



# Continuous Data Protector (CDP) Technical Whitepaper

Using FalconStor CDP with Oracle 11g

**FalconStor**<sup>®</sup>  
Software

---

# Using FalconStor CDP with Oracle 11g

## *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](http://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.

9.18.2009



# Contents

---

<b>Contents .....</b>	<b>iii</b>
<b>Introduction .....</b>	<b>4</b>
Abstract .....	4
Document Scope.....	4
Audience.....	4
Assumptions .....	4
<b>FalconStor Continuous Data Protector.....</b>	<b>6</b>
Overview .....	6
Key features .....	6
Terminology .....	8
<b>Integration with Oracle Database Server .....</b>	<b>9</b>
Overview .....	9
How does it work? .....	9
<b>A Typical Configuration.....</b>	<b>11</b>
Architecture.....	11
Estimating the storage size needed for the CDP appliance.....	12
Oracle database 11g server .....	12
Step 1 – Protecting access to the CDP server (front end and back end) .....	13
Step 2 – Protecting the Oracle server .....	13
Step 3 – Protecting the CDP appliance.....	18
<b>Recovering your Oracle 11g Database with CDP.....</b>	<b>21</b>
Scenario 1: One or multiple files on a disk .....	21
Scenario 2: A non-system disk or partition recovery.....	22
Scenario 3: A system disk or partition recovery .....	22
Scenario 4: Oracle database object recovery .....	22
Scenario 5: Oracle database point-in-time complete recovery .....	23
<b>RMAN and CDP .....</b>	<b>24</b>
<b>Conclusion.....</b>	<b>25</b>
<b>Appendix.....</b>	<b>26</b>
Sources.....	26
Reference documents .....	26



# **Introduction**

---

## **Abstract**

The FalconStor® Continuous Data Protector (CDP) solution provides disk-based 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 an Oracle 11g server and its 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.

Oracle integration is also available with other FalconStor products. FalconStor NSS and FalconStor VTL-SIR reduce Oracle management costs with storage consolidation, achieve 99.999% availability of Oracle databases with storage virtualization, and eliminate redundant data and shrink your backup repository by up to 95% using deduplication technology.

## **Document Scope**

This paper describes the basic concepts and integration guidelines for FalconStor CDP in an Oracle 11g environment. The document is intended to provide an architectural overview of CDP being used with Oracle software along with the benefits of a combined solution. The objective is to propose a procedure to protect an Oracle 11g environment, starting from the operating system (OS) to the relational database management system (RDBMS) server and associated database files. 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 Oracle environment protection concepts, and partners interested in FalconStor CDP. This document is especially beneficial for IT directors, storage administrators, backup administrators, database administrators, datacenter managers, architects and others involved in the administration of backup architecture including Oracle RDBMS. 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:

- Oracle 11g
- Oracle Enterprise Linux operating system
- Network-attached storage and protocols (i.e. iSCSI, FC)
- 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
<b>Recovery Point Objective (RPO)</b>	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.
<b>Recovery Time Objective (RTO)</b>	The maximum amount of downtime a business is willing to accept which is equivalent to the time period from incident of failure, to resumption of business operations.
<b>Service Level Agreement (SLA)</b>	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.
<b>Service Level Objective (SLO)</b>	<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 FalconStor CDP, so an introduction to the product is included.



# FalconStor Continuous Data Protector

---

## Overview

FalconStor CDP is a secondary backup, storage solution that features *per-write data journaling* for local and remote recovery. CDP supports two modes of data protection, continuous and periodic. Continuous protection mode allows organizations to recover data to the most recent point, or transaction, before a service disruption occurred. FalconStor CDP periodic mode protection via FalconStor TimeMark® technology provides point-in-time snapshots with transactional integrity for rapid recovery, data set duplication, backup window elimination, DR validation, and long-term data retention.

Periodic mode snapshots can be created manually or by a defined schedule, such as every hour or every few hours, delivering substantially more recovery points than daily tape backup. Additionally, FalconStor CDP provides WAN-optimized remote replication for recovery at a remote data center. Its flexible features allow switching between continuous and periodic remote replication modes based upon the availability and capability of the WAN link connecting to the DR site.

Traditional tape backup and data archiving focus 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 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 a 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. Supports both 1 and 10 Gb Ethernet.

**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 Provisioning:** 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 Provisioning may be applied to primary storage, replica storage (at the DR site), and mirrored storage.

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

**TimeView<sup>®</sup> 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, Unix, and Linux operating systems (32-bit and 64-bit).

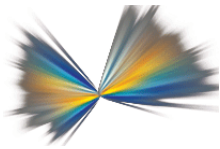
**FalconStor HyperTrac<sup>™</sup> Backup Accelerator option:** Supports serverless file backup, enabling the backup server to connect to a FalconStor CDP appliance and assist with backup by automatically mounting the selected snapshot volume. This option completely backs up protected data volumes to tape or to a virtual tape library such as FalconStor Virtual Tape Library (VTL).

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

## Terminology

The primary components of the FalconStor CDP solution are the CDP appliance, CDP clients, DiskSafe, and Snapshot agents), 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 Administrator Guide* and/or the *FalconStor CDP/NSS Reference Guide*.

