HAL
open science

La protection continue des données

Karim Harfouche

To cite this version:

Karim Harfouche. La protection continue des données. Performance et fiabilité [cs.PF]. 2014. dumas-01588929

HAL Id: dumas-01588929

https://dumas.ccsd.cnrs.fr/dumas-01588929v1

Submitted on 18 Sep 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

CONSERVATOIRE NATIONAL DES ARTS ET MÉTIERS
CENTRE RÉGIONAL DES PAYS DE LA LOIRE

MÉMOIRE
présenté en vue d'obtenir
le DIPLÔME d'INGÉNIEUR CNAM
SPÉCIALITÉ : INFORMATIQUE

par

HARFOUCHE Karim

LA PROTECTION CONTINUE DES DONNÉES

Soutenu le 05/12/2014

JURY

PRÉSIDENT : Mme MÉTAIS

MEMBRES : M. BRIAND
M. GÉRARDIN
M. LASTENNET
M. RABU
M. RÉMY

REMERCIEMENTS

Je tiens à remercier en premier lieu, Philippe RÉMY, qui m'a confié ce projet particulièrement intéressant et qui m'a guidé durant la globalité de cette étude malgré son changement d'affectation durant ce mémoire.

Je remercie également Alain GÉRARDIN, pour son soutien et tous ses conseils avisés qui ont largement contribué à l'amélioration de ce mémoire.

Merci à l'ensemble de l'équipe Storage Open en particulier Muriel, Olivier, William, Fabien, Simon, Jérémy et Ercan pour leur accueil chaleureux, leurs encouragements, le temps qu'ils ont consacré à m'apprendre ce nouveau métier et pour m'avoir permis d'acquérir les connaissances nécessaires à cette étude.

Merci à Raphaël RABU (notre nouveau chef d'équipe) pour ses encouragements, ses conseils, et surtout pour m'avoir permis d'achever ce mémoire en acceptant mes très nombreuses demandes de congés…

Enfin, je terminerai par remercier mes anciens collègues de Filaction qui m'ont soutenu tout au long de ce cursus et que j'ai abandonnés après plus de 12 ans de collaboration.

GLOSSAIRE

Appliance	Équipement informatique répondant à un besoin par une solution clé en main.
CDP	Continious Data Protection
CPU	Central Processing Unit
Cluster	Groupe de serveurs réunis pour assurer une continuité de service ou répartir les charges (réseaux, processeurs, mémoire, etc.).
DNS	Domaine Name System – Système permettant de trouver l'adresse IP d'un équipement réseau en fonction du domaine auquel il appartient
FAT	File Allocation Table (Table d'allocation de fichiers)
IP	Internet Protocol (protocole réseaux permettant à des machines de dialoguer sur des réseaux locaux ou distants)
ISL	Inter-Switch Link – Liaison entre des switchs
I/O	Input/Output – Désigne la transmission d'un bloc (paquet) de données
LUN	Logical Unit Number : Désigne un disque
NAS	Network Attached Storage (serveur de fichiers)
NDMP	Network Data Management Protocol – Protocole réseaux utilisé pour gérer les sauvegardes de certains équipements de stockage (comme les NAS)
OSSV	Open Systems SnapVault – Solution NetApp permettant de synchroniser des données vers un NAS NetApp
PCA	Plan de Continuité d'activité
POC	Proof of concept –
PRA	Plan de Rétablissement d'Activité
RTO	Reestablishment Time Objective
RPO	Reestablishment Point Objective
SAN	Stockage Area Network – Désigne l'ensemble des éléments du réseau de stockage
SMB	Server Message Block. En 1998, Microsoft renomme CIFS (Common Internet File System) en SMB et ajoute plusieurs fonctions comme le support des raccourcis et de fichiers de plus grande taille.
Mappage	Action de présenter des LUN à un serveur
WAN	Wide Area Network
Zoning	Procédé consistant à partitionner une fabrique du SAN en plusieurs sous-réseaux de manière à isoler chaque zone. Ce procédé permet de protéger les LUN de la corruption et d'optimiser le trafic au sein du réseau de stockage.

SOMMAIRE

INTRODUCTION **1**

PARTIE I : LE CONTEXTE

1 LE PROJET **4**

1.1 OBJECTIFS 4
1.2 PRÉSENTATION DE L'ENTREPRISE 4
1.2.1 L'informatique du groupe CM-CIC 5
1.2.2 Euro Information Production 6
1.2.3 L'équipe stockage du "monde ouvert" 7
1.3 LES DIFFÉRENTES INFRASCTUCTURES DE SAUVEGARDE 8
1.3.1 Les caisses et les agences 8
1.3.2 Directions régionales et centres de productions 9
1.3.3 Les centres de données 10
1.4 BESOINS ET PROBLÉMATIQUES 14
1.4.1 Mise en œuvre de PRA et PCA efficace 14
1.4.2 Sauvegarder des volumétries conséquentes 14
1.4.3 Homogénéité des infrastructures 14

2 ÉTAT DE L'ART **15**

2.1 L'ÉVOLUTION DES BESOINS 15
2.2 LES DIFFÉRENTES PROTECTIONS CONVENTIONNELLES 15
2.2.1 RAID / Mirroring 15
2.2.2 Réplications 16
2.2.3 Sauvegardes traditionnelles (journalières) 18
2.2.4 Les prises d'images ou "snapshots" 20
2.2.5 Les Clusters 21
2.2.6 Les logiciels de gestion de versions 21
2.2.7 Les journaux (fichiers de logs) 22
2.3 LE CONCEPT DE LA PROTECTION CONTINUE (CDP) 23
2.3.1 Les principes 23
2.3.2 La cohérence des images 24
2.3.3 Les grandes catégories de la protection continue 24
2.3.4 Les orientations de protection continue 25
2.3.5 Les atouts de la protection continue 27
2.3.6 Les contraintes de la protection continue 30
2.4 LES PRINCIPAUX ACTEURS 32
2.4.1 CommVault Simpana 33
2.4.2 EMC² - RecoverPoint 36

2.4.3 Symantec - Netbackup Realtime 41
2.4.4 IBM Tivoli 43
2.4.5 ASIGRA 46
2.4.6 FalconStor CDP 48
2.4.7 Les NAS : NetApp 52
2.4.8 Microsoft DPM 53
2.4.9 AIMStor 55
2.4.10 R1Soft 57
2.5 LES DIFFÉRENTES SOLUTIONS ÉTUDIÉES 58

PARTIE II : LES EXPÉRIMENTATIONS

3 MISE EN ŒUVRE D'UNE SOLUTION " NEAR CDP " 61

3.1 BESOINS ET OBJECTIFS 61
3.2 ARCHITECTURE EXISTANTE 61
3.3 CHOIX DE L'ARCHITECTURE CIBLE 62
3.3.1 Avantages de cette infrastructure 63
3.3.2 Inconvénients 64
3.4 MISE EN OEUVRE 65
3.4.1 Installation du serveur Windows 65
3.4.2 Installation Symantec Storage Foundation (VVR) 65
3.4.3 Installation Symantec Netbackup 7.5 66
3.4.4 Installation et paramétrage NetApp OSSV 67
3.5 TESTS DE LA NOUVELLE ARCHITECTURE 69
3.5.1 Tests de performance réseaux 69
3.5.2 Tests de transferts de fichiers 70
3.5.3 Netbackup et les politiques de sauvegardes VSS 70
3.5.4 NetApp OSSV 71
3.6 MIGRATION 72
3.6.1 L'organisation 72
3.6.2 La problématique du temps de transfert de fichiers 72
3.7 BILAN 73
3.7.1 Sauvegardes VSS pilotées par Netbackup 73
3.7.2 Utilisation du plugin OSSV Netapp 73
3.7.3 Le Near CDP 74

4 MISE EN ŒUVRE DE FALCONSTOR CDP 75

4.1 BESOINS ET OBJECTIFS 75
4.2 ARCHITECTURE DE TESTS 75
4.2.1 Serveur FalconStor CDP 75
4.2.2 Choix des systèmes d'exploitation 76
4.2.3 Choix de l'architecture de tests de bases de données 76
4.2.4 Tests Netbackups 77
4.3 MISE EN OEUVRE 77
4.3.1 Des appliances CDP 78
4.3.2 Des machines virtuelles 78
4.3.3 Installation HyperTrac 80
4.4 TESTS ET EXPÉRIMENTATIONS 82
4.4.1 Les consoles d'administration 82
4.4.2 Gestion de la politique de protection 90

4.4.3 Les sauvegardes de bases de données "MS SQL Server" 92
4.4.4 Gestion des prises d'images cohérentes 97
4.4.5 Restauration des bases de données MS SQL Serveur 98
4.4.6 Gestion des protocoles de transfert 99
4.4.7 Gestion des sauvegardes par groupe de cohérence 101
4.4.8 HyperTrac sauvegarde par Netbackup 101
4.4.9 Gestion des Linux 102
4.4.10 Gestion des rapports 103
4.5 BILAN 105
4.5.1 Les fonctionnalités 105
4.5.2 Consommateur de stockage 106
4.5.3 Consommateur de réseaux 106
4.5.4 Interopérabilité avec les systèmes d'exploitation 107
4.5.5 FalconStor CDP outil de sauvegarde ? 107
4.5.6 FalconStor Outil de PCA 107
4.5.7 Expérimentation à compléter 108

5 EMC RECOVERPOINT 109

5.1 BESOINS ET OBJECTIFS 109
5.2 MISE EN OEUVRE DE L'ARCHITECTURE DE TESTS 110
5.2.1 Architecture 110
5.2.2 Paramétrage des baies VNX 110
5.2.3 Paramétrage des appliances RecoverPoint 111
5.3 EXPÉRIMENTATIONS 111
5.3.1 Prise d'empreintes 111
5.3.2 Restaurations 114
5.3.3 Logs et rapports 115
5.4 BILAN 116
5.4.1 Mise en œuvre 116
5.4.2 Les fonctionnalités 116
5.4.3 Stabilité et fiabilité 117
5.4.4 Expérimentation à mettre en œuvre 118

PARTIE III : LA SYNTHÈSE

6 BILAN DE L'ÉTUDE CDP 120

6.1 LA PROTECTION CONTINUE DES DONNÉES 120
6.1.1 Les orientations de la protection continue 120
6.1.2 L'intérêt de la protection continue 120
6.1.3 Synthèse des expérimentations 122
6.2 L'ORGANISATION DE L'ÉTUDE 123
6.2.1 Les différentes recherches du projet 123
6.2.2 Mise en œuvre et expérimentations 125
6.2.3 Les difficultés rencontrées 125
6.2.4 Tableaux de bord 127

CONCLUSION 129

ANNEXES

ANNEXE 1 : RPO et RTO 132
ANNEXE 2 : La déduplication 133
ANNEXE 3 : Le "zoning" 134
ANNEXE 4 : Procédure d'installation Storage Foundation 136
ANNEXE 5 : Configuration Policy VSS Netbackup 139
ANNEXE 6 : Management liaison OSSV 142
ANNEXE 7 : Installation DFM Host Agent 144
ANNEXE 8 : Paramétrage DFM Host Agent 145
ANNEXE 9 : Installation du plug-in OSSV 146
ANNEXE 10 : Tests du plugin OSSV 148
ANNEXE 11 : Matrice Compatibilité FalconStor CDP 149
ANNEXE 12 : Installation Appliance FalconStor CDP 152
ANNEXE 13 : Paramétrage Appliance FalconStor 159
ANNEXE 14 : Procédure Installation FalconStor Windows Agent 162
ANNEXE 15 : Paramétrage de l'agent FalconStor pour Microsoft SQL Server 169
ANNEXE 16 : Procédure Paramétrage Replication FalconStor 171
ANNEXE 17 : Installation HyperTrac 178
ANNEXE 18 : Paramétrage HyperTrac 181
ANNEXE 19 : FalconStor expérience n°1 (Backup) 185
ANNEXE 20 : FalconStor expérience n°2 (Restauration) 189
ANNEXE 21 : Paramétrage des baies VNX 195
ANNEXE 22 : Paramétrage RecoverPoint 199
ANNEXE 23 : Restauration RecoverPoint 204

BIBLIOGRAPHIE 216

LISTE DES FIGURES 221

LISTE DES TABLEAUX 224

INTRODUCTION

La protection continue des données (CDP) est pour la sauvegarde, ce que la vidéo est à la photographie. Plus qu'un nouveau moyen pour sécuriser nos systèmes d'informations, il s'agit d'une nouvelle philosophie. Ce concept encore méconnu, offre des perspectives intéressantes, notamment dans le cadre de la mise en œuvre de PRA (Plan de Reprise d'Activité), de PCA (Plan de Continuité d'Activité) ou de la protection contre la corruption de données. C'est dans ce dernier but que la protection continue des données a été déployée dans les infrastructures de messagerie Exchange du groupe CM-CIC.

Euro Information étant consciente qu'il existe d'autres applications pouvant répondre à de nouvelles attentes en termes de protection des données et des infrastructures, il m'a été demandé de réaliser une étude comparative entre EMC RecoverPoint et Netbackup Realtime. J'ai donc décidé avec l'accord de ma direction d'élargir mon champ d'investigation afin de couvrir les principales solutions du marché. L'objectif étant de recenser les fonctionnalités innovantes et de les mettre en application pour vérifier leur pertinence. Il s'agit donc d'un travail de recherche qui a pour objectif d'améliorer notre vision sur les orientations des nouveaux outils de sauvegarde, en les recensant, afin d'en dégager les intérêts et contraintes en fonction des différents types d'infrastructures. La question est donc de déterminer si l'une de ces solutions pourrait apporter des avantages majeurs dans la mise en œuvre des systèmes de protection des données de l'entreprise.

Afin d'y répondre, j'ai dans un premier temps pris un peu de recul en étudiant les différentes infrastructures de protection de l'entreprise et du monde informatique en général afin d'obtenir une vision globale des technologies actuelles. Devant la multitude d'outils apparus sur le marché ces dernières années, j'ai également dû effectuer un état des principales offres afin d'en différencier les caractéristiques propres à chacune et ainsi positionner le CDP parmi les solutions existantes.

Dans un second temps, j'ai mis en œuvre plusieurs architectures de protection continue. J'ai tout d'abord profité d'un projet d'entreprise (suppression d'un centre de données) pour mettre en production une solution "Near CDP" s'appuyant sur des technologies NetApp et Symantec(Netbackup). J'ai ensuite, réalisé de nombreux tests sur plusieurs solutions CDP (FalconStor CDP et EMC Recoverpoint), afin d'acquérir une expérience sur ces types de solutions, d'en déceler les contraintes d'exploitation.

Enfin, dans un troisième temps, j'ai procédé à l'analyse des différents résultats (recherches et expérimentations). Ceux-ci m'ont permis de dégager les solutions les plus pertinentes à mettre en application en fonction des besoins et des infrastructures concernées.

LE CONTEXTE

1 LE PROJET

1.1 OBJECTIFS

La protection continue des données (CDP) met en œuvre une nouvelle génération d'outils de protection permettant, entre autres, de protéger des volumétries importantes de données contre la corruption et de faciliter la reprise d'activité en cas d'incident. Face à l'augmentation des besoins en stockage, le CDP pourrait être un outil particulièrement intéressant pour sécuriser nos données. L'étude de cette nouvelle technologie va permettre de mieux l'appréhender afin d'en évaluer les intérêts pour Euro-Information.

Les principaux objectifs de cette étude sont donc de :

- comparer cette technologie aux systèmes déjà existants ;
- étudier ses principales solutions afin d'en déterminer leurs principaux atouts et inconvénients ;
- mettre en œuvre les solutions qui semblent les plus appropriées pour les infrastructures d'Euro Information afin d'en vérifier les intérêts.

1.2 PRÉSENTATION DE L'ENTREPRISE

Le groupe CM-CIC est un regroupement de banques et de filiales. Les activités sont regroupées en différents pôles d'activités (financier, technologique, assurance, immobilier, etc...) organisés autour de l'activité bancaire. On y retrouve notamment des entités très connues comme NRJ Mobile (opérateur téléphonique), les ACM (assurance), EPS(Télésurveillance), ou encore Cofidis (organisme de financement).

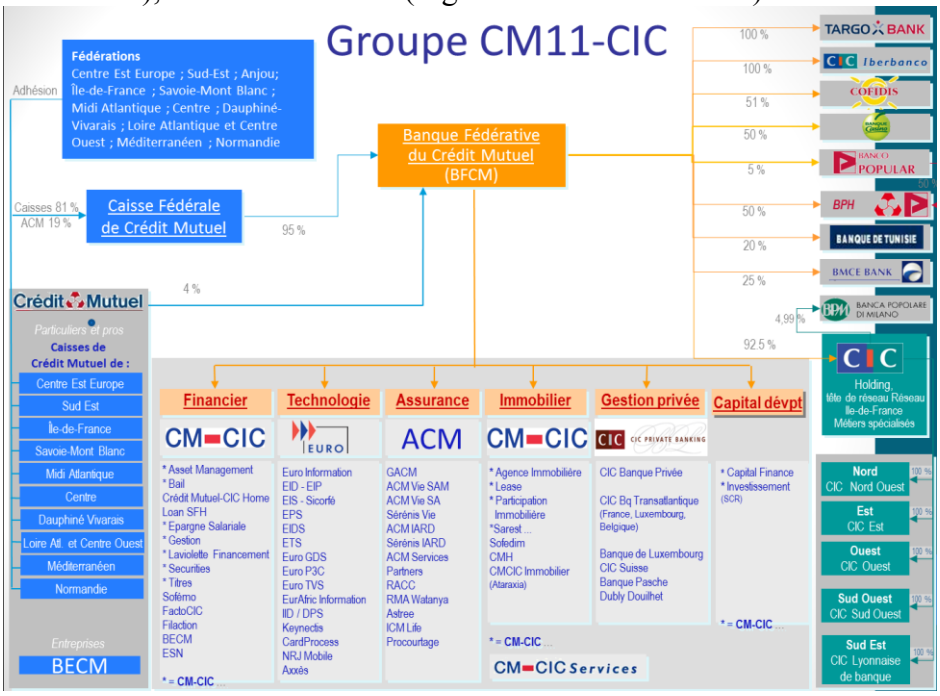


Figure 1-1 : Présentation du groupe CM-CIC

Le groupe est aujourd'hui représenté sur une grande partie du territoire européen. En effet, en 2008, le groupe s'implante en Allemagne grâce à l'acquisition de Targo Bank, mais c'est surtout le rachat de Cofidis en 2009 qui donne au groupe sa dimension européenne.

C'est pour cela que le groupe CM-CIC possède un si grand nombre de points de vente (plus de 6000 uniquement pour le domaine bancaire), de clients (plus de 30 millions) et d'employés (environ 75 800 à ce jour).

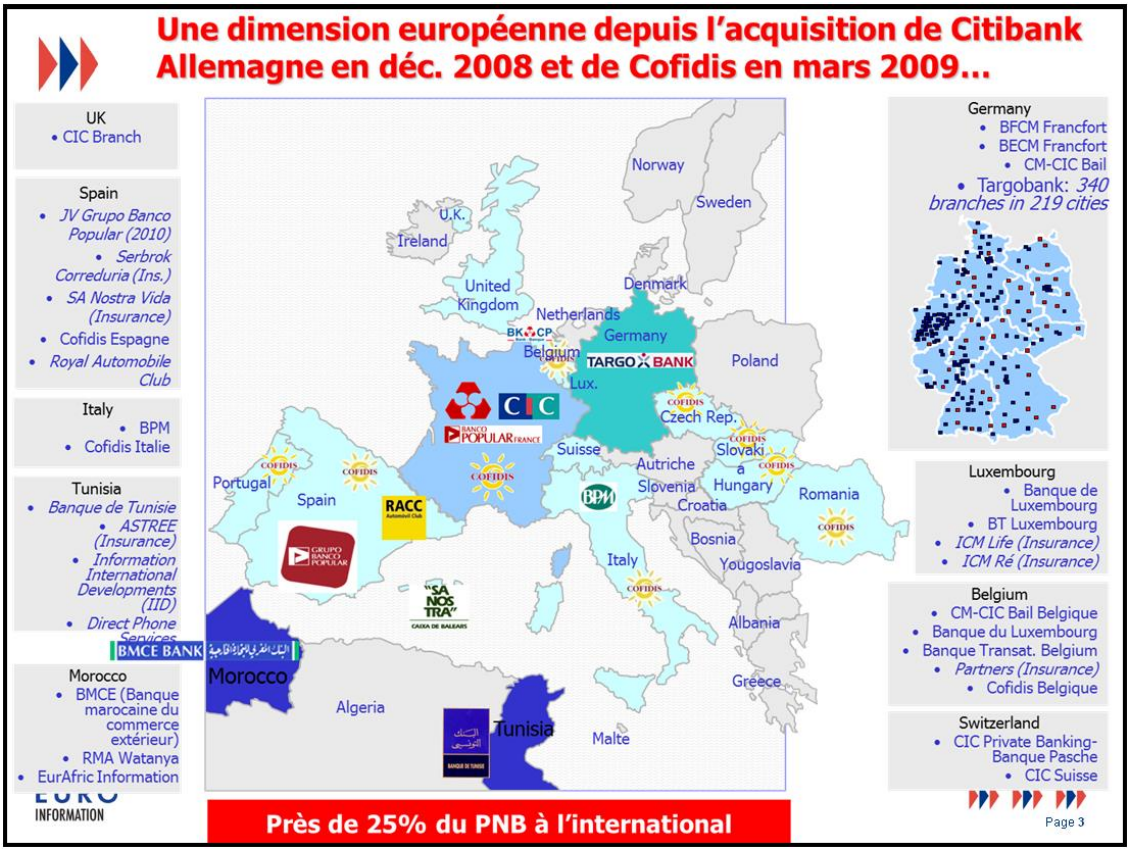


Figure 1-2 : La dimension Européenne du groupe CM-CIC

1.2.1 L'informatique du groupe CM-CIC

Euro-Information mutualise et centralise tous les moyens techniques nécessaires à la gestion des systèmes d'informations (informatiques et téléphoniques). Elle est composée d'environ 2000 personnes (hors prestataires) réparties sur 2 entités :

- Euro-Information Développement(EID) : Son but est de développer et de maintenir les applications nécessaires aux différentes entités du groupe.
- Euro-Information Production(EIP) : Administre l'ensemble des infrastructures techniques et informatiques.

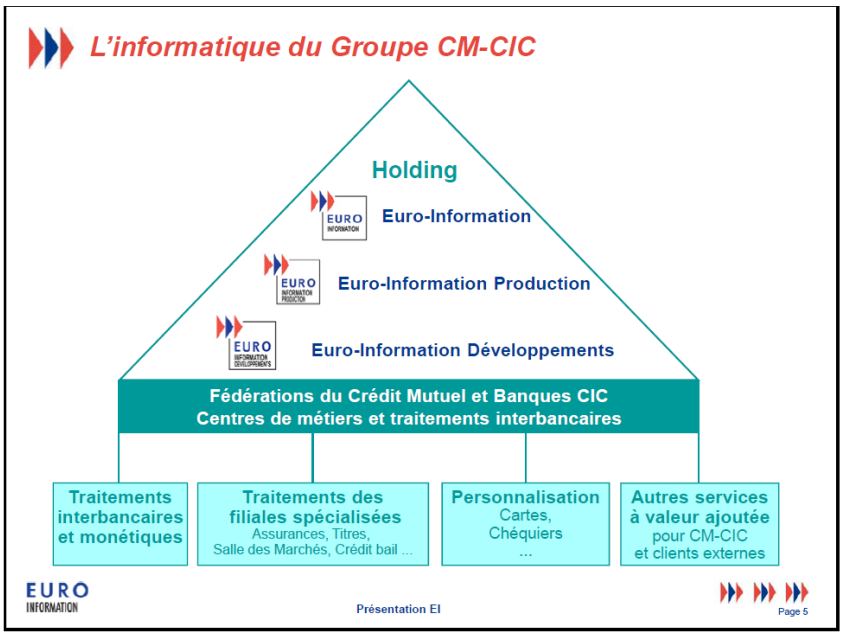


Figure 1-3 : L'informatique du groupe CM-CIC

1.2.2 Euro Information Production

La composition des différents domaines

Mainframe	Monde ouvert	Outils distribués	Réseau / Télécom	Dév. techniques
Stockage	Serveurs spécifiques	Sécurité postes et serveurs	Infrastructures télécom	Dev techniques
Système	Stockage	Sécurité des Biens et des Personnes	Supervision et métrologie	Couches techniques GED
Ordonnanceurs	Systèmes Unix	Technologie LSB	Applications télécom	
TP-DB	Outils de supervision	Nouveaux Outils de Travail		
Middleware	DB			
Transfert	Outils de télédistribution			
Métrologie	Webfarms			
	Messagerie unifiée et AD			

Figure 1-4 : La composition des domaines d'Euro-Information Production

Euro Information Production se compose de 5 domaines :

- Mainframe : Gestion et administration des infrastructures liées au Mainframe (Systèmes centraux)
- Monde ouvert : gestion et administration de toutes les infrastructures des centres de données qui ne sont pas liées au Mainframe et aux réseaux
- Outils distribués : Infrastructure liée aux postes clients (matériel et logiciels)
- Réseaux et Télécommunications : administration des équipements réseaux, téléphoniques et de stockages
- Développements techniques : liés aux équipements spécifiques (les distributeurs par exemple)

1.2.3 L'équipe stockage du "monde ouvert"

1.2.3.1 Le rôle de l'équipe

L'équipe est composée d'une dizaine de personnes, elle a en charge la gestion du stockage des centres de données de France qui se décompose en 2 pôles d'activités :

- Administration des sauvegardes : L'administration des sauvegardes des serveurs représente un nombre important de serveurs (plusieurs milliers). Cela consiste à surveiller leur bonne exécution, mais aussi à rechercher et à mettre en œuvre les solutions matérielles et logicielles adaptées aux contraintes (volume de données et dimensionnements des réseaux) des différents environnements (cf. chapitre 1.3).
- Administration de l'espace de stockage : Ces opérations nécessitent des connaissances pointues sur le paramétrage des équipements de stockage (baies, SAN, NAS). Il s'agit principalement de gérer les demandes d'allocations de LUN, mais aussi de maintenir les infrastructures (migration d'équipement, actualisation de version,…). Les opérations étant réalisées sur des équipements communautaires, chacune des interventions est réalisée avec la plus grande attention.

1.2.3.2 Les problématiques

Le nombre de serveurs et d'infrastructures à surveiller est important. Il est donc indispensable pour l'équipe de stockage de s'appuyer sur des outils fiables, paramétrables, et dont les traitements puissent être les plus automatisés possible.

Le champ d'intervention de l'équipe est vaste : celle-ci agit sur des technologies nombreuses et très différentes. De plus, bon nombre d'équipements sont critiques et ne peuvent subir d'interruption de service. Il est donc impératif d'avoir des outils simples et sécurisés avec plusieurs niveaux d'accréditations pour les opérations les plus délicates.

Compte tenu de son effectif restreint et de l'accroissement rapide des volumétries et des équipements, l'équipe de stockage est en recherche perpétuelle de nouvelles technologies fiables permettant d'optimiser et de faciliter la gestion des équipements.

1.3 LES DIFFÉRENTES INFRASCTUCTURES DE SAUVEGARDE

1.3.1 Les caisses et les agences

Il existe plus de 5875 agences dispersées sur l'ensemble du territoire. Leur taille varie selon les régions et les villes. La particularité des agences est qu'elles ont souvent peu de données à sauvegarder (quelques dizaines de giga-octets par site), mais leur nombre et la qualité de leurs réseaux (souvent quelques Mb/s en SDSL) représentent les principaux obstacles à la sauvegarde des serveurs de ces sites isolés.

1.3.1.1 Les sauvegardes

Les agences sont généralement reliées aux différents centres de données du groupe par des liaisons SDSL de débit moyen. La quantité des données à sauvegarder reste raisonnable. L'architecture qui a été retenue et déployée dans les agences est Avamar (EMC).

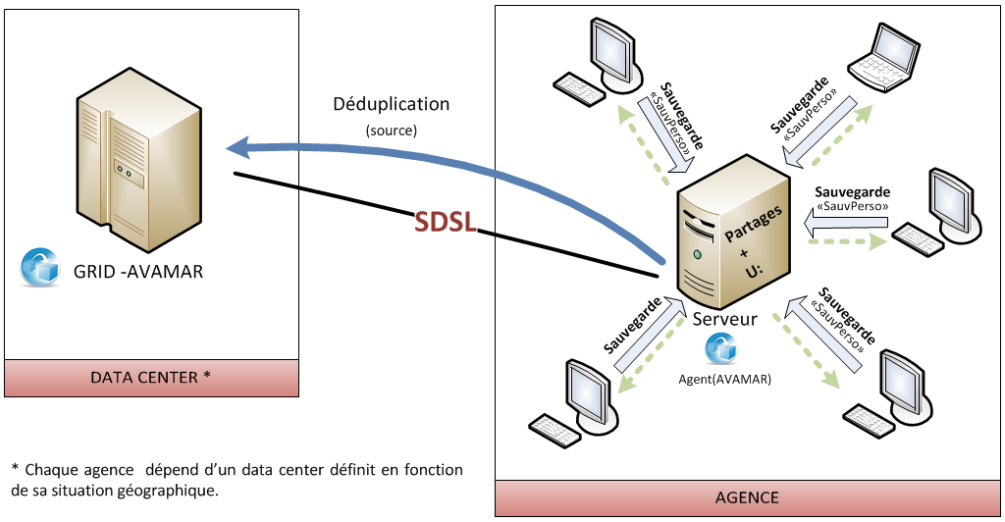


Figure 1-5 : Sauvegardes des agences

La sauvegarde est réalisée en 3 étapes :

- Sauvegarde des postes utilisateurs : les données de chaque utilisateur (répertoires "Mes Documents" et "Bureau") sont copiées sur le serveur agence (lecteur U) à la fermeture de leur session (via l'outil interne SauvPerso).
- Première sauvegarde locale (NTBackup) : elle est réalisée depuis le serveur vers une sélection (dite aléatoire) de quelques postes utilisateurs.
- Deuxième sauvegarde distante : les fichiers sont sauvegardés par l'intermédiaire de l'outil de sauvegarde Avamar vers un centre de données. Les données sont sauvegardées quotidiennement et sont conservées sur une durée de 30 jours.

Problématique des réseaux à faible débit

Les principaux problèmes résident dans la taille de la bande passante vers le centre de données et la volumétrie à transférer (celle-ci dépasse parfois la centaine de gigaoctets). La solution de déduplication (cf. figure 1-6 ci-dessous) proposée par AVAMAR(EMC) permet de réduire considérablement le volume de données à transmettre. Le principe est de décomposer les données en différents blocs selon un algorithme propriétaire et de ne transmettre les blocs identiques qu'une seule fois.

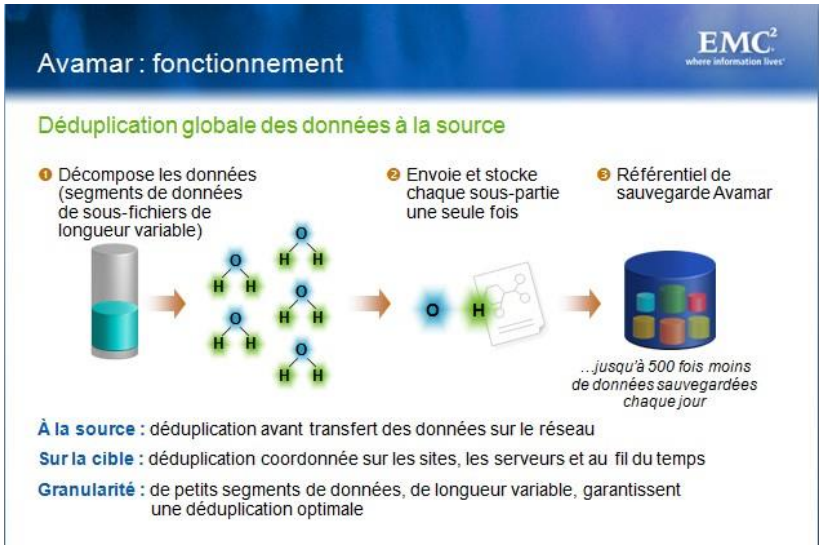


Figure 1-6 : La déduplication selon AVAMAR

Retour d'expériences

L'outil de restauration est assez simple et apprécié par les utilisateurs. La restauration de fichiers s'avère cependant un peu longue, car la déduplication de données ne fonctionne que dans un sens (vers le centre de données). Ainsi, lors d'opérations de restaurations, l'ensemble des données est transmis…

Avamar est très efficace pour sauvegarder quelques dizaines de giga-octets avec une liaison à faible débit mais commence à rencontrer quelques difficultés lorsque la volumétrie dépasse les 100Go de données protégées.

1.3.2 Directions régionales et centres de productions

La problématique des directions régionales est un peu différente. Elles sont peu nombreuses et possèdent beaucoup plus de données à protéger. Leurs liaisons réseaux sont plutôt de bonne qualité et peuvent atteindre plusieurs dizaines de Mb/s.

1.3.2.1 Les sauvegardes

Les volumétries à sauvegarder étant plus importantes, c'est une architecture Netbackup PureDisk (Symantec) qui a été choisie.

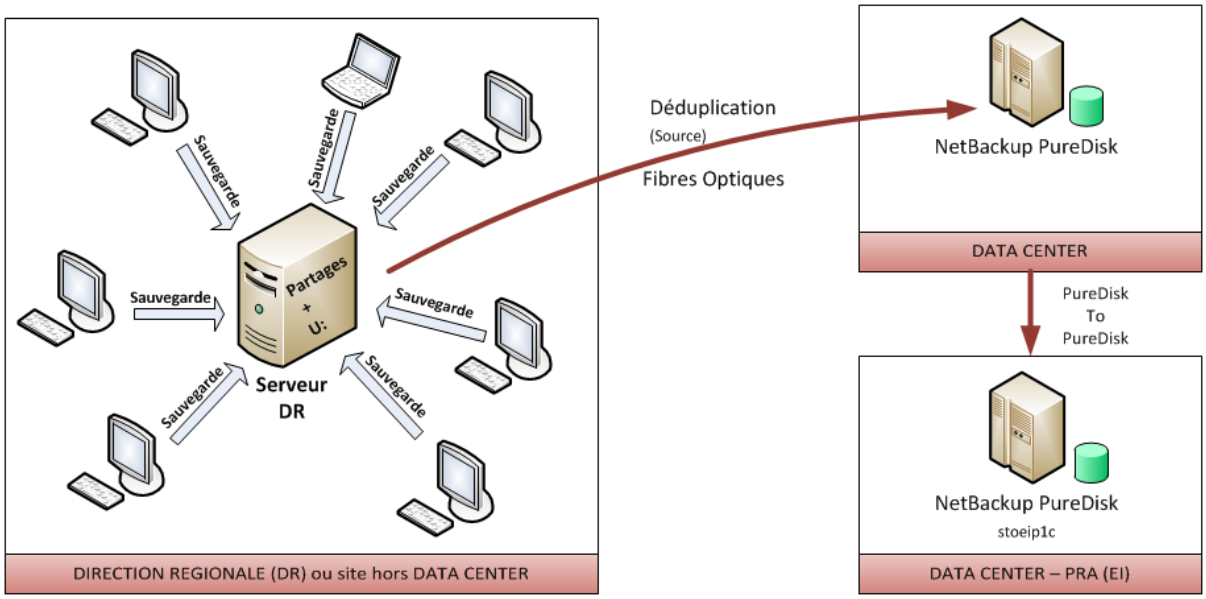


Figure 1-7 : Sauvegardes des directions générales

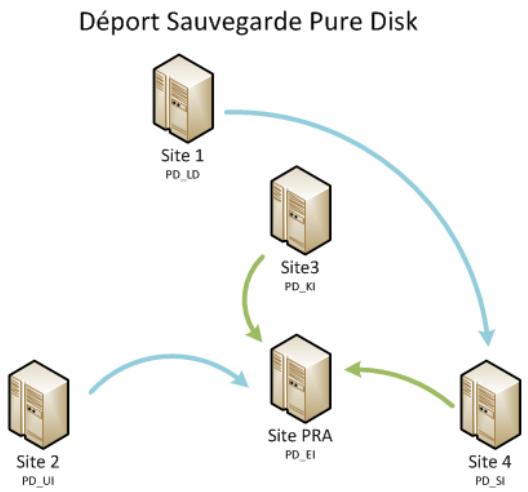


Figure 1-8 : Réplications PureDisk

Comme dans les agences, on commence par rapatrier les données personnelles sur le serveur DR. Ces données, ainsi que les partages publics, sont ensuite transmis vers leur centre de données (cf. figure 1-7) à l'aide d'un algorithme de déduplication à la source (cf. figure 1-6).

Une nouvelle copie est alors réalisée vers un second centre de données (souvent le site de PRA). Cette copie est réalisée entre les serveurs PureDisk suivant un protocole propriétaire (Symantec PureDisk) qui ne transmet que les blocs modifiés.

1.3.3 Les centres de données

Les besoins au sein des centres de données sont différents des directions générales. La volumétrie des sauvegardes à réaliser est sans commune mesure et peut dépasser le pétaoctet. Face à de telles volumétries, l'utilisation de la déduplication sur la cible (cf. annexe 2) se présente comme la solution la plus appropriée. Elle est assurée par une VTL Protectier IBM pilotée par le logiciel de sauvegarde Netbackup.

1.3.3.1 Les sauvegardes des serveurs

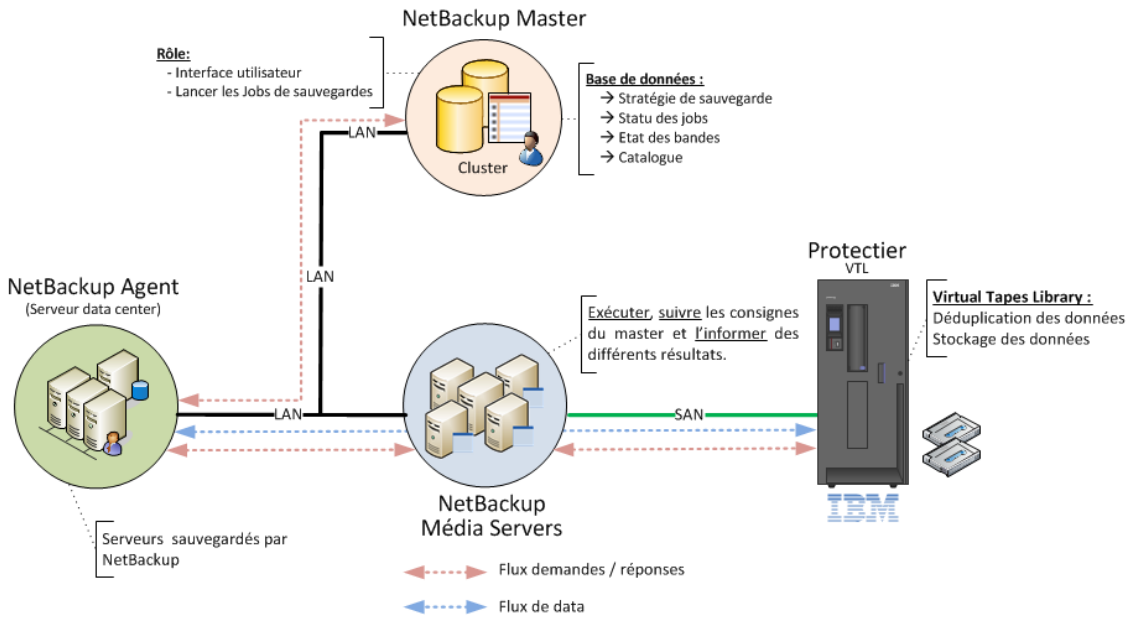


Figure 1-9 : Architecture NetBackup Protectier

La solution de sauvegarde déployée dans les centres de données est basée sur 4 acteurs :

- NetBackup Master : Il détient l'ensemble des informations liées aux sauvegardes
- Les agents NetBackup (serveurs à sauvegarder) :
- NetBackup Média serveurs : Interface avec le support de stockage
- Protectier : Simule une robotique de bande. Les données sont d'abord dédupliquées avant d'être stockées (déduplication à la cible). Ces opérations sont totalement invisibles pour les autres acteurs.

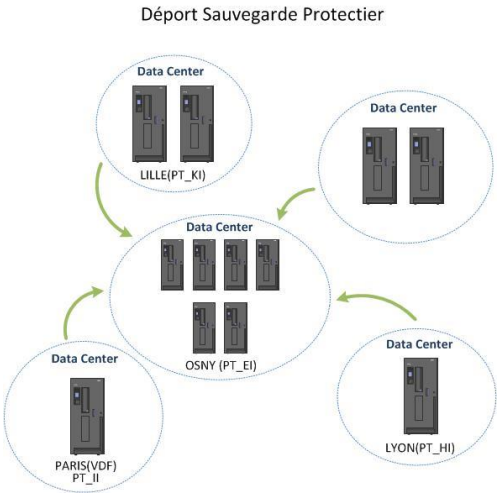


Figure 1-10 : Réplication des Protectiers

La politique de sauvegarde est adaptée en fonction des besoins des serveurs.

