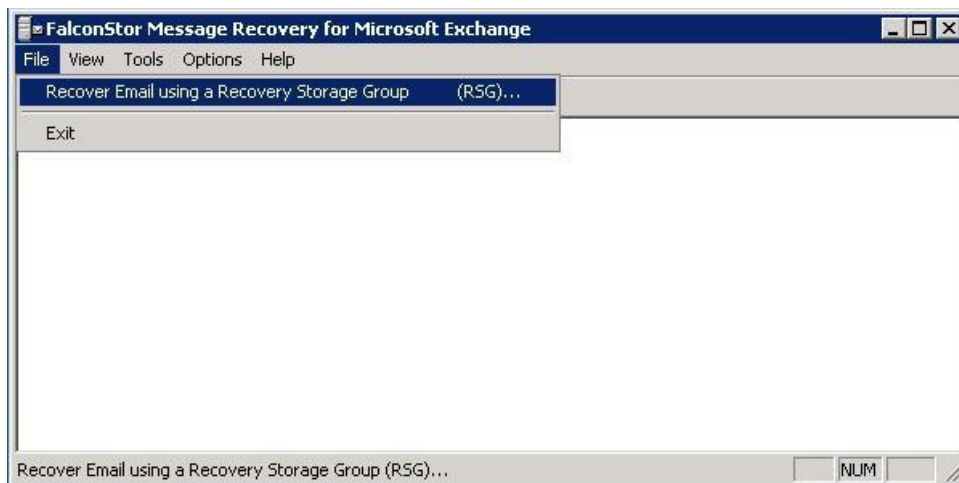
You can retrieve the missing file. As demonstrated, the entire operation takes only a few minutes.

The CDP appliance is able to manage several snapshots (up to 255), allowing the CDP administrator to restore the source system to a specific date or time.

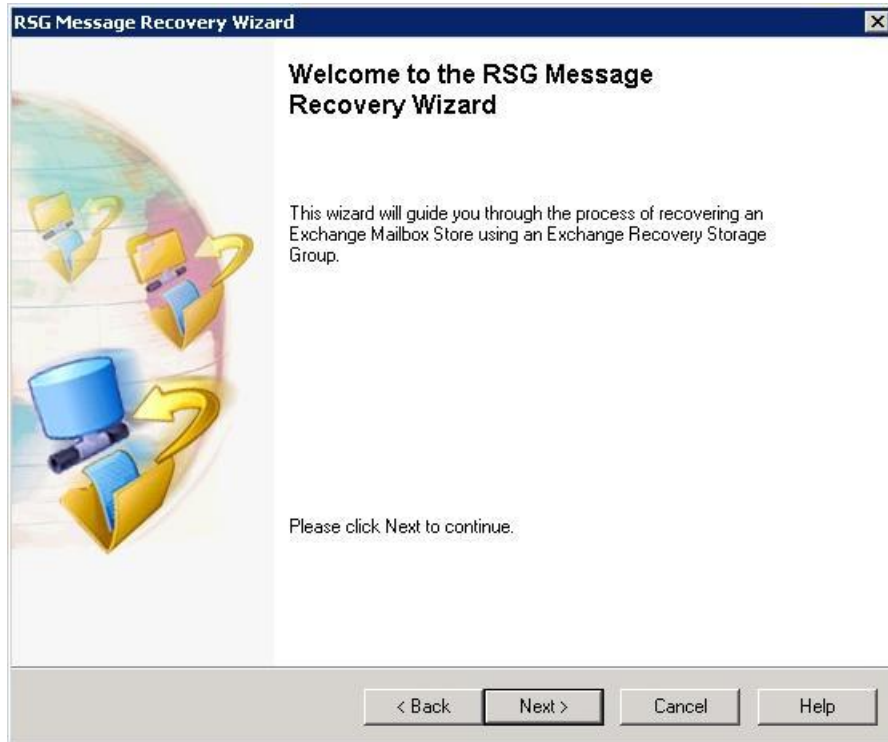
Scenario 2: One or multiple emails

If you want to recover lost emails, you can run the FalconStor Message Recovery for Exchange utility on your Exchange server, as illustrated below:

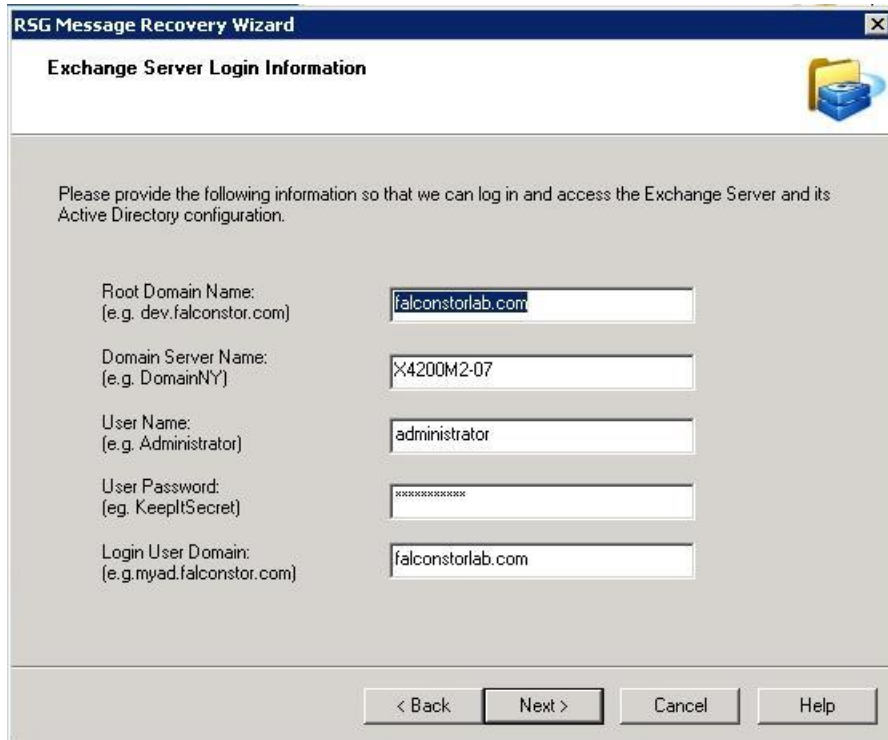
1. Select the recover email option: (File → Recover Email using a Recovery Storage Group)



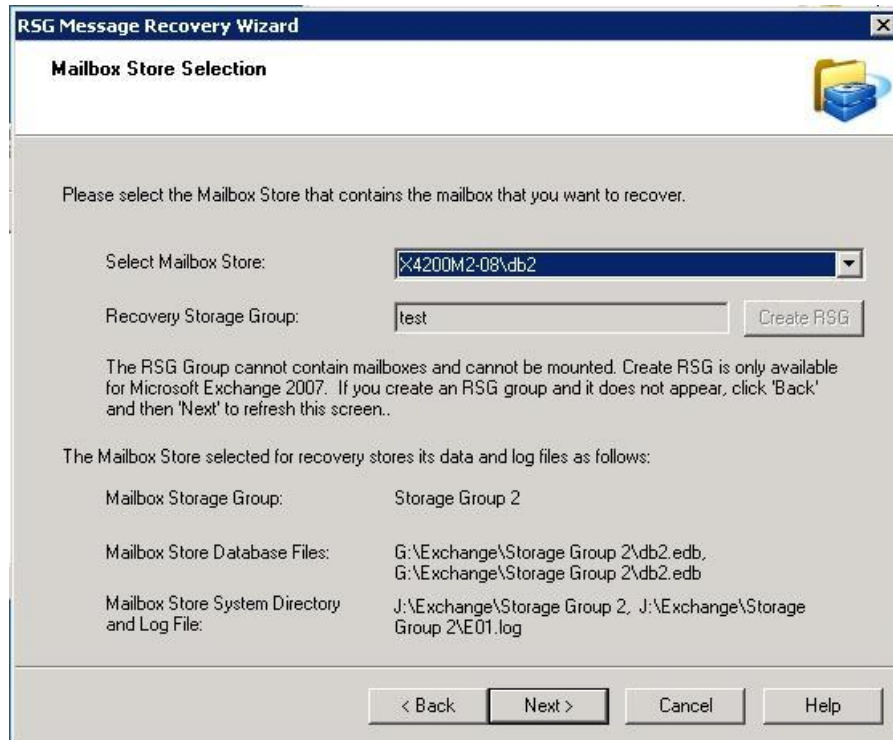
The following window is displayed:



2. Enter Exchange Server authentication information:

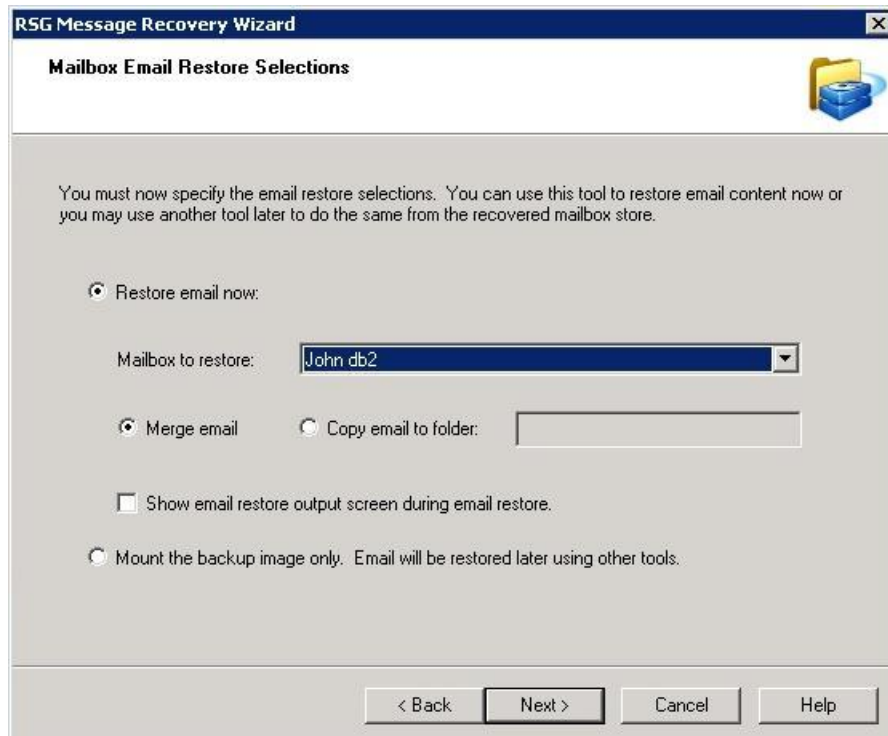


3. Select the database from which you want to recover:

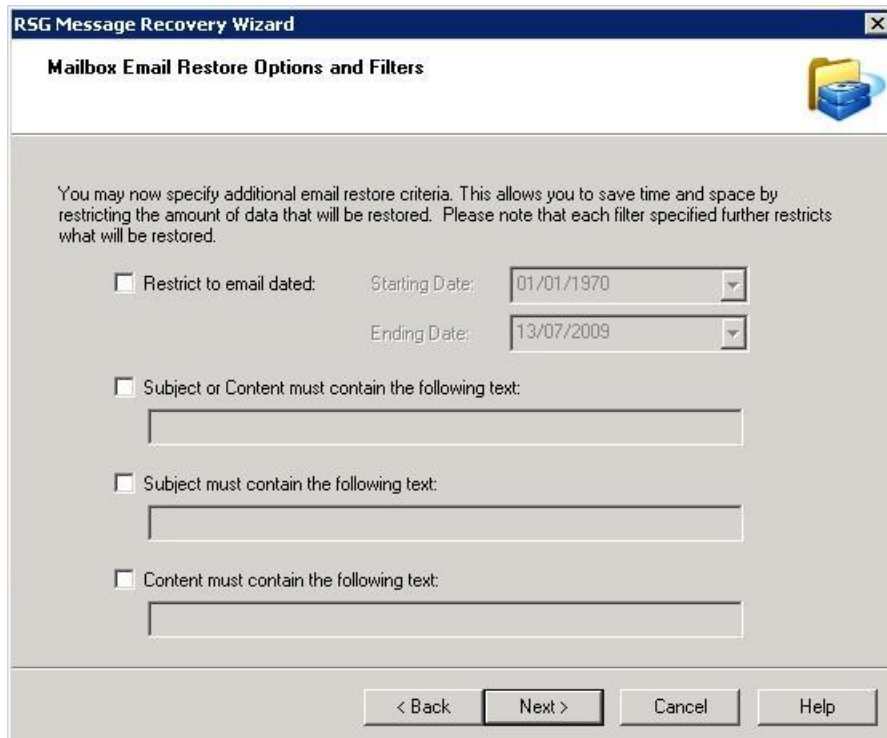


4. Select any mailboxes for restoration.

The following screen shows a single mailbox restoration, merging recovered messages into the user's existing mailbox:



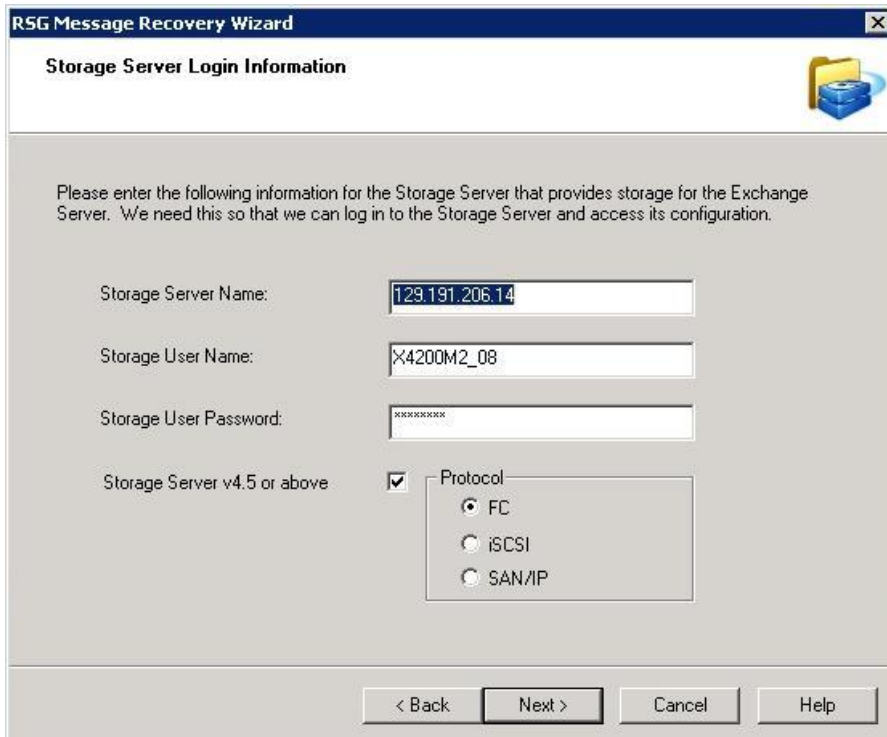
5. Choose optional search filters for the recover emails:



The screenshot shows the 'Mailbox Email Restore Options and Filters' window of the RSG Message Recovery Wizard. It contains the following elements:

- Restrict to email dated:** A checkbox that is unchecked. To its right are two date pickers: 'Starting Date' set to '01/01/1970' and 'Ending Date' set to '13/07/2009'.
- Subject or Content must contain the following text:** A checkbox that is unchecked, followed by an empty text input field.
- Subject must contain the following text:** A checkbox that is unchecked, followed by an empty text input field.
- Content must contain the following text:** A checkbox that is unchecked, followed by an empty text input field.
- Navigation buttons:** '< Back', 'Next >', 'Cancel', and 'Help'.