Component	Definition
<b>Appliance</b>	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.
<b>Clients</b>	The term used to designate all hosts that use the CDP appliance to protect their data. The Oracle server is therefore considered a client.
<b>Console</b>	The administrative tool that allows you to configure your CDP appliance. It is also called the FalconStor Management Console.
<b>Snapshot agent</b>	Software that allows a snapshot to be consistent by forcing an application to be quiescent. It applies to databases, messaging systems, and file systems for fastest point-in-time recovery.
<b>Journal</b>	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.
<b>TimeMark</b>	A consistent snapshot.
<b>TimeView</b>	The mounted image of a TimeMark.
<b>Mirror disk</b>	A full and independent copy of the primary data volume, updated using the journal.
<b>Out-of-band</b>	A solution which is not in the production data path.



# Integration with Oracle Database Server

---

## Overview

The FalconStor CDP solution integrates tightly with Oracle 11g to enable seamless protection, automate and streamline data recovery, and optimize operational efficiency. It allows you to:

- Enable instant recovery of your Oracle application and/or database.
- Achieve the best RPO; depending on the period you have defined for snapshots with transactional integrity (TimeMarks).
- Reduce remote Oracle disaster recovery bandwidth costs with WAN-optimized replication.

## How does it work?

FalconStor CDP can be configured to protect disk volumes over any network protocol. Since Oracle database files require special treatment in order to preserve transactional integrity, the FalconStor Snapshot Agent for Oracle is also used to protect the database files.

FalconStor CDP can be configured to protect the Oracle database application and underlying operating system, as well as the database volume (or volumes) separately; this creates mirror volumes protecting the customized database application and the actual data. The mirror copies are maintained by the CDP server using a journal, allowing granular transaction recovery. Consistent, application-aware, snapshots can be scheduled periodically or triggered on demand.

The FalconStor CDP solution includes:

- **FalconStor CDP:** The core of the solution, the software 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.
- **FalconStor 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 the main interface to use for configuring and manage the data protection.
- **FalconStor Snapshot Agent for Oracle:** DiskSafe coordinates with this Oracle-specific snapshot agent to provide 100% transactionally consistent snapshots, eliminating 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. The agent supports the ASM (Automated Storage Management) file system and OCFS (Oracle Cluster File System) file system.

- **FalconStor Snapshot Agent for File Systems:** This agent functions similarly to the *Snapshot Agent for Oracle* except that it interfaces with the operating file system. Prior to starting the snapshot process, all disk caches and buffers are flushed to disk. Once you install the version corresponding to your operating system, it is automatically triggered by DiskSafe when requesting a new snapshot (TimeMark).
- **FalconStor 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.
- **FalconStor DiskSafe Recovery CD:** If you have lost your system disk, you can boot your server using the DiskSafe Recovery CD. This tool allows you to access the snapshot stored on the CDP to easily recover your system and data on a new system drive.
- **FalconStor DynaPath®:** If your configuration includes multiple HBAs or an HBA with multiple ports, it is a good idea to use the DynaPath tool. DynaPath 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.

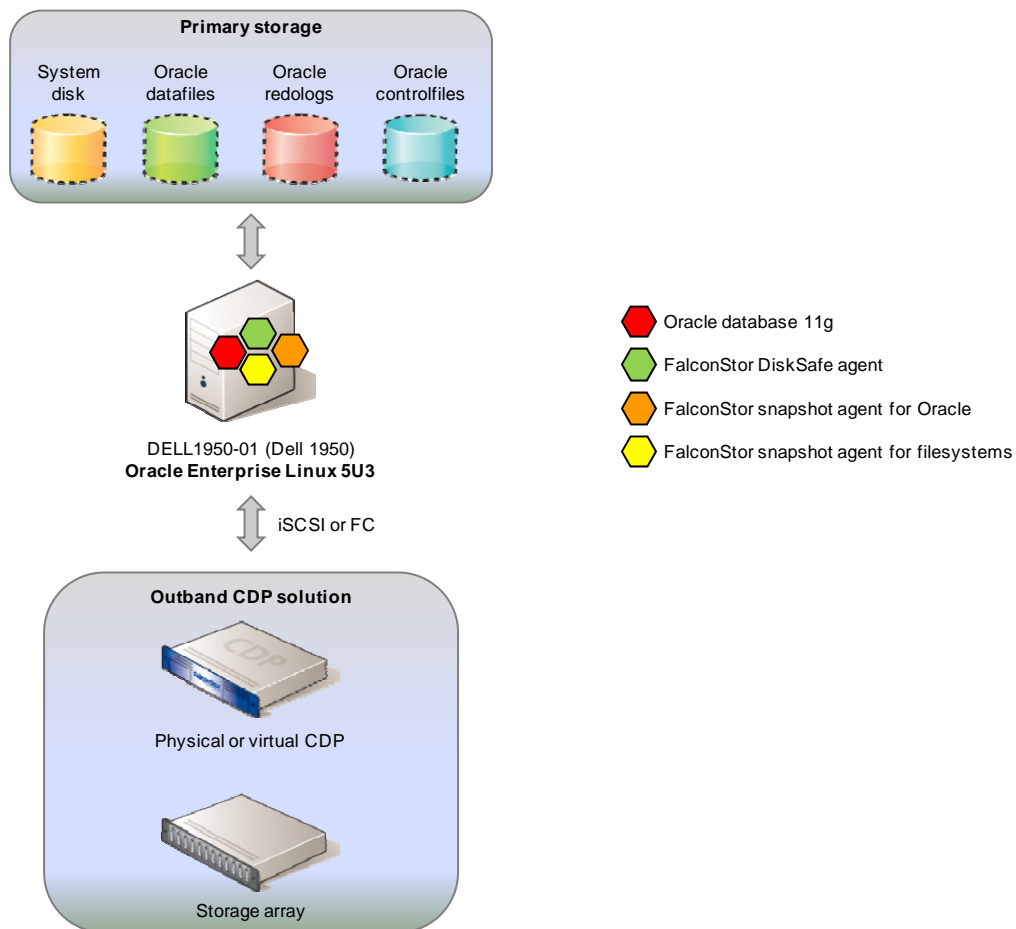


# A Typical Configuration

This section illustrates a simple example of how to protect an Oracle database 11g installed on a Linux server.