Les serveurs sont sauvegardés sur les Protectiers qui sont eux-mêmes répliqués sur le site de PRA. Ainsi, si un centre de données devenait inexploitable, la récupération des données serait possible depuis le site de secours.

Retour d'expériences

malgré la volumétrie à sauvegarder (plusieurs centaines de To par jours), les VTL Protectier sont relativement fiables.

1.3.3.2 Sauvegardes des messageries

Architecture

La solution utilisée pour gérer les agendas et les messageries des employés du groupe CM-CIC est Microsoft Exchange. Cette architecture est protégée par :

- Un processus de réplication multisites interne à Exchange
- EMC RecoverPoint avec plusieurs jours de protection continue

Le processus de réplication permet d'un point de vue fonctionnel de sécuriser l'infrastructure, mais il ne protège pas contre les problèmes de cohérence de données. La solution EMC RecoverPoint a donc été mise en œuvre pour pallier ce problème et permettre un retour arrière (de plusieurs jours) si un incident devait survenir. RecoverPoint héberge sur le site de secours la troisième et la quatrième copie des données de MS Exchange.

Cette infrastructure (cf. figure 1-11 ci-dessous) est composée des serveurs de messageries qui utilisent le stockage d'une première baie EMC VNX 5300. Les appliances RecoverPoint sont paramétrées en cluster (cf. chapitre 2.2.5 Les Clusters) et gèrent la réplication vers une seconde baie VNX 5300 équipée aussi d'appliances RecoverPoint. Des journaux de transactions sont alimentés par les appliances qui historisent toutes les modifications.

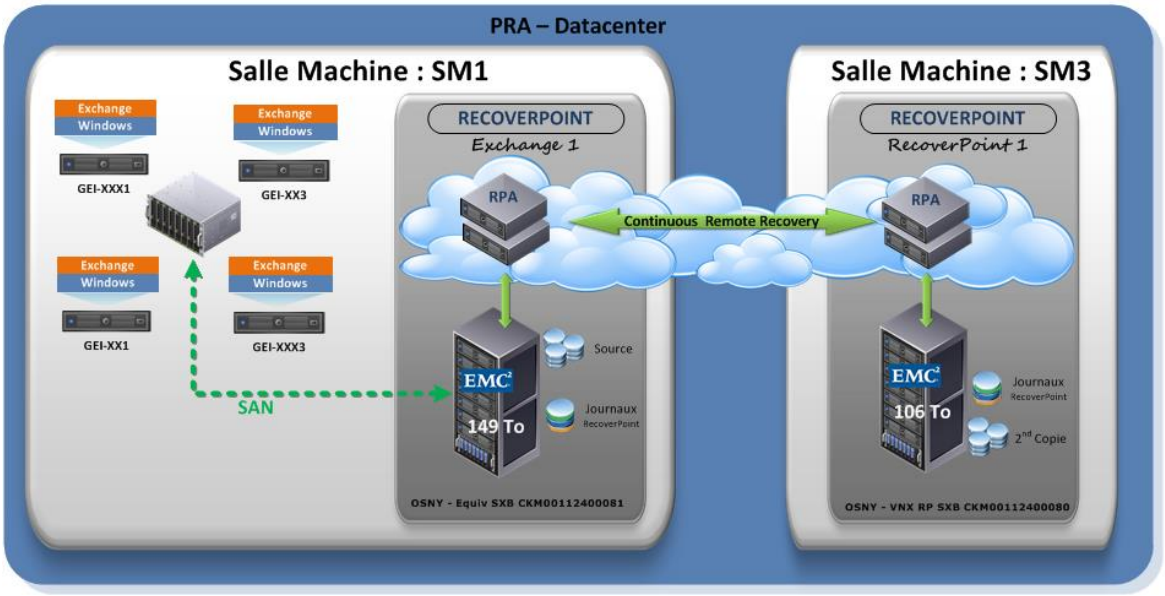


Figure 1-11 : Architecture Exchange EMC RecoverPoint

Les problématiques rencontrées

Depuis leur mise en place, plusieurs problèmes ont été constatés :

- Problème de performances : les 2 baies étaient en réplications synchrones et n'arrivaient pas à écouler les données, générant ainsi des perturbations sur les serveurs Exchange. Le problème a été résolu en passant la liaison en asynchrone.
- Historique beaucoup trop court (à peine 6h) : La taille des journaux avait été sous-évaluée par les équipes EMC. Un réajustement a été réalisé, mais il arrive régulièrement que l'on descende légèrement en dessous du temps défini par le cahier des charges (plusieurs jours).

1.3.3.3 Les NAS (Network Attached Storage)

Les NAS sont utilisés pour stocker les arborescences de fichiers des différents sites du groupe CM-CIC. Ils sont localisés dans tous les centres de données et sont configurés en clusters composés de 2 nœuds (en actif/actif). Ils hébergent au total plus de 7000 partages.

La sécurité de ces données est gérée sur plusieurs niveaux :

- 1er niveau en local : par des prises d'images (snapshots) régulières et qui permettent aux utilisateurs de restaurer leurs fichiers pendant une semaine.
- 2nd niveau sur le site de secours :
  - par un procédé de réplication ;
  - par des prises d'image conservées pendant plusieurs mois.
- 3e niveau sur le site PRA : par une sauvegarde hebdomadaire réalisée par l'outil Netbackup via le protocole NDMP (Network Data Managment Protocol) avec une rétention de plusieurs années.

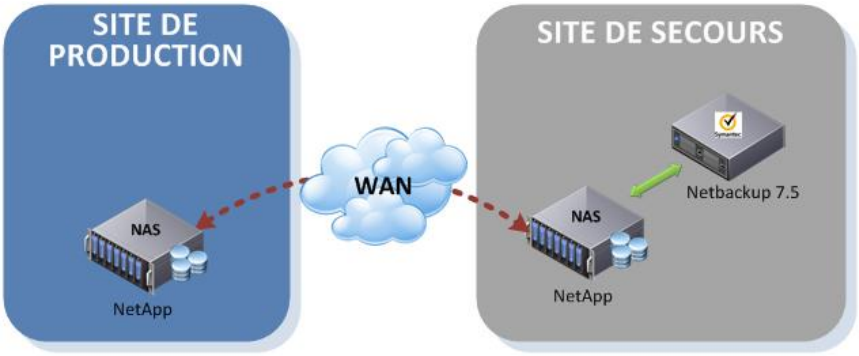


Figure 1-12 : Architecture des NAS Netapp

Problématique rencontrée

La principale problématique rencontrée avec cette architecture est le temps de sauvegarde (réalisé par Netbackup) sur le site PRA. En effet, les données collectées sont volumineuses et le protocole NDMP est moins performant pour sauvegarder et restaurer les données :

- Les sauvegardes sont plus lentes
- La restauration est plus lourde surtout pour les restaurations de fichiers ou de sous répertoires.

1.4 BESOINS ET PROBLÉMATIQUES

1.4.1 Mise en œuvre de PRA et PCA efficace

Certains services commerciaux (pour des raisons financières) ne peuvent se permettre d'avoir une rupture de service. Dans le cadre de mise en œuvre de PRA (Plan de Reprise d'Activité) ou de PCA (Plan de Continuité d'Activité), les temps et le point de restauration doivent être les plus courts possible. Pour y parvenir, il faut augmenter les fréquences de sauvegardes et avoir à disposition plusieurs versions exploitables. Cela est techniquement difficile pour 2 raisons. D'abord, parce que les outils de sauvegardes ont des temps de restauration incompressibles qui dépendent essentiellement de la vitesse des disques, des réseaux et des processeurs (pour les algorithmes de compression). Puis, parce que les équipements de stockage (ex. : les baies de stockage) qui permettent par réplication de récupérer la dernière version des données sont plus exposés aux risques de corruption.

1.4.2 Sauvegarder des volumétries conséquentes

La taille des volumes ne cesse de croitre. Il devient difficile de les sécuriser, car les temps de sauvegarde deviennent beaucoup plus longs (certaines peuvent mettre plusieurs semaines) et les temps de restauration peuvent être plus longs, car la déduplication n'est pas applicable.

1.4.3 Homogénéité des infrastructures

Afin de diminuer les coûts, les équipements sont mutualisés. Cela permet d'avoir des équipes de tailles modérées pour administrer ces systèmes. Il est donc préférable d'avoir des infrastructures homogènes afin de limiter les compétences nécessaires et les risques d'erreurs. Cela nécessite des outils compatibles avec l'ensemble des éléments administrés, tout du moins lorsque cela est possible.

2 ÉTAT DE L'ART

2.1 L'ÉVOLUTION DES BESOINS

L'amélioration des technologies et l'augmentation de l'espace de stockage ont contraint les solutions de sauvegarde à évoluer. En quelques dizaines d'années, nous sommes passés du mégaoctet au pétaoctet de données stockées. Les sauvegardes sur bandes ne suffisent plus à assurer la pérennité des systèmes. Beaucoup trop lentes en lecture, elles posent aussi des problèmes de manutention et stockage.

Depuis la fin du 20e siècle, nous assistons à une évolution des besoins :

- Augmentation des volumétries à sauvegarder ;
- Augmentation du nombre d'utilisateurs par serveur ;
- Multiplication des sites géographiques ;
- Réduction (voir suppression) du temps réservé aux opérations de sauvegarde [CDPF02] ;
- Augmenter le nombre de sauvegardes ;
- Réduire le temps de restauration.

2.2 LES DIFFÉRENTES PROTECTIONS CONVENTIONNELLES

2.2.1 RAID / Mirroring

2.2.1.1 Définition

Ces technologies ont pour objectif de se prémunir contre les défaillances matérielles. Par exemple, pour un problème de support de stockage (type cluster défectueux). Il existe plusieurs typologies de RAID dont les plus connues sont [STORAGEA01, pages 50-53] :

- **RAID 0** : Il permet de regrouper plusieurs disques physiques afin d'en constituer un nouveau. Cela permet d'augmenter la capacité de stockage et de diminuer le temps d'accès (plus de tête de lecture). En revanche, en cas de problème sur l'un des disques, c'est la totalité du disque qui risque d'être perdue…
- **RAID 1 :** Les disques sont montés en miroir. Toutes les écritures sont réalisées simultanément sur les 2 disques. En cas d'erreur sur un disque, l'information peut être récupérée sur l'autre. Cela permet de sécuriser les données sans impacter les performances. En contrepartie, la capacité totale est divisée par 2 (2 disques d'un téraoctet permettent de créer un disque d'un téraoctet) ;

- **RAID 3 / RAID 4** : C'est un dispositif de stockage composé de plusieurs disques dont un est réservé à la parité. La perte d'un disque n'engendre pas la perte de données. Le RAID 3 est peu utilisé, car il n'est pas efficace sur les petits fichiers ;
- **RAID 5 :** Il s'agit d'un groupe de disques où chacun contient la parité d'un autre. Ce principe permet de perdre un disque sans induire des pertes de données ;
- **RAID 6 :** C'est une organisation de disques (dont 2 de parité) qui autorise la perte de deux disques. Il est plus lent en écriture que le RAID 5, mais reste beaucoup plus fiable ;
- **RAID 10 :** Il s'agit d'un mélange entre le RAID 1 et le RAID 0. L'objectif étant d'augmenter la capacité et les performances, tout en sécurisant les données. Ce procédé est souvent utilisé pour héberger des bases de données.

2.2.1.2 L'inconvénient du RAID / Mirroring

Malheureusement, ces dispositifs ne permettent pas de se protéger des virus ou des mauvaises manipulations d'utilisateurs. Ainsi, les données modifiées sont automatiquement répercutées sur le disque miroir ou de parité. Il sera alors impossible pour l'utilisateur de récupérer ses données [CDPA04, CDPA01].

2.2.2 Réplications

2.2.2.1 Définition

Le procédé de réplication consiste à recopier l'ensemble des données sur un autre équipement. Le transfert peut être amélioré par divers algorithmes de compression ou de déduplication, mais la destination reste strictement identique à la source. L'objectif de ce procédé est d'avoir plusieurs copies des données qui puissent être exploitables en l'état afin de permettre l'accès à l'information sur plusieurs sites. Cela à plusieurs avantages :

- multiplier la copie des données et diminuer les risques de perte de l'information en cas de sinistres ;
- réduire le temps de rétablissement en cas de sinistre en basculant l'activité sur les données répliquées ;
- faciliter l'accès à l'information sur une zone de données ;
- améliorer la vitesse d'accès aux données sur des zones géographiques étendues.
- …

En fonction de l'environnement réseau et des besoins, on distingue 2 types de réplications :

La réplication synchrone

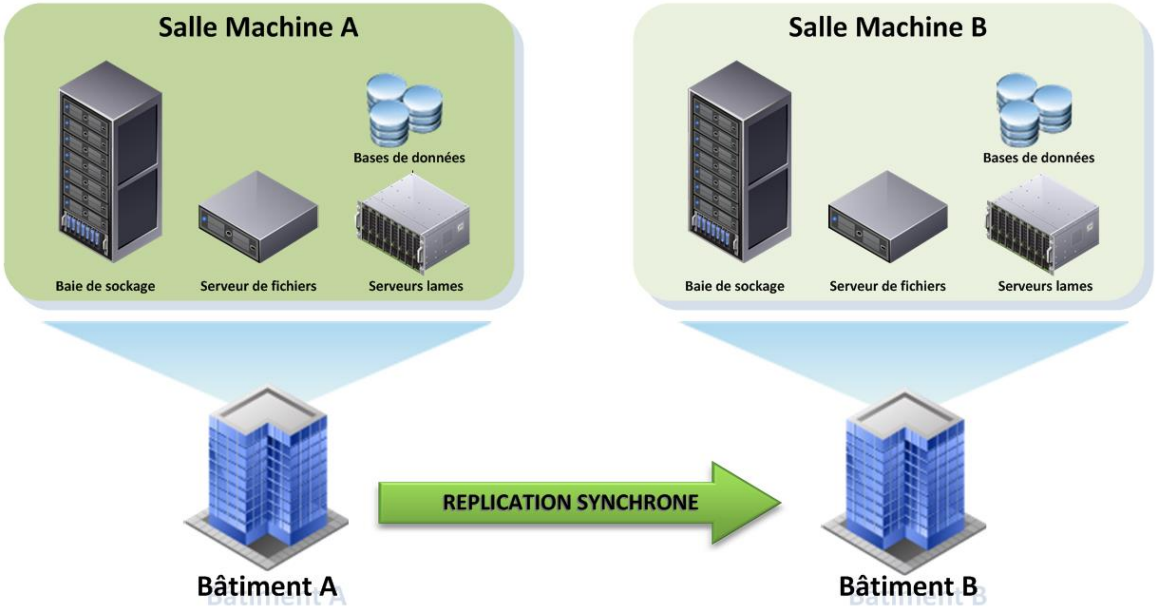


Figure 2-1 : Exemple de réplication synchrone

Dans le cas de réplication synchrone, il est nécessaire d'avoir une bande passante élevée avec un temps de latence faible (LAN ou réseaux en fibres optiques), car pour qu'une donnée soit écrite dans le système de stockage source (par exemple en salle machine A), il faut qu'il reçoive un acquittement attestant que l'information a aussi été écrite dans le système de stockage cible (par exemple en salle machine B). Cela limite fortement la distance puisque même avec un réseau en fibres optiques, il est recommandé de ne pas dépasser les 200 km [STORAGE01, page 80].

La réplication asynchrone

Elle est par définition une synchronisation différée. Elle est généralement utilisée lorsque l'on veut réaliser une réplication sur un site distant ne bénéficiant pas d'une liaison suffisamment dimensionnée ou dont les données sont énormément sollicitées. Les données peuvent être synchronisées :

- à un moment opportun défini par l'administrateur (la nuit par exemple) ;
- par un algorithme d'analyse de ressources (charge réseaux / charge processeur / …) ;
- au fil de l'eau ;
- …

Ce type de réplication à l'avantage de permettre une meilleure optimisation des flux de données, notamment grâce à l'utilisation d'algorithmes de compression avancée (tel que la déduplication) qui réduisent considérablement les besoins en bande passante.

2.2.2.2 Les inconvénients des réplications

La source étant identique à la cible, la réplication de données implique que l'espace de stockage soit au moins doublé. Elle nécessite aussi d'avoir une liaison réseau de bonne qualité entre les différents éléments (notamment dans le cas de réplication synchrone).

Au moment de la mise en place d'une réplication, il faut prendre en considération le temps de la première synchronisation. En effet, s'il y a un écart important (plusieurs téraoctets par exemple) entre les différentes entités (source et cible), cette première réplication peut mettre un temps assez important (des jours ou des semaines,…).

Exemple : Pour synchroniser un LUN de 1 To sans compression avec une liaison de 5 Mo/s il faudra : 1048576 Mo / (5 * 3600) ≈ 58.25 heures soit presque 2.5 jours

2.2.3 Sauvegardes traditionnelles (journalières)

2.2.3.1 Définition

Les sauvegardes traditionnelles étaient historiquement réalisées sur des bandes magnétiques (support fiable et économique). Leurs taux de transfert étant assez faible, les sauvegardes étaient lancées la nuit pour quelques centaines de mégaoctets voire quelques gigaoctets… Pour pallier ces problèmes de performance, les notions de sauvegardes différentielles (différence avec la sauvegarde complète) et incrémentales (différences avec la dernière sauvegarde) ont été inventées et ont permis de répondre temporairement à cette problématique.

L'expansion des données est telle que les différentes évolutions technologiques suffisent à peine à compenser les besoins de performance pour sauvegarder ce supplément d'information. De fait, elles restent souvent longues et peuvent solliciter beaucoup de ressources (processeur, mémoire, disques, réseaux, …).

2.2.3.2 Les évolutions technologiques

Prise d'image

Afin d'éviter l'arrêt des services sur les serveurs pendant les phases de sauvegardes, la plupart des logiciels de sauvegarde utilisent les nouvelles fonctionnalités des systèmes d'exploitation (ex : VSS sous Windows), pour prendre une empreinte des disques à sauvegarder (nécessitant quelques dixièmes de secondes) avant de procéder à la recopie des données. Ce procédé ne diminue pas le temps de sauvegarde, mais cela évite de bloquer le serveur pendant les opérations qui peuvent durer plusieurs jours.

Bibliothèque de bandes virtuelles - Virtual Tape Library (VTL)

Devant une croissance quasi exponentielle des besoins en stockage, il devenait de plus en plus contraignant d'utiliser les bandes magnétiques comme support de sauvegarde. La diminution des coûts de fabrication et l'augmentation des capacités de stockage des disques durs ont permis de mettre en place des solutions permettant la substitution des bandes par des disques.

Le principe vise à constituer un espace de stockage et à simuler le comportement d'un lecteur de bande. Ces équipements viennent remplacer les lecteurs de bandes magnétiques en toute transparence et corrigent les principaux inconvénients (manutention / temps d'accès / capacités). Par ailleurs, ce procédé permet de proposer de nouveaux services :

- La réplication de données : L'utilisation de bandes magnétiques ne favorisait pas la copie de ce support. La virtualisation permet une manipulation beaucoup plus souple. Les données peuvent ainsi être copiées, ou transmises sur un réseau distant, en utilisant des algorithmes de compression ou de déduplication ;
- La déduplication : Cela peut permettre d'économiser jusqu'à environ 95% de l'espace de stockage. Le même serveur sauvegardé 5 fois, ne prendrait ainsi que le stockage d'un serveur (cf. annexe 2) ;

Bien que les VTL soient plus simples à gérer que les supports magnétiques, les disques restent des supports plus fragiles que les bandes et les données manipulées atteignent des capacités importantes qui peuvent dépasser le pétaoctet de données sauvegardées. Dans ces conditions, il est préférable de mettre en place une réplication de ces données. Le phénomène est aggravé par l'utilisation d'algorithme tel que la déduplication, qui certes, optimise le stockage, mais qui en cas de corruption compromet l'ensemble des données hébergées…

Stockage sur pool de disques

De plus en plus de logiciels de sauvegarde s'affranchissent complètement des VTL pour stocker leurs données en utilisant leur propre espace de stockage, mais ce procédé ne permet pas (pour le moment) d'atteindre la capacité de stockage des VTL.

2.2.3.3 Les inconvénients des sauvegardes traditionnelles

Durant les dernières décennies, les sauvegardes journalières ont beaucoup évolué pour tenter de répondre aux principaux problèmes induits par cette technologie [STORAGE01, page 229]) :

- Les supports sur bandes magnétiques sont trop contraignants
  - L'accès aux données en lecture séquentiel n'est pas efficace, même si certaines technologies arrivent à des taux de transferts de 180 Mo /s ;
  - La taille des supports est trop petite (inférieur à 1,6 To) :
  - Les cartouches posent des problèmes de manutention
- La consommation des ressources (réseaux, processeurs, mémoire) peut être importante lors des sauvegardes.

Malgré les évolutions majeures des technologies, les problèmes liés au temps de sauvegardes et de restaurations restent entiers tant l'augmentation des volumétries est importante.

Certaines sauvegardes nécessitent plusieurs jours de traitements (exemple : cas de sauvegarde complète). Lorsque celle-ci n'aboutit pas, l'intervalle de temps sans sauvegarde est augmenté, puisqu'en cas de problème, il ne sera possible que d'effectuer une restauration qu'à partir de la dernière sauvegarde valide…

2.2.4 Les prises d'images ou "snapshots"

Le principe est de réaliser une image à un moment précis d'une ressource que l'on souhaite sauvegarder. Ainsi, on peut restaurer tout, ou partie de cette image. Cette technologie est souvent orchestrée par un planificateur de tâches qui va par exemple réaliser une image toutes les 4 heures.

La plupart des systèmes d'exploitation (Windows, Linux,…) donnent la possibilité de prendre des empreintes de disques en quelques secondes. Ce procédé permet de récupérer le contenu d'un disque à un moment donné, mais, ne s'agissant pas d'une copie, elle reste dépendante de son support physique. En cas de problème sur le disque, toutes les images seront perdues…

2.2.5 Les Clusters

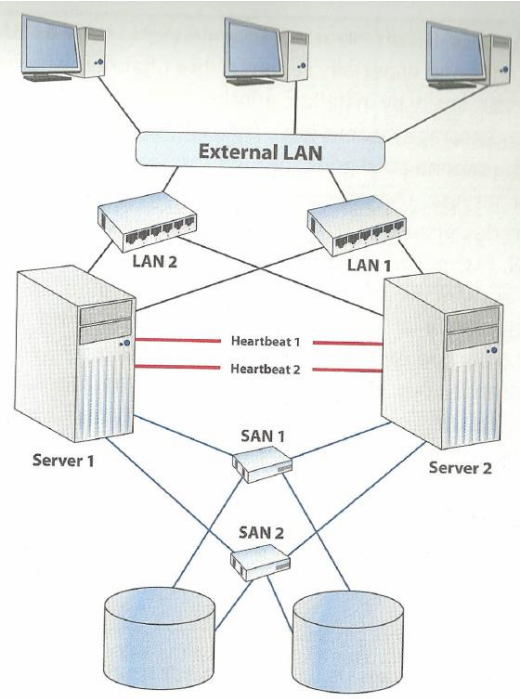


Figure 2-2 : Les Clusters [STORAGEA02, page 162]

Un Cluster est un groupe de serveurs réunis pour assurer une continuité de service ou répartir les charges (réseaux, processeurs, mémoire, etc…). Si l'un des serveurs (aussi appelé nœud) n'est plus fonctionnel, la charge est alors transférée sur les autres serveurs.

Les serveurs vérifient l'état de santé des autres nœuds au travers des "lignes de vie" (aussi appelé "Heartbeat" en anglais).

Chaque nœud travaille avec ses données et ses disques, mais ils ont souvent la possibilité de voir les volumes des autres serveurs afin de pouvoir reprendre leurs activités en cas d'incident.

Bien qu'ils permettent de fiabiliser et de parer aux défaillances matérielles ou logicielles (fuite mémoire, blocage,…), ils ne permettent pas de protéger le contenu des données qu'ils manipulent de la corruption. C'est d'ailleurs leur plus grande faiblesse, car si un nœud considère à tort qu'un autre ne fonctionne plus, il se peut qu'il modifie les mêmes données, qu'il les corrompt et les rend inexploitables…

2.2.6 Les logiciels de gestion de versions

Ils permettent ainsi de référencer toutes les versions d'un fichier ou de dossiers. Ils sont principalement adaptés pour les fichiers bureautiques et les développeurs (sources et packages d'installation) qui ont un taux de modification modéré (quelques modifications par jour). Ces outils ne sont pas élaborés pour réaliser des traitements de masse.

Le principe consiste à réaliser une copie vers un autre emplacement (éventuellement en le compressant) et de lui adjoindre une information de date ou de version, afin de garantir un état et de pouvoir le récupérer ultérieurement.

Il existe plusieurs formes d'actualisation :

- Soit au moment de l'enregistrement du fichier
- Soit lorsque l'utilisateur dépose ses fichiers (cas de Visual SourceSafe)
- Soit à l'aide d'un processus qui vérifie de manière régulière les fichiers qui ont été modifiés

De fait, certaines contraintes en découlent :

- En cas d'incident, c'est la précédente version sauvegardée qui pourra être récupérée (qui peut avoir plusieurs jours) ;
- Le périmètre est restreint aux fichiers et dossiers et ne permet pas de protéger les fichiers qui sont en constantes modifications.

2.2.7 Les journaux (fichiers de logs)

Ils sont fréquemment utilisés dans tous les systèmes informatiques pour historiser le séquencement d'actions ou d'évènements. Ses applications sont nombreuses :

- Diagnostiquer un problème ;
- Tracer une séquence d'actions (exemple : démarrage d'un ordinateur) ;
- Loguer les accès des utilisateurs ;
- Référencer les transactions d'utilisateurs ;
- Référencer des anomalies ;
- …

Lors de transactions (ex. virements bancaires) elles permettent de retrouver des informations manquantes.

Les bases de données (MS SQL serveurs, Oracle, …) alimentent des journaux de transactions particulièrement complets. Ils permettent de restaurer une base de données, mais également de rejouer une partie des transactions de manière assez précise.

2.3 LE CONCEPT DE LA PROTECTION CONTINUE (CDP)

2.3.1 Les principes

La protection continue des données (Continuous Data Protection) est un concept où toutes les modifications du stockage sont journalisées et copié sur un support de stockage privatif de sorte que l'on puisse restaurer les données à n'importe quel moment (révolu) sur une période de temps définie. Ces différentes versions peuvent ensuite être transmises en temps réel ou en différé dans un centre de données de secours.

C'est tout un procédé de journalisation et de réplication qui permet la mise en œuvre de cette protection sur des fichiers, mais aussi sur des applications comme les serveurs de bases de données ou de messageries...

Ainsi, si un incident intervient en fin de journée, les utilisateurs ne perdent pas leur travail. Alors qu'avec les autres moyens de sauvegarde ils ne récupéreraient que les données issues des dernières sauvegardes (pouvant remonter à plusieurs heures).

De même, si des fichiers sont modifiés à plusieurs reprises, l'utilisateur pourra récupérer la version qui l'intéresse le plus et pas uniquement la dernière.

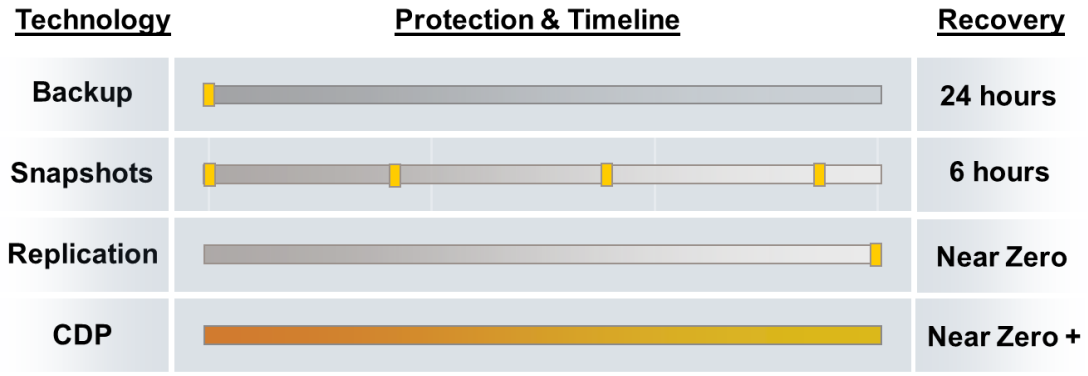


Figure 2-3 : Différences entre CDP et les autres technologies [NETBKPA03,page 6]

Le schéma ci-dessus illustre les différences qu'il existe entre les différentes technologies et la protection continue :

- Sauvegardes journalières traditionnelles : point de restauration pouvant attendre les 24h
- Cliché instantané : Ils sont souvent espacés de plusieurs heures
- Réplication : données à jour, mais seul la dernière version est accessible

2.3.2 La cohérence des images

La cohérence des données

Les données modifiées étant transmises et enregistrées sur le serveur CDP en continu dans un environnement souvent en mouvement, il est difficile de garantir que chacun des états soit exploitable. Cette situation peut être comparée aux problèmes que rencontrent les photographes. Si un acteur bouge pendant la prise de vue, la photographie peut être floue et inexploitable. Il en est de même avec le flux d'information. Par exemple, une copie de fichiers de plusieurs giga-octets peut prendre plusieurs dizaines de secondes (voir plusieurs minutes). Tant que le fichier n'est pas totalement copié, il sera impossible d'avoir un état stable puisqu'il manquera une partie du fichier. Cela peut rendre le fichier totalement inexploitable et engendrer des pertes majeures d'informations… Quand un cliché est pris, il doit être net, et la totalité des informations doit être accessible et lisible.

Afin de garantir la cohérence des données copiées, les différentes solutions du marché dispose d'un agent ou d'un service qui interroge régulièrement (selon la politique de protection) le système d'exploitation ou les logiciels pour qu'ils se positionnent dans un état dit :"cohérent" ("consistent" en anglais) avant de procéder à la sauvegarde.

Notion de groupe cohérence

Synchroniser un disque ou un LUN peut être dans certains cas insuffisants. Il arrive que des fichiers soient liés et disposés sur plusieurs disques. Cela peut par exemple être le cas des bases de données (MS SQL Server) où les fichiers de données sont en corrélation avec les journaux de transaction. Dans ce cas, il faut que la prise d'image intervienne en même temps. Cette notion de synchronisation d'un groupe de disques lors des prises d'images est définie comme étant "un groupe de cohérence" ("consistency group" en anglais).

2.3.3 Les grandes catégories de la protection continue

Deux types de protections continues sont souvent comparés :

- **Le "Near CDP" :** Ces solutions effectuent des sauvegardes planifiées et cycliques. Elles s'appuient généralement sur le système d'exploitation pour réaliser des prises d'images. La fréquence des snapshots est augmentée et peut osciller en fonction des solutions et du paramétrage entre une minute et une heure. Il ne s'agit donc pas réellement d'une solution CDP puisque, même s'il est court, il existe un temps entre chaque point de restauration. Ces produits ont moins d'exigence en terme d'équipements et de fait sont généralement moins onéreux. Cependant, elles sollicitent souvent plus les ressources des serveurs hôtes.

- **Le "True CDP" :** Dans ce cas, toutes les transactions sont enregistrées. Ainsi, il est possible de restaurer n'importe quels états du système sur une période définie. Cependant, chaque moment ou point de restauration n'est pas forcément cohérent (cf. 2.3.6.4 la problématique de la cohérence des données). Elles sont généralement issues de fournisseurs de stockage (ex : EMC/ FalconStor) et nécessitent souvent la mise en œuvre d'infrastructures onéreuses (baies, SAN, switchs, splitter,…).

L'opposition de ces deux modes de fonctionnement ne serait-elle pas simplement un argument commercial ? Aucune solution CDP ne peut garantir la cohérence de l'ensemble des modifications, en particulier lorsque les données sont gérées par des applications. Dans ces conditions, restaurer un état du système dans un état non fiable réduit l'intérêt de la solution. Afin de remédier à ce problème, les éditeurs de solutions "True CDP" proposent, tout comme les produits "Near CDP" de réaliser régulièrement (soit en fonction du temps, soit en fonction du nombre d'octets différents) des points de restauration cohérents. Or, en étudiant les différents produits ("True CDP" et "Near CDP"), on s'aperçoit que la fréquence des images cohérentes préconisées oscille entre 15 et 30 minutes… Ces solutions présentent donc des services qui semblent similaires…

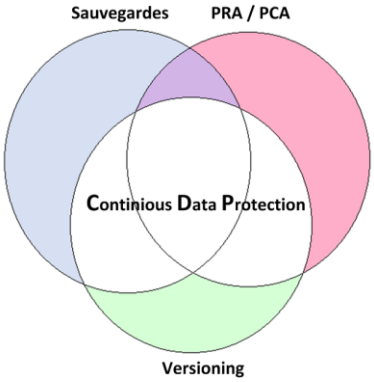


Figure 2-4 : Les orientations du CDP

On peut alors se demander quelles sont réellement les différences et les intérêts de ces technologies. Pour le comprendre, il faut avoir une approche plus fonctionnelle, en étudiant les principales variantes de la protection continue :

- Outil de sauvegarde : Optimisé pour le stockage de l'information
- PRA / PCA : Réduire le temps de reprise d'activité
- Versioning : Avoir la granularité la plus fine.

2.3.4 Les orientations de protection continue

2.3.4.1 Le CDP : outils de sauvegardes

Les outils CDP qui se présentent comme des outils de sauvegarde ont pour objectifs principaux de sécuriser les données à moyen ou long terme (multi-versions) et d'économiser le stockage à l'aide d'algorithmes de compression évolués (type déduplication). Les images prises sont quasi systématiquement réalisées avec un agent ou un module adéquat (bases SQL / Messagerie,..) afin d'obtenir un état cohérent et stable. L'outil utilise les propriétés du système d'exploitation et du système de fichier pour prendre une empreinte qu'il

sauvegardera par la suite (seules les différences seront transmises). S'agissant d'outils de sauvegardes, des restrictions sur des sous-arborescences peuvent souvent être paramétrées via les politiques de sauvegardes. Cela forme un système relativement efficace et optimisé qui permet de réaliser des économies de stockage et de bandes passantes.

Un autre inconvénient de ces produits est que les données sauvegardées ne sont pas exploitables en l'état et elles nécessitent d'être restaurées sur le stockage primaire de production. Cela peut être long à réaliser et augmente le temps de rétablissement.

2.3.4.2 Le CDP : outil de PRA ou de PCA

L'objectif est de permettre une reprise d'activité le plus rapidement possible avec un point de restauration (RPO) le plus proche de l'incident. Afin de répondre à ces attentes, les moyens mis en œuvre sont liés aux services proposés par des infrastructures de stockage évoluées (Baie, NAS, SAN, etc.) où des journaux, des snapshots et des processus de réplications sont mis en œuvre. Cette architecture induit cependant quelques contraintes :

- Le coût : La mise en œuvre de ces solutions nécessite souvent l'utilisation d'un SAN et ces équipements de stockage représentent un cachet assez élevé (plusieurs dizaines ou centaines de milliers d'euros).
- L'utilisation plus importante d'espace de stockage : Afin d'être plus réactif lors des opérations de restauration, les données ne sont jamais compressées. L'espace utilisé par le CDP dépasse ainsi la taille du stockage primaire, car il faut également stocker le journal de transactions dont la taille varie en fonction des modifications et de la politique de protection.
- La granularité de restauration est moins fine : ce type d'outil favorise la restauration des volumes dans leur globalité. La restauration unitaire de fichiers n'est pas une priorité.
- Risque de corruption de données **:** La méthode de stockage fait que les journaux et les prises d'images sont fortement liés au stockage primaire. Si celui-ci est endommagé, c'est l'ensemble des données et des versions qui seront perdues. De ce fait, il est préférable d'ajouter soit une copie supplémentaire ou une solution de sauvegarde adaptée. Ceci est particulièrement pertinent si l'on a besoin d'une rétention assez longue (plus d'un mois).

2.3.4.3 Le CDP : outil de versioning

Ces produits sont souvent à destination des postes utilisateurs ou sur des emplacements (partages de fichiers) parfaitement délimités. Ils ne demandent pas d'infrastructures onéreuses et s'appuient principalement sur une architecture logicielle.

Ces outils sont principalement développés pour protéger des fichiers bureautiques. Ils ont une granularité plus fine (elle va jusqu'aux fichiers) et certains produits (Tivoli, Atempo) permettent d'enregistrer et de conserver toutes les versions (à condition d'avoir l'espace disque nécessaire).

La principale contrainte de ces outils est qu'ils risquent de consommer trop de ressources sur le poste client (cf. les faiblesses de Tivoli CDP for files en section 2.4.4).

2.3.5 Les atouts de la protection continue

2.3.5.1 Réduction des fenêtres de sauvegardes

Les modifications sont loguées au fur et à mesure du temps. De ce fait, ce système permet en quelques dixièmes de seconde (en fonction des modifications réalisées) de récupérer une image complète et cohérente. Il n'est donc plus nécessaire de prévoir une fenêtre de sauvegarde pouvant atteindre plusieurs heures [CDPA04]. Cela est très utile lorsque l'on souhaite sauvegarder de fortes volumétries.

Remarque : les données sont hébergées dans un stockage local, l'externalisation ou la déduplication des données peut représenter un temps non négligeable qu'il convient d'étudier…

2.3.5.2 Réduction des pertes de données (RPO=0)

L'ensemble des modifications étant journalisé, si un problème intervient, les dernières modifications sont accessibles et peuvent être facilement récupérées. C'est d'autant plus vrai lorsque les solutions intègrent une réplication des disques de production comme c'est le cas de certaines solutions (EMC RecoverPoint, Netbackup Realitime, Falconstor CDP,…).

2.3.5.3 Protection contre la corruption de données

Les données sont conservées sur une période préalablement définie. L'objectif étant en cas de corruption, de pouvoir les récupérer lorsqu'elles étaient cohérentes (c'est-à-dire avant que l'anomalie ne survienne).

2.3.5.4 Facilite la reprise d'activité

Toutes les modifications sont stockées sur le serveur CDP. En fonction de la demande de restauration et de ses journaux, la solution CDP régénère l'image souhaitée de l'état du système. Il ne s'agit pas d'une copie de fichiers, mais plutôt d'une indexation des données. Cela permet de présenter une image cohérente en quelques secondes qui peut être déployée soit en production, soit dans une architecture auxiliaire (de secours).

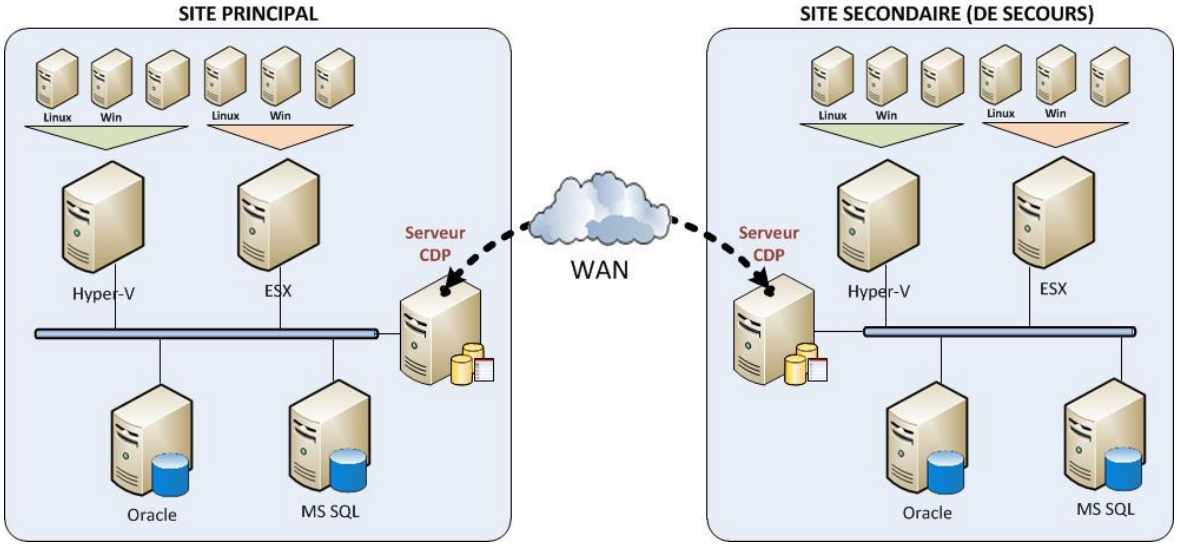


Figure 2-5 : Exemple d'architecture CDP favorisant la reprise d'activité

Certaines solutions (ex : FalconStor CDP) permettent même de générer un cliché instantané bootable qui peut être converti en serveur virtuel, le temps de remonter un nouveau serveur physique.