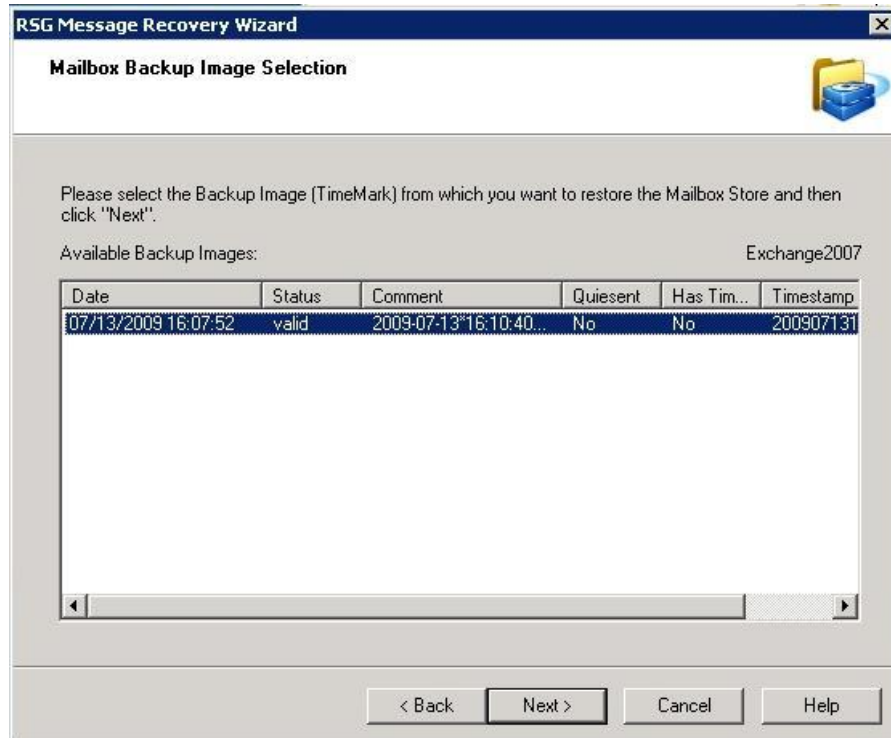
6. Choose the CDP Server you are going to use:



The screenshot shows the 'Storage Server Login Information' window of the RSG Message Recovery Wizard. It contains the following elements:

- Storage Server Name:** A text box containing '129.191.206.14'.
- Storage User Name:** A text box containing 'X4200M2_08'.
- Storage User Password:** A text box containing '*****'.
- Storage Server v4.5 or above:** A checkbox that is checked.
- Protocol:** A group box containing three radio buttons: 'FC' (selected), 'iSCSI', and 'SAN/IP'.
- Navigation buttons:** '< Back', 'Next >', 'Cancel', and 'Help'.

7. Finally, choose the snapshot from which you want to recover, and let the RSG Message Recovery Wizard complete the process:



At the end of this process, the emails are restored in the user's mailbox. This procedure is totally transparent from the end user perspective. Again, if multiple snapshots are available, the CDP administrator can select the one that corresponds to a specified date when the system must be restored.

Scenario 3: Recovering from scratch after a system disk failure or a major disaster

What if you have a crash of your entire server disk, which not only contains your operating system but also your exchange binaries? In this case, you can recover it very quickly using the DiskSafe Recovery CD. Insert a new system disk at the same slot in your server, boot the server using the Recovery CD, use the software to access the CDP server, choose the snapshot volume you want to use and let the software restore the data onto your new disk.

You can also restart from a new physical machine as long as the new server is the same type as the server impacted by the major disaster. The recovery process restores exactly the same configuration as before the disaster occurred.



Conclusion

Compared to traditional backup methods, which significantly impact production Exchange servers, the FalconStor Continuous Data Protector (CDP) allows you to backup your Exchange data faster and with minimal impact on your production operations. Recovering lost data to any point of time is also faster and easier.

Different technologies such as TimeMark[®], DiskSafe[™], and HyperTrac[™] can be combined to completely protect Microsoft Exchange environments. These technologies allow implementation of different levels of protection to fit any business requirement.

FalconStor CDP replaces or compliments your legacy tape backup solution; providing instant recovery capability, eliminating the backup window and reducing costs associated with tape-based backup solutions. FalconStor CDP helps you to reduce the *Total Cost of Ownership* of your backup solution. Several Exchange environments can be protected by the same CDP appliance, and can share the same repository as the VTL. As a Totally Open[™] solution, the FalconStor CDP also maximizes the Return on Investment (ROI) associated with your current backup solution.

This document demonstrates that the implementation of this data protection and recovery solution can be made quickly and without complex training. The solution is simple, scalable, reliable and powerful; it can take advantage of several FalconStor products, including FalconStor CDP, HyperTrac and FalconStor VTL.



Appendix

References

- CDP-NSS Reference Guide
- Snapshot Agents User Guide
- Recovery Agents User Guide
- HyperTrac User Guide
- DiskSafe User Guide
- http://en.wikipedia.org/wiki/Service_level_agreement
- http://en.wikipedia.org/wiki/Service_level_objective