## Architecture

The Linux server has an internal SATA disk as a system disk, but uses FC LUNs to store Oracle 11g binaries and all database files.



## Estimating the storage size needed for the CDP appliance

The amount of storage required to protect an Oracle 11g database 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)	0
Number of Linux 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 an essential first step in estimating the size of the CDP appliance needed. The next step is an assessment of the Oracle solution. Because the objective of the CDP integration is not just to calculate the amount of data to be set for the CDP, but also to explain and propose the best methodology to integrate the CDP into the existing Oracle environment. This might include modification of the existing backup procedures as well as the way disaster recovery is managed and performed.

### Oracle database 11g server

In order to demonstrate a CDP solution, we will assume that the Oracle database 11g (11.1.0.6.0) software has been installed on a Dell 1950 server running Oracle Enterprise Linux release 5 update 3. In this example, the Oracle 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 will be also applicable to a RAC configuration in a near future.

The Oracle server has been configured with one single test instance called *orcl*. Two LUNs have been assigned via FC to the server. They are mounted on /u01 and /u02. The file system /u01 contains Oracle binaries, configuration files, basic log files, one Oracle control file, and the redo logs. The file system /u02 contains the data files, another control file, and the archived redo logs.

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

In order to ensure protection of the entire Oracle solution, both the CDP front end and back end must be protected. By connecting the Oracle server to the CDP via multiple paths, you can secure access to the CDP front end. CDP is able to manage multiple paths by using FalconStor DynaPath.

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 Oracle solution. By doing this, you can ensure the access to the CDP buffer via the preferred path. If a path fails, the CDP automatically moves the disk workflow to the alternate path.

## Step 2 – Protecting the Oracle server

Protecting the Oracle server is the foundation of the proposed solution. Once all of the required software mentioned in the previous chapter has been installed on the server (FalconStor DiskSafe + FalconStor Snapshot Agent for File systems + Snapshot Agent for Oracle), some simple configuration steps will allow you to use FalconStor DiskSafe to protect every disk (system and data).

The example below uses standard ext2 file system but it also works with ASM or OCFS partitions.

The following steps describe how to protect your Oracle resources using DiskSafe CLI on the Oracle server.

1. Configure the CDP server and the preferred protocol (iSCSI or FC):

```
# dscli server add server=129.191.206.14 user=DELL1950_01 passwd=*** protocol=fc
# dscli server list
Total IPStor server: 1
IPStor server: X4600M2-03
IP      : 129.191.206.14
Server type : IPStor
Version  : 6.0 (Build 6086)
Protocol  : Fiber Channel SAN/IP
```

The CDP server is now enable to protect the Oracle server resources.

2. Protect every disk and/or partition mounted on the Oracle server.

The example below illustrates the first partition /dev/sdb mounted on /u01, which contains Oracle home and other Oracle related files:

```
# dscli disk protect primary=sdb
Protect sdb with new disk in continuous mode

Allocating mirror disk with 20480000 sectors

Please select a storage server to assign mirror disk:
1) 129.191.206.14
0) Exit
Your choice: 1
Mirror disk has been successfully assigned using Fibre Channel protocol.

Disk successfully protected.
Command succeeded
```

For full protection of your Oracle server, you must protect the Oracle disks along with all others disks including the disk with the operating system. This will simplify the recovery in case of a disaster.

Once all disks and/or partitions are protected (mirrored on the CDP server), you have to create a group so that you will be able to create a snapshot that is consistent across all the protected resources.

### 3. Create a group and assign the disks to it.

In the example below, the disks sdb (/u01) and sdc (/u02) are added to the newly created group:

```
# dscli group new oracle
# dscli group join oracle sdb
# dscli group join oracle sdc
# dscli group list
All groups:

Group Count: 1
Group 1: oracle
Mode = Continuous
Snapshot Scheduled = False
Take Temporary Snapshot Before Sync = False
Remove Temporary Snapshot After Sync = False
Invoke Snapshot Agent = True
Maximum Snapshots = 255
Retry Interval = 60 S
Member Count = 2
Members:
  Member ID = 1
  Disk = sdb
  Primary Disk Path = /dev/sdb
  Disksafe Disk = /dev/disksafe/sdb
  Mount Point(s) = /u01
  Primary DiskSafe ID = FALCON_IPSTOR_DISK_____6000d779000077eb3c2f706620789f6c
  Mirror Disk Path = /dev/sdf
  Mirror DiskSafe ID = FALCON_IPSTOR_DISK_____6000d778bb3a0d223cde00004a85ccdd

  Member ID = 2
  Disk = sdc
  Primary Disk Path = /dev/sdc
  Disksafe Disk = /dev/disksafe/sdc
  Mount Point(s) = /u02
  Primary DiskSafe ID = FALCON_IPSTOR_DISK_____6000d779000058341d356ffcf9c9c23e9
  Mirror Disk Path = /dev/sdg
  Mirror DiskSafe ID = FALCON_IPSTOR_DISK_____6000d779218470ecc05c00004a8c0591

Command succeeded
```

**Note:** The above example also shows the devices (sdf and sdg) that have been created on the CDP server as targets for the mirroring operation.