2.3.5.5 Facilitation de tests et de migrations

La possibilité de revenir en arrière est un atout majeur pour les développeurs ou les techniciens cherchant à valider une nouvelle application ou une architecture logicielle.

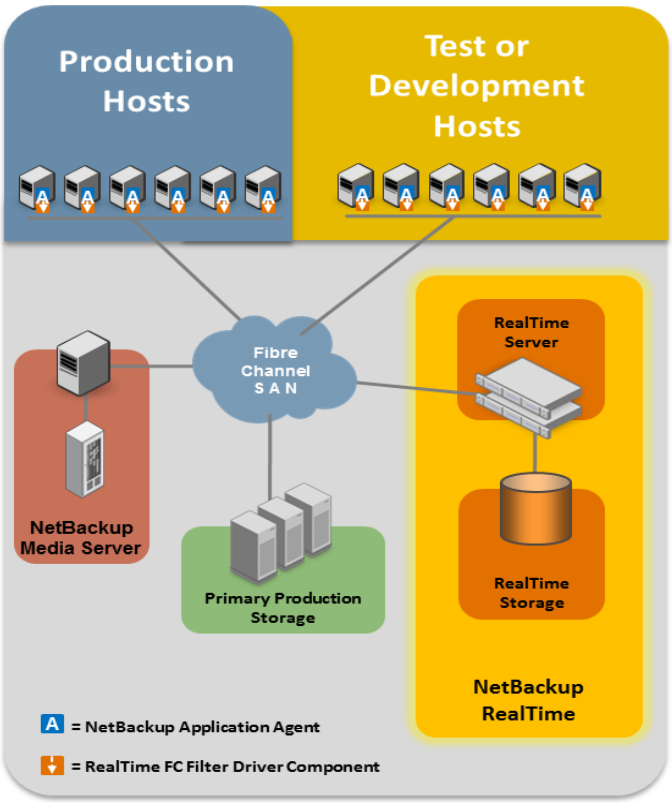


Figure 2-6 : Architecture Netbackup Realtime (Symantec)

Ces fonctionnalités peuvent intervenir sur plusieurs niveaux :

- Lors du processus de développement : La protection continue permet de dupliquer des serveurs ou des architectures assez facilement. Cela peut s'avérer très pratique pour cloner des environnements de production afin de vérifier le comportement de nouvelles applications
- Lors du processus de mise en production : Pouvoir restaurer l'état d'un serveur, d'une base de données ou d'une application, permet d'ajouter un niveau de sécurité lors de la mise en production d'upgrade ou de nouvelles applications. En effet si un incident intervient durant une mise à jour logicielle, l'ancienne version peut être redéployée en quelques minutes. Alors qu'en faisant appel aux outils de restaurations conventionnelles cela pourrait demander plusieurs heures (temps de restauration).

2.3.6 Les contraintes de la protection continue

2.3.6.1 Consommateur de ressources

L'objectif du CDP est de conserver toutes les modifications. Ce qui implique que lorsqu'une donnée est sauvegardée sur un disque, cette donnée est dupliquée sur le serveur gérant le produit CDP. Cela occasionne donc une montée en charge du processeur, des disques de stockages et réseaux. Le problème est que d'une manière générale, les serveurs devant bénéficier de ce type de protection sont souvent déjà fortement sollicités [CDPA01].

Le choix de la solution CDP joue un rôle déterminant sur l'impact qu'elle peut avoir sur le serveur. En effet, les solutions (comme Asigra et EMC RecoverPoint) ne nécessitent pas forcément de déployer un agent sur les serveurs à protéger. De fait, elles ne les affectent quasiment pas. En revanche, d'autres solutions (comme Cofio AIMStor, FalconStor CDP,…), requièrent l'installation d'un agent, qui sollicite (plus ou moins) les ressources Ethernet ; processeurs et mémoire de leurs serveurs.

2.3.6.2 Consommateur d'espace de stockage

En fonction du type de solution CDP (cf. 2.3.4-Les orientations de protection continue), la consommation de stockage varie énormément... Les solutions orientées « sauvegardes » utilisent des algorithmes de déduplication qui optimisent le stockage et, avec une bonne stratégie, elles n'occupent pas plus d'espace qu'une sauvegarde traditionnelle.

Pour les solutions qui favorisent la reprise d'activité, les disques étant répliqués, il faut au minimum doubler la capacité et ajouter la taille des journaux et des éventuelles images capturés.

Exemple : pour protéger un LUN de 100 Go, il faudra prévoir en plus :

- 100 Go pour le stockage secondaire :
- 20 Go pour les journaux de transactions CDP (dépend des actions réalisées sur les LUN protégés et du temps que l'on souhaite conserver)
- 20 Go pour les différentes images (snapshots)

➔ Soit un espace de stockage total d'au moins 240 Go.

2.3.6.3 Complexité de paramétrage

La mise en œuvre de solution de sauvegarde nécessite d'avoir une vision globale. Si la stratégie n'est pas bien définie, il peut en résulter certains désagréments comme une surconsommation de ressources réseau et système, mais aussi des coûts d'infrastructures [COFIOA01].

2.3.6.4 La cohérence des données

L'enregistrement de l'ensemble des écritures n'est pas en soi une protection suffisante pour garantir la reprise d'activité en cas de plantage [COFIO01]. En effet, certaines applications ou certains systèmes d'exploitation (exemple: Linux) peuvent utiliser à des fins d'optimisation des zones de mémoire temporaire. Ces données n'étant pas écrites sur disques, elles peuvent ne pas être récupérées en cas d'incident brutal. Il en est de même pour les sauvegardes : si, au moment de la prise d'image, l'application ne s'est pas positionnée dans un état cohérent, il est possible que les données sauvegardées ne soient pas exploitables.

Il existe cependant une alternative. Certaines applications (Exchange, Oracle, MS SQL Serveur) peuvent se positionner dans un état permettant une prise d'image cohérente. Cependant, cette opération ne doit pas être réalisée trop souvent (surtout sur des serveurs fortement sollicités). En effet, dans ce cas les écritures sont bloquées (parfois pendant plusieurs secondes) et cela peut gérer quelques désagréments sur les serveurs, notamment une augmentation des temps de latence et des phénomènes de congestion.

2.3.6.5 La rétention des données

La protection continue des données est organisée selon un procédé de stockage cyclique dépendant essentiellement des ressources allouées (ex : taille des journaux de transactions). Lorsque les ressources de stockage sont épuisées, les points de restauration les plus anciens sont écrasés. Le temps de conservation des données dépend donc du paramétrage, de l'espace de stockage, mais aussi du nombre d'écritures.

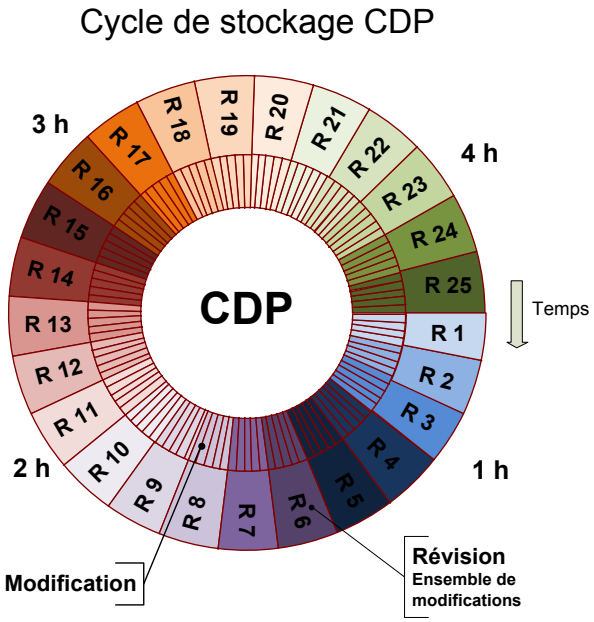


Figure 2-7 : Problématique corruption de données

Prenons comme exemple le cas d'une base de données où la solution CDP génère un point de restauration toutes les 10 minutes. Si les différents paramètres ont été étudiés pour conserver 25 points de restauration (soit un peu plus de 4 h), alors il sera possible de récupérer n'importe quel état sur une période d'environ 4 heures. Au-delà, les données seront perdues [CDPA01]. De plus, si l'activité de la base de données a été sous-évaluée, la fenêtre de protection peut descendre bien en dessous de ce seuil de 4 h.

La rétention des données est donc une notion variable qui dépend d'évènements non maitrisés (demandes d'écriture). Cela complique et rend le paramétrage difficile de ces applications et peut engendrer le non-respect de cahier des charges (fenêtre de protection trop courte)

2.4 LES PRINCIPAUX ACTEURS

Les rapports Gartner sont particulièrement appréciés dans les différentes filières de l'informatique. Ils permettent notamment de situer les principaux acteurs dans chacun des domaines. Ci-dessous, le "Magic Quardrant" (Gartner, janvier 2011) a recensé les principaux acteurs des entreprises spécialisées dans la sauvegarde sur disques :

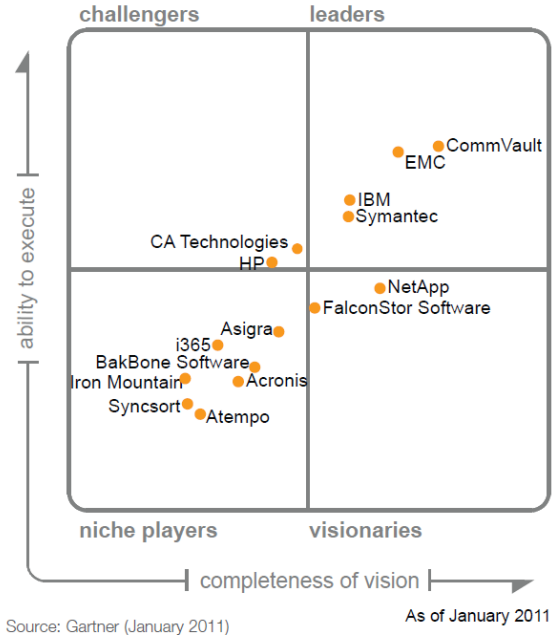


Figure 2-8 : Sauvegardes sur disques (Gartner 2011)

Quatre entreprises (CommVault, EMC, Symantec, IBM) se détachent des autres en se positionnant comme les principaux animateurs du domaine. Netapp reste aussi bien placée, notamment grâce à son système de prise d'images optimisé ([STORAGEA04]).

FalconStor se détache pour ses technologies de CDP, de réplication et de déduplication [STORAGEA04].

Asigra connu pour ses outils de "Cloud Backup" offre des solutions sans agent (Agentless) sur une très grande variété de plateformes.

2.4.1 CommVault Simpana

2.4.1.1 Présentation

Largement plébiscité par les derniers rapports GARTNER (2011 et 2012) . La solution Simpana n'est pas uniquement un utilitaire de sauvegarde, mais un outil complet permettant de gérer l'information.

L'objectif est d'optimiser le stockage de l'information et son administration en ne proposant qu'un seul et même outil. Chaque module est totalement intégré à la solution Simpana et possède les dernières innovations technologiques : la déduplication, l'archivage par fichier stubs, la protection continue,… .

CommVault possède de solides références dans le milieu bancaire avec l'utilisation de cette solution par le Crédit Mutuel de Bretagne, ainsi que la Banque Postale qui possède en France plus de 10 000 agences (dont les débits sont de qualités variables).

2.4.1.2 Principe de fonctionnement

Le serveur applicatif "CommServe" (pouvant être virtualisé) administre et gère l'ensemble de l'architecture Simpana. Il utilise une base de données MS SQL serveur qui lui permet de stocker les informations nécessaires aux différents modules.

Les MédiaAgents servent d'interface entre les clients et les éléments de stockage (Disques ;VTL ; lecteur de bandes).

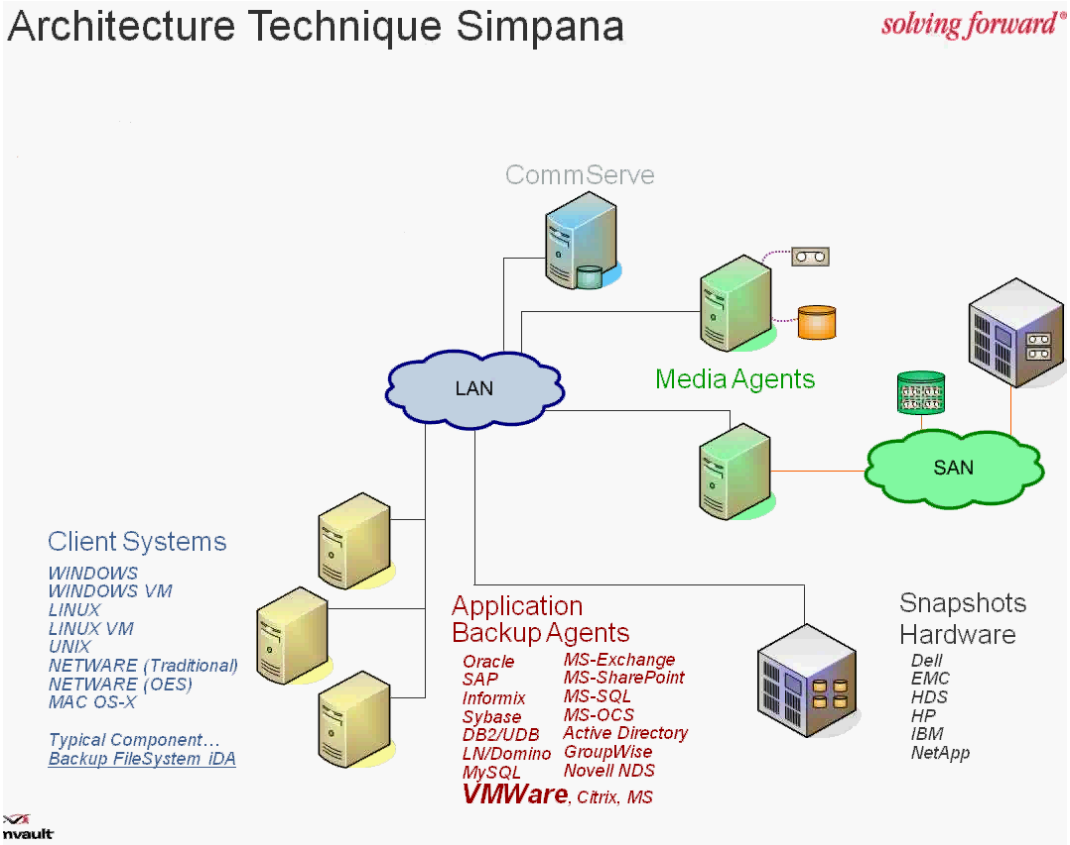


Figure 2-9 : Architecture Simpana (Commvault)

L'architecture est assez ouverte et propose une compatibilité avec la plupart des systèmes d'exploitation (Unix,/ Windows, Netware, etc.). La solution n'est pas uniquement dédiée aux serveurs, car une version est aussi disponible pour les postes utilisateurs et les ordinateurs portables.

ContinuousDataReplicator

La protection continue est réalisée par l'intermédiaire du module ContinuousDataReplicator(CDR). Il permet la mise en œuvre de répliquas qui peuvent être de plusieurs formes :

- Direct Réplication : une source pour une destination
- Fan-In : plusieurs sources vers une destination
- Fan-Out : une source vers plusieurs destinations

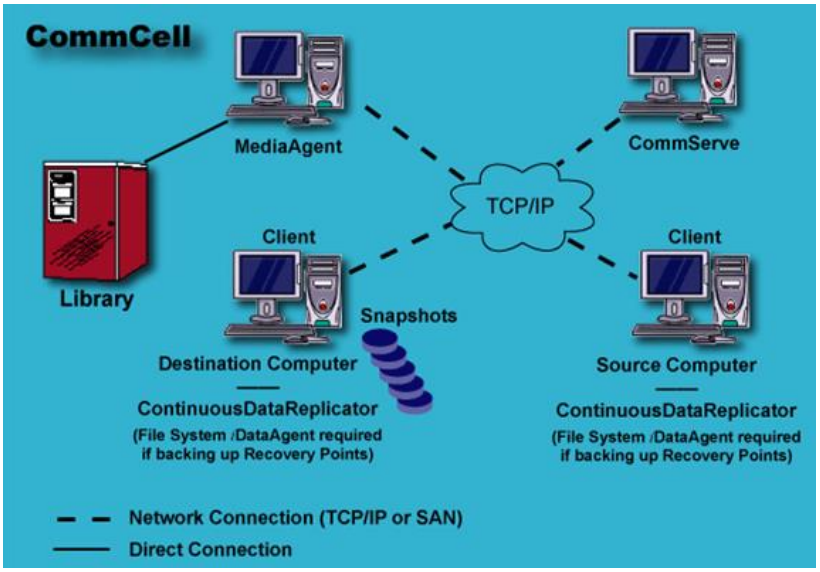


Figure 2-10 : ContinuousDataReplicator (commvault)

Ces différents modes de réplication facilitent la consolidation des données. La solution nécessite l'installation d'un agent sur les différents postes, mais celui-ci s'installe sur une couche assez basse du système d'exploitation de manière à minimiser l'utilisation de ressources sur les machines hôtes.

La synchronisation des données est réalisée au travers des réseaux (TCP/IP ou SAN). L'agent positionné sur le poste client transfère les données vers sa destination. Afin de ne pas surcharger le réseau, les données peuvent être dédupliquées selon un algorithme de décomposition en blocs de tailles fixes, mais paramétrables (la taille initiale est fixée à 128 Ko).

Interfaces et gestion des utilisateurs

Les outils servant à administrer la solution existent en plusieurs versions :

- Applicatif internet Web
- Client lourd
- Ligne de commandes

L'installation des différents composants est grandement facilitée par la mise à disposition des packages segmentés en modules et la possibilité de les déployer par l'intermédiaire de scripts. Cela permet de limiter la taille des fichiers et facilite le déploiement sur les sites les plus isolés.

Les droits utilisateurs sont paramétrables et peuvent être définis dans l'active directory (AD). Ainsi, plusieurs rôles peuvent être définis :

- Administrateur ;
- Restaurations ;
- Opérateurs de sauvegarde ;
- Restauration distante ;
- …

2.4.1.3 Expérimentation impossible

La direction commerciale Cincom n'a pas souhaité me fournir des licences pour que l'on teste leur solution. Bien que le produit paraisse prometteur en termes de fonctionnalités, il m'a été impossible de l'évaluer.

2.4.2 EMC² - RecoverPoint

2.4.2.1 Présentation

EMC RecoverPoint est une solution matérielle de protection continue. Elle s'appuie sur des équipements de stockage (Baie) sur laquelle des appliances ont été ajoutées afin de proposer des services supplémentaires.

Son rôle n'est pas de remplacer une solution de sauvegarde, mais d'être un complément permettant de répondre à des besoins spécifiques ou à des problématiques induites par des volumétries conséquentes de données.

Elle représente notamment un atout pour la mise en place de Plan de Reprise d'Activité (PRA). Alors que les outils de sauvegarde se contentent de sauvegarder et de restaurer des données, EMC propose une solution qui permet de substituer très rapidement (à partir de quelques secondes) des données de production corrompues par une version antérieure (sur le serveur de production ou de secours).

La solution EMC RecoverPoint propose un large éventail de fonctionnalités permettant en autre :

- la restauration à n'importe quels moments révolus ;
- la gestion de réplications synchrone ou asynchrone intelligente ;
- des optimisations de la bande passante des réseaux;
- une solution « agentless » (Il n'y a pas d'agent installé sur les serveurs) ;
- de facilité et d'amélioré la mise en place de PRA/PCA ;
- de travailler sur les réplications sans impacter les données de production ;
- de faire du LUNs Mapping (présentation de LUN);
- de prendre des images cohérentes avec certaines applications (Exchange / MS SQL Serveur / Oracle, etc...);
- de gérer les groupes de cohérence ;
- La mise en œuvre de règles de rétention.

La solution est étudiée pour qu'il n'y ait aucun problème de performances (CPU / Mémoire / Réseaux) sur les serveurs protégés.

EMC RecoverPoint est compatible avec la plupart des systèmes d'exploitation courants (Windows / Unix / Linux, etc…)

2.4.2.2 Principe de fonctionnement

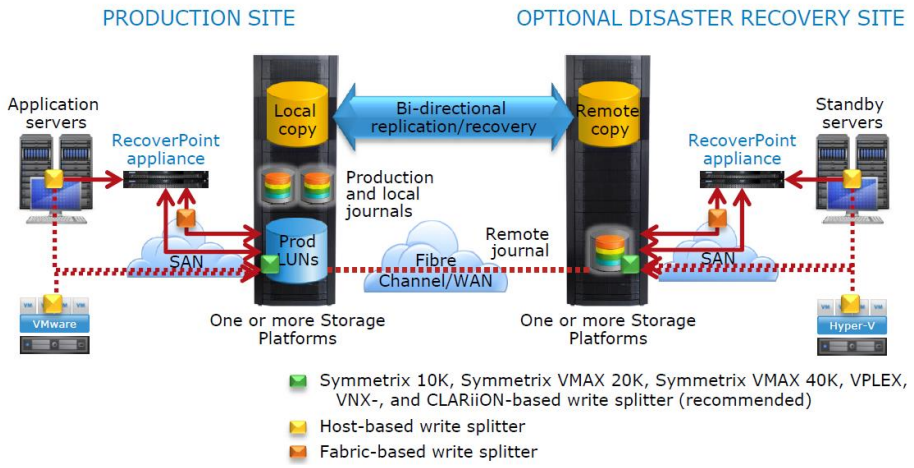


Figure 2-11 : Architecture EMC RecoverPoint(EMC)

Les demandes d'écritures sont dupliquées et transmises à l'appliance RecoverPoint et à la baie de stockage. Les appliances se chargent ensuite d'alimenter leur journal de transactions et les différentes copies des données (locale et/ou distante).

Principe de réplication

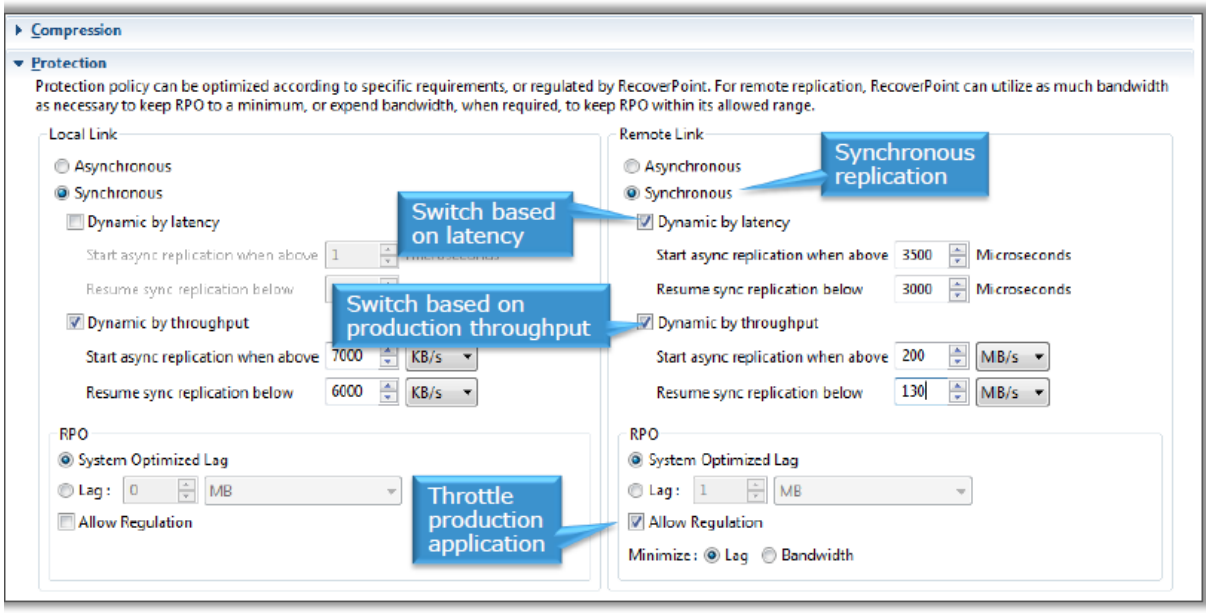


Figure 2-11 : Optimisation de la liaison RecoverPoint (EMC)

Les algorithmes de réplications sont particulièrement évolués et savent optimiser l'utilisation de la liaison :

- Dans le cas d'une liaison dynamique (en temps réel), EMC RecoverPoint analyse régulièrement l'état du réseau (Temps de latence / débits), afin de ne pas surcharger la bande passante. Si la liaison devient insuffisante (cf. figure 2-11 ci-dessus), l'appliance peut revoir son comportement et différer sa synchronisation (en fonction du RPO).
- Dans le cas d'une liaison asynchrone, les données modifiées peuvent être compressées et dédupliquées (lors de la transmission vers un site distant).

EMC RecoverPoint distingue 3 modes de fonctionnement :

- Continuous Data Protection (CDP):

  Il s'agit d'une protection locale. Les données stockées sont dupliquées dans le même site. Il existe donc 2 copies distinctes.
- Continuous Remote Recovery (CRR):

  Les données sont répliquées sur le site distant de manière synchrone. Si le site principal devient hors services, le second peut prendre le relais. Lorsque le problème est résolu, le site de secours peut actualiser le site principal avant sa reprise d'activité.

- Concurrent Local and Remote (CLR):

  Méthode la plus évoluée : une copie locale et distante est réalisée. Ainsi en cas de problème, il est possible de trouver une solution sur le site local ou de secours.

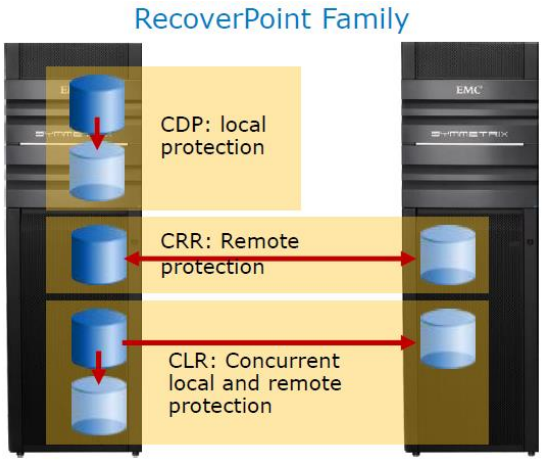


Figure 2-12 : Les réplications RecovertPoint(EMC)

Optimisation du réseau

Le trafic réseau lié aux réplications des données peut être optimisé en utilisant la déduplication à la source. Il s'agit du même moteur utilisé que le produit AVAMAR. La taille des blocs est de 512 octets [EMCRPPDF]

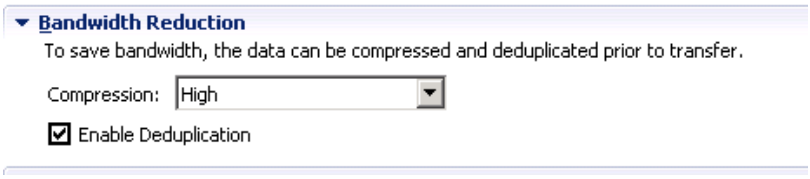


Figure 2-13 : Options d'optimisation réseaux

Optimisation des ressources CPU/ Mémoire

Aucun agent ou service n'est nécessaire (hormis pour les prises d'images cohérentes) sur les serveurs. Ainsi aucune ressource n'est sollicitée sur les serveurs protégés. Les demandes d'écritures sont dupliquées à l'aide d'un splitter afin d'être loguées et copié sur un disque miroir.

Principe de génération d'images cohérentes

Pour réaliser une image cohérente, RecoverPoint a besoin qu'un agent soit déployé sur le serveur hôte afin de dialoguer avec le système d'exploitation ou l'application que l'on

souhaite protéger. Ainsi, le serveur ou l'application peuvent se positionner dans un état "crash consistant" avant la prise d'image.

Gestion des règles de rétentions

Les rétentions RecoverPoint sont dégressives (cf. figure 2-14 ci-après) :

- Protection Continue : toutes les écritures sont capturées
- Quotidienne : une fois le délai de la protection continue échue, les points de restaurations sont consolidés en un point quotidien de restaurations.
- Hebdomadaire : une fois le nombre de points de restaurations quotidiens atteint, ils sont consolidés en en un point de restauration hebdomadaire
- Mensuel : une fois le nombre de points de restaurations hebdomadaires atteint, ils sont consolidés en en un point de restauration mensuel qui sera conservé jusqu'à la prochaine consolidation mensuelle

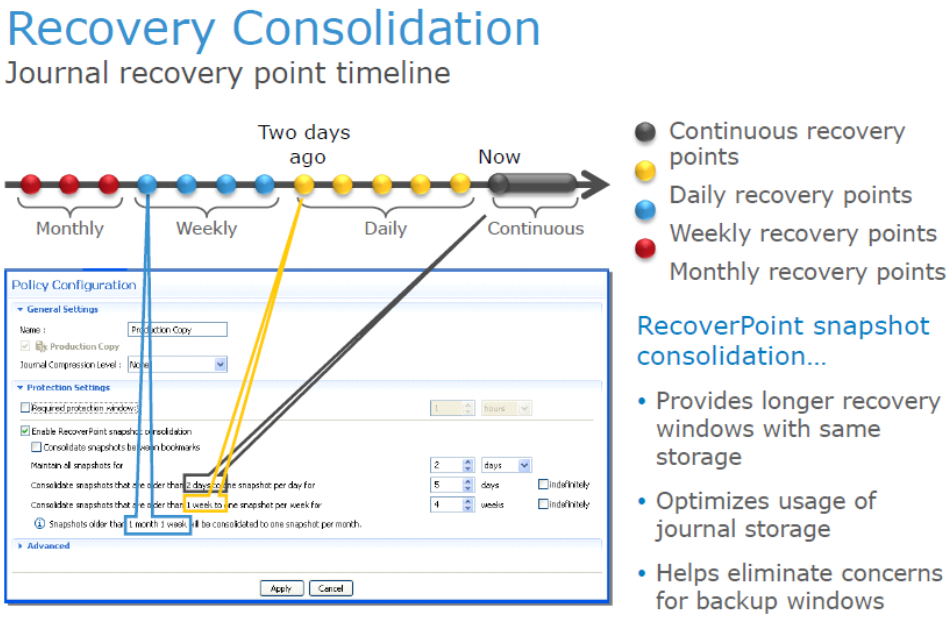


Figure 2-14 : Paramétrage des rétentions RecoverPoint(EMC)

2.4.2.3 Tarification de la solution

Le prix d'une infrastructure RecoverPoint dépend de la volumétrie à protéger, ainsi que du nombre d'appliances (1 à 4 configurées en cluster) et du nombre de baies VNX (1 baie en mode CDP ou 2 baies en mode CLR ou CRR) utilisées. Le coût des équipements SAN ainsi que des licences à ajouter sur les baies VNX sont les principaux freins à la mise en œuvre de ce type d'infrastructure.

2.4.3 Symantec - Netbackup Realtime

2.4.3.1 Présentation

Netbackup Realtime est un outil de protection continue de données (CDP). Il journalise toutes les modifications et les recopies dans un volume de stockage dédié. Ces données permettent ainsi de reconstruire un disque à n'importe quel moment désiré. Il s'agit d'un outil qui privilégie la reprise d'activité et qui facilite les sauvegardes.

2.4.3.2 Principe de fonctionnement

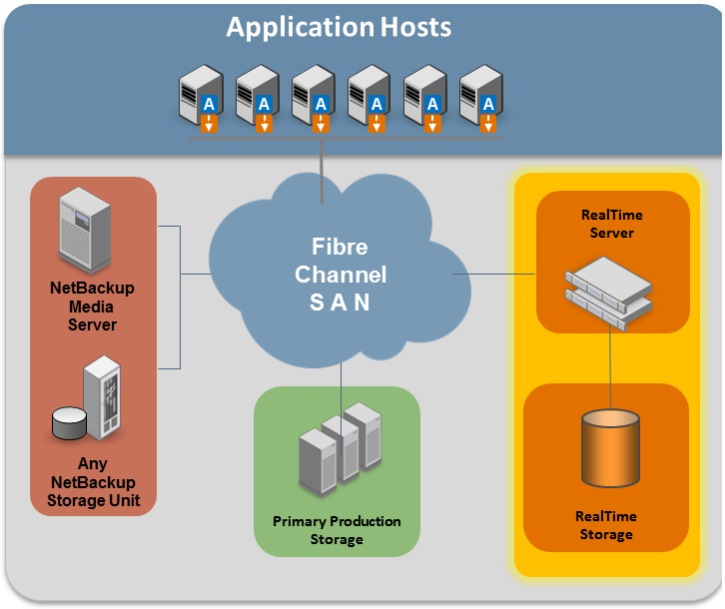


Figure 2-15 : Architecture Netbackup Realtime (Symantec)

L'infrastructure Netbackup Realtime nécessite d'être interconnecté sur un réseau en fibres optiques. Les demandes d'écritures sont transmises par l'agent installé sur le serveur hôte vers son stockage primaire et vers la zone de stockage Realtime.

Ces données ainsi copiées peuvent ensuite être sauvegardées par l'outil de sauvegarde Netbackup.

Pas de perte de données et rapidité de reprise (RPO et RTO proches de 0)

Les données étant répliqué et non compressées ou dédupliqués, elles restent directement accessibles. En quelques secondes, Netbackup Realtime peut mettre à disposition plusieurs téraoctets de données. Il reconstruit un LUN ou un disque (à l'aide de son journal de transactions) qui peut remplacer l'unité logique de production et permettre ainsi une reprise rapide de la production.

Réduction de la fenêtre de sauvegarde

Les données étant toutes enregistrées lors de leurs modifications, le serveur CDP dispose des dernières versions des serveurs à protéger. Il n'est donc pas nécessaire de lancer un traitement qui peut se relever assez lourd. L'agent Netbackup Realtime ne sollicite le système d'exploitation ou les applications que pour récupérer une image cohérente (soit quelques secondes). Ce qui réduit considérablement la fenêtre de sauvegarde.

Réplication sur site distant

Afin de sécuriser complètement les données, Netbackup Realtime permet d'externaliser ses données vers un des sites distants. Il analyse l'état du réseau afin de limiter et d'optimiser son utilisation selon des paramètres (latences, limitation de bandes passantes, etc...). Il possède son propre algorithme de compression et de déduplication qui lui permet de transmettre les blocs identiques qu'une seule fois.

2.4.3.3 L'échec de Netbackup Realtime

Les raisons

Malgré une solution ouverte et ne nécessitant que la mise en place d'un SAN, Netbackup Realtime n'a pas réussi à s'imposer sur ce marché. Symantec a donc décidé en juin 2012 d'annoncer la fin de vie de ce produit et de revoir sa stratégie commerciale.

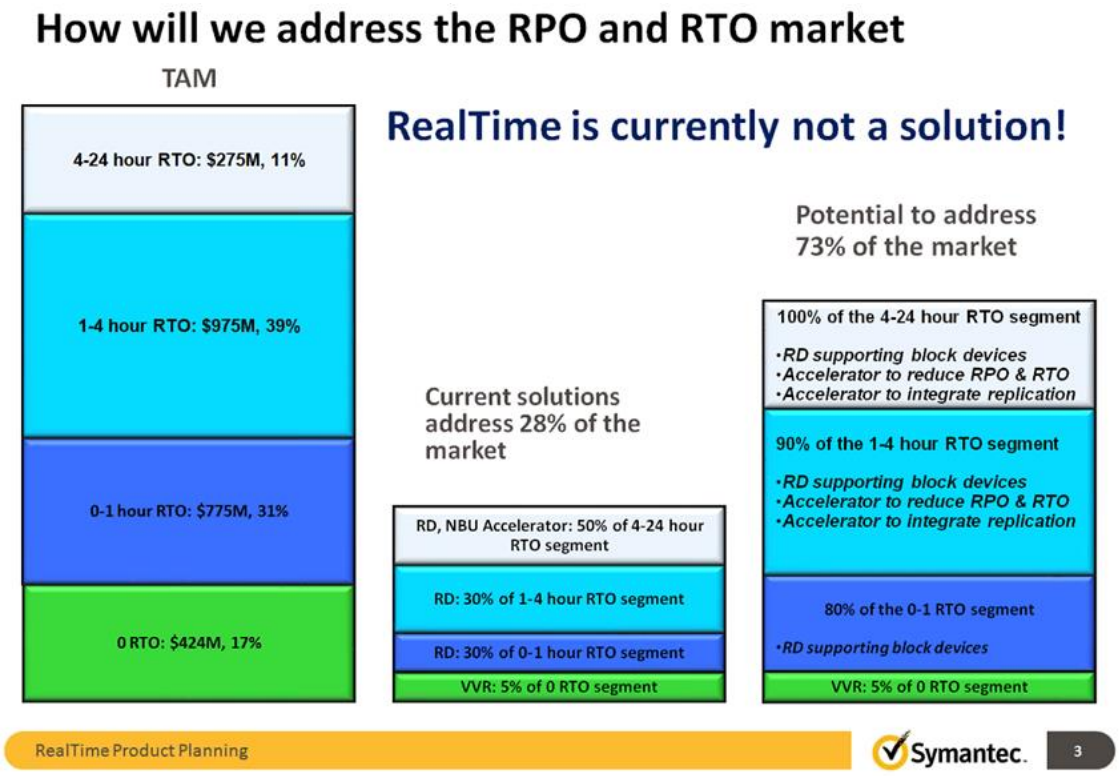


Figure 2-16 Les besoins en PRA selon Symantec

Les principaux arguments de vente de Netbackup Realtime (RTO et RPO proche, voire égale à 0) ne représentent pas un enjeu suffisant pour continuer d'investir sur ce produit. D'une part, le marché n'est pas aussi intéressé par cette technologie (selon leurs études) et d'autre part, la multitude de produits Symantec permet de répondre à une grande partie de ces besoins.

Les propositions de Symantec

Suite à cette annonce, Symantec m'a donné deux axes de recherche :

- Replication Director : permet de répliquer des données des NAS (pour le moment uniquement compatible avec les NAS NetApp.
- Netbackup Accelerator : permet de réduire les temps de sauvegardes.

Ces deux technologies sont en cours d'expérimentation, mais sont pour le moment loin des fonctionnalités qui étaient offertes par Netbackup Realtime, notamment pour ce qui concerne les temps de reprise d'activité…

2.4.4 IBM Tivoli

2.4.4.1 Présentation

Tivoli CDP for files est l'une des premières solutions CDP qui a été introduit sur le marché en 2005. Précurseur dans le domaine, elle permet sans infrastructure onéreuse de mettre en œuvre une protection continue. La solution comprend plusieurs versions à déployer sur des serveurs ou des postes utilisateurs. L'installation est rapide et la configuration permet de définir plusieurs niveaux de protection

2.4.4.2 Principe de fonctionnement

Lors de l'enregistrement d'un fichier (protégé par la politique de sauvegarde), celui-ci est également copié vers une zone de stockage local. En fonction du paramétrage (fréquence de réplication) défini par l'utilisateur, un processus le transférera tous les fichiers ainsi modifiés dans une autre zone de stockage (par réseau TCP/IP). Ils pourront ensuite être sauvegardés.

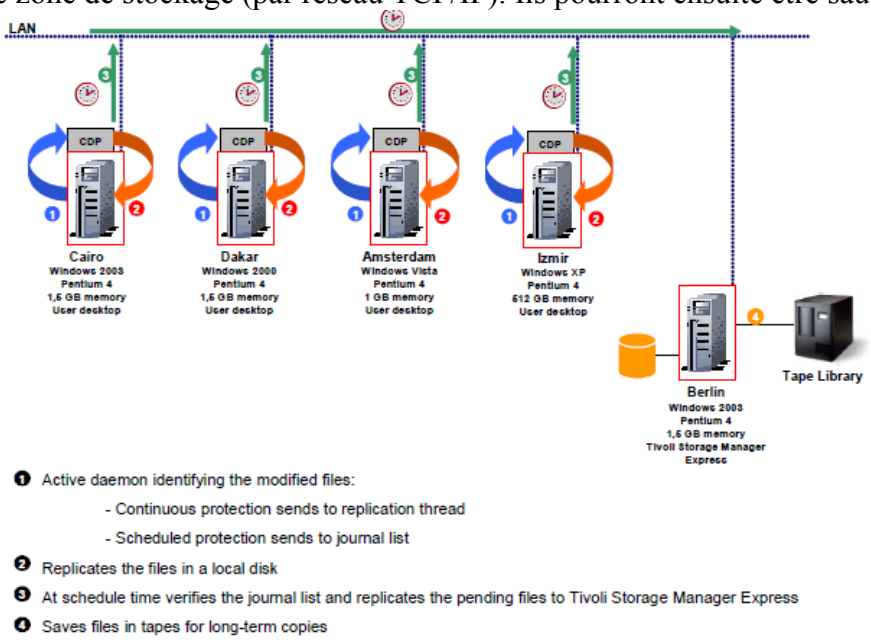


Figure 2-17 : Architecture Tivoli CDP for files [IBMA02 ,page 152]

L'utilisateur définit le niveau d'importance des différentes ressources. Il existe 3 modes de protection :

- Protection continue des données : un agent surveille les ressources à protéger et capte toutes les modifications (lors de l'enregistrement. À chaque fois qu'un fichier est enregistré, les modifications sont journalisées et copiées ;
- Planifié : l'utilisateur définit une fréquence de sauvegarde ;
- Protégé ("Vault") : les fichiers sont protégés en écritures. Ils ne peuvent ni être modifiés, ni supprimés.

L'interface graphique utilisateur

Il s'agit d'une interface WEB (intégré dans un navigateur internet). Les pages sont assez ludiques et permettent à une personne ayant un minimum de connaissance en informatique de paramétrer le produit.

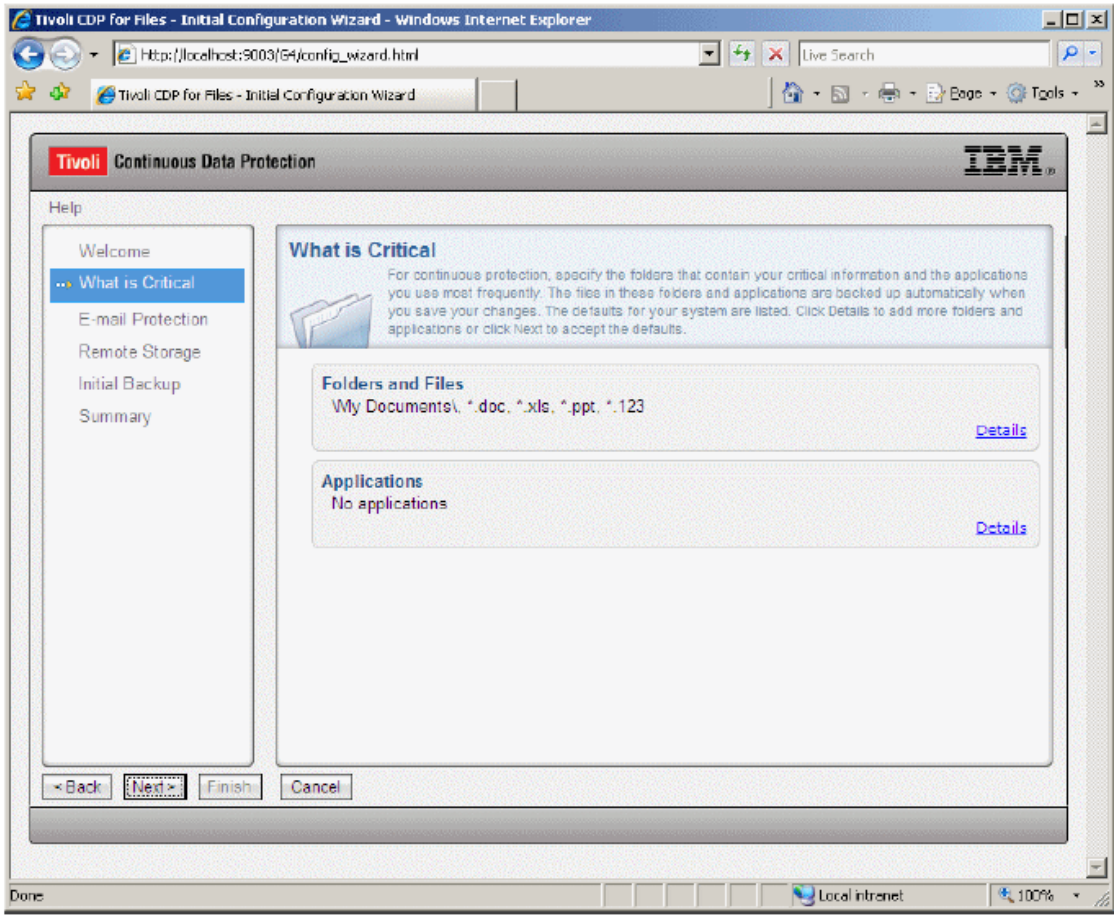


Figure 2-18 L'interface de Tivoli CDP for files

Le prix des licences

IBM propose deux types de licences : poste utilisateur ou serveur à des prix attractifs (cf. tarifs 2011 en euros ci-dessous) susceptibles d'intéresser les petites et moyennes entreprises.

Tarif détaillé

Sélection	Description de l'élément	*Tarif IBM, taxes non comprises	*Tarif IBM, taxes comprises
☐	IBM Continuous Data Protection for files Starter Edition Single Client License + SW Subscription & Support 12 Months (D613ALL)	44.03	52.66
☐	IBM Continuous Data Protection for files - Server Edition Single Server License + SW Subscription & Support 12 Months (D615SLL)	316.00	377.94

Figure 2-20 Prix public des licences IBM CDP for files

2.4.4.3 Les faiblesses du produit

Les fichiers ouverts ou constamment modifiés

Les journaux de Tivoli CDP ne sont alimentés uniquement lorsque les fichiers sont enregistrés. Cela convient globalement aux fichiers bureautiques, mais pose des problèmes lorsque les fichiers restent ouverts ou lorsqu'ils sont constamment modifiés.

Espace de stockage de réplication

La documentation du produit indique clairement que si l'espace de stockage distant (qui contient toutes les versions de fichiers) s'avérait trop petit, les versions les plus anciennes sont libérées pour permettre l'enregistrement des fichiers les plus récents.

When the storage space becomes full, Tivoli Continuous Data Protection for Files deletes older backup copy versions of files that have several backup copy versions. After deleting the versioned backup copies, if more space is needed for new backup copies, Tivoli Continuous Data Protection for Files deletes the last remaining backup copies of enough files to make room for the newest backup copy.

Figure 2-19 : Extrait documentation [IBMA02, page 60]

Travailler sur des fichiers volumineux représente donc un risque pour l'ensemble des versions des fichiers sauvegardés, surtout, si l'espace de stockage a mal été évalué.

Produit inadapté à l'environnement d'Euro-Information

La solution n'est fonctionnelle que sur les systèmes d'exploitation Windows. Elle est par ailleurs limitée à la protection de fichiers. Son utilisation est plus appropriée pour des postes utilisateurs. De plus, les tests réalisés ont montré qu'à la suite de son installation, il pouvait y avoir quelques latences sur certaines applications (Navigateur Internet)…

Enfin, dans la mesure où il existe dans l'environnement d'Euro Information des solutions de stockage de type "NAS", l'intérêt de ce produit semble minimisé.

2.4.5 ASIGRA

2.4.5.1 Présentation

Société américaine de plus de 25 ans d'expériences dans les domaines de sauvegarde, restauration et archivage. Elle est particulièrement réputée pour être l'un des leaders en outils de sauvegardes déportés (Cloud backuping).

Ce sont d'ailleurs les premiers à avoir proposé un algorithme de déduplication à la source (block-level incremental client-side) [STORAGEA04]

2.4.5.2 Principe de fonctionnement

Asigra possède ses propres centres de données et propose ces services pour héberger des données. Fort de leurs expériences dans le domaine des sauvegardes déporté, ils ont adapté leurs outils pour permettre la mise œuvre dans un environnement privatif. La solution est particulièrement ouverte et est compatible avec un grand nombre de systèmes d'exploitation (Windows, Unix, AS400,etc…) et de type de terminal (serveur, ordinateur, portable, tablette, smartphone).

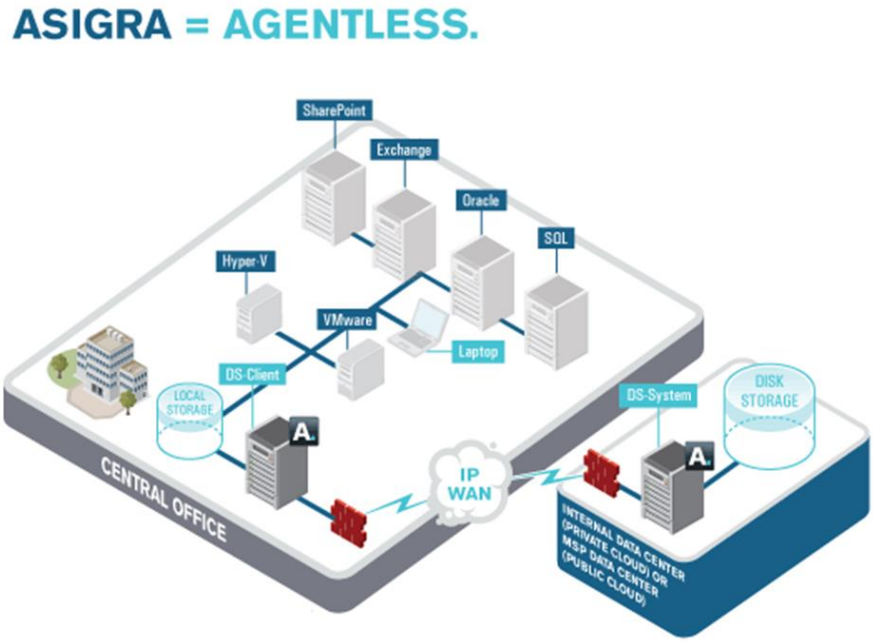


Figure 2-21 : Architecture ASIGRA [ASIGRAA01]

Asigra est composé :

- Modules ASIGRA :
  - DS-System : Stock les données
  - DS-Client : Collecteur de données
  - Autres modules…
- Stockage : Disques de stockage

- Client :
  - Serveurs
  - Postes Utilisateurs
  - Équipements mobiles (portables ;smartphones ;tablettes)

Les clients accèdent à leurs données stockées en local. Le DS-Client collecte toutes les modifications lorsque les fichiers sont sauvegardés et les transmet aux DS-System par le WAN en réalisant une déduplication à la source.

La solution ASIGRA est "Agentless" : les clients n'ont pas besoin d'avoir un agent installé. Cela simplifie la maintenance (pas de mise à jour) et aucune ressource n'est nécessaire sur les différents terminaux.

Figure 2-22 : Les Agents ASIGRA [ASIGRAA01]

Toutefois, dans certains cas des agents seront tout de même nécessaires :

- Postes isolés : lorsque les données à protéger se trouvent sur un équipement qui ne possède pas une liaison suffisamment dimensionnée. L'agent ainsi installé sur le terminal collecte et transmet les modifications lorsqu'il accède au réseau.
- Prises d'images cohérentes : Pour positionner certaines applications spécifiques dans un état "crash-consistent". Utilisé notamment pour Oracle (RMAN) ou MS SQL Serveur(VSS)

2.4.5.3 Les faiblesses du produit

Selon le rapport Gartner 2011, les interfaces d'administrations peuvent être complexes à utiliser [STORAGEA04, page 7].

Un autre inconvénient du module CDP est qu'il n'est utilisable que sur des partages de fichiers. Dans la mesure où la grande majorité des fichiers du groupe CM-CIC sont hébergés sur des NAS, l'intérêt pour ce produit est fortement réduit. Ceci est d'autant plus vrai que la sauvegarde des données sur des NAS EMC ou NetApp n'est pas supportée par Asigra [STORAGEA04, page 7].

Malgré ces points négatifs, ses capacités à sauvegarder des postes isolés seraient sans doute à étudier et à comparer avec l'outil de sauvegarde AVAMAR actuellement utilisé pour les agences du groupe CM-CIC.

2.4.6 FalconStor CDP

2.4.6.1 Présentation

Société créée au début du siècle, elle se démarque dès 2003 pour ses solutions de VTL(Virtual Tape Libraires) et de réplication. Leur gamme de produits n'étant pas suffisamment étendue, FalconStor travaillait principalement en partenariat avec d'autres revendeurs (EMC par exemple). L'arrivée de nouveaux produits tels que FalconStor CDP et Network Storage Server(NSS) ont largement contribué à améliorer leur notoriété et à devenir un revendeur de solution autonome.

FalconStor CDP propose une solution plus accessible que ces concurrents (EMC, Netbackup), car aucune infrastructure particulière n'est requise. L'agent installé sur le poste à protéger duplique toutes les écritures vers l'appliance FalconStor CDP qui les journalise et les stocke dans sa zone de stockage. Cette réplication est paramétrable et peut être synchrone ou asynchrone. Cette architecture demande peu de moyens, mais peut en revanche être consommatrice de ressources (réseaux IP ou SAN).

La protection des données concerne la totalité du disque (LUN ou partitions logiques). Il n'est pas possible de protéger uniquement un répertoire ou une sous-arborescence.

La solution couvre les principaux systèmes d'exploitation (Windows / Linux / Unix) (cf. Matrice de comptabilité : http://www.falconstor.com/certification-matrix/operating-systems)

2.4.6.2 Principe de fonctionnement

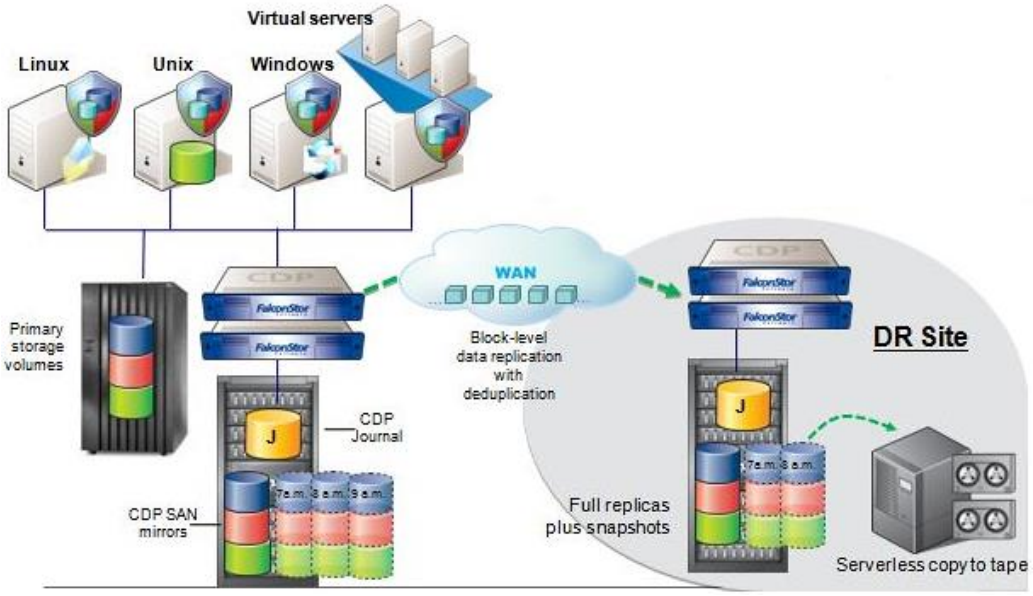


Figure 2-23 : Architecture FalconStor CDP (FalconStor)

L'architecture de FalconStor s'appuie sur plusieurs éléments :

- les agents :
- l'appliance FalconStor CDP
- le stockage

L'Agent

Son premier rôle est d'être une interface entre la machine hôte et l'Appliance CDP et de jouer un rôle de :

- Console Administration : permet le paramétrage de la politique de sauvegarde, de réaliser les prises d'images et les opérations de restaurations.
- Mirroring logiciel : l'agent se loge dans les couches basses de la machine afin de dupliquer toutes les écritures (mode bloc de 256kb) et de les transmettre à l'appliance CDP qui les consigne dans son système d'information. Cette opération est peu couteuse en CPU, mais consomme des ressources réseau.
- Prises d'images cohérentes (OS et applicatifs) : il dialogue directement avec le système d'exploitation et/ou des applications (Exchange, Oracle, MySQL,Sharepoint,…), afin de positionner l'espace de stockage du serveur dans un état cohérent avant la prise d'image.

L'Appliance FalconStor CDP

L'Appliance FalconStor CDP est le cœur de l'architecture CDP. Elle est administrée par l'interface graphique nommé "IPStor". Elle se comporte comme une baie de stockage. Elle

permet de présenter (mapper) des LUNs aux serveurs et de réaliser les opérations d'allocation ; de prise d'images et de gérer :

- la gestion des politiques de sauvegarde (planifications, rétentions, type, ….)
- l'administration des réplications
- l'administration du système de stockage (Présentations des LUN, prise d'image et génération de snapshots(à partir des journaux en mode CDP)
- l'édition de rapports

Le stockage

L'appliance FalconStor CDP a besoin d'un espace de stockage conséquent. Il doit être supérieur à la taille des disques à protéger. Falconstor préconise d'allouer en moyenne 120%, car en plus des données, l'appliance alimente des journaux de transaction.

Le stockage peut être hébergé sur une baie de stockage ou tout simplement utiliser les disques physiques hébergés par l'appliance.

2.4.6.3 Les fonctions avancées

LUN Mapping

La console d'administration IPStor permet de présenter des LUN à n'importe quels serveurs via le protocole ISCSI ou au travers du SAN. Cette fonctionnalité peut être automatisée à l'aide du module HyperTrac de FalconStor.

Plan de Continuité d'Activité (PCA)

La solution FalconStor CDP permet de repositionner ou de présenter les LUN protégés quel que soit la version souhaitée dans la mesure où celle-ci est présente dans la fenêtre de protection. Le module RecoverTrac de FalconStor permet de préparer la bascule sur le site de secours. Cela consiste à préparer le script (réalisable au travers de l'interface graphique) orchestrant la reconstruction d'un serveur sur le site local ou de secours. Il n'est pas nécessaire que le serveur de secours soit identique au serveur source. RecoverTrack est capable de reconstruire celui-ci (quelles que soient ses caractéristiques) aussi bien vers un serveur physique que vers un virtuel :

- une machine Physique peut être transférée vers une autre machine Physique (PtoP) ;
- une machine Physique peut être transférée vers une machine Virtuelle (PtoV) ;
- une machine Virtuelle peut être transférée vers une autre machine Virtuelle (VtoV) ;
- une machine Virtuelle peut être transférée vers une machine Physique (VtoP) (même si cela ne présente pas un grand intérêt).

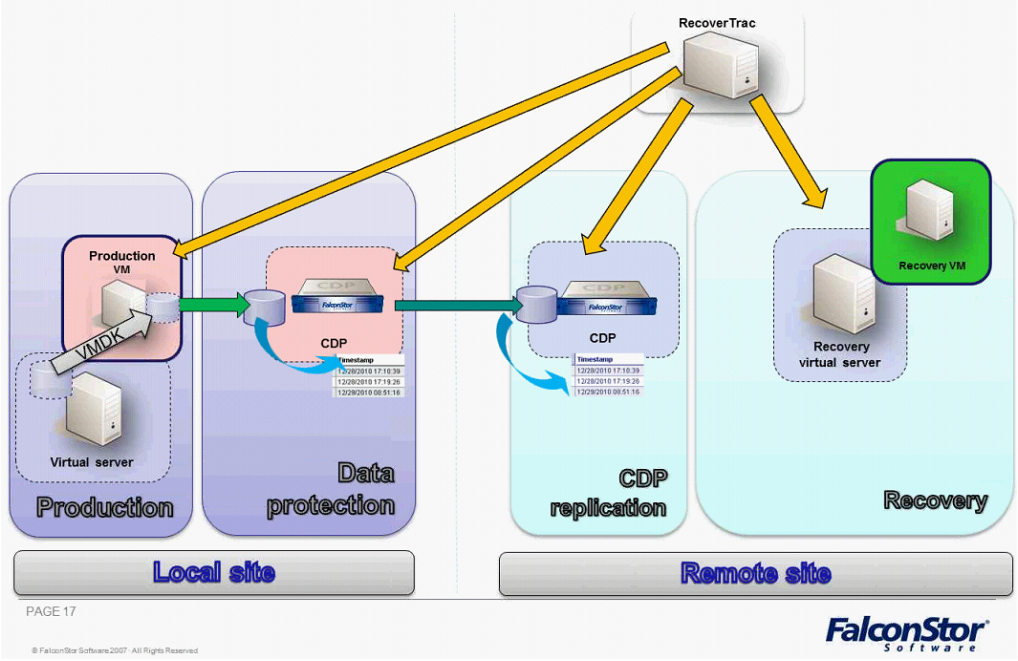


Figure 2-24 : Présentation de RecoverTrac

La demande de reconstruction d'une machine est réalisée en quelques secondes. Soit à l'aide de l'interface graphique (cf. figure 2-25), soit en ligne de commande. Le temps de reconstruction varie en fonction des serveurs, mais dans le cas d'une machine virtuelle (VM), cela ne prend que quelques minutes…

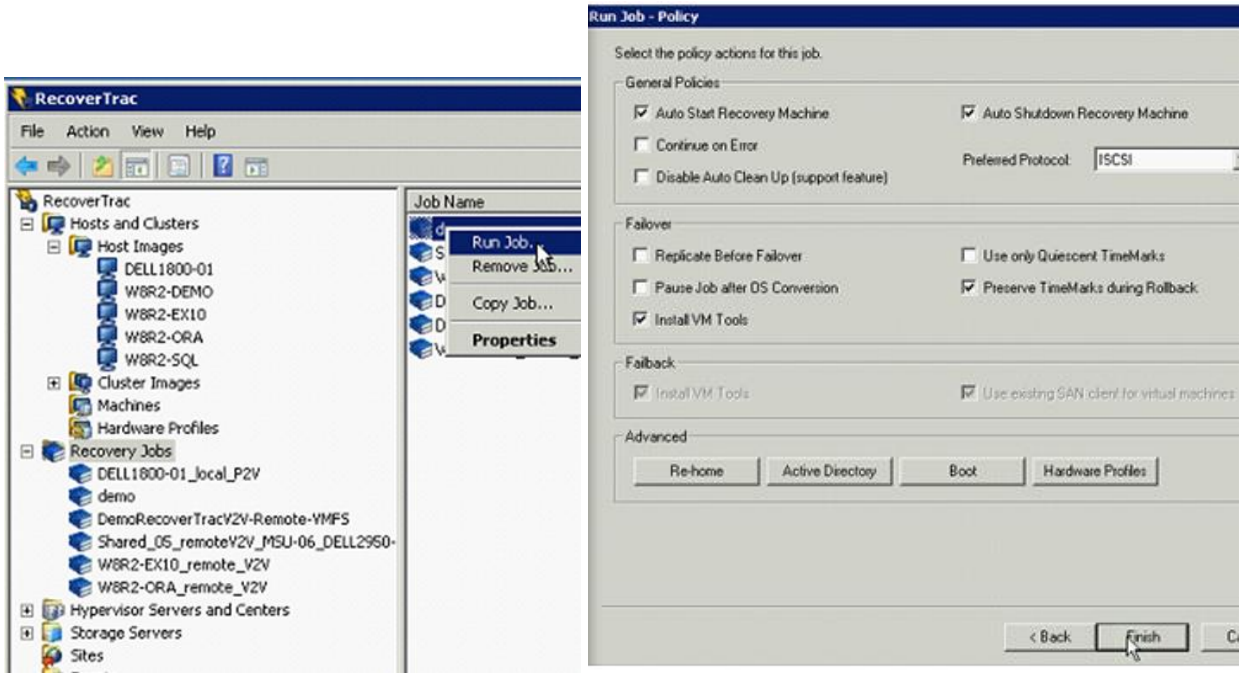


Figure 2-25 : Lancement d'un script de reconstruction d'une VM avec RecoverTrac

2.4.7 Les NAS : NetApp

2.4.7.1 Présentation

Leader sur le marché des serveurs de fichiers, NetApp bénéficie de son ancienneté et de son expérience dans ce domaine. Ses NAS permettent des partages de fichiers, tout en proposant des services complémentaires :

- optimisation du stockage (Déduplication)
- planifications régulières de prises d'images
- consolidation des données vers des sites distants (Snapvault)
- prises d'images cohérentes sur des serveurs ou certaines applications (MSSQL)
- …

2.4.7.2 Principe de fonctionnement

Optimisation du stockage

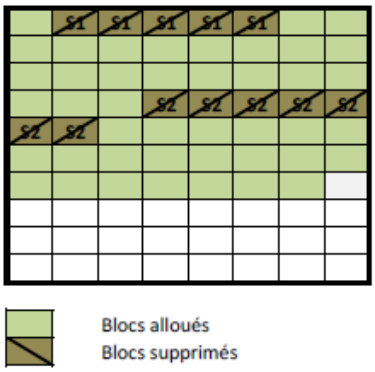


Figure 2-26 : Stockage NetApp

Les NAS NetApp ont pour particularité d'intégrer dans leur volume de stockage les différentes prises d'images. Ce procédé de stockage, qui mélange les données et les snapshots, permet d'optimiser l'espace disque.

Lors d'une prise d'image, les blocs actifs (alloués) sont affectés à un snapshot. Tant que celui-ci ne sera pas libéré, l'ensemble de ces blocs restera affecté au stockage : les blocs supprimés sont conservés jusqu'à ce qu'aucune image n'y fasse plus référence.

Planification des prises d'images (snapshot)

Les NAS donnent la possibilité de programmer des prises d'images régulières de tous les volumes hébergeant des partages de fichiers. Ces programmations peuvent être de plusieurs ordres : hebdomadaires, journalières ou toutes les heures.

Exemple de paramétrage nécessitant 43 images :

- Toutes les heures, avec conservation des 5 dernières prises d'images (soit 5 heures de rétention).
- Tous les soirs '(sauf le samedi), à 23 h, avec une rotation sur 30 versions (soit 30 jours de rétention).
- Tous les samedis soir à 23 h. avec une conservation des 8 dernières prises d'images (soit 2 mois de rétention).

On ne peut considérer ce procédé comme un outil de sauvegarde, car en cas de perte des données du volume (corruption, problème matériel ou autre), les snapshots deviennent inutilisables, et la totalité de ces données sera perdue. Toutefois, elles permettent aux utilisateurs de restaurer un fichier ou une sous-arborescence sur une période suffisante pour l'utilisateur.

2.4.8 Microsoft DPM

2.4.8.1 Présentation

Très rapidement, le concept novateur de la protection continue a séduit le géant américain Microsoft qui s'est lancé sur les traces de ses précurseurs (IBM et EMC).

La solution Microsoft Data Protection Manager permet d'administrer les sauvegardes des serveurs et des postes utilisateurs. La prise en considération des applications Microsoft telles qu'Exchange (Messagerie), MS SQL Serveur (base de données), SharePoint (Partage de documents) permet d'assurer la validité des différentes sauvegardes.

Microsoft DPM est une solution "Near CDP". Elle n'enregistre pas l'ensemble des modifications ou des interactions. La solution permet essentiellement d'administrer les sauvegardes des produits Microsoft

2.4.8.2 Principe de fonctionnement

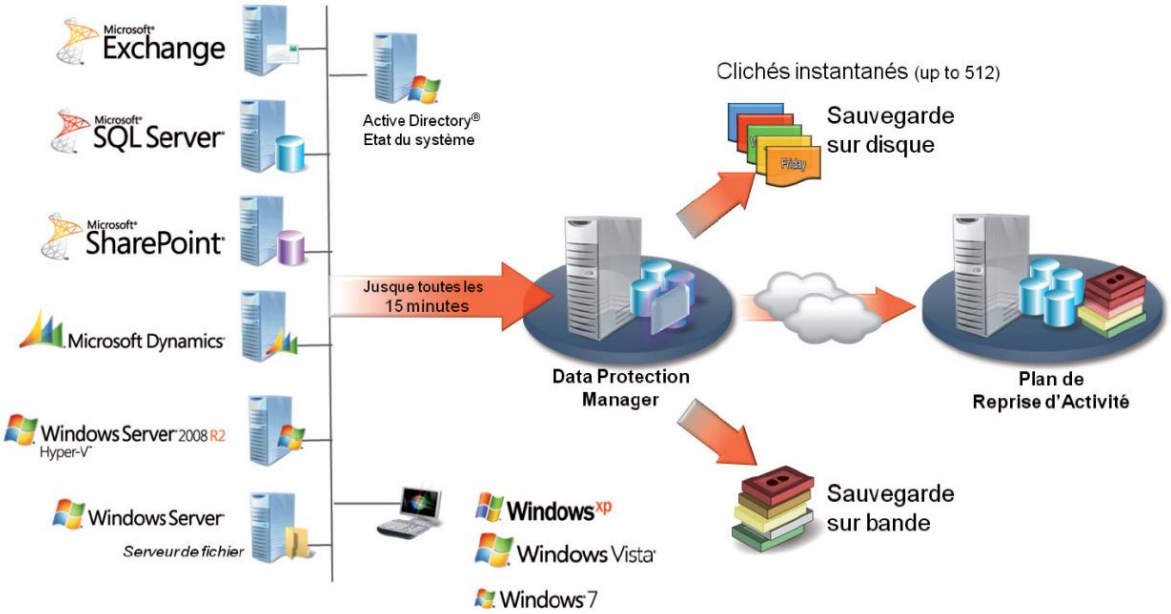


Figure 2-27 : Architecture MS DPM (Microsoft)

Un agent est installé sur chacune des machines à protéger et dialogue avec le serveur DPM. Il récupère les données modifiées pour les stocker. Les données peuvent ensuite être sauvegardées sur bandes ou transférées sur le site de PRA

Il s'agit d'un produit "near CDP". Selon la politique de protection, il peut générer des prises d'images régulières jusqu'à une fréquence de 15 minutes.

Paramétrages et fonctionnalités

Le paramétrage se réalise par l'interface graphique ou en lignes de commandes. Il ne s'agit pas d'une application de sauvegarde évoluée, mais elle possède les fonctionnalités de base dont la réplication multisites. Il manque notamment les outils de recherche de fichiers et de suivis de statistiques.

Le paramétrage est intuitif et guide l'utilisateur (cf. capture d'écran ci-après) au travers d'assistants.

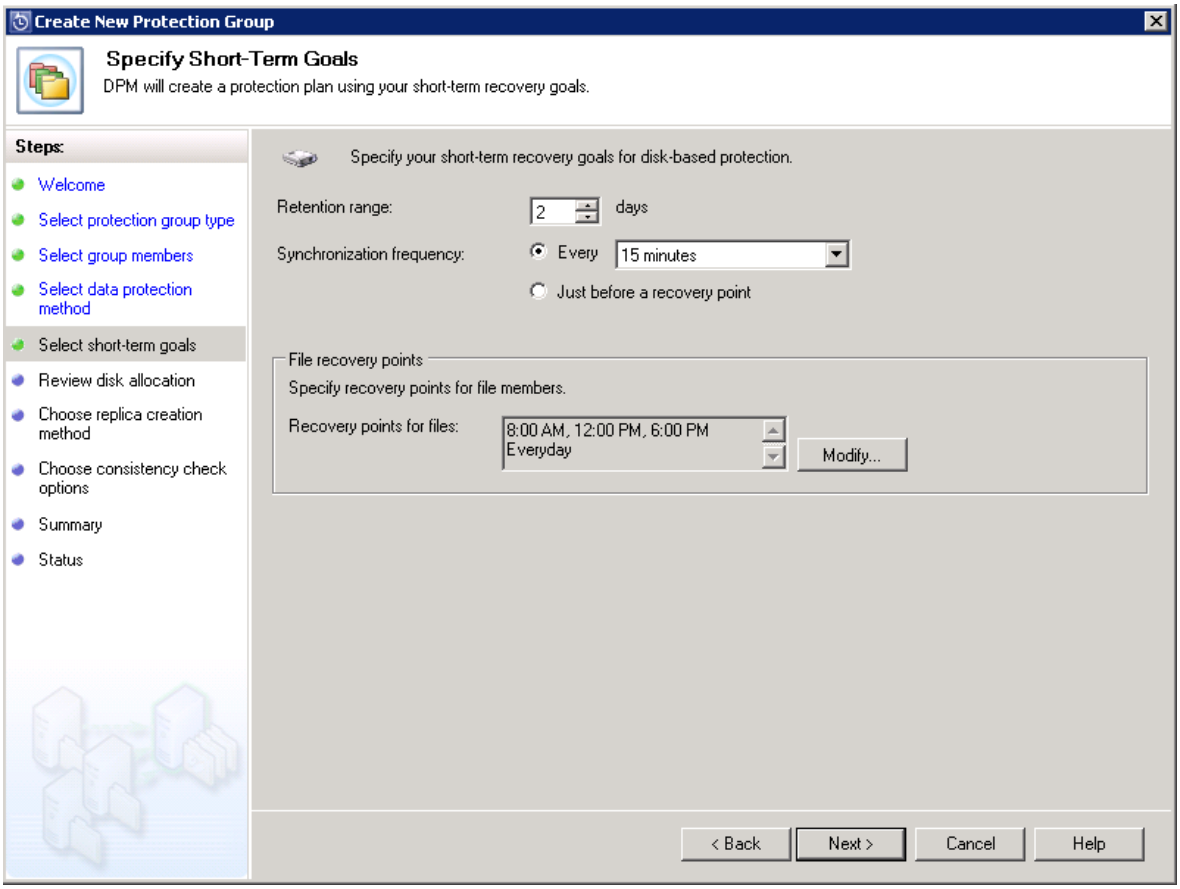


Figure 2-28 : MS DPM - Création d'un groupe de protection

2.4.8.3 Les faiblesses du produit

Cette solution near CDP est principalement prévue pour fonctionner sur des plateformes Microsoft avec des produits Microsoft. En effet, si aucun doute ne subsiste sur le bon fonctionnement avec les serveurs Microsoft, MS DPM ne permet pas de protéger d'autres systèmes d'exploitation (ex. : Linux/ Unix). De plus, l'outil n'est pas fait pour gérer des données sur de longues périodes. En effet, si cela est nécessaire, il est préférable d'externaliser les données via un lecteur de bande ou une VTL (Vitual Tape Library).

2.4.9 AIMStor

2.4.9.1 Présentation

AIMStor est un outil de sauvegarde assez complet et propose des fonctionnalités avancées :

- Continuous Data Protection il permet entre autres, une prise d'image toutes les minutes
- pilotage des réplications (en temps réel et asynchrone)
- optimisation du stockage déduplication
- optimisation du réseau (déduplication à la source)
- prise d'images cohérentes (Exchange ; MS SQL serveur ; Hyper-V ; VMware ESX)
- outils de recherche
- rapports et statistiques

2.4.9.2 Principe de fonctionnement

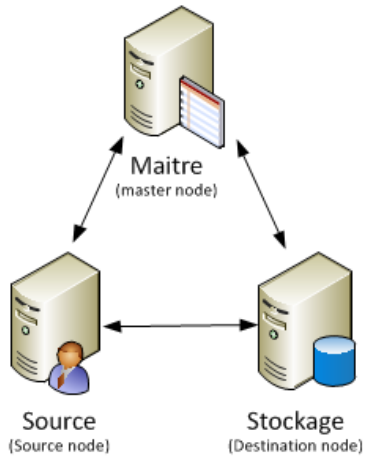


Figure 2-29 : Architecture AIMstor

Dans l'architecture AIMstor, les équipements (serveurs, VM, postes utilisateurs) peuvent avoir différents rôles :

- "Master Node" : Administration de la solution
- "Source Node" : Serveur ou poste utilisateur à protéger. Il joue aussi un rôle d'audit du poste.
- "Destination Node" : Zone de stockage servant à la réplication ou au stockage des données.

Les rôles peuvent être cumulés tant qu'il n'y a qu'un seul "master" présent par réseau.

L'interface utilisateur

L'interface utilisateur est particulièrement simple et visuelle (cf. figure 2-30).

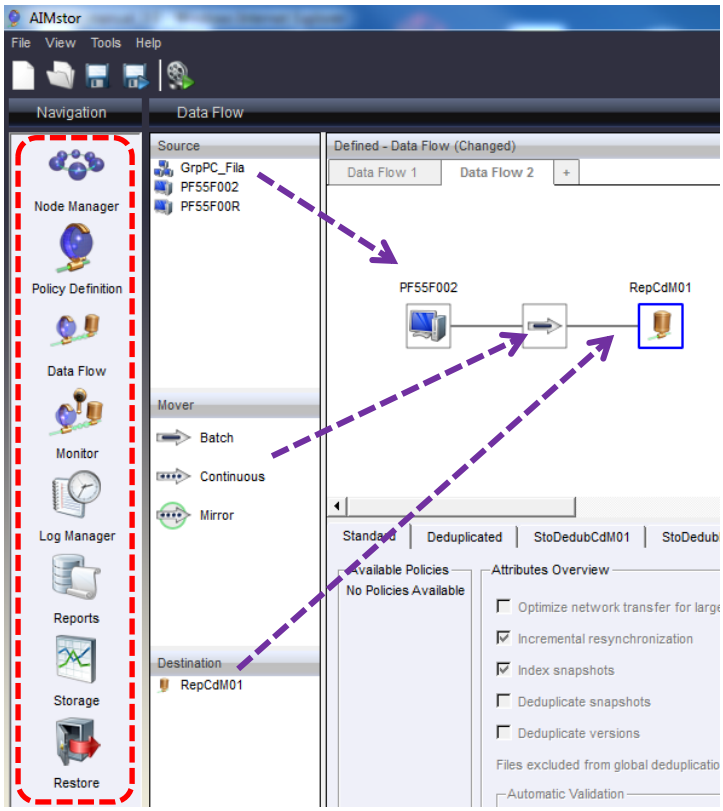


Figure 2-30 : Interface utilisateur AIMstor

On retrouve dans l'encadré rouge les rubriques permettant de naviguer entre les différentes fonctionnalités.

L'administrateur définit son architecture à l'aide de la souris (clics glissés) en sélectionnant les différents éléments (source ; type d'opérations et destination).

Ce mode de paramétrage facilite la prise en main de l'outil et donne à l'administrateur une vision plus globale des stratégies de sauvegarde en vigueur.

Cette présentation a malheureusement aussi des limites. En effet la taille des écrans étant restreinte, il parait difficile de maintenir des infrastructures complexes. On peut également regretter qu'AIMstor ne possède pas de jeu de commandes pour administrer sa solution. Son interface utilisateur bien que très intuitive et agréable, complique sa gestion au quotidien (déploiement / administration / surveillance). Cet outil semble plus adapté aux petites et moyennes entreprises.

Remarque : La société Cofio Software qui éditait AIMStor a été rachetée par HDS (Hitachi Data Systems) en 2012. La solution a ainsi été intégrée et rebaptisée HDIM (Hitachi Data Instance Manager) en 2013 par HDS [COFIOA04].

2.4.10 R1Soft

2.4.10.1 Présentation

Créée en 2006, R1Soft est une solution de sauvegarde "Near CDP" qui protège les machines Windows ou Linux. Elle est compatible avec la plupart des hyperviseurs (VMWare, Hyper-V, KVM, Xen). R1Soft possède un agent qui lui permet de capturer des images "crash-consistents" de bases de données (MySQL, MS SQL) ou d'applications de messageries (Exchange 2010).

2.4.10.2 Principe de fonctionnement

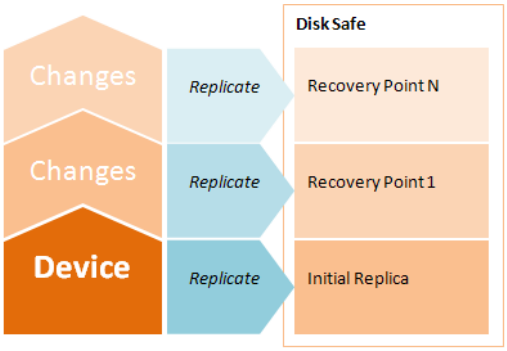


Figure 2-31 : R1Soft – Principe de sauvegarde [R1SOLFTA01]

R1Soft est basé sur une architecture client/serveur. Un agent installé sur le serveur à protéger prend régulièrement (5 minutes, au plus cours) une image et la transmet à son serveur qui stocke les modifications dans une zone de stockage compressée ("DiskSafe"). Lors de la première sauvegarde, toutes données sont transmises. Pour les sauvegardes suivantes, seuls les blocs modifiés seront transmis.

Fonctionnalités et licences

R1Soft est commercialisé en 3 versions :

Compare All	CDP 3.0 Standard	CDP 3.0 Advanced	CDP 3.0 Enterprise
Features:			
High Performance CDP Backup	✔	✔	✔
Central Backup Repository	✘	✘	✔
Powerful File Excludes	✔	✔	✔
Portable Backup Storage	✔	✔	✔
Multi-Point Replication	✘	✘	✔
New CDP 3.0 Web Interface	✔	✔	✔
Faster Compression	✔	✔	✔
Data Retention Policy	✔	✔	✔
Email Reporting	✘	✔	✔
Bare-Metal Restore	✘	✔	✔
MySQL Database*	✘	✔	✔*
MSSQL Database	✘	✔	✔
SOAP API	✘	✔	✔
Multi-User and Multi-Tenant	✘	✘	✔
Retail Pricing	$299	$499	$699

Figure 2-32 : Les différentes versions de R1Soft [R1SOLFTA01]

R1Soft est une solution de sauvegarde adaptée aux petites et moyennes entreprises. Elle est assez complète et propose des fonctionnalités avancées pour un prix modeste :

- le CDP ;
- la réplication des sauvegardes ;
- l'optimisation du réseau ;
- la gestion des rapports et des statistiques.