Check the protection status using the following command:

```
# dscli group stat oracle
Status and statistics for group: oracle

Group: oracle
Group Status = IN-SYNC
LastSync = 2009/08/19 17:34:21
LastScheduledSync = 2009/08/19 14:50:40
Mode = Continuous
Snapshot Scheduled = False
Take Temporary Snapshot Before Synchronization = False
Remove Temporary Snapshot After Synchronization = False
Invoke Snapshot Agent = True
```

```

Maximum Snapshots                = 255
Retry Interval                   = 60 S
Member Count                     = 2

Member status and statistics:
Member 1:
  Disk                           = sdb
  Primary Disk Path              = /dev/sdb
  Disksafe Disk                  = /dev/disksafe/sdb
  Mount Point(s)                 = /u01
  DiskSafe ID                    =
FALCON__IPSTOR_DISK_____6000d779000077eb3c2f706620789f6c
  Mirror Disk Path               = /dev/sdf
  Mirror DiskSafe ID            =
FALCON__IPSTOR_DISK_____6000d778bb3a0d223cde00004a85ccdd
  Mirror State                   = IN-SYNC
  Different Data                 = 0 KB
  Total Data Mirrored           = 13824 KB
  Primary Total Read             = 144957 KB
  Primary Total Written          = 162912 KB
  Mirror Total Read              = 0 KB
  Mirror Total Written          = 173928 KB
Statistics Since Last Sync:
  Primary Total Read             = 2004 KB
  Primary Total Written          = 59836 KB
  Mirror Total Read              = 0 KB
  Mirror Total Written          = 59964 KB
  Last Sync Time                 = 2009/08/19 17:34:21
  Duration in Current State     = 7859 S

Member 2:
  Disk                           = sdc
  Primary Disk Path              = /dev/sdc
  Disksafe Disk                  = /dev/disksafe/sdc
  Mount Point(s)                 = /u02
  DiskSafe ID                    =
FALCON__IPSTOR_DISK_____6000d779000058341d356ffcfc9c23e9
  Mirror Disk Path               = /dev/sdg
  Mirror DiskSafe ID            =
FALCON__IPSTOR_DISK_____6000d779218470ecc05c00004a8c0591
  Mirror State                   = IN-SYNC
  Different Data                 = 0 KB
  Total Data Mirrored           = 512 KB
  Primary Total Read             = 189617 KB
  Primary Total Written          = 155640 KB
  Mirror Total Read              = 0 KB
  Mirror Total Written          = 156036 KB
Statistics Since Last Sync:
  Primary Total Read             = 680 KB
  Primary Total Written          = 64284 KB
  Mirror Total Read              = 0 KB
  Mirror Total Written          = 64412 KB
  Last Sync Time                 = 2009/08/19 17:34:21
  Duration in Current State     = 7859 S

Command succeeded

```

As you can see, the *invoke agent snapshot* option is set to *true*. This means that registered snapshot agents available on the server will be triggered when a snapshot is launched.

**Note:** Do not forget to add all other disks and/or partitions to the DiskSafe group to simplify recovery in case of a disaster.

You are now ready to schedule snapshots or request a snapshot on demand, as shown below:

```

# dscli group snapshot take oracle
Take a snapshot for group: oracle

```

```
Taking snapshot.....
Command succeeded
```

The snapshot operation typically lasts one or two seconds, but the entire operation takes a little bit more time when triggering snapshot agents.

During the operation, the database remains online, but is put in *backup mode* by the FalconStor Snapshot Agent for Oracle. While in *backup mode*, the database files are "frozen" and all incoming data is written in the redo log files. Once the snapshot is complete, the agent notifies the database to end the backup, synchronizing all data back to the database.

The following example shows an extract of the alert.log file when the snapshot is requested:

```
...
Thu Aug 20 10:21:07 2009
ALTER database backup controlfile to
'/u01/app/oracle/diag/rdbms/orcl/orcl/trace/is_oractl00.bak'
Completed: ALTER database backup controlfile to
'/u01/app/oracle/diag/rdbms/orcl/orcl/trace/is_oractl00.bak'
alter database backup controlfile to trace
Backup controlfile written to trace file
/u01/app/oracle/diag/rdbms/orcl/orcl/trace/orcl_ora_8560.trc
Completed: alter database backup controlfile to trace
ALTER tablespace "SYSTEM" begin backup
Completed: ALTER tablespace "SYSTEM" begin backup
ALTER tablespace "SYSAUX" begin backup
Completed: ALTER tablespace "SYSAUX" begin backup
ALTER tablespace "UNDOTBS1" begin backup
Completed: ALTER tablespace "UNDOTBS1" begin backup
ALTER tablespace "USERS" begin backup
Completed: ALTER tablespace "USERS" begin backup
ALTER tablespace "EXAMPLE" begin backup
Completed: ALTER tablespace "EXAMPLE" begin backup
Thu Aug 20 10:21:13 2009
ALTER tablespace "SYSTEM" end backup
Completed: ALTER tablespace "SYSTEM" end backup
ALTER tablespace "SYSAUX" end backup
Completed: ALTER tablespace "SYSAUX" end backup
ALTER tablespace "UNDOTBS1" end backup
Completed: ALTER tablespace "UNDOTBS1" end backup
ALTER tablespace "USERS" end backup
Completed: ALTER tablespace "USERS" end backup
ALTER tablespace "EXAMPLE" end backup
Completed: ALTER tablespace "EXAMPLE" end backup
Thu Aug 20 10:21:14 2009
...
```

In our example the database remains in *backup mode* for 7 seconds.

If you want to list the available snapshots for the group, use the command below:

```
# dscli group snapshot list oracle
List snapshots for group: oracle

Snapshot 1:
  Snapshot Timestamp      = 1250686831(2009/08/19 15:00:31)
  Snapshot Blocks Count   = 200519680

Snapshot 2:
  Snapshot Timestamp      = 1250754757(2009/08/20 09:52:37)
  Snapshot Blocks Count   = 10305536

Snapshot 3:
  Snapshot Timestamp      = 1250755053(2009/08/20 09:57:33)
  Snapshot Blocks Count   = 301740032

Snapshot Count: 3
```

```
Command succeeded
```

You can also list the available snapshots for a specific disk:

```
# dscli snapshot list sdb
All snapshots of sdb

Snapshot 1:
  Snapshot Timestamp   = 1250686831(2009/08/19 15:00:31)
  Snapshot Blocks Count = 132395008
  Mounted              = NO

Snapshot 2:
  Snapshot Timestamp   = 1250754757(2009/08/20 09:52:37)
  Snapshot Blocks Count = 4112384
  Mounted              = NO

Snapshot 3:
  Snapshot Timestamp   = 1250755053(2009/08/20 09:57:33)
  Snapshot Blocks Count = 177328128
  Mounted              = NO

Snapshot count : 3

Command succeeded
```

Scheduled snapshots are the best way to protect the database and its environment. Each snapshot can be considered a full database backup. And thanks to the speed of the snapshot operation, you can schedule the snapshots within a short period. For example, you can schedule a snapshot every 15 minutes using a *crontab* or the *dscli group snapshot enable* command.

The maximum and default number of snapshots supported by the CDP server is 255. When this limit is reached, newer DiskSafe snapshots replace older DiskSafe snapshots.

The number of snapshots you keep and the frequency with which you take them determines how far back you can retrieve data. For example, with a limit of 255 and a schedule of every 15 minutes, you can retrieve any data from the past 63 hours.

**Note:** A short period for snapshots allows the DBA to store less archived redo logs.

Third-party tape backup products can be used in conjunction with FalconStor CDP for long-term retention or archival purposes, greatly reducing tape and license costs. Once a consistent snapshot has been taken, you can use CDP to mount an image of the snapshot (called a TimeView) on a backup server and proceed with the backup without impacting the operations on the production database. It is simple, powerful, and eliminates the usual backup window. It is also a good way to integrate CDP in an existing Oracle Recovery Manager (RMAN) based backup solution.

This process can also be fully automated using FalconStor HyperTrac software, a tool that interfaces with the backup application and automatically creates the snapshot and mounts the data for the backup. More details about this solution are provided below.

Note that the TimeView technology is also especially helpful for qualification or migration purposes. In a matter of minutes, you can easily have a full copy of your production database environment available on another server and ready for experimentation.

After completing the configuration steps described above, the Oracle server is fully protected. This includes both Linux operating system and Oracle RDBMS software. The next section describes how to recover your data in case of a loss.

### Step 3 – Protecting the CDP appliance

#### 1. Autosave option

Once the CDP appliance is installed and configured, you can save the configuration via the FalconStor Management Console. The CDP *autosave* option allows you 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 CDP data is to mirror its storage. 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 at a remote site. Mirroring the CDP data ensures access to the CDP data but it does not cover the failure of the CDP node.