On peut toutefois noter que les sauvegardes des bases de données Oracle ne sont pas natives et nécessitent la mise en œuvre d'une architecture spécifique.

2.5 LES DIFFÉRENTES SOLUTIONS ÉTUDIÉES

L'étude des précédentes solutions CDP m'a permis de réaliser le tableau de synthèse suivant :

Tableau I : Récapitulatif des principales solutions étudiées

Solutions	Type	Orientation	Système d'exploitation	Préco.	Réplication	Stockage finale	Avantages	Inconvéniants	Prix des licences
ASIGRA	True CDP	Sauvegarde	Windows,Linux, Unix,AS400		Déduplication	Deduplication	Pas d'agent Stockage optimisé	CDP sur fichiers à plat	ND
EMC RecoverPoint	True CDP	PCA	Windows,Linux, Unix,...	SAN	Déduplication	Complète + logs	Pas d'agent Facilite le PCA	Coût infrastructure Besoin en stockage	ND
FalconStor CDP	True CDP	PCA	Windows , Linux, Unix		envoi de blocs	Complète + logs	Facilite le PCA Faible coût d'infrastructure	Gestion des droits utilisateurs Augmente la charge réseau Besoin en stockage	800 + 400€ / To
IBM Tivoli CDP For Files	True CDP	Versioning	Windows		Compression	Compression	Peu honéreux	Uniquement sur Windows Consomateur de ressources	Serveur(378€) Poste(53€)
NetBackup Realtime	True CDP	PCA	Windows, Linux, Unix	SAN	Déduplication	Complète + logs	Interopérabilité Symantec	Nécessite un SAN Besoin en stockage Coût infrastructure	ND
AISMTOR	Near CDP	Sauvegarde	Linux, Windows		Déduplication	Déduplication	Interface utilisateur Coût infrastructure Stockage optimisé	Pas de commande en ligne	ND
Microsoft DPM	Near CDP	PCA	Microsoft		envoi de blocs	Complète + logs	Interopérabilité Microsoft	Fonctions basiques Environnement Microsoft Besoin en stockage	ND
R1Soft CDP	Near CDP	Sauvegarde	Linux, Windows		envoi de blocs	Efficient Backup Storage	Faible coût d'infrastrcture Stockage optimisé		699 $
Simpana CDR	Near CDP	PCA	Windows,Mac, Unix,Linux,...		Déduplication	Complète + logs	Réplication multiple	Augente la charge réseau Besoin en stockage	ND

L'analyse de ce tableau permet de dégager les conclusions suivantes :

- En violet, on peut observer que les solutions CDP ayant une orientation d'outils de sauvegarde optimisent leur stockage à l'aide d'algorithmes de compression et ne nécessitent pas nécessairement d'infrastructures onéreuses, car ils s'appuient principalement sur des applicatifs ;
- En rose, on peut au contraire remarquer que les solutions CDP favorisant la reprise d'activité utilisent beaucoup d'espace de stockage. En effet, celles-ci ont besoin d'une part de l'espace de stockage de production, et d'autre part d'espace de stockage pour héberger les différents journaux et snapshots nécessaires à la reconstruction des différentes versions.

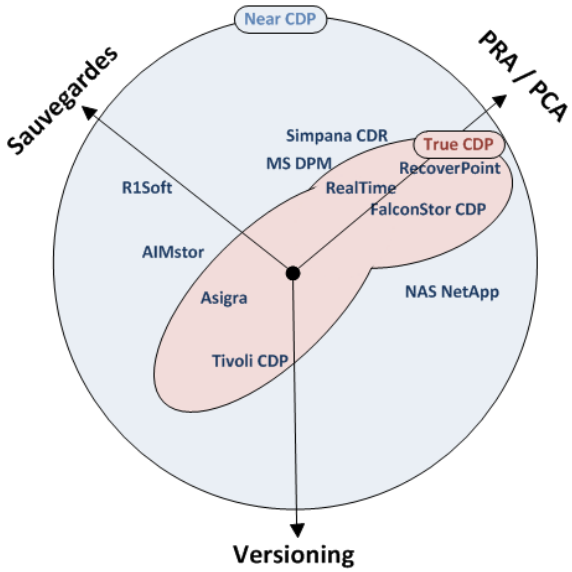


Figure 2-33 : Orientation des solutions étudiées

Afin d'avoir une meilleure appréhension du positionnement de chacune des solutions, j'ai réalisé la figure ci-contre. Elle montre qu'il n'y a pas nécessairement de relation directe entre le type de CDP et leur orientation. On peut toutefois remarquer que les solutions True CDP se regroupent autour des outils orientés versioning et de PCA.

Les outils de sauvegardes semblent être plus proches des produits Near CDP. Cela est sans doute lié aux contraintes induites par les applications spécifiques (base de données, Messagerie,…) et les fortes volumétries qui compliquent la mise en œuvre de solution True CDP.

LES EXPÉRIMENTATIONS

3 MISE EN ŒUVRE D'UNE SOLUTION " NEAR CDP "

3.1 BESOINS ET OBJECTIFS

La suppression du centre de données de Lyon nous oblige à revoir les infrastructures de stockage. Les utilisateurs devront désormais se connecter sur des équipements du centre de données de Strasbourg pour accéder à leurs données partagées (entreprise, services, équipe, etc. …).

En plus de cette externalisation de données, plusieurs demandes ont été formulées :

- les partages de fichiers devront être compatibles SMB 2.1 (Server Message Block) ;
- les données devront être sauvegardées au minimum toutes les heures ;
- les données devront être consolidées sur un site distant (PRA) ;
- la migration de données devra impacter le moins possible la production (la nuit ou le weekend).

Le contenu de ces partages est bureautique. Il est destiné aux utilisateurs et ne contient que des fichiers administratifs et bureautiques. Aucune application privative n'utilise ces partages à des fins de stockage ou de fichiers temporaires.

3.2 ARCHITECTURE EXISTANTE

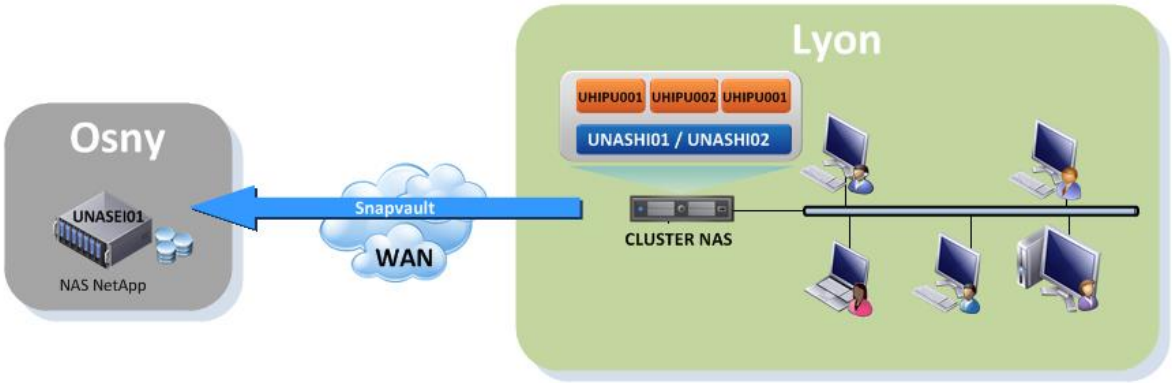


Figure 3-1 : Architecture existante

Trois serveurs sont concernés :

- UF50-051 alias pointant vers le VFiler NetApp UHIPU001 (environ 1.7 To de données pour 149 partages réseaux) ;
- UF50-002 alias pointant vers le VFiler NetApp UHIPU002 (environ 80 Go pour 32 partages réseaux) ;
- UF50-018 alias pointant vers le VFiler NetApp UHIPU003 (environ 600 Go pour 55 partages réseaux).

Les "VFilers" sont assimilés à des serveurs. Il n'existe pas de liaison directe entre eux (hormis la tête de NAS qui les régit). Certains dossiers partagés portent le même nom et sont présents sur plusieurs VFilers (ex : "modèles", "commun").

Les données sont régulièrement transmises sur le site de PRA via le protocole Snapvault (NetApp) à Osny, où elles sont conservées pendant plusieurs semaines.

Plusieurs centaines d'utilisateurs (moins de 300 personnes) utilisent ces données ; certains travaillent la nuit et le weekend (notamment les services de sécurité).

3.3 CHOIX DE L'ARCHITECTURE CIBLE

L'architecture actuelle est basée sur un NAS NetApp. Malheureusement, aucun NAS en notre possession (HNAS, NetApp et Celerra) n'est compatible avec le protocole SMB 2.1 et ne le sera pas avant plusieurs mois. Cette contrainte m'a donc obligé à revoir l'architecture existante.

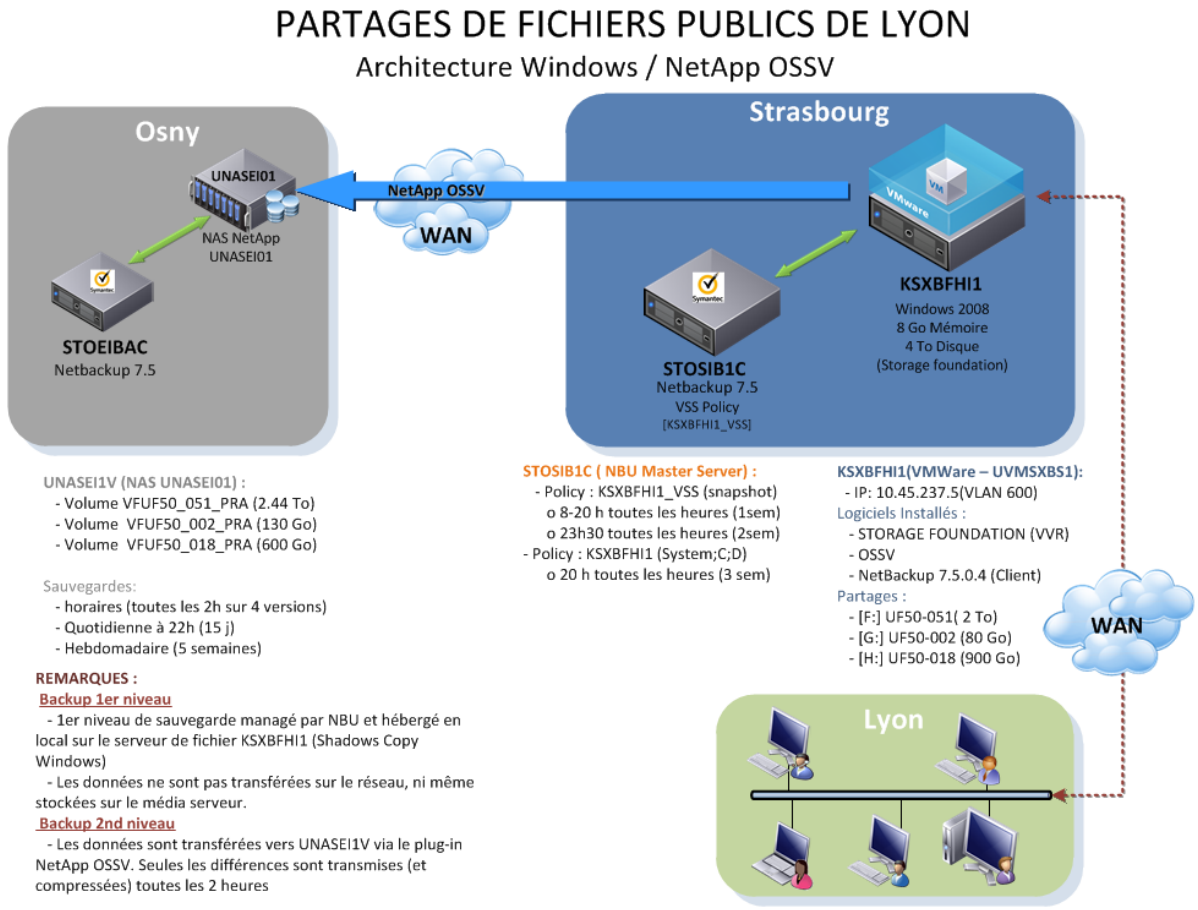


Figure 3-2 : Architecture cible

La nouvelle architecture s'appuie sur plusieurs technologies :

- Windows 2008 R2 64 bits : Le système d'exploitation Microsoft est, d'une part, compatible SMB 2.1 et d'autre part, il permet de prendre des clichés instantanés via la technologie VSS de Microsoft ;
- NetApp OSSV (Open System Snap Vault): son rôle consiste à externaliser les données vers le site de PRA. Les données seront compressées durant la phase de transfert.
- Netbackup 7.5 : il sera chargé de piloter les prises d'images du serveur de fichiers. Il jouera également le rôle d'outil de restauration de premier niveau.
- Symantec Storage Foundation : Cet outil permet de donner de la souplesse à la gestion des disques du nouveau serveur de fichiers. Par ailleurs, il permet aussi de répliquer les données vers d'autres serveurs. Cela pourrait être utile si le module NetApp OSSV ne s'avérait pas satisfaisant.

3.3.1 Avantages de cette infrastructure

3.3.1.1 Accessibilité des données sur le site de PRA

Le module NetApp OSSV (Open System Snap Vault) transmet toutes les modifications vers le NAS de PRA. Ainsi, les données sont directement accessibles. En cas de basculement de la production vers le site de secours, il n'y aurait pas besoin de restaurer les données.

3.3.1.2 Coût et rapidité de mise en œuvre

Hormis le serveur de fichiers, l'architecture cible ne s'appuie que sur des composants déjà existants (NAS, ESX, baie de stockage). Ce nouveau serveur (KSXBFHI1) sera une machine virtuelle (VM). Il n'y aura donc pas d'attente liée aux commandes, aux livraisons et aux configurations matérielles. Seuls les paramétrages et les opérations de migration seront nécessaires…

3.3.1.3 Optimisation du stockage

En s'appuyant sur la technologie de Shadow Copies de Microsoft, chaque image de disque prendra un minimum de place ; en effet, seules les données supprimées seront présentes dans ces images (cf.2.2.4 en page 20).

De plus, le module de NetApp OSSV gère de manière optimisée les synchronisations distantes, il n'a donc pas été jugé utile de réaliser une première copie sur un NAS de Strasbourg ; ce qui a permis d'économiser 8To de disques (4to primaire + 4To secondaire)

3.3.1.4 Optimisation des réseaux

Les transferts réseau sont particulièrement limités. Il n'y a pas de déplacement de données lors des sauvegardes Netbackup et seuls les blocs modifiés sont transmis sur le volume du NAS NetApp.

3.3.2 Inconvénients

3.3.2.1 Sauvegarde de premier niveau non sécurisée

Netbackup ne sauvegarde pas, au sens littéral du terme, il se contente de demander des prises d'images sur le serveur de fichiers (KSXBFHI1) et d'en mémoriser leurs métadonnées. Ce procédé permet, d'une part, d'économiser du stockage, et, d'autre part, d'être réalisé en quelques secondes. Toutefois, en utilisant VSS, le stockage primaire est lié à l'ensemble des prises d'images. On peut certes récupérer n'importe quel fichier effacé, mais si le disque hébergeant le stockage subit une panne, il sera impossible de réaliser la moindre restauration.

3.3.2.2 Consommateur de ressources (CPU / Mémoire)

Le module NetApp OSSV consomme beaucoup de ressources CPU et de mémoire, particulièrement lors des opérations de synchronisation avec le NAS du site distant (Osny). La CPU est notamment sollicitée lors de la compression des blocs à transmettre. D'ailleurs, lors de la mise en production du serveur, j'ai dû doubler le nombre de processeurs (de 2 à 4) ainsi que la capacité de la mémoire vive (4 à 8 Go).

3.3.2.3 Problématique de temps de la première copie

Le serveur de fichiers et le NAS étant distants de plusieurs centaines de kilomètres, le débit réseau entre les deux sites est limité à plusieurs dizaines de mégaoctets. Le temps nécessaire pour transférer presque 3 To de données dépasse une semaine de transfert.

3.4 MISE EN OEUVRE

3.4.1 Installation du serveur Windows

Le système d'exploitation a été installé a l'aide du kit d'installation Euro Information .

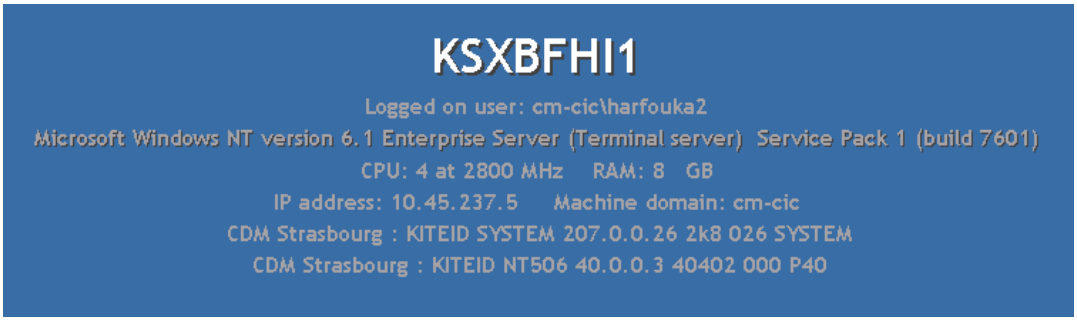


Figure 3-3 : Description du nouveau serveur de fichiers

Il s'agit d'un Windows 2008 R2 64 bits paramétré par les équipes d'Euro-Information.

3.4.2 Installation Symantec Storage Foundation (VVR)

Symantec Storage Foundation est une application permettant de gérer et administrer le stockage de données. Dans notre cas, ce sont les fonctions de virtualisation qui sont intéressantes. Elles permettent de faciliter l'administration des disques en donnant entre autres les possibilités de :

- redimensionner les disques ;
- créer des liens vers des arborescences existantes ;
- réaliser des réplications vers d'autres serveurs VVR (Veritas Volume Replicator).

3.4.2.1 Installation du logiciel

La procédure détaillée de l'installation est donnée en annexe 4 (Procédure installation Storage Foundation). Lors de l'installation de Storage Foundation, les paramètres par défaut ont été appliqués dans les différentes étapes. Seuls le répertoire d'installation (dont la cible a été changée en "D:\ProgramFile") et l'ajout du module VVR (Virtual Volume Replicator) dans la liste des composants à déployer ont été modifiés.

3.4.2.2 Mise à disposition du stockage

L'équipe qui administre la machine virtuelle VMware m'a mis à disposition 9 disques :

- 1 disque de 80 Go qui héberge les lecteurs logiques "C:" (40 Go pour la partie système) et "D:" (40 Go pour la partie applicative) ;
- 8 disques de 500 Go qui seront utilisés pour stocker les données des différents partages.

Le paramétrage de Storage Fondation est assez intuitif et ne nécessite pas de grande expérience pour accéder aux fonctions de base. Il s'intègre et remplace les outils Windows d'administrations du stockage (cf. figure 3-4).

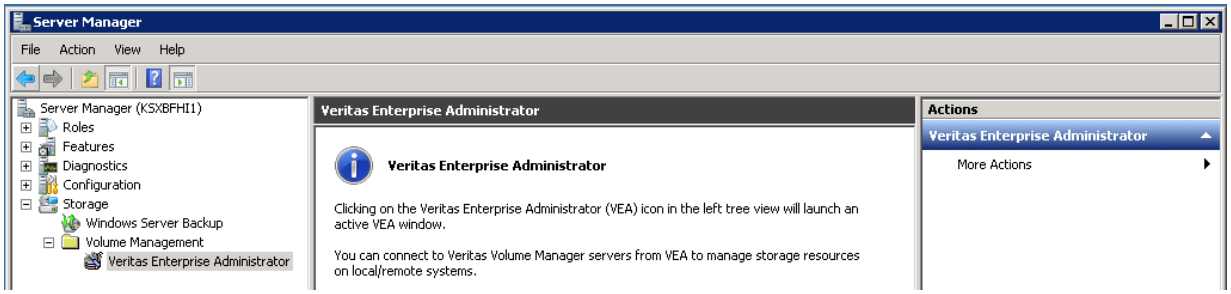


Figure 3-4 : Intégration de Storage Foundation dans les outils d'administration Windows

L'espace de stockage nécessaire est estimé à 4 To de données ; 3 partitions seront créées et affectées aux différents serveurs de fichiers actuels :

- UF50-051 : environ 1.7 To de données
- UF50-002 : environ 80 Go
- UF50-018 : environ 600 Go

Afin de faciliter les opérations de migration, de maintenance, et de synchronisation, j'ai choisi de maintenir les partages de ces serveurs sur des partitions (ou lecteurs logiques) différentes.

3.4.3 Installation Symantec Netbackup 7.5

3.4.3.1 Installation du logiciel

L'installation du client Netbackup 7.5.0.4 sur le serveur KSXBFHI1 a été réalisée avec les paramètres par défaut. Le Cluster STOSIB1C (Serveur Netbackup de l'architecture existante à Strasbourg) a été désigné comme "Master".

3.4.3.2 Paramétrage des sauvegardes

Le paramétrage de la politique de sauvegarde a été réalisé en suivant la procédure décrite en annexe 5. J'ai ainsi paramétré :

- Un "Disk Pool" (espace de stockage) ;
- Un "StorageUnit (Unité de stockage)" ;
- Deux SLP (Storage Life Policy) ;
- Une politique de Sauvegardes.

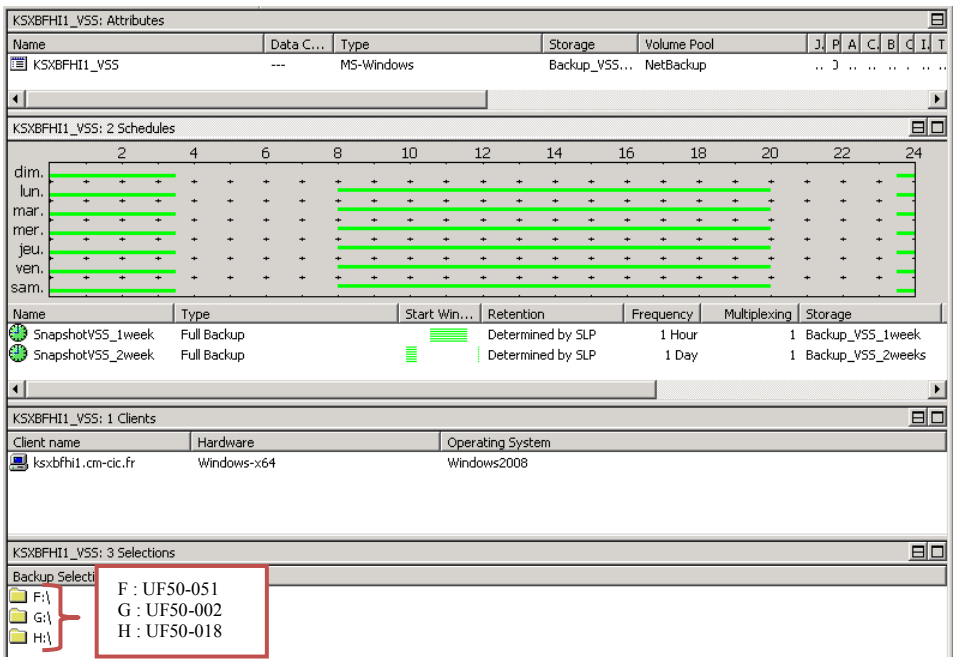


Figure 3-5 : Paramétrage de la politique de sauvegarde Netbackup du serveur KSXBFHI1

Afin de limiter le nombre de snapsots, j'ai décidé de définir une rétention dégressive. Ainsi, les images prises toutes les heures seront conservées la première semaine et seule une image par jour sera conservée la seconde semaine. Ce paramétrage permet ainsi de réaliser une économie de 70 images sur une période de 2 semaines :

- système de rétention unique :10 images x 14 jours + 14 images quotidiennes =154 images
- système de rétention variable :10 images x 7 jours + 14 images quotidiennes =84 images

3.4.4 Installation et paramétrage NetApp OSSV

3.4.4.1 Agent Host DFM

Le plug-in OSSV nécessite l'installation de l'agent DFM (Data Fabric Manager). Ce module est requis pour dialoguer avec la console d'administration des NAS NetApp.

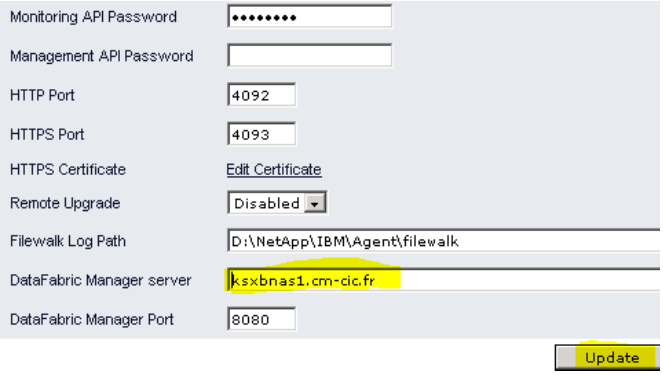


Figure 3-6 : Paramétrage de l'agent DFM

Aucun paramètre spécifique n'est nécessaire lors de l'installation de ce module. J'ai réalisé la procédure décrite en annexe 7.

Pour ce qui concerne le paramétrage (cf. annexe 8), j'ai simplement précisé le nom du serveur DFM : ksxbnas1 (cf. figure ci-contre).

3.4.4.2 Installation plugin OSSV

Tout comme pour les autres modules précédemment installés, aucune précaution particulière n'est nécessaire lors de l'installation (cf. annexe 9). Il faut toutefois connaître le numéro du port qui a été utilisé pour les requêtes NDMP (ici 1000) ainsi que le nom du VFiler (unasei1v) qui sera utilisé pour la réplication vers le site secondaire.

Une fois ce paramétrage effectué, il ne reste plus qu'à vérifier que tout fonctionne correctement à l'aide de la commande : "D:\NetApp\IBM\snapvault\bin\vinstallcheck" (cf. résultat en annexe 10).

3.4.4.3 Paramétrage NAS NetApp

Initialisation des liaisons

Cette première étape permet d'initialiser et de rapatrier une première fois les données vers le NAS d'Osny. Cette opération est à réaliser sur chacun des volumes à répliquer (F,G,H). J'ai donc lancé les commandes (cf. annexe 6) sur la tête NAS NetApp d'Osny :

- Initialisation de la réplication de KSXBFHI1:G: vers le volume KSXBFHI1_PU2_PRA de unasei1v :

```
"vfiler run unasei1v snapvault start -o compression=on -SKSXBFHI1:G: UNASEI1V:/vol/KSXBFHI1_PU2_PRA/qtree_UHIPU002"
```

- Initialisation de la réplication de KSXBFHI1:H: vers le volume KSXBFHI1_PU3_PRA de unasei1v :

```
"vfiler run unasei1v snapvault start -o compression=on -SKSXBFHI1:H: UNASEI1V:/vol/KSXBFHI1_PU3_PRA/qtree_UHIPU003"
```

- Initialisation de la réplication de KSXBFHI1:F: vers le volume KSXBFHI1_PU1_PRA de unasei1v :

```
"vfiler run unasei1v snapvault start -o compression=on -SKSXBFHI1:F: UNASEI1V:/vol/KSXBFHI1_PU1_PRA/qtree_UHIPU001"
```

Planification des snapshots

Une fois la liaison initialisée, il faut définir les fréquences de réplication ainsi que le nombre de versions conservées. Les NAS NetApp possèdent plusieurs niveaux de sauvegardes :

- régulières (sv_hourly) ;
- quotidiennes (sv_daily) ;
- hebdomadaires (sv_weekly).

Dans la mesure où la durée de transfert de certains volumes pouvait dépasser une heure, j'ai choisi de réduire la fréquence des sauvegardes régulières des 2 volumes les plus conséquents en les planifiant de manière à ce qu'ils ne se lancent pas simultanément.

Programmation horaire

```
"vfiler run unasei1v snapvault snap sched -x -o preserve=default,warn=0 KSXBFHI1_PU2_PRA  sv_hourly 4@0-21"
"vfiler run unasei1v snapvault snap sched -x -o preserve=default,warn=0 KSXBFHI1_PU1_PRA sv_hourly 4@0,2,4,6,8,10,12, 14,16,18,20"
"vfiler run unasei1v snapvault snap sched -x -o preserve=default,warn=0 KSXBFHI1_PU3_PRA sv_hourly 4@1,3,5,7,9,11,13, 15,17,19,21"
```

Programmation quotidienne

```
"vfiler run unasei1v snapvault snap sched -x -o preserve=default,warn=0 KSXBFHI1_PU1_PRA  sv_daily 15@22@sun-fri"
"vfiler run unasei1v snapvault snap sched -x -o preserve=default,warn=0 KSXBFHI1_PU2_PRA  sv_daily 15@22@sun-fri"
"vfiler run unasei1v snapvault snap sched -x -o preserve=default,warn=0 KSXBFHI1  PU3  PRA  sv  daily 15@23@sun-fri"
```

Programmation hebdomadaire

```
"vfiler run unasei1v snapvault snap sched -x -o preserve=default,warn=0 KSXBFHI1_PU1_PRA  sv_weekly 5@22@sat"
"vfiler run unasei1v snapvault snap sched -x -o preserve=default,warn=0 KSXBFHI1_PU2_PRA  sv_weekly 5@23@sat"
"vfiler run unasei1v snapvault snap sched -x -o preserve=default,warn=0 KSXBFHI1_PU3_PRA  sv_weekly 5@23@sat"
```

3.5 TESTS DE LA NOUVELLE ARCHITECTURE

3.5.1 Tests de performance réseaux

Afin de mesurer l'impact induit par le déplacement des données "utilisateurs" de Lyon vers le serveur de Strasbourg, j'ai réalisé des tests de performance (copie de fichiers vers le poste client) entre différents environnements depuis un poste d'utilisateur à Lyon :

- sur la configuration actuelle (NAS sur Lyon) ;
- sur le nouveau serveur (Windows 2008 à Strasbourg).

Tableau II : Tests de performances

	NAS Lyon (local)		Windows Strasbourg (distant)	
	Tps	Mo/s	Tps	Mo/s
Fichiers VSS (beaucoup de petits fichiers)	54''	0.36	9'19	0.035
Fichiers Logs (fichiers de quelques Mo)	2'12	8.78	4'13	5.34
Fichiers PST (gros fichier 2.5 Go)	3'39	10.72	5'25	7.22

Les répertoires VSS (Virtual SourceSafe) qui contiennent une multitude de petits fichiers ne sont malheureusement pas exploitables sur un serveur distant. La latence des réseaux pénalise très lourdement leur gestion. Il a donc été décidé de ne pas déplacer ces dossiers.

En revanche, les caractéristiques de transfert des fichiers Logs et PST vers le site de Strasbourg restent acceptables et permettent l'exploitation des données à distance, bien qu'elles soient moins performantes que celles du NAS de Lyon.

3.5.2 Tests de transferts de fichiers

Afin d'évaluer les temps de transferts nécessaires à la migration des données (entre Lyon et Strasbourg), le rapatriement des données sur le serveur cible (KSXBFHI1) a été réalisé avec la commande Windows :"robocopy". Elle ne transfère que les nouveaux fichiers ou ceux qui ont été modifiés.

Tableau III : Temps de transferts des données de Lyon vers Strasbourg

	UF50-002	UF50-018	UF50-051
Temps Initial	4h	3J	6J
Temps actualisation	15 min	1h15	8h

Remarques :

- Le programme "robocopy" est bridé par le système d'exploitation. Afin d'améliorer la vitesse de transfert, j'ai développé un script qui permet l'exécution simultanée de plusieurs commandes (environ une trentaine).
- L'actualisation du serveur UF50-051 nécessite un délai trop important. Certaines dispositions ont dû être mises en œuvre pour le migrer (cf. section 3.6.2).

3.5.3 Netbackup et les politiques de sauvegardes VSS

Les prises d'images, pilotées par Netbackup 7.5., font partie des nouvelles fonctionnalités de ce produit. J'ai donc jugé utile de réaliser quelques tests pour vérifier son comportement lors des opérations de restaurations:

Tableau IV : Tests de restaurations Netbackup VSS

	Contexte	Résultat
Restauration d'un fichier	Sur un répertoire lié	Échec
Restauration d'un dossier		
Restauration d'un fichier	À partir du lecteur logique	Validé
Restauration d'un dossier		

Dans la mesure où il est impossible de sauvegarder un lien, j'ai affecté un lecteur logique à chacun des alias de serveurs afin qu'ils puissent être sauvegardés et restaurés par Netbackup :

- "F:" pour UF50-051
- "G:" pour UF50-002
- "H:" pour UF50-018

3.5.4 NetApp OSSV

3.5.4.1 Temps de transferts

La commande "snapvault" (cf. annexe 6) permet de vérifier l'état des transferts vers le NAS Netapp.

```
D:\NetApp\IBM\snapvault\bin>snapvault  status
Snapvault  primary is ON
Source        Destination                          State   Lag       Status
KSXBFHI1:H:\   UNASEI1V:/vol/VFUF50_018_PRA/qtree_UF50_018   Source  00:25:31   Idle
KSXBFHI1:F:\   UNASEI1V:/vol/VFUF50_051_PRA/qtree_UF50_051   Source  01:25:33   Idle
KSXBFHI1:G:\   UNASEI1V:/vol/VFUF50_002_PRA/qt_UF50_002      Source  00:25:31   Idle
```

Figure 3-7 : Statut des liens OSSV

La commande " snapvault status -l " permet de voir l'état de la réplication, ainsi que les informations relatives aux transferts.

```
D:\NetApp\IBM\snapvault\bin>snapvault status –l UNASEI1V:/vol/VFUF50_051_PRA/qtree_UF50_051

Source:                  KSXBFHI1:F:\
Destination:             UNASEI1V:/vol/VFUF50_051_PRA/qtree_UF50_051
Status:                  Idle
State:                   Source
Lag:                     1:25:30
Mirror Timestamp:        -
Base Snapshot:           -
Current Transfer Type:   -
Contents:                -
Last Transfer Type:      -
Last Transfer From:      -
Last Transfer Size:      140 KB (Compression=36%)
Last Transfer Duration:  01:05:27
Total files to transfer: 3
Total files transferred: 2
Current File Size:       -
Current File Progress:   -
Current File Name:       -
Transfer Error ID:       -
Transfer Error Message:  -
```

Figure 3-8 : Statut détaillé des liens OSSV

La durée de réplication du serveur UF50-051 étant supérieure à 1 heure, il a été décidé de porter le délai entre deux opérations à 2 heures (afin que le serveur puisse achever une réplication avant d'en commencer une autre)°.

3.5.4.2 Vérification du versioning

Les NAS NetApp permettent, à l'aide de l'explorateur Windows, de vérifier le contenu des partages et de leurs précédentes versions. Il suffit d'un "clic droit" sur le dossier souhaité pour accéder à ses différentes versions (cf. figure ci-dessous).

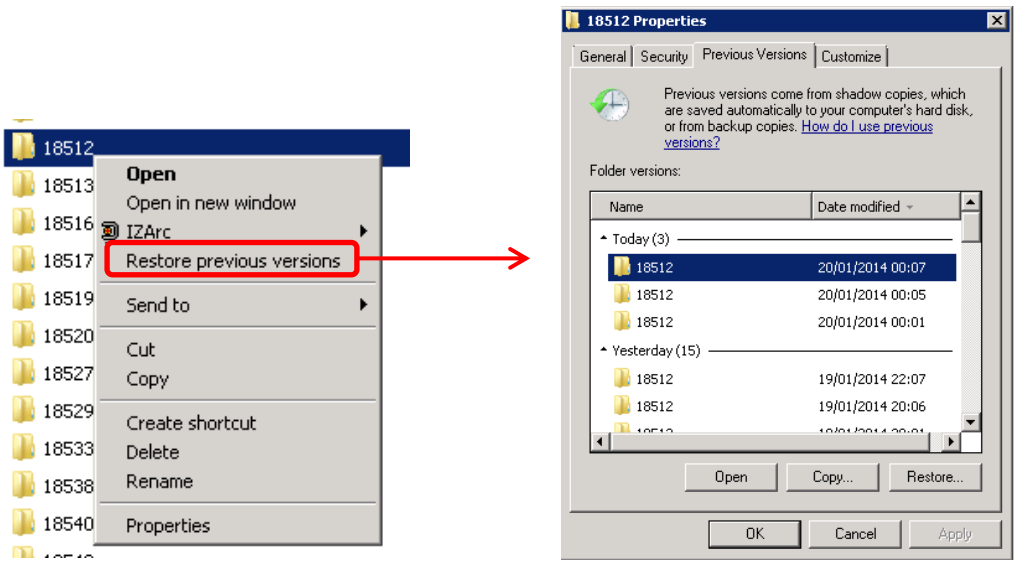


Figure 3-9 : Accès aux précédentes versions depuis l'explorateur Windows

Plusieurs dossiers du NAS ont été comparés avec le contenu du serveur Windows afin de valider le bon fonctionnement de la solution.

3.6 MIGRATION

3.6.1 L'organisation

Il y a près de 3 To de données à déplacer de Lyon à Strasbourg. Les utilisateurs travaillent principalement sur ces données entre 7h et 22h00. La bascule des données doit se faire avec la procédure suivante :

- blocage des partages en lecture seule
- transfert des données
- mise en service des nouveaux partages
- changement des adresses IP des DNS

3.6.2 La problématique du temps de transfert de fichiers

La migration a été effectuée en trois phases :

- migration du serveur UF50-002 (60 Go de données) ;
- migration du serveur UF50-018 (600 Go) ;
- migration du serveur UF50-051(1.7 To) .

Pour réduire les temps de transferts des données (réalisés avec la commande "robocopy"), j'ai en œuvre un batch en powershell qui lance simultanément plusieurs processus de copie de

partages. Afin de ne pas saturer les différentes ressources (mémoires, processeurs et réseaux), le batch ne lance pas plus d'une trentaine de tâches en parallèle.

Pour réaliser les différentes migrations des serveurs, il a fallu :

- UF50-002 : 12 min ;
- UF50-018 :1h08 min ;
- UF50-051 :4h18 min.

3.7 BILAN

3.7.1 Sauvegardes VSS pilotées par Netbackup

Les snapshots pilotés par Netbackup présentent beaucoup d'avantages et fonctionnent correctement. Cependant, le fait de ne pas sauvegarder véritablement (copier sur un support distinct) les données les rend beaucoup trop vulnérables.

Par ailleurs, les snapshots générés par Netbackup ne sont pas accessibles aux utilisateurs qui, de fait, sont obligés de demander à leur service technique la restauration d'un fichier ou d'un répertoire. Malheureusement, Symantec (qui a développé Netbackup) m'a indiqué qu'aucune évolution n'est prévue pour corriger cette contrainte.

Dans de telles conditions, il serait judicieux d'ouvrir une réflexion sur les solutions Microsoft qui intègrent dans leurs systèmes d'exploitation des fonctionnalités permettant aux utilisateurs de restaurer leurs fichiers

3.7.2 Utilisation du plugin OSSV Netapp

Après plusieurs mois d'utilisations, le plug-in NetApp montre une certaine instabilité. En effet, à plusieurs reprises, il est arrivé que l'une des liaisons entre le serveur Windows et le volume du NAS Netapp ne soit plus opérationnelle ("the qtree is not the source for the replication destination."). Il est alors malheureusement impossible de réinitialiser la liaison ; il faut la supprimer et en créer une nouvelle. Cette opération a pour conséquences :

- de doubler l'espace de stockage nécessaire ; en effet, on est obligé de conserver le volume défectueux jusqu'à la fin de la période de rétention (8 semaines).
- de retransmettre la totalité des données du serveur Windows vers le NAS.

Cette solution n'est pas viable en l'état, une alternative s'avère nécessaire.

3.7.3 Le Near CDP

La mise en œuvre d'une technologie "near CDP" sur des partages publics (contenant des fichiers bureautiques : excel, word …) ne semble pas indispensable aux utilisateurs. Bien souvent, ils ne savent pas quand leurs fichiers ont été supprimés et la plupart du temps une restauration au jour près leur convient.

Le service est certes apprécié, mais semble plus approprié :

- à certaines catégories d'utilisateurs spécifiques (les informaticiens, par exemple)
- à certains partages de données ayant besoin de continuité de service (PCA)
- à certains partages ayant besoin de faire du "versioning" sur de courtes périodes.

4 MISE EN ŒUVRE DE FALCONSTOR CDP

4.1 BESOINS ET OBJECTIFS

L'expérience de FalconStor dans le domaine de la protection de données est certes de moindre importance, comparée à celle des différents géants du marché (EMC/IBM/Symantec,…), mais son produit est très attrayant compte tenu de son coût et de sa facilité de mise en œuvre.

L'objectif initial de réaliser un POC (Proof Of Concept) était ambitieux, car FalconStor CDP est susceptible d'intégrer de nombreuses architectures (VMWare, Linux, Windows, Oracle, MS SQL Serveur,…). L'étude de cette solution nécessiterait beaucoup de ressources et la mobilisation de nombreuses équipes d'Euro-Information. J'ai donc décidé de limiter notre action à l'évaluation des différentes fonctionnalités dans l'environnement Euro-Information. Il s'agit de vérifier le comportement des différents modules de la solution (sauvegarde, restauration, réplication, PRA) dans les principaux environnements du monde open (systèmes d'exploitation et logiciels) pour en faire ressortir les inconvénients, les avantages et les fonctionnalités secondaires qui ne m'ont pas été présentés :

- Compatibilité avec les systèmes d'exploitation :
- Complexité d'installation de paramétrages des différents outils
- Interopérabilité avec nos applications et outils de sauvegardes
- Mettre en application les principales fonctionnalités de la solution
- …

4.2 ARCHITECTURE DE TESTS

Afin de limiter les coûts d'infrastructure, l'utilisation des machines virtuelles a été favorisée. L'usage des machines physiques sera réservé aux serveurs nécessitant des équipements spécifiques (cartes SAN) et aux serveurs de tests de reprise d'activité.

4.2.1 Serveur FalconStor CDP

FalconStor CDP propose une version gérée par des appliances. Toutefois, cette solution n'a pas été retenue, car Euro-Information préfère rester maître de son infrastructure. Des serveurs physiques seront déployés afin d'éviter des interventions externes dans ses centres de données et de garder le contrôle des équipements.

Les serveurs seront des HP DL380 G7 équipés de 2 cartes SAN QLogic Dual ports. Ils seront connectés au SAN.
Le système d'exploitation sera installé sur un disque local, alors que les données seront hébergées sur une baie de stockage à l'aide de 2 liens de 8 Gb en fibre optique.

4.2.2 Choix des systèmes d'exploitation

Les systèmes d'exploitation utilisés dans le monde open sont principalement :

- Windows
- Linux (RedHat)
- Unix (différentes versions)
- AS400 : assez rare, principalement utilisé lorsqu'une filiale possédant un AS400 intègre l'architecture d'Euro-Information.

Dans un souci d'efficacité, j'ai décidé de concentrer les tests sur machines Windows et Linux. Il ne m'a pas paru opportun (pour le moment) de réaliser des tests supplémentaires sur les systèmes d'exploitation Unix dans la mesure où ils sont relativement proches de Linux. Quant à l'AS400 (aussi nommé iSeries par IBM), non compatible avec la solution, il a été écarté de l'environnement de tests.

4.2.3 Choix de l'architecture de tests de bases de données

Les bases de données génèrent beaucoup d'écritures et peut occuper des espaces de stockage assez importants ce qui peut poser problème lors des opérations de sauvegardes et de restauration. Dans ce contexte, une étude sur le comportement d'une solution CDP prend tout son sens. Elle permettra, notamment, de mesurer les bénéfices de FalconStor CDP par rapport aux outils fournis par les gestionnaires de base de données. Dans le monde "Open" du groupe CM-CIC, trois principales bases de données sont utilisées :

- MS SQL Server 2008
- Oracle
- MySQL (en cours d'abandon)

MySQL n'étant pas un gestionnaire de bases de données pérenne (dans le groupe), aucun test ne sera effectué sur cet outil.

Dans la mesure où les équipes en charge des bases de données n'ont pas souhaité participer aux tests, je n'étais pas en mesure de monter un cluster SQL, ni même de réaliser des tests approfondis sur la solution (en particulier pour Oracle).

Malgré ces contraintes, et compte tenu de l'intérêt potentiel du CDP pour les bases de données, j'ai décidé de réaliser nos tests sur une base de données MS SQL Server 2008 que j'avais à disposition avec les compétences suffisantes pour l'administrer.

4.2.4 Tests Netbackups

FalconStor CDP n'est pas prévu pour conserver des données sur de longues périodes. Il est préférable d'utiliser un outil de sauvegarde. L'outil actuellement utilisé par le groupe étant Netbackup, une étude sur l'interopérabilité de ces 2 outils serait intéressante.

4.3 MISE EN OEUVRE

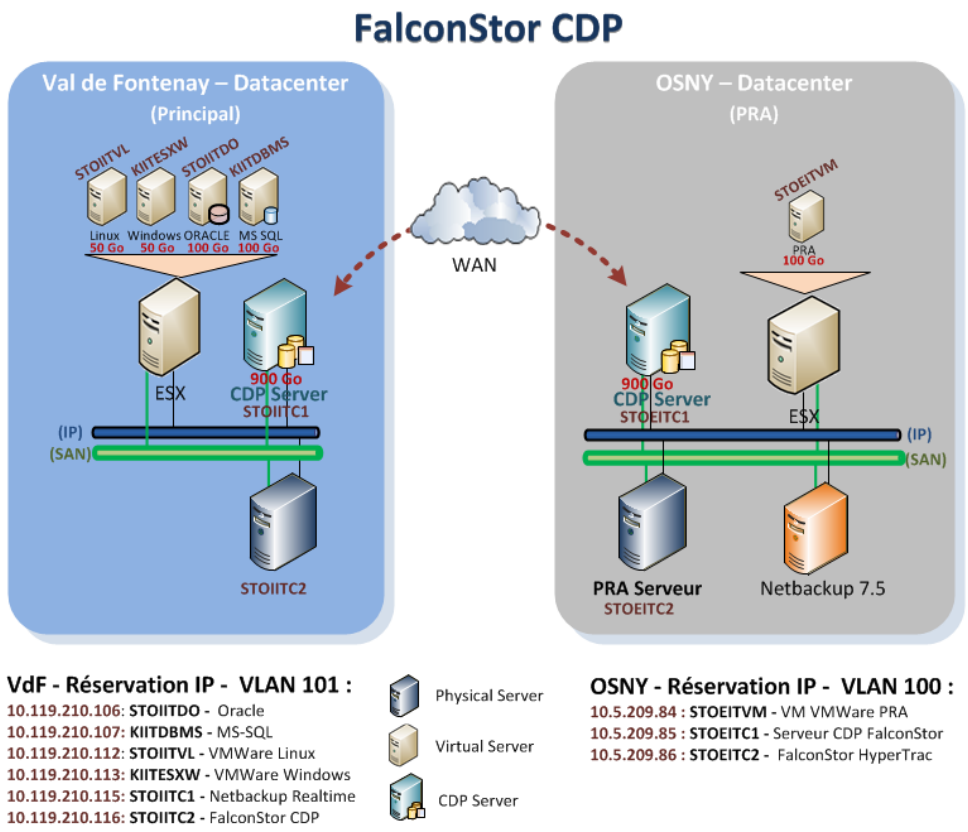


Figure 4-1 : Architecture de tests FalconStor CDP

4.3.1 Des appliances CDP

Les serveurs destinés à recevoir les appliances sont des serveurs HP DL380 G7. Ils ont été installés à partir d'une image fournie par FalconStor appelée "gUSB3919MB-Install-5.1.81b-CDP-7.00-7088-OEL5U7".

La procédure qui a été suivie pour réaliser l'installation des serveurs CDP est détaillée en annexe 12. L'installation est assez basique et ne nécessite pas de grandes compétences en informatique. Une fois le serveur CDP installé, il ne reste plus qu'à réaliser le paramétrage. Cette opération est décrite en annexe 13.

4.3.2 Des machines virtuelles

4.3.2.1 Serveur Windows 2008 R2 64 bits

J'ai utilisé le kit d'Euro-Information pour déployer les serveurs Windows 2008 R 64bits avant d'installer l'agent FalconStor (DiskSafe).

Déploiement de l'agent FalconStor CDP

Le détail de la procédure d'installation est décrit en annexe 14. La mise en œuvre se décompose en plusieurs étapes :

1- activation du protocole ISCSI Initiator ;
2- installation de l'agent (nécessite un redémarrage) ;
3- paramétrage du serveur (via l'interface utilisateur Disksafe).

4.3.2.2 Serveur MS SQL Serveur 2008 : KIITDBMS

Dans la mesure où ce ne sont pas les performances qui m'intéressent et puisqu'il s'agit d'un serveur qui ne sera jamais mis en production, j'ai décidé de le déployer sur une machine virtuelle dimensionnée avec des ressources (processeur et mémoires) assez réduites.

L'installation du système d'exploitation a été réalisée avec le kit d'installation standard d'Euro-Information (Windows 2008 64 R2).

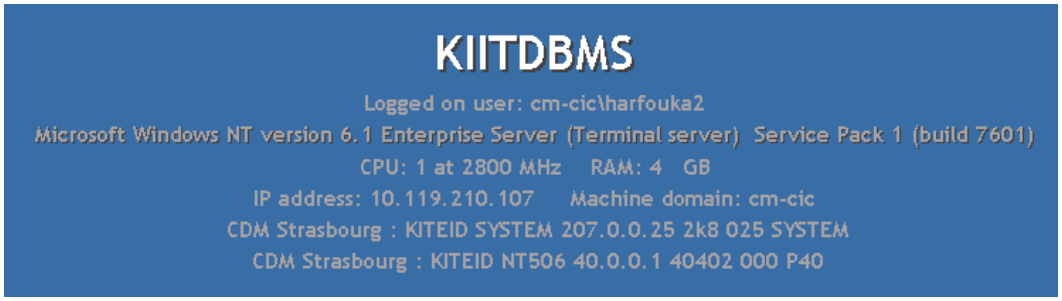
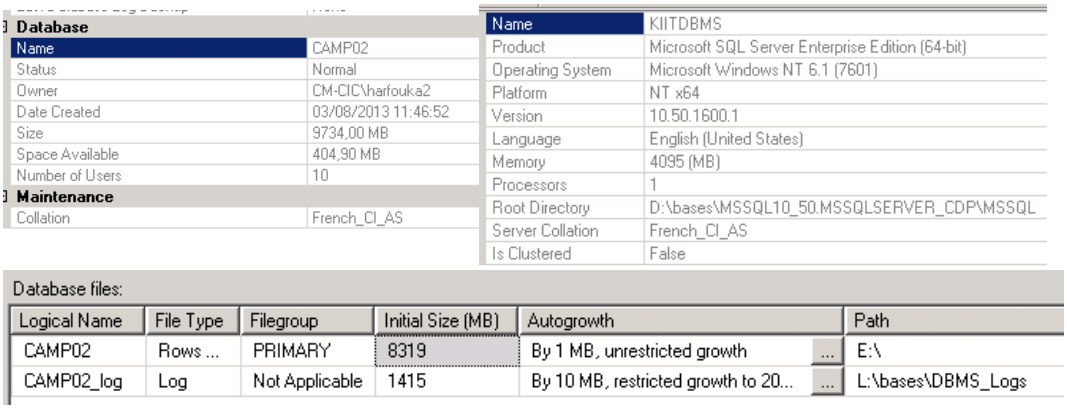


Figure 4-2 : Architecture de tests FalconStor CDP

4.3.2.3 Installation de la base de données

Le kit d'installation de la base de données a été fourni par l'équipe "BDD Open" qui administre les bases de données du groupe CM-CIC du monde Open. Il s'agit de la version "entreprise" de Microsoft SQL Server 2008 R2.

Afin de réaliser les différents tests, et pour avoir suffisamment de données, j'ai utilisé une ancienne base de plusieurs giga-octets.



Database	
Name	CAMP02
Status	Normal
Owner	CM-CIC\harfouka2
Date Created	03/08/2013 11:46:52
Size	9734,00 MB
Space Available	404,90 MB
Number of Users	10
Maintenance	
Collation	French_CI_AS

Name	KIITDBMS
Product	Microsoft SQL Server Enterprise Edition (64-bit)
Operating System	Microsoft Windows NT 6.1 (7601)
Platform	NT x64
Version	10.50.1600.1
Language	English (United States)
Memory	4095 (MB)
Processors	1
Root Directory	D:\bases\MSSQL10_50.MSSQLSERVER_CDP\MSSQL
Server Collation	French_CI_AS
Is Clustered	False

Database files:

Logical Name	File Type	Filegroup	Initial Size (MB)	Autogrowth		Path
CAMP02	Rows ...	PRIMARY	8319	By 1 MB, unrestricted growth	...	E:\
CAMP02_log	Log	Not Applicable	1415	By 10 MB, restricted growth to 20...	...	L:\bases\DBMS_Logs

Figure 4-3 : Caractéristiques de la base de données de tests

Chaque base de données est composée de deux fichiers : un fichier de données et un fichier de transactions. Dans un souci de performance, ils sont souvent localisés sur des disques différents. Ils ont donc été séparés, et j'ai organisé les lecteurs logiques de la manière suivante :

- lecteur C réservé au système d'exploitation ;
- lecteur D réservé aux applications ;
- lecteur E réservé aux données des bases de données ;
- lecteur L réservé aux journaux de transactions des bases de données ;
- lecteur M réservé aux sauvegardes des bases de données.

Déploiement de l'agent FalconStor CDP MS SQL Serveur

Afin de vérifier que les images des bases de données soient cohérentes lors des prises d'images, il faut que l'agent Disksafe (FalconStor) soit installé (cf. procédure en annexe 14). Il faut aussi déployer le plug-in FalconStor qui permet de positionner les bases de données de MS SQL Serveur dans un état cohérent lors de la prise d'images (cf. procédure en annexe 15).

Ce plug-in est relativement simple à installer, car il n'y a aucun paramètre à modifier. Il suffit de suivre les paramètres par défaut.

4.3.2.4 Serveur Linux

Le déploiement du client Linux a été beaucoup plus laborieux, car il a fallu procéder à de multiples tests. Finalement, c'est la version Linux RedHat 6.2 qui a été installée. L'installation de l'agent FalconStor a été réalisée en lançant les commandes :

1- Installation de DiskSafe :tar -xvf DiskSafe-3.63-1286.tgz
2- cd DiskSafe-3.63-1286/RHEL5/el5/x86_64/
3- sudo yum install ./DiskSafe-3.63-1286.x86_64.rpm

4.3.3 Installation HyperTrac

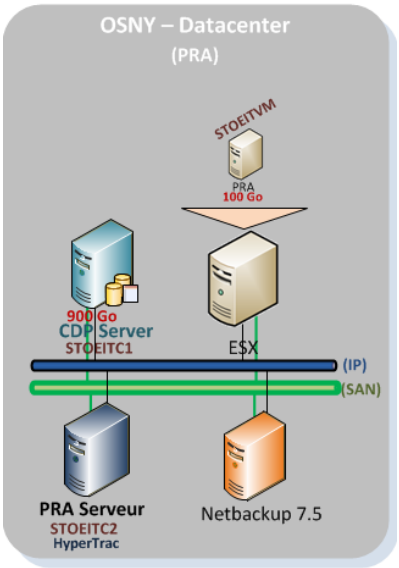


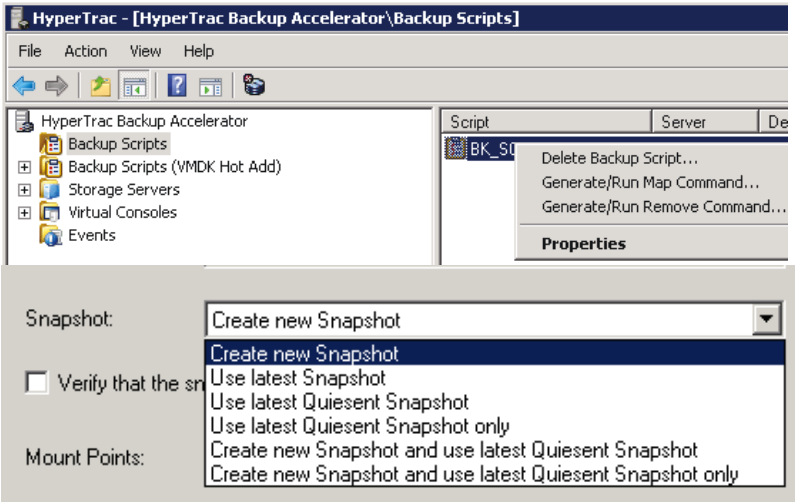
Figure 4-4 : Architecture HyperTrac

La mise en œuvre de sauvegardes peut s'opérer à l'aide de l'outil HyperTrac. J'ai monté une architecture (cf. schéma ci-contre) sur le site de secours (PRA) permettant de sauvegarder une image précédemment enregistrée par FalconStor CDP avec l'outil Netbackup.

Le principe est de paramétrer le client Netbackup (installé sur le serveur HyperTrac) pour qu'il exécuter une commande permettant de lui présenter une image valide à sauvegarder. Une fois la sauvegarde réalisée, il ne reste plus qu'à lancer une seconde commande pour démonter le LUN.

4.3.3.1 Installation et paramétrage de l'application Hypertrack

L'installation de l'outil Hypertrac a été réalisée selon la procédure détaillée en annexe 17. En ce qui concerne le paramétrage (cf. annexe18), j'ai préparé un script qui permet de monter et démonter un point de montage via l'interface graphique ou une ligne de commande d'un LUN.



Le script détermine notamment le point de montage et le LUN (du serveur à sauvegarder) mais pas la version à présenter ; celle-ci sera définie soit par la commande en ligne "HTRun", soit par l'intermédiaire de l'interface graphique qui permet de choisir entre différentes stratégies (cf. figure ci-contre).

Figure 4-5 : Présentation d'un LUN à l'aide de l'interface HyperTrac

Il est préférable de ne choisir que les "Quiescent Snapshot" car il est plus judicieux d'avoir une image dite "cohérente" pour une sauvegarde.

4.3.3.2 Paramétrage Netbackup

Le paramétrage Netbackup est à réaliser sur le client Netbackup (serveur HyperTrack :STOEITC2) et non dans la console d'administration Netbackup. Il faut créer 2 scripts qu'il faudra déposer dans le répertoire d'installation de l'agent Netbackup (ex : C:\Program Files\VERITAS\NetBackup\bin\) et qui seront lancés durant les différentes étapes de la sauvegarde. Ces scripts devront également respecter les règles suivantes :

- Le script exécuté au démarrage devra :
  - avoir un nom du type : bpstart_notify.[nom de la politique de sauvegarde].bat
  - contenir la ligne de commande HyperTrac (permettant de monter le LUN à sauvegarder).

```
Ex. : HTRun.exe Map "C:\Program Files\FalconStor\HTBA\Script\BK_SQL_DATA.hts" -lq -m -eISCSI -v -@df
```

- Un script exécuté à la fin de la sauvegarde devra :
  - avoir un nom du type : bpend_notify.[nom de la politique de sauvegarde].bat
  - contenir la ligne de commande HyperTrac (permettant de monter le LUN à sauvegarder).

```
Ex. : HTRun.exe Remove "C:\Program Files\FalconStor\HTBA\Script\BK_SQL_DATA.hts" -x -m -eISCSI -v
```

Third party backup software Integration

When backing up with HyperTrac with VMware, there are special considerations to keep in mind. If you are using third party software (i.e. NetBackup) that has integrated VMware capability to view, select, and mount devices, you will skip the VM mount point creation step. In this case, you would just use HyperTrac to mount the TimeView devices. If the backup software does not have this capability or you choose not to use it, then you will need to use the HyperTrac mount utility.

As best practice, select the following options when running your backup script (if applicable with your backup software):

- *Run Job only if pre-command is successful*
- *Run post-command even if job fails*
- *Run post-command after job verification completes*

By default certain backup software is set to cancel the job if the pre-command does not complete within 30 minutes. Depending on your environment, and the number of devices selected in the HyperTrac script, you may need to increase this value if possible. It is recommended that you test run each map script that you create to determine the amount of time required, and adjust this value accordingly.

Refer to How do I get HyperTrac to work with my backup software? in the Troubleshooting / FAQ chapter for more information regarding integrating HyperTrac with your Backup Software.

HyperTrac User Guide 37

Figure 4-6 : Extrait de la documentation

Remarque: Avec cette méthode, il faut vérifier lors des mises à jour Netbackup que cette procédure est toujours d'actualité et que les fichiers créés n'ont pas été supprimés.

4.4 TESTS ET EXPÉRIMENTATIONS

4.4.1 Les consoles d'administration

Le paramétrage peut être réalisé de différentes manières:

- avec l'interface Disksafe (locale sur le serveur agent) ;
- via le jeu de commandes en ligne "dscli" (en locale) ;
- à partir de la console administration ;
- en ligne de commande depuis l'appliance Falcon CDP.

4.4.1.1 Console Disksafe (Windows)

Cette interface graphique "utilisateur" est uniquement destinée au poste client Windows. Elle nécessite d'avoir les droits administrateurs. Ce qui, dans l'environnement très compartimenté d'Euro-Information, doit être pris en considération.

Cette console est destinée à faciliter l'utilisation des fonctionnalités de FalconStor CDP sur le serveur où il a été installé. Outre la mise en œuvre de la protection des disques, il permet de faciliter la restauration de données à l'aide des images capturées par la solution, de manière manuelle (montage d'une image sur un nouveau lecteur logique) ou assistée.

L'interface est assez sobre et permet de réaliser la très grande majorité des opérations d'administrations du poste client :

- mise en œuvre des politiques de sauvegardes (cf. encadré orange n°1)
- mapper et démapper les images précédemment enregistrées (cf. encadré bleu n°2)
- accès aux journaux de l'agent FalconStor (cf. encadré vert n°3)

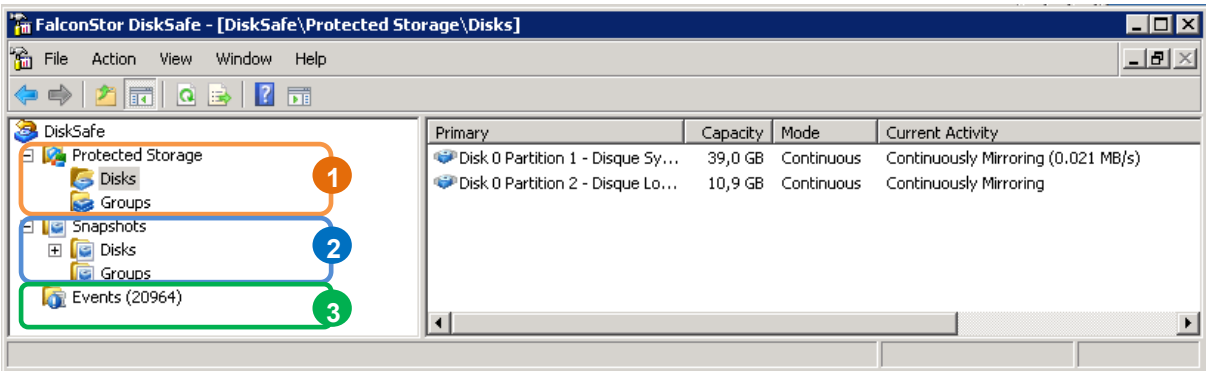


Figure 4-7 : Interface graphique d'administration FalconStor CDP (DiskSafe)

Protection des disques

La configuration de la protection des disques est rapidement accessible depuis l'interface Disksafe (cf. figure 4-8). On peut ainsi réaliser les différentes opérations d'administration des LUN à protéger :

- choix de la protection (CDP / snapshot) ;
- planification ;
- rétention ;
- restauration ;
- …

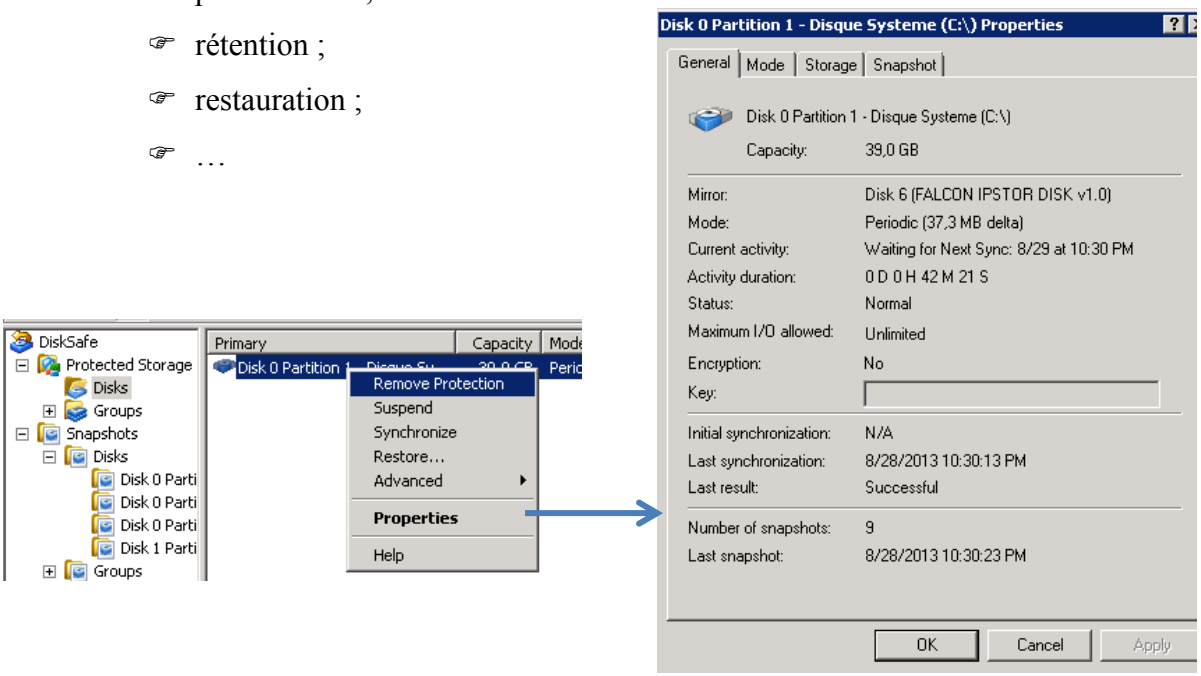


Figure 4-8 : Accès aux propriétés des disques par l'outil (DiskSafe)

Gestion des snapshots

L'outil permet de lister toutes les images disponibles et de visualiser leurs informations :

- dates et heures des prises d'image ;
- si elles ont été prises avec l'agent en mode "Quiesced") ;
- si elles sont en cours d'utilisation.

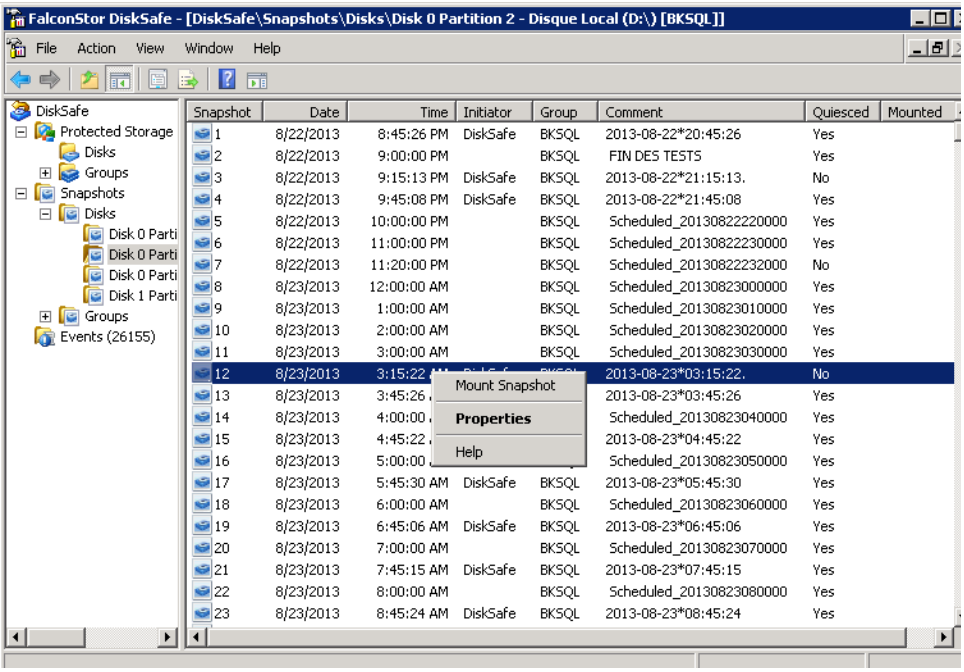


Figure 4-9 : La gestion des snapshots par l'interface graphique Disksafe

Peu d'actions sont possibles à partir de cette interface : nous ne pouvons que monter une image ("Mount Snapshot") en vue de procéder à une restauration manuelle et libérer un snapshot qui aurait été préalablement monté.

Seules les images référencées sont accessibles ; il ne sera pas possible de récupérer une image à partir des journaux en mode CDP, il faudra le faire depuis la console IPStor.

Suivi des journaux

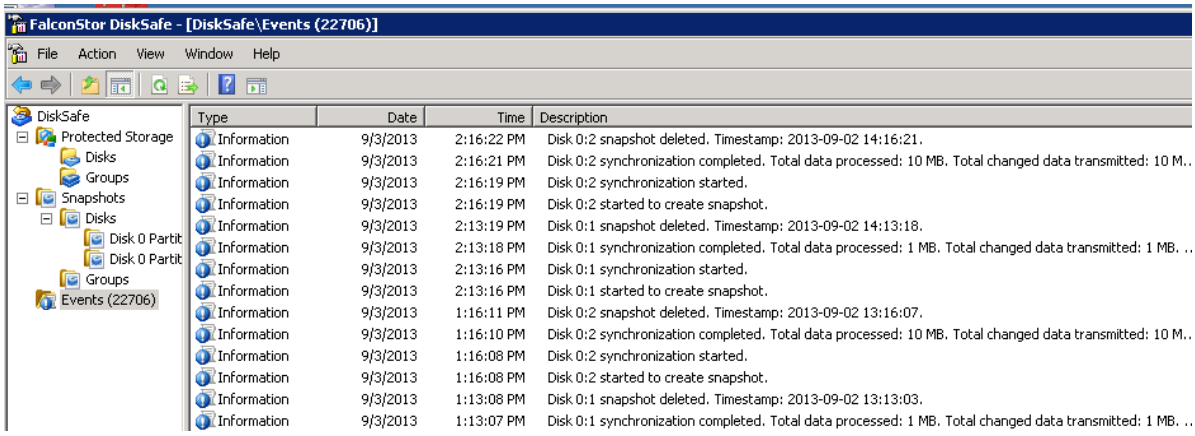


Figure 4-9 : Extrait des journaux du client Falconstor CDP (Disksafe)

Ce journal enregistre toutes les actions et tous les événements liés aux LUN protégés :

- prises d'images (réussies ou en échec) ;
- demandes de prises d'images et de restaurations ;
- modifications des paramétrages ;
- …

Il est également possible d'appliquer un filtre qui permette de récupérer les évènements selon leur degré d'importance (cf. capture d'écran ci-dessous).

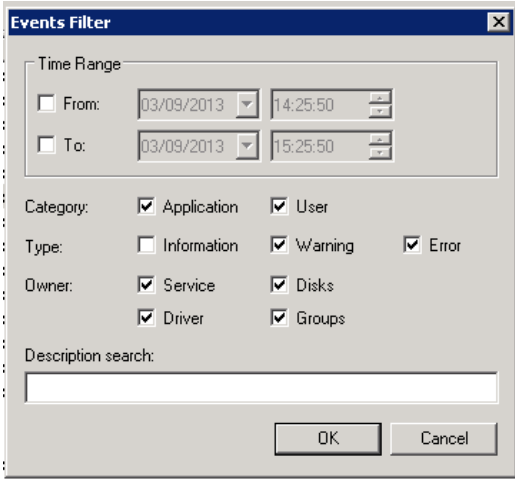


Figure 4-10 : Filtre du journal DiskSafe

4.4.1.2 Jeu de commandes DSCLI

Les commandes DSCLI (DiskSafe Command Line Interface) ne fonctionnent que sur les systèmes d'exploitation référencés dans la matrice de compatibilité FalconStor (cf. annexe 11). De plus, elles nécessitent d'être lancées à partir d'un compte "administrateur" du poste.

DSCLI autorise uniquement l'administration et la sécurisation du serveur depuis la machine locale. Il ne permet pas de gérer et d'administrer les réplications sur les autres machines. Ses commandes permettent de réaliser l'ensemble des actions possibles à partir de l'interface graphique utilisateur DiskSafe :

- protection des disques ;
- gestion des groupes de cohérence ;
- administration des politiques de sauvegardes (dont la planification)
- demandes de prises d'images ;
- montage démontage de snapshots ;
- restauration de fichiers ou de LUN (disque complet) ;
- …

L'aide en ligne permet d'avoir une vision assez globale des possibilités de ces commandes.

```
FalconStor DiskSafe Command Line Interface Version 3.63.0.1286 Patch 0
Copyright 2001-2012 by FalconStor Software, Inc. All Rights Reserved.

Syntax: dscli <command class> <operation> [parameters]

Command Class/Operations:
disk     [list | protect | unprotect | stat | suspend | resume | stop |
         schedule | limitio | maxpendingios | sync | stopsync | analyze | stopanalyze |
         restore | retrysync | delete | help]
group    [new | delete | list | stat | join | leave | suspend | resume | stop |
         schedule | sync | stopsync | snapshot enable | snapshot disable |
         snapshot protectenable | snapshot protectdisable | snapshot agentenable |
         snapshot agentdisable | snapshot take | snapshot list | snapshot delete |
         rollback | retrysync | help]
snapshot [list | take | delete | mount | unmount | enable | disable |
         protectenable | protectdisable | agentenable | agentdisable | help]


event    [get | filter | help]
trace    [set | get | help]
service  [start | stop | restart | stat | help]
license  [list  | add  | delete  | import | export      | help]
server   [list  | add  | enable  | delete | recoverypwd | setccmserver | listccmserver | help]
xray     [<path and filename> | help]
file     [search | restore | help]
help

Note:
* DiskID is a string for disk/partition identification.
  It is shown after "Disk" or "Partition" in the result of command: "dscli disk list"
  e.g. hda or sdb is for a disk
       hda1 is the first slice of disk hda
       sdb3 is the third slice of disk sdb
```

Voici en exemples des commandes permettant de récupérer les informations concernant :

- la liste des disques du serveur :

```
dscli disk list d:
```

- la liste des images disponibles :

```
dscli snapshot list
```

- l'état des services FalconStor :

```
dscli service stat
```

- la liste des derniers évènements :

```
dscli event get
```

4.4.1.3 Console IPStor

L'interface graphique

La console IPStor est la seule interface graphique qui permet d'avoir une vision globale de la protection des données, tant au niveau des différents LUN (ou disques), qu'au niveau des réplications. Elle permet de gérer l'ensemble des serveurs administrés par les appliances FalconStor CDP.

L'interface est segmentée en 2 parties :

- à gauche, une arborescence permettant d'afficher les différents éléments administrés ;
- à droite, le détail de l'élément sélectionné, avec un système d'onglets pour faciliter l'accès à l'information.

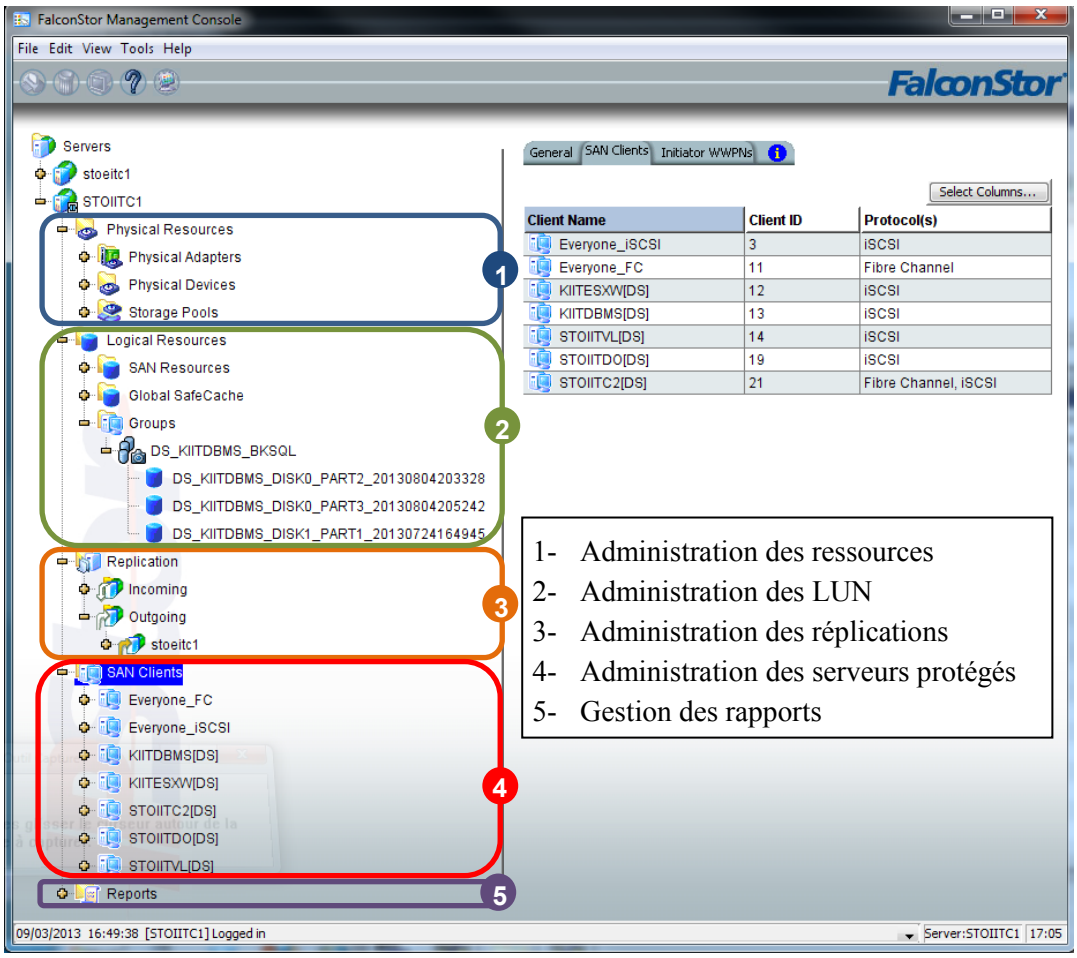


Figure 4-10 : Filtre du journal DiskSafe

Pour l'ensemble des appliances, il est ainsi possible :

- ☞ d'administrer les ressources (cf. encadré bleu n°1)
- ☞ d'administrer les LUN protégés et de définir les politiques de sauvegardes ainsi que les assignations aux différents clients (cf. encadré vert n°2).
- ☞ de gérer les réplications entre les différentes appliances (cf. encadré orange n°3)
- ☞ de manager les différents serveurs protégés (cf. encadré rouge n°4)
- ☞ de générer et suivre les rapports (cf. encadré violet n°5)

Les ressources physiques

Cette console d'administration permet d'avoir une vision globale de la protection des données et de gérer les ressources nécessaires :

- réseaux
- SAN (FC)
- storage (espace de stockage des LUN , journaux et snapshots,…)

Les ressources logiques

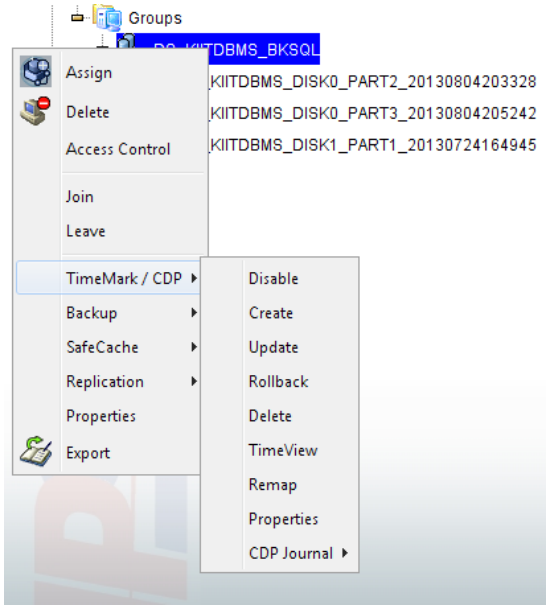


Figure 4-11 : La gestion des ressources logiques

Il s'agit certainement de la section la plus importante car elle permet :

- de définir les politiques de sauvegardes ;
- de présenter des LUN ou des snaphots aux serveurs,
- de gérer des réplications ;
- de créer des images à partir des journaux CDP ;
- de suivre l'état des protections ;
- de gérer les groupes de cohérence ;
- …

Indépendamment des serveurs, chaque LUN protégé est référencé dans cette section. Son contenu y est recopié ainsi que ses snapshots et ses différents journaux (CDP).