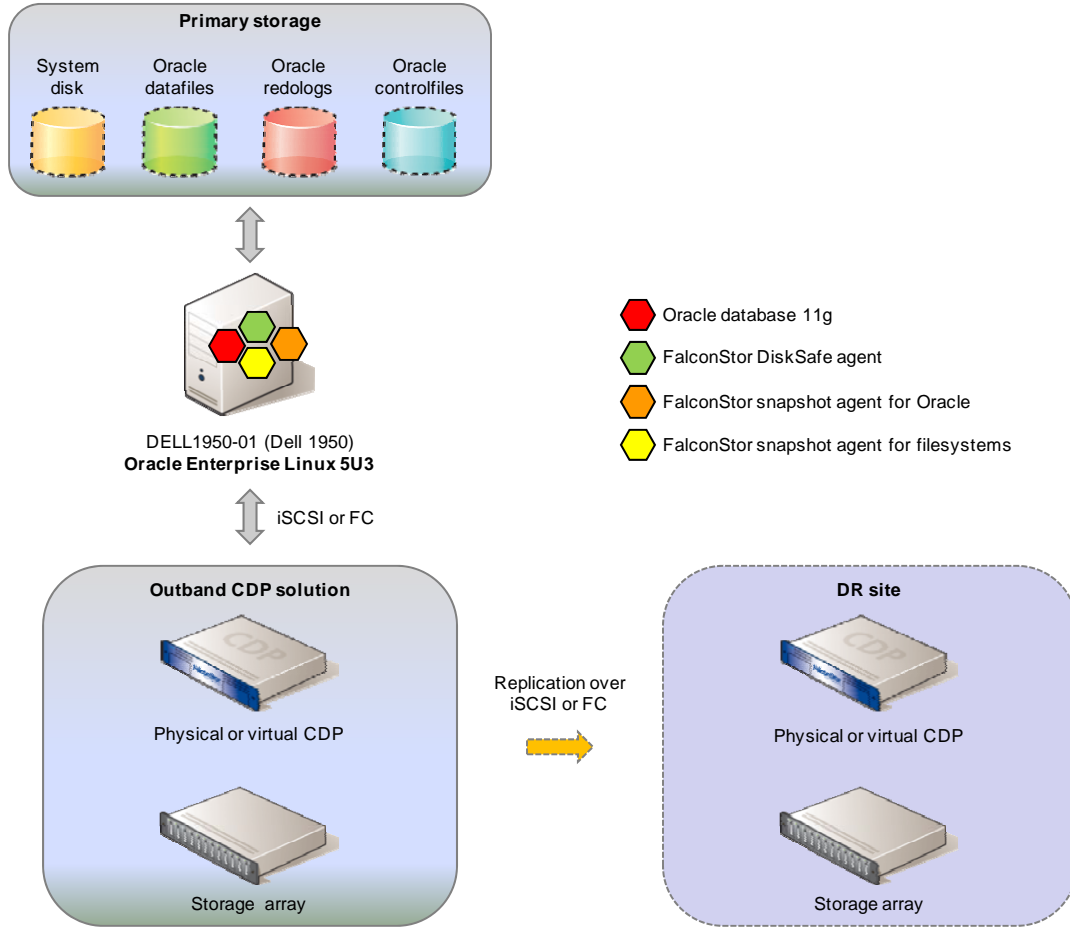
#### 3. CDP Replication

In order to secure the actual CDP appliance, another way to protect CDP data is to use FalconStor Replication. This feature allows you to replicate data over any existing 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 DR solution by allowing multiple virtual appliances to run on a single consolidated server.

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

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), reducing bandwidth and associated storage 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. The replication process itself is tunable on a per-volume basis to match the available bandwidth. Lastly, data can be compressed or encrypted.



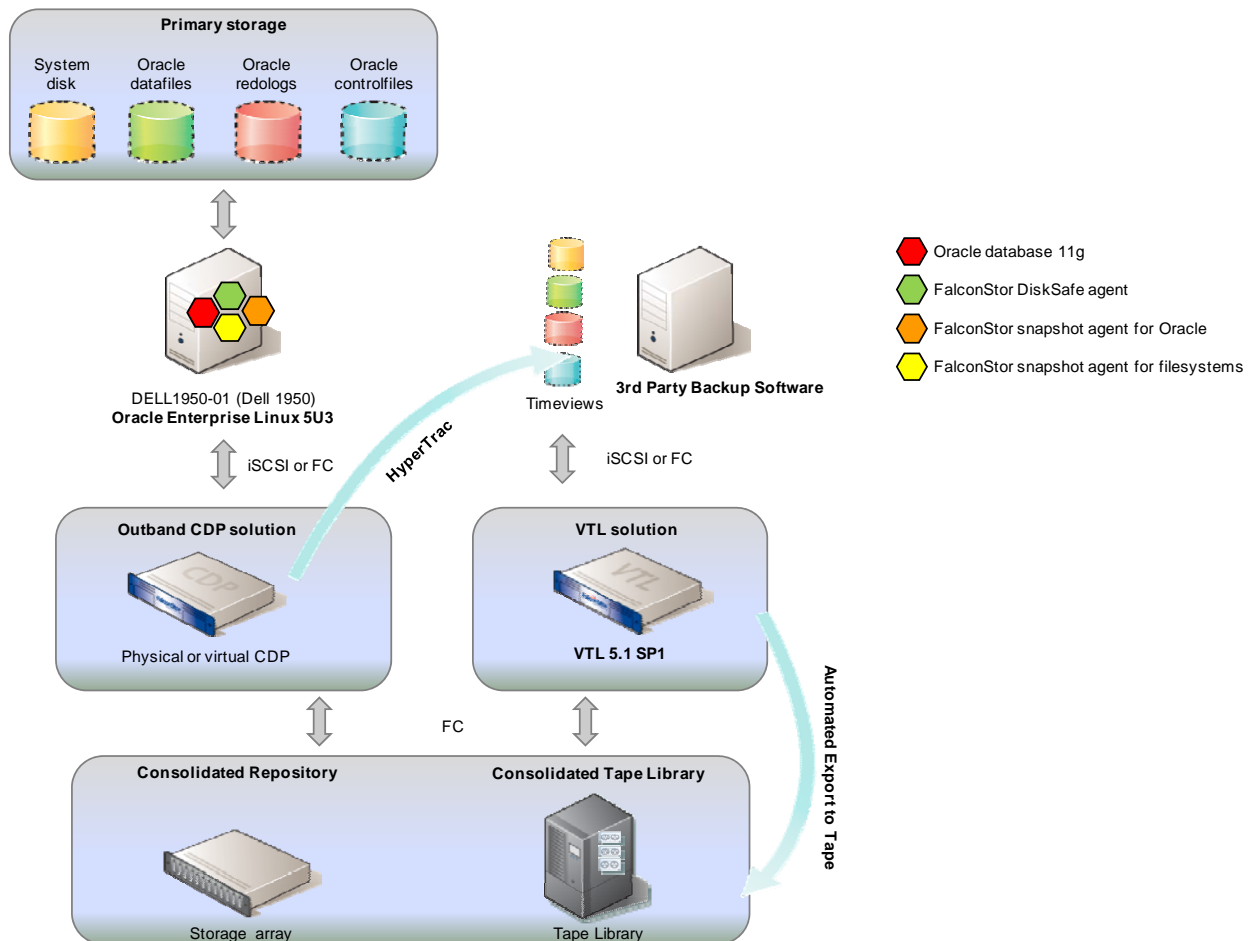
#### 4. FalconStor CDP and HyperTrac : Backup acceleration