Remarque : Hormis la gestion des groupes de cohérence, les mêmes actions sont réalisables depuis la section "SAN Clients" .

Les réplications

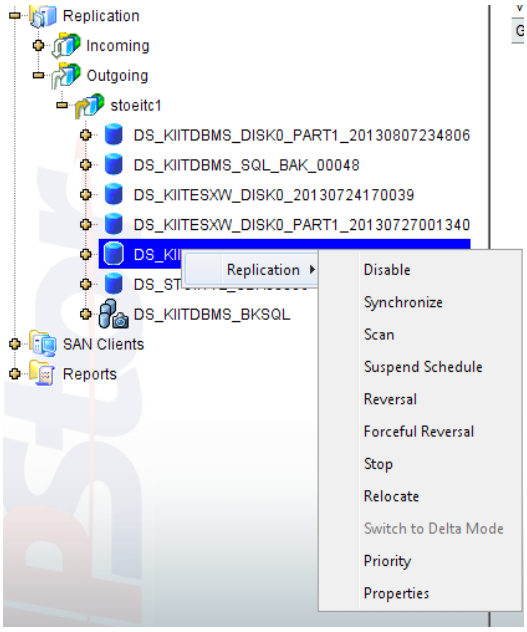


Figure 4-12 : La gestion des réplications (IPStor)

Cette section permet d'administrer les réplications :

- définition des fréquences de synchronisation ;
- vérifications de leurs états ;
- arrêt / démarrage ;
- inversement du sens de réplication ;
- …

Les clients SAN

Cette section organise les différents LUN en fonction des serveurs auxquels ils sont affectés et de leur protocole de connexion (iSCSI ou fibre optique).

Les opérations réalisables dans la section "SAN Clients" sont identiques à celles de la section "Logical Resources ", hormis le mappage d'un LUN vers un autre serveur.

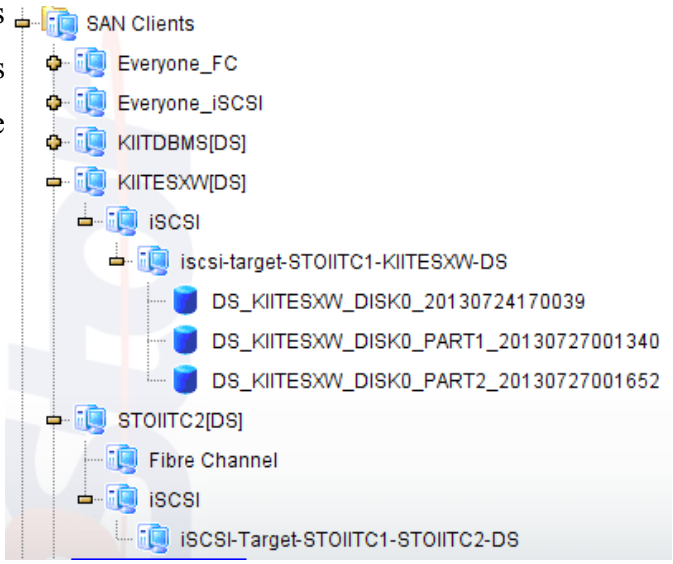


Figure 4-13 : La gestion des clients SAN (IPStor)

Les rapports

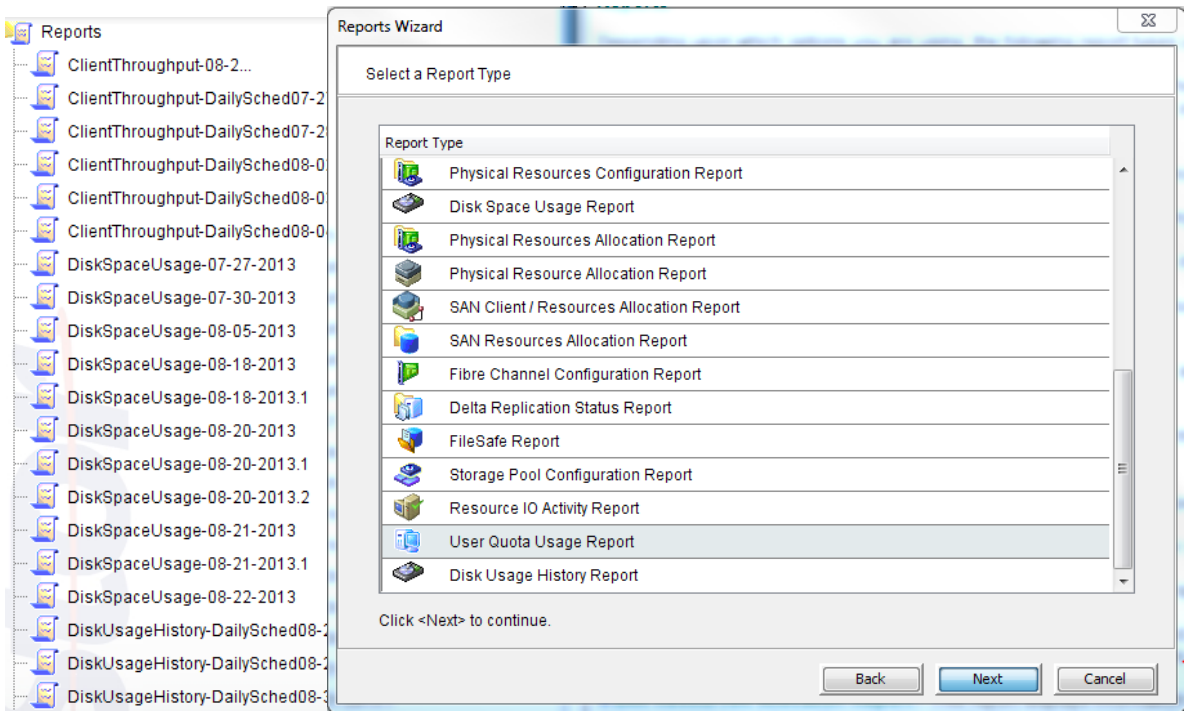


Figure 4-14 : Liste non exhaustive de rapports proposés par la console IPStor

Près d'une trentaine de rapports sont ainsi disponibles. Ils permettent principalement de suivre l'utilisation des ressources réseau et de stockage. D'autres concernent la gestion des réplications vers les autres appliances.

Par défaut, les rapports générés sont placés à la racine sans qu'il soit possible de les classer.

On peut néanmoins mettre en place l'envoi de rapports vers des messageries.

4.4.2 Gestion de la politique de protection

4.4.2.1 Planification des snapshots

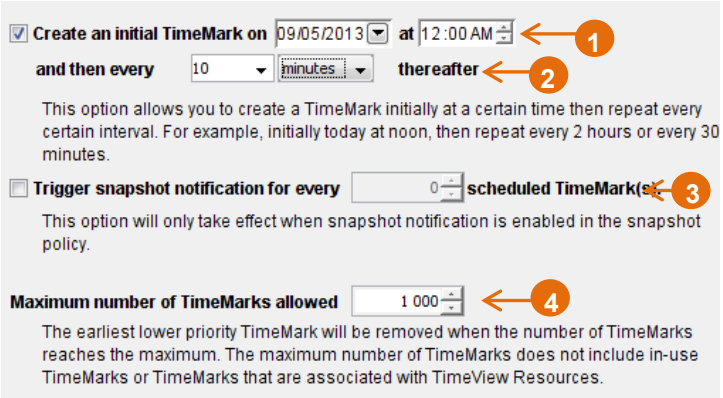


Figure 4-15 : Configuration de la planification des prises d'images

La planification des sauvegardes nécessite de définir au maximum 4 paramètres (cf. configuration ci-contre):

1- la date de début de protection
2- la fréquence des snapshots (laps de temps entre deux prises d'images)
3- le rythme des snapshots cohérents (ex : prise d'une image cohérente toutes les 6 images)
4- le nombre de snapshots conservés

Remarque : Pour certains environnements, il peut être difficile (trop coûteux en ressources) de demander au système de geler ses écritures. La fréquence de notification permet ainsi de ne pas trop perturber le serveur et les applications concernées.

4.4.2.2 Gestion des rétentions des images

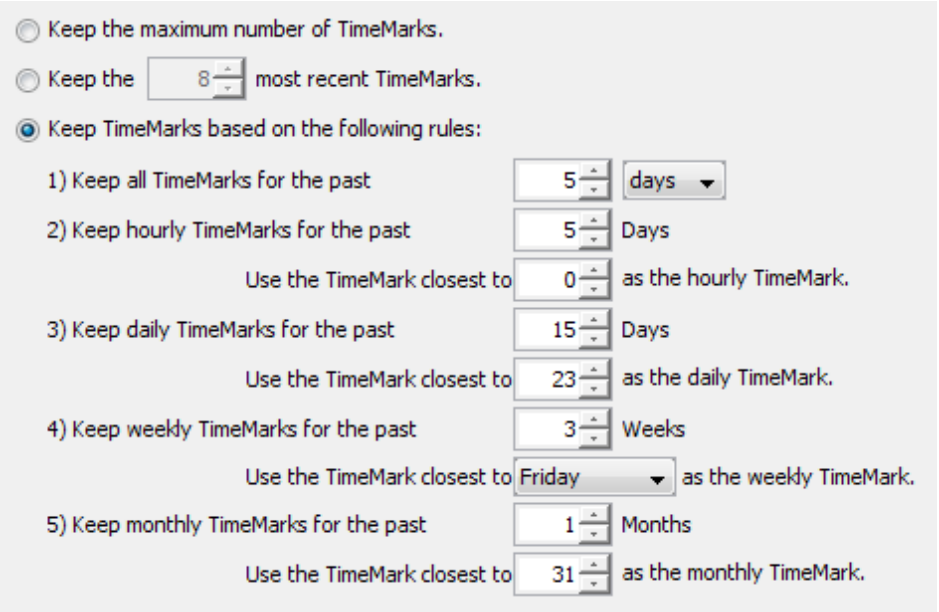


Figure 4-16 : Gestion des rétentions de FalconStor CDP

FalconStor CDP nous donne le choix entre 3 algorithmes, pour définir une règle de rétention de ses images :

- conserver le maximum d'images (en fonction de l'espace disque disponible) ;
- ne conserver que les images les plus récentes (en indiquant le nombre d'images souhaitées) ;
- personnaliser la rétention des images de manière dégressive :
  - les images prises toutes les heures sont gardées pendant "X" jours ;
  - une image journalière sera conservée pendant "X" jours ;
  - une image par semaine sera conservée pendant "X" semaines ;
  - une image mensuelle sera conservée pendant "X" mois.

4.4.2.3 La fenêtre de protection continue

La protection continue permet de journaliser toutes les écritures effectuées à partir de l'instant présent et jusqu'à ce que l'espace alloué au journal soit saturé. La taille du journal est l'un des seuls critères que l'on peut paramétrer (cf. encadré rouge n°1) et détermine la taille de la

fenêtre de protection (cf. encadré vert n°2). Celle-ci sera plus ou moins grande en fonction du nombre d'écritures. Son dimensionnement nécessite une étude approfondie afin d'estimer la taille optimale du journal pour couvrir la période souhaitée.

General | Resources | Layout | TimeMark | TimeMark Retention | CDP | Replication

Name	Value
CDP Journal Resource ID	5000006
Total Size	10000 MB
Status	Accessible
CDP Journal Suspended	Yes
Performance Level	Moderate
Available Journal Time Range	08/22/2013 23:20:00.100.258 - 08/23/2013 10:13:11.444.692
CDP Usage	453.774 MB (4%)
Uncommitted Journal Data	0.0 KB
CDP Journal Data Copy Status	Idle

Figure 4-17 : Propriétés du journal CDP de FalconStor CDP

4.4.3 Les sauvegardes de bases de données "MS SQL Server"

Architecture de tests

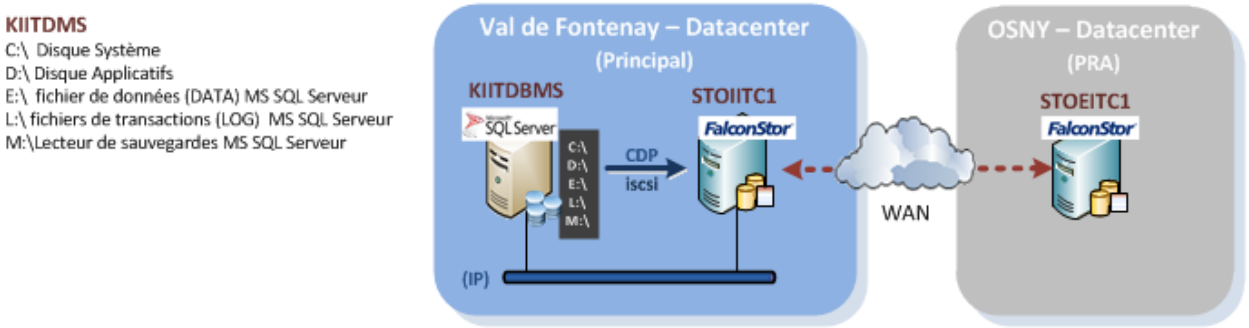


Figure 4-18 : Architecture de tests d'une base MS SQL Server protégée par FalconStor CDP

J'ai mis en place une stratégie qui alimente un fichier de sauvegarde :

- sauvegarde complète à 2h du matin avec une rétention d'un jour ;
- sauvegarde différentielle toutes les heures à partir de 3h15 du matin avec une rétention d'un jour.

L'expérience consiste à générer de l'activité sur la base de données en ajoutant et en supprimant des tables (cf. tableau ci-dessous) afin d'en étudier l'impact sur l'appliance FalconStor CDP.

Tableau V : Récapitulatif des différentes phases de l'expérimentation

N°	Dates / heures	Actions réalisées	Taille (Mo)	Nb lignes
1	22/08/2012 18:45	Ajout de la table DELETE_ME_2	9 931	12 665 766
2	22/08/2012 19:29	Ajout de la table DELETE_ME_3	340	561 756
3	22/08/2012 20:01	Demande de prise d'image (M:\)		
4	22/08/2012 20:10	Suppression des tables DELETE_ME_2 et DELETE_ME_3	10 271	13 227 522
5	22/08/2012 20:25	Sauvegarde de la base de données vers "M:"		
6	22/08/2012 20:38	Élagage de la base de données		
7	22/08/2012 20:40	Suppression du fichier de sauvegarde sur "M :"		

Pour cette expérimentation, j'ai étudié les évolutions :

- du stockage primaire ;
- du stockage secondaire (réplica sur l'appliance CDP) ;
- de l'espace occupé par les sauvegardes de la base de données sur le lecteur M (de KIITDBMS).

Afin de simplifier la compréhension et l'analyse des différents évènements, j'ai effectué une analyse en deux temps : tout d'abord celle du LUN de sauvegarde (lecteur "M") puis celle des LUN de production (lecteur "E" et "L").

4.4.3.1 Analyse du comportement de FalconStor CDP sur lecteur de sauvegarde de la base de données MS SQL Server

Le détail de chacune de ces opérations est détaillé dans les prochaines sous-sections (étapes 0 à 7). Le détail du déroulement de l'expérimentation est donné en annexe 19.

Durant cette expérience, j'ai constaté lors de la première étape que les écritures sont affectées à la dernière image prise.

J'ai aussi remarqué, plus de 13h après cette expérience qu'une valeur du tableau ci-après avait changée. La taille de l'empreinte de 20h20 (encadré en vert) est redescendue à 64 Ko.

Tableau VI : Étape 6 – Détail des snapshots du lecteur M

	Timestamp	Used Size	Comment	Priority	Quiescent	TimeView Data	Status
1	08/22/2013 18:56:01	64.0 KB	DEBUT DU TEST	Medium	Yes	none	N/A
2	08/22/2013 18:59:29	8.35 GB	@initcdpsnapAug 22 18:59:29	Medium	Yes	none	N/A
3	08/22/2013 19:20:00	1.265 GB	Scheduled_20130822192000	Medium	Yes	none	N/A
4	08/22/2013 20:01:24	28.623 MB	Ajout tale DELETE_ME_3	High	Yes	none	N/A
5	08/22/2013 20:20:00	10.28 GB	Scheduled_20130822202000	Medium	Yes	none	N/A
6	08/22/2013 21:03:09	64.0 KB	apres suppression fichier TRN	Medium	Yes	none	N/A

Après étude et analyse, la cause de cette modification a été identifiée : bien que toutes les modifications du stockage soient enregistrées par le CDP, le journal fonctionne avec une zone de stockage et une fenêtre de protection limitées.

General | Layout | Snapshot Resource | TimeMark | TimeMark Retention | CDP | Replication | Replication

Name	Value
CDP Journal Resource ID	2000048
Total Size	4092 MB
Status	Accessible
Performance Level	Moderate
Available Journal Time Range	08/23/2013 02:00:00.832.772 - 08/23/2013 23:15:50.336.896
CDP Usage	111.22 MB (2%)
Uncommitted Journal Data	0.0 KB
CDP Journal Data Copy Status	Idle

Figure 4-19 : Caractéristiques du journal CDP

Une fois cette fenêtre dépassée, l'appliance libère les ressources allouées et supprime toutes les écritures du journal qui ne sont pas comprises dans la fenêtre de protection.

4.4.3.2 Analyse du comportement de FalconStor CDP lors des sauvegardes "à chaud" des fichiers de données et de transactions de MS SQL Server

Dans la mesure où les différents fichiers qui composent la base de données étudiée sont placés sur plusieurs LUN (Logical Unit Number), il est indispensable de créer un groupe de cohérence. J'ai créé un groupe de cohérence GRP_BKSQL composé de 3 disques (LUN) :

- la partition applicative ;
- la partition réservée aux données ;
- la partition réservée aux journaux de transactions.

FalconStor permet de suivre les évolutions au niveau du groupe, mais aussi au niveau de chaque LUN qui le compose.

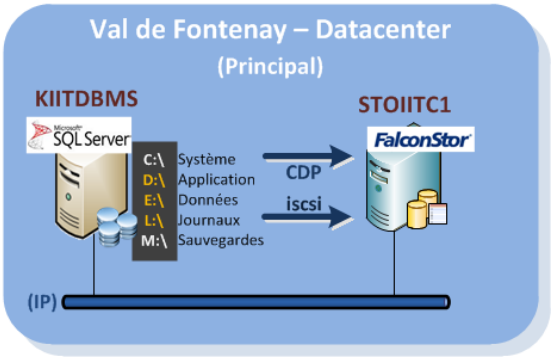


Figure 4-20 : Architecture de tests MS SQL Server

J'ai en plus planifié une prise d'image toutes les vingt minutes. Le module de demande de synchronisation avec la base de données MS SQL Serveur a été paramétré pour qu'il ne s'active que toutes les 3 prises d'images.

L'analyse de cette expérimentation est basée sur le jeu d'actions réalisées dans la section précédente (rappelé dans le tableau ci-après 4-12).

Tableau VII : Rappel du séquencement du test

N°	Dates / heures	Actions réalisées	Taille (Mo)	Nb lignes
1	22/08/2012 18:45	Ajout de la table DELETE_ME_2	9 931	12 665 766
2	22/08/2012 19:29	Ajout de la table DELETE_ME_3	340	561 756
3	22/08/2012 20:01	Demande prise d'image (M:\)		
4	22/08/2012 20:10	Suppression des tables DELETE_ME_2 et DELETE_ME_3	10 271	13 227 522
5	22/08/2012 20:25	Sauvegarde de la base de données vers "M:"		
6	22/08/2012 20:38	Élagage de la base de données		
7	22/08/2012 20:40	Suppression du fichier de sauvegarde sur "M :"		

Les résultats de cette nouvelle expérience, assez proches de ceux de la précédente, sont facilement analysables à partir de ce tableau récapitulatif des snapshots du groupe de cohérence (lecteurs D, E et L).

Tableau VIII : Détail des snapshots du groupe de cohérence GRP_BKSQL (lecteur "D","E","L")

	Timestamp	Used Size	Comment	Priority	Quiescent
8	08/22/2013 18:42:04	17.122 GB	Debut TESTS backup	High	Yes
9	08/22/2013 19:00:00	2.756 GB	Scheduled_20130822190000	Medium	No
10	08/22/2013 19:15:25	1.73 MB	2013-08-22*19:15:25.	Medium	No
11	08/22/2013 19:20:00	381.782 MB	Ajout table DELETE_ME_3	Medium	No
12	08/22/2013 19:40:00	331.244 MB	Scheduled_20130822194000	Medium	No
13	08/22/2013 19:45:09	2.161 MB	2013-08-22*19:45:09@4@	Medium	Yes
14	08/22/2013 20:00:00	42.102 MB	Scheduled_20130822200000	Medium	Yes
15	08/22/2013 20:15:00	1.347 MB	repsnap@Aug 22 20:15:00 2013	Medium	Yes
16	08/22/2013 20:15:02	10.163 MB	2013-08-22*20:15:02.	Medium	No
17	08/22/2013 20:20:00	3.527 MB	Scheduled_20130822202000	Medium	No
18	08/22/2013 20:40:00	2.688 MB	Scheduled_20130822204000	Medium	No
19	08/22/2013 20:45:26	1.618 MB	2013-08-22*20:45:26@4@	Medium	Yes
20	08/22/2013 21:00:00	17.277 MB	FIN DES TESTS	Medium	Yes

Tout comme lors du test précédent, le snapshot a une taille initiale de 64 Ko. À partir du lancement de la requête d'ajout à 18:45, la taille utilisée augmente jusqu'à la fin de son exécution.

L'ajout de la table "DELETE_ME_3" (taille initiale : 340 Mo) a généré une augmentation de l'espace alloué de plus de 700 Mo (cf. encadré noir du tableau 4-13).

Pour comprendre ce qui s'est passé, il faut regarder plus en détail ce qui se passe au niveau de chaque LUN qui compose le groupe de cohérence :

Tableau IX : Disque logique applicatif

	Timestamp	Used Size	Comment	Priority	Quiescent
10	08/22/2013 19:15:25	1.596 MB	2013-08-22*19:15:25.	Medium	No
11	08/22/2013 19:20:00	19.064 MB	Ajout table DELETE_ME_3	Medium	No
12	08/22/2013 19:40:00	3.751 MB	Scheduled_20130822194000	Medium	No

Tableau X : Disque de données MS SQL Serveurs

	Timestamp	Used Size	Comment	Priority	Quiescent
10	08/22/2013 19:15:25	64.0 KB	2013-08-22*19:15:25.	Medium	No
11	08/22/2013 19:20:00	13.363 MB	Ajout table DELETE_ME_3	Medium	No
12	08/22/2013 19:40:00	329.405 MB	Scheduled_20130822194000	Medium	No
13	08/22/2013 20:00:00	1.82 MB	Scheduled_20130822200000	Medium	Yes

Tableau XI : Disque des journaux de la base de données

	Timestamp	Used Size	Comment	Priority	Quiescent
10	08/22/2013 19:15:25	73.5 KB	2013-08-22*19:15:25.	Medium	No
11	08/22/2013 19:20:00	349.355 MB	Ajout table DELETE_ME_3	Medium	No
12	08/22/2013 19:40:00	255.5 KB	Scheduled_20130822194000	Medium	No

Alors que sur le disque applicatif, aucune modification majeure n'est recensée, on remarque une augmentation des écritures de plus de 320 Mo sur les 2 autres LUN, mais à des moments différents :

- ☞ 349 Mo dans les journaux de la base de données entre 19:20 et 19:40
- ☞ 329 Mo dans le fichier de données entre 19h40 et 20:00

Ce phénomène peut s'expliquer d'après l'hypothèse suivante :

- ☞ La création de la table à partir de 19h29 semble avoir généré des écritures sur le LUN contenant les journaux de la base de données. Or, il a été précédemment montré que les nouvelles écritures sont comptabilisées dans la dernière empreinte. Il est donc très probable qu'elles aient été par la suite intégrées au fichier de la base de données (entre 19h40 et 20h00).

Cette expérience met donc en évidence qu'une base de données MS SQL Server induit des flux de données supplémentaires (le double des données qu'elle contient) et que ces flux sont

1 Mo ajouté = 4 Mo (1 Mo de données + 1 Mo de journaux + 2 Mo de CDP) de stockage

4.4.4 Gestion des prises d'images cohérentes

FalconStor CDP donne la possibilité de synchroniser sa prise d'image avec le système d'exploitation ou des applicatifs spécifiques (MS SQL Serveur). Afin que les prises d'images trop fréquentes ne perturbent pas les serveurs, un paramètre (cf. encadré rouge ci-dessous) permet d'utiliser l'agent que toutes les 3 demandent.

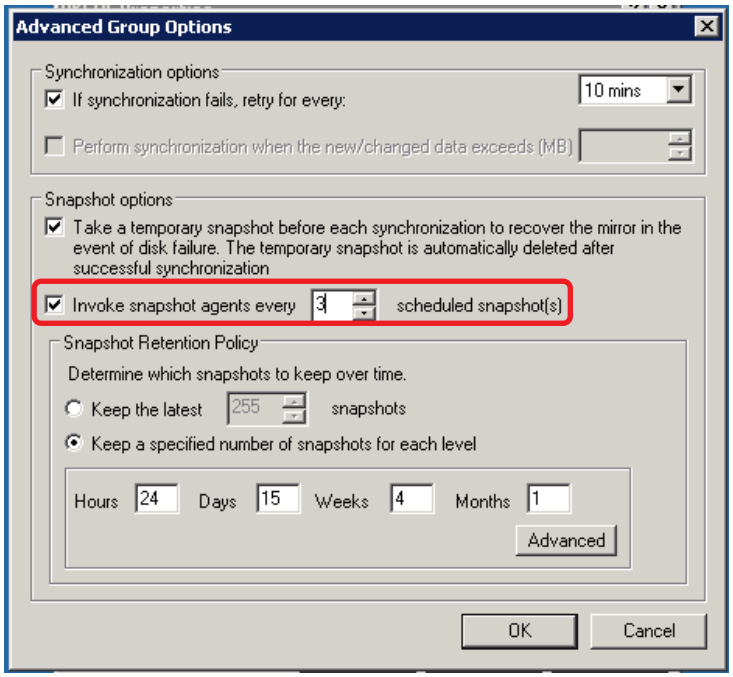


Figure 4-21 : Paramétrage des prises d'images

Le tableau ci-après nous montre le résultat obtenu. Lorsque le "Quiescent" est positionné à "Yes", cela indique que l'image a été prise à l'aide de l'agent et que les disques étaient au repos (les écritures sont gelées pendant quelques secondes).

Tableau XII : Détail des snapshots d'un LUN Falconstor

	Timestamp	Used Size	Comment	Priority	Quiescent
441	08/27/2013 22:00:00	2.396 MB	Scheduled_20130827220000	Medium	Yes
442	08/27/2013 22:20:00	2.328 MB	Scheduled_20130827222000	Medium	No
443	08/27/2013 22:40:00	2.353 MB	Scheduled_20130827224000	Medium	No
444	08/27/2013 23:00:00	2.447 MB	Scheduled_20130827230000	Medium	Yes
445	08/27/2013 23:20:00	2.267 MB	Scheduled_20130827232000	Medium	No
446	08/27/2013 23:40:00	2.432 MB	Scheduled_20130827234000	Medium	No
447	08/28/2013 00:00:00	2.438 MB	Scheduled_20130828000000	Medium	Yes

Cette synchronisation n'est pas toujours un succès, et il arrive que le serveur ou l'application n'arrive pas dégager suffisamment de ressources pour interrompre ses écritures. Dans ce cas, l'action est interrompue et reportée de quelques minutes (la durée du report est paramétrable).

Ces échecs de synchronisation génèrent des erreurs que l'on peut retrouver de l'application DiskSafe (cf. ci-dessous).

Information	08/28/2013	05:19:34 PM	IMA	Snapshot notification is successfully taken. Action start. Drives M:;. Timeout 480.
Information	08/28/2013	05:19:27 PM	IMA	start to take snapshot notification on drives M:; with timeout 480.
Information	08/28/2013	05:19:27 PM	IMA	[service] Received snapshot notification with event 0301.
Error	08/28/2013	04:59:29 PM	IMA	The snapshot notification could not be performed. Action stop. Drives . Timeout 480.

Figure 4-22 : Extrait du journal Disksafe du serveur KIITDBMS

4.4.5 Restauration des bases de données MS SQL Serveur

4.4.5.1 Restauration à partir des prises d'images CDP

Principe

L'appliance FalconStor CDP a à disposition dans son stockage interne l'historique des modifications des LUN du serveur SQL. L'administrateur peut ainsi à partir de ce serveur ou de l'IPStor demander la reconstruction des LUN de la base de données au moment opportun et lui présenter. Il ne reste plus qu'à récupérer les fichiers de la base de données concernée afin de les substituer aux fichiers de la base de production.

Pour ce test, j'ai supprimé une table et réalisé la restauration à partir du serveur SQL en suivant les différentes étapes référencées dans le tableau ci-dessous.

Tableau XIII : Les étapes de l'expérimentation de restauration d'une base de données MS SQL Serveur

N°	Date /heures	Action réalisée
1	14/10/2013 16:35	Suppression de la table DELETE_ME_4
2	14/10/2013 17:00	Arrêt de la base de données CAMP02
3	14/10/2013 18:42	Restauration de la base de données
4	14/10/2013 19:05	Redémarrage de la base de données CAMP02
5	14/10/2013 19:25	Démontage des images de restauration

Le détail des différentes étapes de l'expérimentation se trouve en annexe 20. L'étape de restauration consiste à présenter au serveur une version des LUN contenant les fichiers de base de données et d'écraser les fichiers de production.

Bilan de L'expérimentation

Cette expérience montre qu'il est possible de restaurer une base de données à partir des fichiers de production de cette dernière, qui ont été sauvegardés "à chaud". Toutefois, cette manière de procéder peut se révéler assez longue sur des bases de données de taille conséquente.

4.4.5.2 Restauration par substitution de LUN

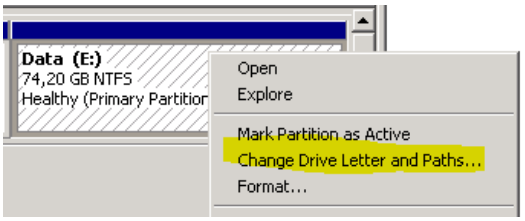


Figure 4-27 : Modification du nom du disque

J'ai utilisé la même infrastructure que la section précédente et restauré la table "DELETE_ME_4" de la base de données "CAMP02". La procédure utilisée diffère peu de la précédente, au lieu de recopier les fichiers "camp02.mdf" et "CAMP02.ldf", j'ai désactivé les lecteurs logiques de production "D:" (lecteur contenant le fichier de data) et "L:" (lecteur des journaux de transactions). Je les ai ensuite remplacés par les LUN FalconStor à l'aide de l'interface "Server manager" de Windows (cf. figure ci-contre).

Cette opération permet de restaurer beaucoup plus rapidement, puisqu'il n'y a pas de recopie de données. Cependant, cette restauration reste provisoire ; d'une part, car les LUN mis à disposition ne sont pas protégés, et d'autre part, selon FalconStor, la solution n'est pas faite pour héberger des LUN de production. En effet, ils préconisent plutôt d'utiliser leur produit "FalconStor NSS (Network Storage Server)". Il faudra donc prévoir une intervention pour rebasculer les données vers leur stockage initial en utilisant l'option "Rollback" de la console IPStor ou "Restore disk or partition" de la console DiskSafe.

Il faut toutefois préciser que durant ce type de restauration, c'est la totalité des LUN qui sont restaurés. Cela implique que chaque base de données ait ses propres LUN.

4.4.6 Gestion des protocoles de transfert

4.4.6.1 Protocole iSCSI

Le protocole iSCSI (Small Computer System Interface) permet de gérer des flux de stockage au travers d'un réseau IP. Il permet ainsi de s'affranchir d'infrastructures onéreuses, et d'en faciliter la mise en œuvre.

Quel que soit le système d'exploitation (Windows ou Linux), aucune difficulté n'a été rencontrée sur ce protocole. Néanmoins, il faut prendre en considération que pour des raisons

de bandes passantes, ce mode de transfert ne convient pas aux serveurs qui sollicitent le réseau ou qui génèrent beaucoup d'écritures sur ses disques (exemple : les bases de données). En effet, pour ces derniers une demande d'écriture peut transiter plusieurs fois :

- lors de la demande d'écriture (un serveur "X" demande le chargement de données à la base de données) ;
- lorsqu'elle est écrite dans les journaux de la base de données ;
- lorsqu'elle est déplacée dans la partie Data de la base de données ;
- lors des sauvegardes.

Cela peut s'avérer d'autant plus problématique lorsque ces demandes interviennent dans le même laps de temps (exemple : une demande d'écriture et de son exécution) sur la même interface réseau.
Ce protocole est donc plus approprié aux serveurs générant peu d'écritures ou de manière modérée.

4.4.6.2 Protocole par Fiber Channel (FC)

Malgré plusieurs tentatives de paramétrages sous différents environnements (Windows et Linux), je n'ai pas pu réellement tester ce protocole. Il semble qu'il y ait besoin de pilotes spécifiques qui permettent de voir les LUN présentés par l'appliance FalconStor CDP.

Après plusieurs tests à l'aide de différents pilotes, dont certains nécessitaient d'être recompilés, j'ai toutefois réussi à activer la protection des disques d'un serveur Linux (recopie des écritures vers l'appliance CDP). Mais, il n'a pas été possible de présenter un LUN à ce serveur provenant de l'appliance FalconStor. Dans ces conditions, le processus de restauration était impossible.

Les tests sous Windows n'ont pas non plus été concluants, et mes différents contacts chez FalconStor) n'ont pas su m'expliquer comment résoudre ce problème. N'étant pas un client, mais aussi par manque de temps, il n'a pas été possible de créer une demande officielle auprès de leur service technique.

Des tests seront donc à refaire avec l'aide de FalconStor si Euro Information estime que ce produit représente un quelconque intérêt.

4.4.7 Gestion des sauvegardes par groupe de cohérence

Falconstor permet de grouper des LUN afin de synchroniser leurs prises d'images et de garder une cohérence entre elles. C'est indispensable lorsque l'on a des fichiers hébergés sur plusieurs disques et qui dépendent de la même application.

Bien que cette fonctionnalité soit fonctionnelle, tout au long des différentes expérimentations qui ont été réalisées, il est arrivé à plusieurs reprises qu'il soit impossible de monter une image. Une erreur s'affiche et indique que le journal n'est pas consultable.

L'utilisation de cette option semble être assez contraignante et des tests complémentaires seraient nécessaires pour en comprendre les raisons.

4.4.8 HyperTrac sauvegarde par Netbackup

La mise en œuvre de ce test n'a malheureusement pas pu aboutir. Lors du lancement du job pour présenter le LUN à sauvegarder, le serveur STOEITC1 se bloque systématiquement (cf. capture d'écran ci-dessous qui trace l'exécution du script).

```
Unassign old TimeViews...
volume name (\\?\Volume{a3fbf260-1239-11e3-95b9-806e6f6e6963}\)
No TimeMark volumes found.
Volume SQL_Logs not found.
No mounted volume to dismount
Unassign old TimeViews done
Remove old TimeViews...
DynaPath not present
Skipping call to DynaPath.
DynaPath returned success.
Remove old TimeViews done.
Collecting device information ...
Device information collected.
Filtering DiskSafe Protect timemark (20130912230812)-(2013-09-12*23:08:12<Protec
t>>.
Filtering DiskSafe Protect timemark (20130914004057)-(2013-09-14*00:40:57<Protec
t>>.
Filtering DiskSafe Protect timemark (20130915005734)-(2013-09-15*00:57:34<Protec
t>>.
Filtering DiskSafe Protect timemark (20130915031938)-(2013-09-15*03:19:38<Protec
t>>.
Filtering DiskSafe Protect timemark (20130915032045)-(2013-09-15*03:20:45<Protec
t>>.
Filtering DiskSafe Protect timemark (20130915032130)-(2013-09-15*03:21:30<Protec
t>>.
Filtering DiskSafe Protect timemark (20130915034810)-(2013-09-15*03:48:10<Protec
t>>.
Filtering DiskSafe Protect timemark (20130915035129)-(2013-09-15*03:51:29<Protec
t>>.
Filtering DiskSafe Protect timemark (20130915041534)-(2013-09-15*04:15:34<Protec
t>>.
Filtering DiskSafe Protect timemark (20130916011822)-(2013-09-16*01:18:22<Protec
t>>.
Filtering DiskSafe Protect timemark (20130916070624)-(2013-09-16*07:06:24<Protec
t>>.
Filtering DiskSafe Protect timemark (20130917010113)-(2013-09-17*01:01:13<Protec
t>>.
Filtering DiskSafe Protect timemark (20130917130541)-(2013-09-17*13:05:41<Protec
t>>.
TimeView BackupTV-STOEITC2[DS]-BK_LOG_MSSQL-1 created for Device STOIITC1-DS_KII
TDBMS_DISK1_PART1_20130724164945 using TimeMark 20130918154514.
Assigning TimeViews to the client...
Disk signature of DiskSafe device [BackupTV-STOEITC2[DS]-BK_LOG_MSSQL-1] flipped
.
TimeView BackupTV-STOEITC2[DS]-BK_LOG_MSSQL-1 assigned to SAN Client.
Search and find devices locally.
Waiting for Virtual device (BackupTV-STOEITC2[DS]-BK_LOG_MSSQL-1), id=(47), seri
al=(BIL81MEQ6OYO) to be ready.
Waiting for BackupTV-STOEITC2[DS]-BK_LOG_MSSQL-1 BIL81MEQ6OYO to be ready.
Rescan SCSI devices...
Max disk scanning 32, count= 128.
```

Figure 4-28 : Trace de l'exécution du job HyperTrac

L'image se monte sur le serveur, mais le serveur commence à devenir instable. Petit à petit, les différentes applications se bloquent, jusqu'à ce que le système d'exploitation ne réponde plus. Un redémarrage du serveur ne permet pas de corriger le problème puisqu'il se fige avant même que l'on arrive à se connecter… Pour remédier au problème, il faut démonter le LUN à l'aide de la console IPStor et redémarrer le serveur.

Après quelques tests et recherches, j'ai découvert que cette anomalie est liée au numéro de LUN (0) qu'HyperTrac essayait de monter (cf. capture d'écran ci-dessous). Le système d'exploitation (Windows 2008) ne semble pas supporter cet identifiant de LUN. Malheureusement, cette découverte a été identifiée trop tardivement et il ne m'a pas été possible de refaire un test : entre-temps, le serveur a été réinstallé pour expérimenter une autre solution.

Tableau XIV : Descriptif du LUN qui posait problème au script HyperTrac

General | Layout | Snapshot Resource | TimeMark | TimeMark Retention | Replication

Name	Value
Allocation Type	Virtual Device
Lun	0
Access	Read/Write Non-Exclusive
Total Size	42 399 MB
Total Sectors	86 831 232
Sector Size	512
Virtual ID	60
Serial Number	63PBG4333LH4
Write Cache	Enabled
Group	DS_KIITDBMS_BKSQL (ID:6)

4.4.9 Gestion des Linux

Bien que la quasi-totalité des fonctionnalités soit opérationnelle (hormis l'utilisation du SAN), j'ai constaté une instabilité sur l'ensemble des machines virtuelles installées. Après plusieurs jours ou semaines, le serveur se met à consommer toutes ses ressources "processeur" et devient incontrôlable…Un redémarrage s'avère nécessaire :

```
[<ffffffff814ed777>] ? panic+0x78/0x143
[<ffffffff814f1904>] ? oops_end+0xe4/0x100
[<ffffffff810423fb>] ? no_context+0xfb/0x260
[<ffffffff81042685>] ? __bad_area_nosemaphore+0x125/0x1e0
[<ffffffff81042753>] ? bad_area_nosemaphore+0x13/0x20
[<ffffffff81042e0d>] ? __do_page_fault+0x31d/0x480
[<ffffffff81047277>] ? pte_alloc_one+0x37/0x50
[<ffffffff81137d3b>] ? __pte_alloc+0xab/0x160
[<ffffffff811380fe>] ? copy_pte_range+0x30e/0x4e0
[<ffffffff814f38be>] ? do_page_fault+0x3e/0xa0
[<ffffffff814f0c75>] ? page_fault+0x25/0x30
[<ffffffff8127223b>] ? __rb_rotate_left+0xb/0x90
[<ffffffff812723ed>] ? rb_insert_color+0x9d/0x160
[<ffffffff8113ff60>] ? __vma_link_rb+0x30/0x40
[<ffffffff81067863>] ? dup_mm+0x303/0x520
[<ffffffff810687cc>] ? copy_process+0xcdc/0x13b0
[<ffffffff8115fff2>] ? kmem_cache_alloc+0x182/0x190
[<ffffffff81068f34>] ? do_fork+0x94/0x480
[<ffffffff811940e2>] ? alloc_fd+0x92/0x160
[<ffffffff81174497>] ? fd_install+0x47/0x90
[<ffffffff810d4d72>] ? audit_syscall_entry+0x272/0x2a0
[<ffffffff81009598>] ? sys_clone+0x28/0x30
[<ffffffff8100b413>] ? stub_clone+0x13/0x20
[<ffffffff8100b0f2>] ? system_call_fastpath+0x16/0x1b
```

Figure 4-29 : Erreur générée sur les serveurs Linux

Il est impossible de certifier que cela vienne effectivement des modules FalconStor puisque tous ces serveurs ont subi une migration d'ESX. Néanmoins, cela laisse un doute quant à leur compatibilité avec les kits d'installation d'Euro Information. D'autres tests seront nécessaires pour valider la solution sous Linux.