In environments where regulatory or compliance requirements mandate some type of permanent data storage or archives, tape backups can easily be created off CDP protection volumes. FalconStor HyperTrac automates and accelerates tape backup operations.

With HyperTrac, you can back up data at any time without disruption, even during peak production hours. HyperTrac resides on the backup server, automatically initiating and mounting FalconStor TimeMark snapshots when backup jobs are performed.

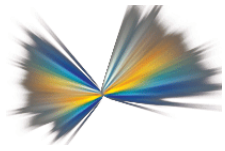
FalconStor HyperTrac Backup Accelerator (HyperTrac) also works in conjunction with FalconStor VTL, allowing faster backup and restore. In this context, you can share the same disk storage pool as VTL (no need to invest in another set of controllers). This type of architecture essentially eliminates the 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 looks 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.



# Recovering your Oracle 11g Database with CDP

Once you have protected a disk or partition, DiskSafe provides several ways to restore your data. You can restore either to your original disk or to another disk, making it easy to create duplicate systems/data. The best method to use depends on your restore objective.

This section gives some examples of generic data recovery and some examples of Oracle specific recovery.

## **Scenario 1: One or multiple files on a disk**

If you have accidentally deleted a file on a disk or if you want to retrieve some older information from a file that has changed, the easiest way to recover it is to mount an image of a snapshot containing the missing or original file. Any snapshot generated prior to the time of the file deletion or the file modification can be selected. Once the snapshot image is mounted, simply copy the file you need to the desired location.

When you mount a snapshot, a separate, virtual disk is created. The mounted snapshot is an exact image of the mirror as it existed when the snapshot was taken. Since a mounted snapshot is simply a representation of the current mirror plus the changed data, in the snapshot area, it does not require any additional disk space.

The example below shows the Oracle disk sdb mounted on /u01.

```
# dscli snapshot list sdb
All snapshots of sdb

Snapshot 1:
  Snapshot Timestamp   = 1250686831(2009/08/19 15:00:31)
  Snapshot Blocks Count = 132395008
  Mounted              = NO

Snapshot 2:
  Snapshot Timestamp   = 1250754757(2009/08/20 09:52:37)
  Snapshot Blocks Count = 4112384
  Mounted              = NO

Snapshot 3:
  Snapshot Timestamp   = 1250755053(2009/08/20 09:57:33)
  Snapshot Blocks Count = 177328128
  Mounted              = NO

Snapshot count : 3

Command succeeded
```

First, you will need to list the current sdb snapshots available and choose the one you want to mount as a TimeView.

Then, request CDP to make the TimeView available (as shown below):

```
# dscli snapshot mount sdb Timestamp=1250754757
Mount snapshot with timestamp 1250754757 of sdb

Command succeeded
```

Next, identify the TimeView among existing disks and mount it on the server:

```
# dscli disk list
...
Disk sdh
Device Name           = /dev/sdh
DiskSafe ID           = FALCON__IPSTOR_DISK_____6000d77f55825d5e02b800004a8dc59c
Mount Point(s)       =
Capacity              = 10000.00 MB
VSC Supported         = YES
Snapshot Capability   = NO
Status                = NORMAL
...

# mkdir /u03; mount /dev/sdh /u03
```

Now, browse the TimeView to retrieve the lost data and unmount the TimeView:

```
# cp /u03/<my_precious_data> <path_to_safe_place>
# umount /u03
# dscli snapshot unmount sdb Timestamp=1250754757
Dismount snapshot with timestamp 1250754757 of sdb

Command succeeded
```

## ***Scenario 2: A non-system disk or partition recovery***

This method is exactly the same as above: mount the corresponding TimeView and restore the entire disk or partition to either your original disk or another disk.

Keep in mind that after you restore a local disk or partition to a new disk which is larger (volume) than the primary disk, you must manually un-protect and re-protect the new disk so that the protection policy refers to the new disk.

## ***Scenario 3: A system disk or partition recovery***

If you need to restore your system disk or partition you typically boot from, you can do so using the bootable DiskSafe Recovery CD. This is particularly useful if the hard disk or operating system has failed and been repaired or replaced.

Once your server has booted on the DiskSafe Recovery CD, the software allows you to access the CDP server and restore the entire disk or partition from either the mirror or from a selected snapshot. The data can be restored to either your original disk or another disk.

## ***Scenario 4: Oracle database object recovery***

If a database object (or table) has been corrupted or deleted, the easiest way to recover it is to use an Oracle backup server to mount an image of a snapshot containing the original object. Once the database is opened, you can export the original object from the instance to a dump file and finally import it into your running production database.

Note that Oracle 11g has introduced the recycle bin concept: if you drop a table accidentally, the table is not actually deleted but is put into the recycle bin, you can use the *undrop* command to retrieve it.

### ***Scenario 5: Oracle database point-in-time complete recovery***

If one or more data files have been lost due to a disk failure, you may want to recover the entire database. In this case, the obvious method is to mount the image of the last snapshot before the failure and use it to recover your data onto new disks.

A mounted snapshot is not intended to be a working disk. Any changes made to a mounted snapshot are lost as soon as the snapshot is unmounted. This means that you should only use the mounted snapshot to recopy Oracle data to your production disks. Your RTO will depend mostly on the time needed to copy the data from the TimeView (snapshot) to the production storage.

If you have a large database and you want a short RTO, it is a good idea to use CDP replication. Once set up, the replication maintains an image copy of the protected disks on a local or remote server. If the main disks fail on the primary site, then the replica disks on the secondary site can be promoted, assigned to the Oracle server, mounted, and the database will be back up and running with minimal down time. The database will be at the state of the last complete replication.

If you recover your database with the last snapshot, you will lose all of the committed transactions between that snapshot and the crash. While this may be acceptable in some situations, you can achieve a complete recovery by retrieving the redo log files that have been produced between the last snapshot and the crash using the CDP mirror. Then, use the Oracle *recover* command to reach the desired SCN (System Change Number).



## ***RMAN and CDP***

Recovery Manager (RMAN) is Oracle's main backup and recovery tool and is a built-in component of the Oracle server. Since its introduction as part of the Oracle 8 release, RMAN has become a powerful and popular tool to back up and recover Oracle databases. It is now widely used for Oracle protection; so why use a CDP solution?

While RMAN is part of the Oracle RDBMS software and can be used without incurring any additional licensing fees, combining it with CDP provides an enterprise-class solution that helps you achieve better recovery time objectives, provides a low-cost disaster recovery solution, consolidates your backup storage, and can fit into any existing RMAN-based backup environment. Used together, customers can benefit from RMAN's tight integration with Oracle databases plus all the benefits of an out-of-band journaling solution. This can protect the database and application server from many types of failures, increase the mean time between failures, decrease the mean time to recover, and minimize the loss of data and business revenue when there is a database failure.

For example, if you use RMAN to make periodic *cumulative incremental backups* coupled with *full backups*, then a CDP configuration allows you to keep the same strategy but eliminate the backup windows and unload the production server from the backup I/Os. Using FalconStor HyperTrac to automate the mounting of a TimeView on a backup server can make *full backups* of your database without any impact to production server.

**Note:** If you want to make full backups and save disk space, ask about FalconStor Virtual Tape Library and its deduplication technology with optimization for Oracle data.

FalconStor CDP replication to a remote server over IP or FC is a convenient and easy way to implement a simple and efficient disaster recovery plan. Your replica disks can even be accessed for offsite long-term backups.

FalconStor CDP is also quite helpful when you want to configure a test server or run a test migration using production data. Simply mount the TimeViews on another Oracle server, then recover the database and you are ready to test anything you want using a copy of the production data without impacting the production server.

If your environment runs multiple Oracle instances, you can use just one CDP server to protect all your databases on consolidated storage. The consolidation is even more effective if you use your CDP appliance to back up other applications, not just Oracle databases. Other snapshot agents are available for products like Microsoft Exchange or SQL Server.



# Conclusion

---

Compared to backup methods that significantly impact production servers, FalconStor CDP uses a variety of technologies, such as TimeMark, Replication, and Snapshot Agents that work together to protect your Oracle environment without impacting your production operations.

With FalconStor CDP, back up of your Oracle applications and RDBM data is faster and more comprehensive than traditional tape-based backup methods, and the ability to recover lost files, disks, partitions, database objects, or even a complete database to any point of time makes instant recovery possible.

Because each FalconStor CDP solution is comprised of a variety of technologies, customers can choose the level of data protection that suits their needs.

By consolidating your backup infrastructure, FalconStor CDP helps you to reduce the total cost of ownership of your backup solution. For example, several Oracle databases can be protected by the same CDP appliance. As a totally open solution, FalconStor CDP also maximizes the Return on Investment (ROI) associated with your backup solution.

This document demonstrates that the implementation of the FalconStor CDP solution can be done quickly and easily. As management and configuration of CDP is intuitive, you do not need complex training to enable the protection and recovery of data. The solution is simple, scalable, reliable, powerful, and can be expanded to take advantage of the full suite of FalconStor products.



# Appendix

---

## **Sources**

- [http://en.wikipedia.org/wiki/Service\\_level\\_agreement](http://en.wikipedia.org/wiki/Service_level_agreement)
- [http://en.wikipedia.org/wiki/Service\\_level\\_objective](http://en.wikipedia.org/wiki/Service_level_objective)

## **Reference documents**

- FalconStor CDP Administration Guide
- FalconStor CDP-NSS Reference Guide
- [Holistic and efficient protection for Oracle databases with FalconStor CDP](#)
- FalconStor Snapshot Agents User Guide
- FalconStor HyperTrac User Guide