4.4.10 Gestion des rapports

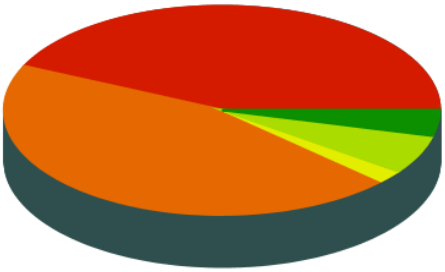
Contenu des rapports

L'IPStor met à disposition une trentaine de rapports permettant de suivre les consommations de ressources (stockage / LAN / SAN) de tous les LUN ou serveurs protégés. Les résultats peuvent être affichés sous forme de graphiques ou de tableaux.

La gestion d'onglets est assez pratique et permet de récupérer le détail des informations relevées (cf. captures d'écrans ci-dessous).

Data Utilization

Disk Space Usage Report
STOIITC1
08/22/2013



IPStor Disk Space Usage

Storage Allocated Space	390 GB	43 %
Snapshot Allocated Space	410 GB	45 %
Cache Allocated Space	0 GB	0 %
HotZone Allocated Space	0 GB	0 %
Journal Allocated Space	17 GB	2 %
CDR Allocated Space	55 GB	6 %
Configuration Allocated Space	0 GB	0 %
Total Free Space	34 GB	4 %

tor Disk Space Usage Data Utilization

Disk Space Usage Report
STOIITC1
08/22/2013

Total Capacity:	921 593 MB
Total Allocated Space:	886 656 MB (96%)
Total Free Space:	34 938 MB (4%)

Physical Resource	SCSI Address	Capacity(MB)	Allocated(MB)	Allocated(%)	Free(MB)	Free(%)
HITACHI:DF600F.000	102:0:1:0	921 593	886 656	96,21	34 938	3,79
HITACHI:DF600F.000	102:0:2:0	(alias for 102:0:1:0)	N/A	N/A	N/A	N/A
HITACHI:DF600F.000	103:0:3:0	(alias for 102:0:1:0)	N/A	N/A	N/A	N/A
HITACHI:DF600F.000	103:0:4:0	(alias for 102:0:1:0)	N/A	N/A	N/A	N/A

Stor Disk Space Usage | Data | Utilization

Disk Space Usage Report
STOIITC1
08/22/2013

Total Capacity:	921 593 MB
Total Allocated Space:	886 656 MB (96%)
Total Free Space:	34 938 MB (4%)

Type	Allocated Size(MB)	% / Allocated	% / Total Space
Storage	399 236	45,03	43,32
Snapshot	420 022	47,37	45,58
Cache	0	0	0
HotZone	0	0	0
Journal	17 419	1,96	1,89
CDR	56 674	6,39	6,15
Configuration	0	0	0

Figure 4-30 : Exemple de rapport sur l'utilisation de l'espace de stockage

Rapport sur la protection des serveurs

Les rapports que propose l'IPStor sont assez complets, notamment pour tout ce qui concerne l'utilisation de ses ressources. On peut toutefois remarquer qu'il n'existe pas de rapport répertoriant les serveurs qui ne sont plus protégés. En effet, si la connexion n'est plus assurée vers les serveurs, aucune remontée d'erreur ne se fera sur la console d'administration. Elles ne seront présentes que dans les journaux des systèmes d'exploitation des serveurs.

4.4.10.1 Planification des rapports

Tous ces états sont consultables dans l'interface IPStor et peuvent être transmis par messageries électroniques. Le paramétrage s'effectue lors de la création de l'état. Un résumé des planifications est accessible (cf. ci-dessous) et permet leur administration.

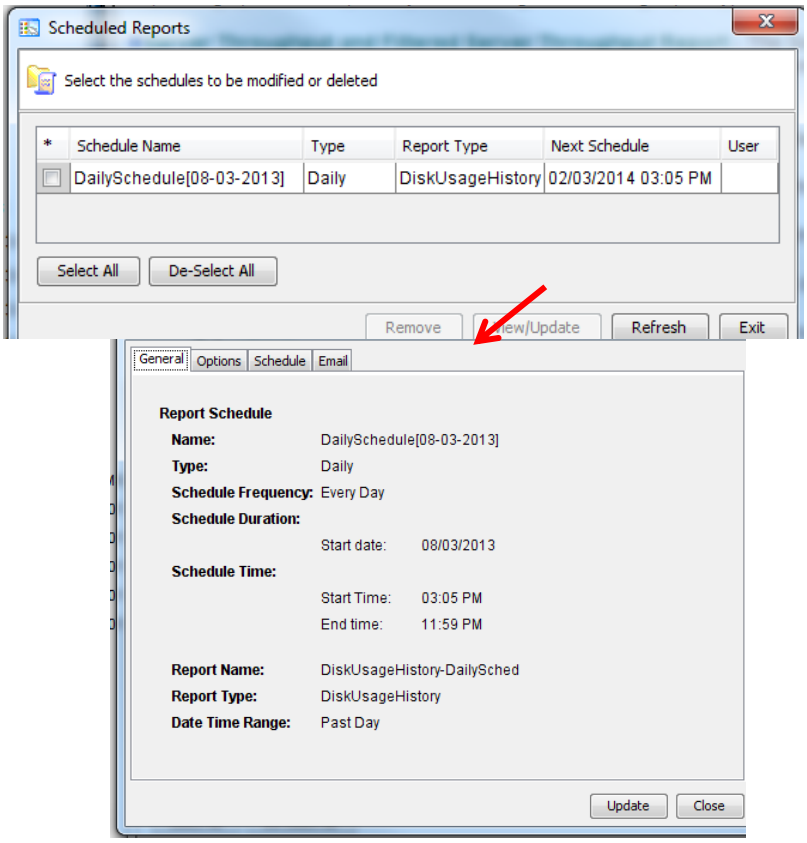


Figure 4-31 : Planification d'un rapport

4.4.10.2 Classement des rapports

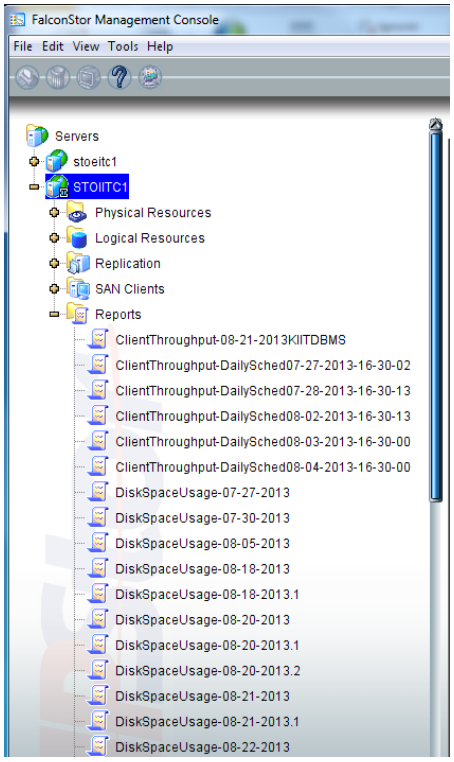


Figure 4-31 : Classement des rapports

Les rapports sont tous classés au même niveau dans l'arborescence. Cela ne facilite pas la recherche. La mise en œuvre d'un ou deux niveaux supplémentaires classés par type de rapport ou clients permettrait d'améliorer l'interface d'accès aux différents rapports…

4.5 BILAN

4.5.1 Les fonctionnalités

La solution FalconStor CDP est assez complète en termes de fonctionnalité. Le produit est relativement ouvert et capable de s'intégrer aussi bien dans les centres de données que dans des sites isolés (sans SAN).

L'interface graphique est quant à elle simple et pratique à utiliser, même si la gestion des rapports aurait besoin d'être améliorée (classement des dossiers).

Aucune anomalie n'a été décelée sur les fonctionnalités principales qui gèrent la capture des écritures ainsi que leur réplication sur le site distant. Les opérations de sauvegardes et de restaurations sont simples et fiables. La possibilité de présenter n'importe quels LUN à un serveur est relativement pratique et facilite grandement les opérations de reprise d'activité.

Néanmoins, les différentes expérimentations ont mis en évidence certaines interrogations concernant :

- la stabilité de la solution FalconStor CDP :
  - envers le kit Linux d'Euro Information ;
  - de l'outil HyperTrac censé présenter des LUN aux serveurs.
- la gestion des groupes de cohérence ;
- le bon comportement de la solution sur un SAN.

4.5.2 Consommateur de stockage

Durant les différents tests, j'ai dû apporter une attention particulière à l'espace de stockage de l'appliance qui totalisait environ 900 Go :

Alors que l'espace utilisé par les différents serveurs atteint 390Go, il y a plus de 410 Go utilisés pour les différentes prises d'images des serveurs.

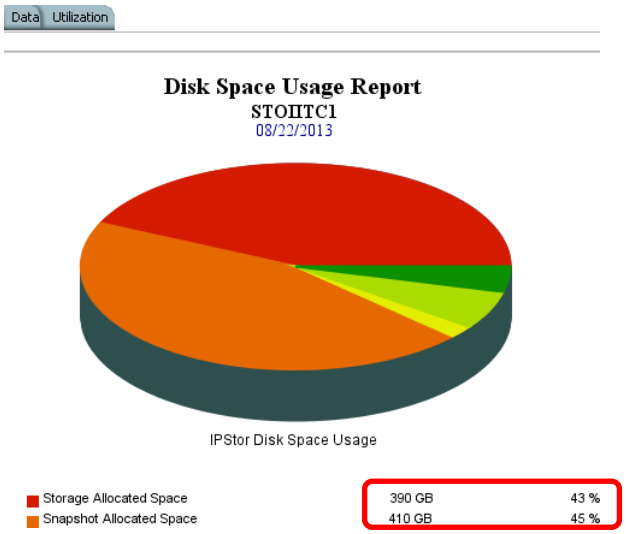


Figure 4-31 : Rapport de stockage (IPStor)

Selon FalconStor cette consommation excessive viendrait d'un problème de paramétrage. La consommation moyenne serait plutôt de 20 à 30%.

Quoi qu'il en soit, cela met en évidence l'importance du paramétrage des politiques de protection.

4.5.3 Consommateur de réseaux

Le principe de fonctionnement de FalconStor CDP est de dupliquer les écritures disques vers son système de stockage. Il double le trafic et est susceptible de générer des perturbations sur le SAN, les réseaux IP, et les serveurs protégés.

L'utilisation de FalconStor CDP sur des serveurs ayant une activité de stockage élevée (type base de données) demandera une grande attention, notamment dans le choix de leur architecture. Elle pourra en autre nécessiter :

- la mise en œuvre de réseaux privés pour assurer la duplication des flux d'écritures vers l'appliance CDP ;
- la mise en œuvre de cartes réseaux dédiées au CDP ;
- une réflexion sur la localisation de l'appliance CDP par rapport aux baies de stockage et des serveurs à protéger ;
- …

4.5.4 Interopérabilité avec les systèmes d'exploitation

Les tests réalisés avec les systèmes Linux et Windows ont montré, lors des processus de restauration, qu'il est souvent nécessaire de forcer la resynchronisation des disques. En effet, les modifications ne sont pas forcément prises en compte par le système d'exploitation qui, de fait, peut envoyer des informations erronées.

Pour remédier à cette problématique, FalconStor recommande de déconnecter les disques avant ce type d'opérations.

4.5.5 FalconStor CDP outil de sauvegarde ?

La solution CDP n'est pas un outil de sauvegarde. Il faut le considérer comme un système de réplication évolué facilitant la reprise d'activité. Au-delà de plusieurs semaines de rétention, il est indispensable d'avoir en complément une solution de sauvegarde adaptée. Les opérations de restaurations depuis le site distant nécessitent la plus grande attention, car une mauvaise action (ex : inversion du sens de réplication) peut conduire à la perte du journal de transactions et des images précédemment sauvegardées…

4.5.6 FalconStor Outil de PCA

Les tests de restaurations ont montré que FalconStor CDP est capable de mettre rapidement à disposition des LUN préalablement sauvegardés par la solution. Les différents modules mis à disposition, comme HyperTrac ou RecoverTrac (même s'il n'a pas été testé), permettent de faciliter le basculement sur le site de secours ou la reprise d'activité.

Néanmoins, FalconStor ne préconise pas d'utiliser les LUN de l'IPStor comme LUN de production. Cela implique qu'en cas d'incident, il est préférable de repositionner les données sur les LUN de production le plus rapidement possible. Cette contrainte n'est pas négligeable, puisqu'il faudra interrompre la production pour rétablir l'état initial.

Cette méthode de travail le distingue d'autres solutions telles que FalConStor NSS (Network Storage Server) ou EMC RecoverPoint qui travaillent directement sur les LUN de production.

4.5.7 Expérimentation à compléter

Cette expérimentation possède certaines lacunes notamment en ce qui concerne les tests de charge sur les différents réseaux (WAN, LAN, SAN). Une étude réalisée avec des volumétries beaucoup plus importantes (plusieurs téraoctets par exemple) et sur des sites géographiques distants de plusieurs centaines de kilomètres permettrait de vérifier le comportement et les impacts de cette solution CDP sur les différentes infrastructures réseau.

Par ailleurs, aucun test n'a été réalisé sur les différentes technologies d'hyperviseurs qu'utilise Euro Information (VMWare et Hyper-V). Il conviendrait de les comparer aux fonctionnalités de FalconStor CDP et RecoverTrac afin d'en dégager d'éventuels avantages.

5 EMC RecoverPoint

5.1 BESOINS ET OBJECTIFS

5.1.1.1 Le contexte

La mise en place de l'expérimentation du produit "RecoverPoint" a été assez laborieuse. Plusieurs scénarios ont été élaborés pour permettre une étude sur des équipements qui n'étaient pas en production. Pour diverses raisons (abandon de projet, temps de câblage trop longs, etc…), il n'a pas été possible de les concrétiser dans un délai acceptable. De ce fait, j'ai été contraint d'utiliser des équipements en cours d'exploitation. Cela a eu pour conséquences d'exclure toute expérimentation susceptible de mettre en péril l'architecture existante et notamment les tests de performance (ex : test de vitesse d'écriture). De plus, les tests de réplications distantes se feront sur le même site, car tous les équipements RecoverPoint se trouvent au même endroit.

Par ailleurs, la solution d'EMC RecoverPoint est composée de plusieurs modules dont Replication Manager. Cette application permet d'orchestrer les prises d'images cohérentes. N'ayant pas de serveur et de licence à dispositions, je n'ai pas pu le tester.

5.1.1.2 Les objectifs

La solution RecoverPoint est déjà utilisée pour protéger les messageries Exchange du groupe CM-CIC. Elle a été déployée pour se prémunir des risques de corruptions de données. Elle offre toutefois d'autres intérêts, notamment celui de faciliter la reprise d'activité en cas de sinistre (RTO et RPO de quelques minutes). L'objectif est donc de réaliser une étude afin de mieux comprendre les possibilités de cet outil. J'ai choisi de décomposer notre analyse en plusieurs phases :

- mises en place d'une infrastructure comprenant un serveur de production et un serveur de secours afin de déterminer les contraintes de mise en œuvre. ;
- réalisation de sauvegardes et de restaurations. Ces opérations permettront ainsi de recenser les difficultés qui peuvent être rencontrées lors de ces types d'exercices.

5.2 MISE EN OEUVRE DE L'ARCHITECTURE DE TESTS

5.2.1 Architecture

Pour réaliser cette expérimentation, je me suis appuyé sur l'infrastructure Exchange existante à Osny, sur laquelle j'ai ajouté 2 serveurs de tests (STOEITC1 et STOEITC2). Ces deux machines sont totalement indépendantes. Aucun service ne dialogue avec les appliances RecoverPoint.

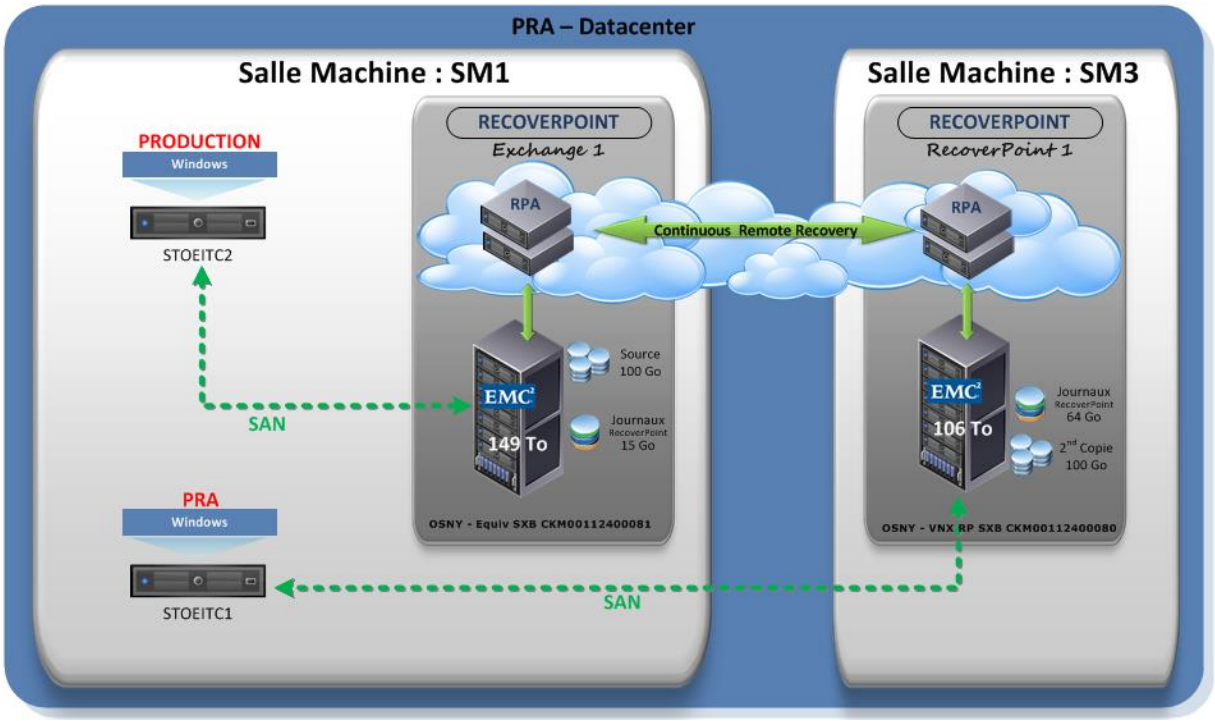


Figure 5-1 : Architecture de tests EMC RecoverPoint

Le LUN protégé aura une taille de 100 Go. Cette capacité sera donc allouée sur les 2 baies.

Les journaux de transaction RecoverPoint seront de 10 Go sur la première baie et de 64 Go sur la seconde. Il n'a pas été possible d'en allouer plus sur la première, car il n'y avait pas assez de disques non attribués disponibles.

5.2.2 Paramétrage des baies VNX

La configuration des baies VNX est sans doute la partie la plus difficile techniquement. Elle fait appel à des notions de stockage. Tout d'abord, il faut réaliser les opérations de "zoning" par le biais du SAN (Stockage Area Network). Ces interventions permettent de relier les serveurs aux baies. Puis, il faut créer 2 types de LUN sur chacune des baies :

- "RAID Group" pour les journaux de transactions RecoverPoint ;
- "Volume Pool" pour les LUN de données de 100 Go.

La procédure de création et de présentation des LUN de la première baie est donnée en annexe 18.

5.2.3 Paramétrage des appliances RecoverPoint

Le paramétrage des appliances RecoverPoint est décomposé en plusieurs étapes :

- la création du groupe de cohérence : paramétrage général de la réplication
- le paramétrage de la politique de protection des données de production (rétentions, compressions...)
- le paramétrage de la politique de protection des LUN secondaires (rétentions, compressions...)
- la sélection des LUN de productions et secondaires sur la baie VNX
- la sélection des LUN des journaux de transactions (productions et secondaires).

La procédure de configuration est donnée en annexe 21.

Remarque : Lors du test, ce sont les paramètres par défaut qui ont été sélectionnés. Dans le cas d'une mise en production réelle, une étude approfondie de ces paramètres serait indispensable, afin de les ajuster aux besoins réels. Dans le cas contraire, cela risquerait d'engendrer une consommation excessive de ressources et de réduire la fenêtre de protection.

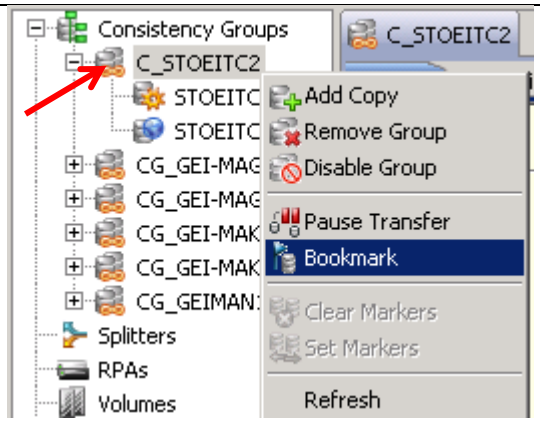
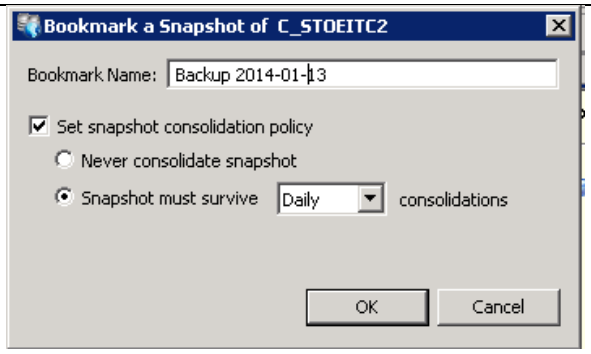
5.3 EXPÉRIMENTATIONS

5.3.1 Prise d'empreintes

5.3.1.1 Manuelle (non cohérente)

L'opération est particulièrement simple. On peut soit renommer un point de restauration, soit demander la création en précisant éventuellement le temps de conservation (cf. procédure ci-après).

Figure 5-1 : RecoverPoint - Procédure manuelle de prise d'images depuis la console d'administration

PRISE D'IMAGES
☞ "Clic droit" sur le "Consistency Group" souhaité (ex "C_STOEITC2") ☞ Choisir "Bookmark"

☞ Renseigner le nom de l'image ☞ Saisisser éventuellement sa rétention ☞ Cliquer sur "OK"


L'image apparaît ensuite dans le journal et pourra être restaurée au moment voulu.

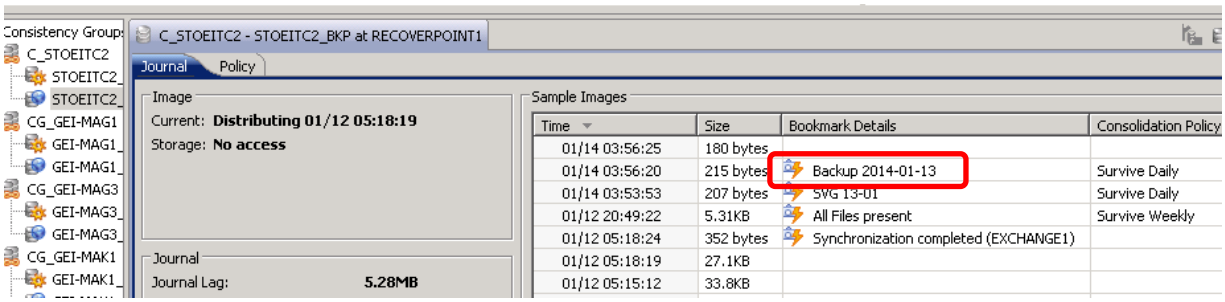


Figure 5-2 : Détail du journal du groupe de cohérence "C_STOEITC2" après une prise d'image manuelle

5.3.1.2 Planifications et rétention d'images

EMC RecoverPoint enregistre les écritures des disques en continu. Pour obtenir une protection plus longue, les appliances regroupent les snaphots en jours, en semaines ou en mois…

Ce paramétrage est accessible dans l'onglet de paramétrage du groupe de cohérence.

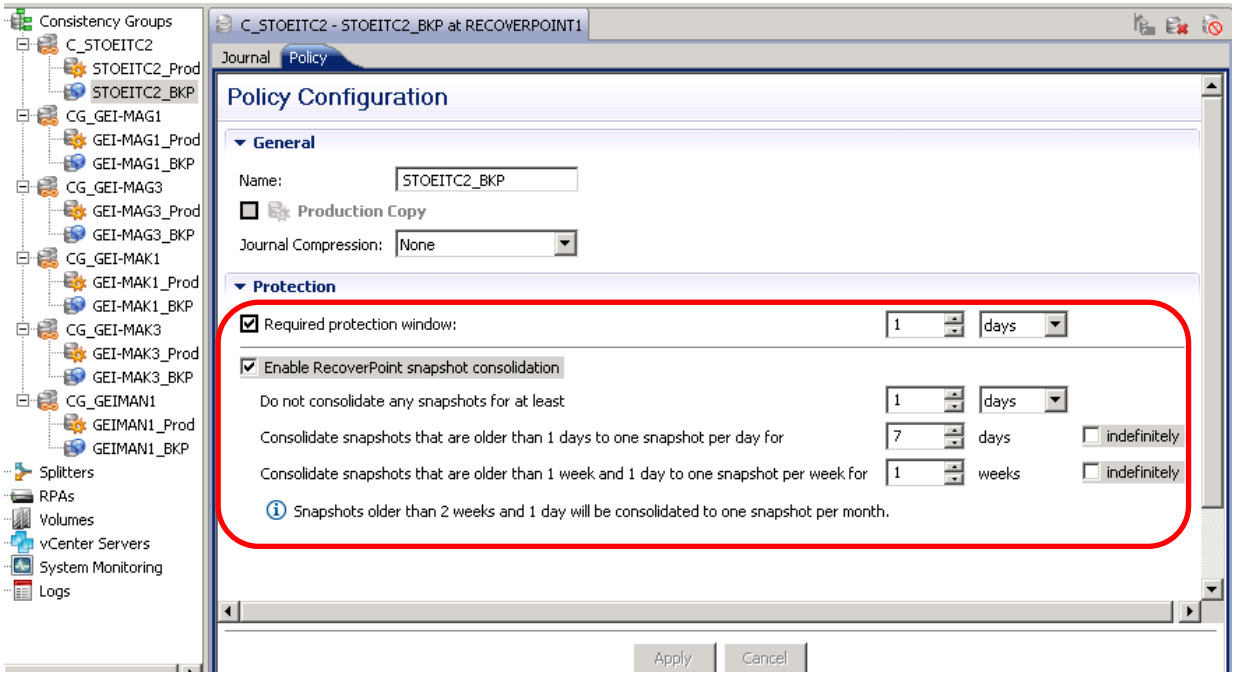


Figure 5-3 : RecoverPoint - Paramétrage de la politique de consolidation des snapshots

Le processus de consolidation regroupe toutes les modifications d'une période en un point de restauration.

Exemple : Les modifications du 16 janvier sont consolidées en une image de 2.04 Go.

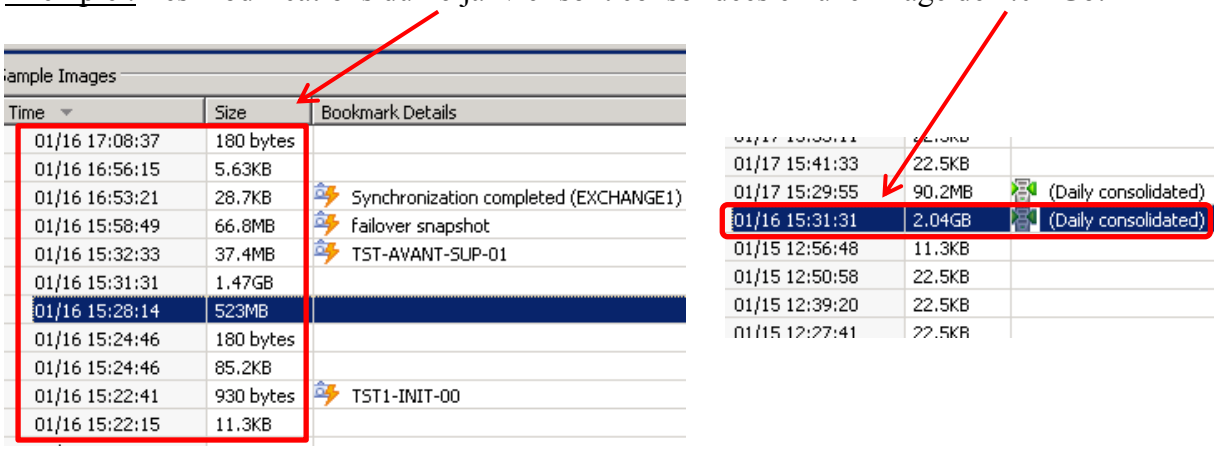


Figure 5-4 :RecoverPoint – Notion de consolidation des sanpshots

5.3.2 Restaurations

La solution RecoverPoint permet de protéger des LUN dans leur globalité. La restauration unitaire de fichiers n'est pas une priorité. Son rôle est de faciliter la reprise d'activité et de permettre le repositionnement de LUN dans un état antérieur. Afin de tester ces fonctionnalités, j'ai mis en œuvre le scénario suivant :

Tableau XV : Séquencement de l'expérimentation

N°	Date /heures	Actions réalisées	Taille (Mo)	Temps
1	16/01/2014 10:20	Prise d'une image témoin : "TST-INIT-00"		10 s
2	16/01/2014 10:25	Ajout de données sur le serveur STOEITC2	1.84 Go	3 min
3	16/01/2014 10:30	Prise d'une image la suppression des données : "AVANT-SUP-01"		10 s
4	16/01/2014 10:35	Suppression de tous les fichiers et dossiers sur STOEITC2	- 1.84 Go	35 s
5	16/01/2014 10:45	Restauration de l'image "AVANT-SUP-01" sur STOEITC1 (Serveur PRA)	1.84 Go	1 min
6	16/01/2014 11:17	Ajout d'un fichier témoin sur STOEITC1		30 s
7	16/01/2014 11:35	Recopie de la LUN vers le serveur de Production (STOEITC2)		1 min
8	16/01/2014 11:51	Réactivation de la réplication vers le site de PRA		30 s

Le déroulement de l'expérimentation est détaillé dans l'annexe 23. Elle permet en autre de mieux comprendre le comportement de l'appliance lors des différentes opérations (ajout de données, présentation de LUN sur le serveur de secours, inversion du sens de réplication, etc…).

Durant les tests, l'application s'est montrée fiable et aucun problème majeur n'a été décelé. J'ai tout de même rencontré des problèmes de synchronisation entre le serveur de secours et son stockage durant les étapes 5 et 6. En effet, lorsque l'appliance RecoverPoint modifie le contenu du LUN, le serveur n'est pas nécessairement informé de cette modification. De fait, les disques modifiés ne sont pas systématiquement resynchronisés et les informations retournées à l'utilisateur peuvent être erronées.

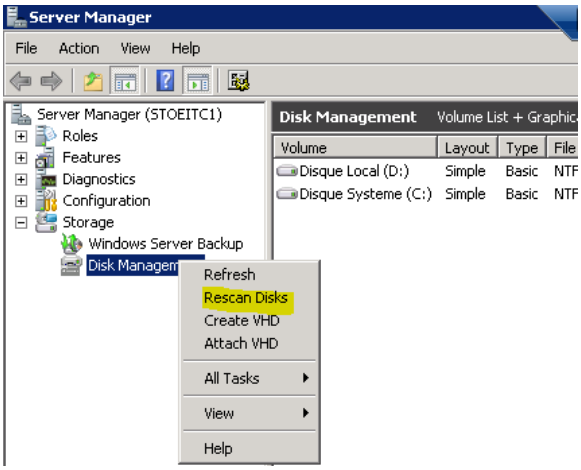


Figure 5-5:"Recan" des disques (Server Manager)

Pour corriger ce problème, il a fallu forcer la resynchronisation des disques à l'aide de l'interface d'administration Windows (cf. figure ci-contre).

L'expérience a aussi montré que l'on pouvait rapidement basculer dans l'environnement de secours, reprendre une activité et se repositionner dans l'état initial. Le journal CDP peut être conservé, mais cela nécessite de ne pas activer le « failover » qui a pour conséquence de l'effacer. Cette situation peut être assez dommageable, puisqu'il ne sera plus possible de restaurer une version antérieure …

5.3.3 Logs et rapports

Tous les évènements relatifs aux infrastructures RecoverPoint (appliance, splitter,réplications,..) sont consultables au travers de l'interface graphique, ou en ligne de commande. Ce système permet de faire remonter les évènements plus ou moins importants (cf. capture d'écran ci-après).

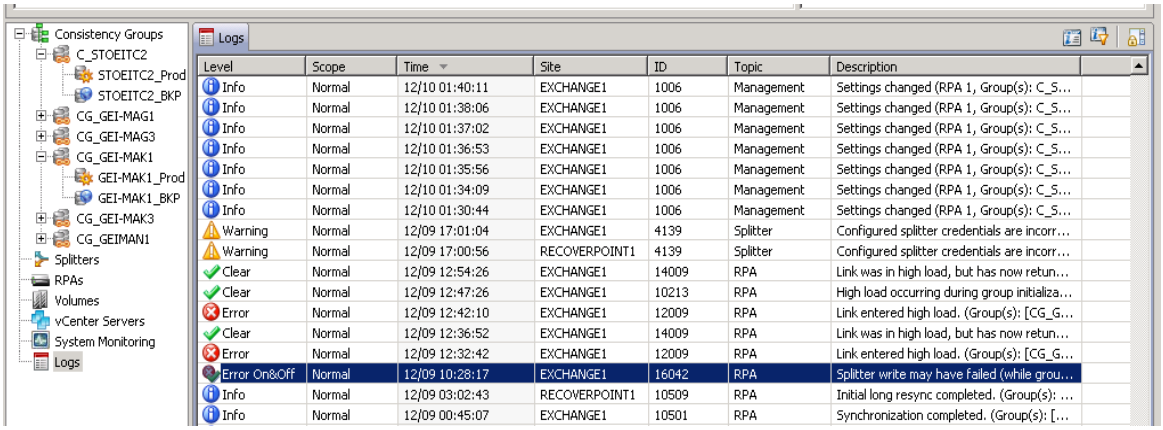


Figure 5-7 : Extrait des logs RecoverPoint

EMC RecoverPoint intègre dans son interface des statistiques en temps réel pour chacun des groupes de cohérence. Cela permet de surveiller et d'adapter les différentes politiques de protection. Elles sont regroupées en deux catégories : l'analyse du trafic, et celle des performances des réplications.

Analyse du trafic (nombre d'écritures, débits…) :

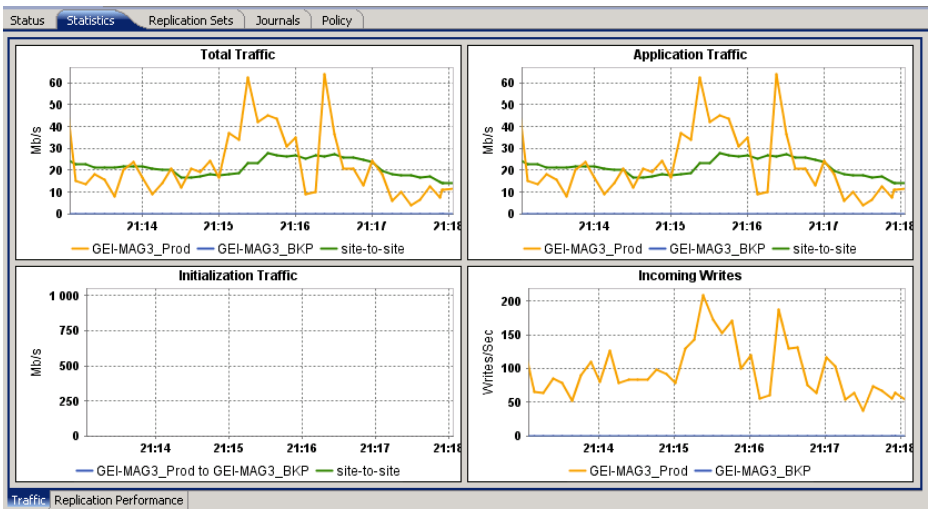


Figure 5-8 : Exemple de statistiques du trafic d'un groupe de cohérence

Analyse des performances des réplications (taux compression, retards,…) :

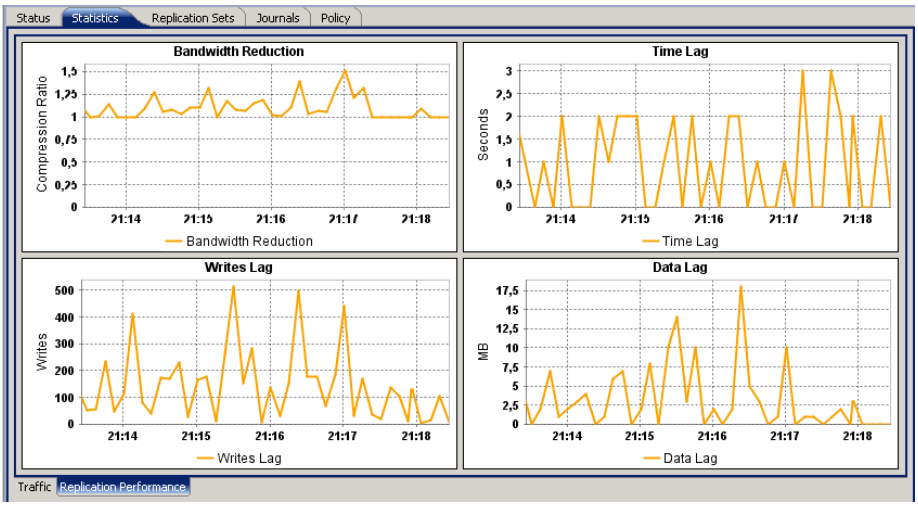


Figure 5-9 : Exemple de statistiques sur les performances d'un groupe de cohérence

5.4 BILAN

5.4.1 Mise en œuvre

La mise en œuvre d'une solution EMC RecoverPoint nécessite une attention particulière. De nombreux paramètres sont à prendre en considération et le paramétrage s'effectue sur les appliances mais aussi sur divers composants du SAN. Les baies de stockage, les switches du réseau de stockage, et les services EMC, sont autant d'éléments qui compliquent le paramétrage et qui pourtant influent fortement sur la durée de protection.

L'estimation est d'autant plus délicate lorsque l'on protège des données pour lesquelles l'administrateur n'a aucune maîtrise par exemple comme le trafic réseau généré par des applications (ex :Exchange, base de données,…).

5.4.2 Les fonctionnalités

5.4.2.1 L'interface et l'accessibilité

L'interface est simple et assez visuelle. La représentation de l'architecture facilite la compréhension de l'outil. Toutefois, les fonctions offertes représentent un danger pour l'environnement de production. Chaque action doit être mesurée. Une mauvaise action peut avoir des conséquences désastreuses :

- Bascule sur l'infrastructure de PRA ;
- Écrasement des données de la production ;
- Pertes des journaux de transactions (et donc de toutes les images) ;
- …

Il est donc important que le personnel en charge de ces équipements soit bien formé afin d'éviter une mauvaise manipulation lors d'une opération de restauration. En effet, ce type de technologie est généralement utilisé sur des infrastructures sensibles où l'erreur n'est pas permise.

5.4.2.2 Prise d'image et restaurations

Les prises d'image sont réalisées très rapidement par les appliances RecoverPoint. Cependant, les images ne sont pas "crash-consistent". Il est donc possible que leur restauration ne soit pas totalement fonctionnelle. L'utilisation de Replication Manager et l'installation d'un agent sur le serveur à protéger devrait permettre de lever cette contrainte.

Pour ce qui concerne les restaurations, les tests réalisés montrent que l'on peut basculer rapidement dans l'environnement de PRA et procéder à une reprise de la production par la suite. Il faut toutefois prendre conscience que les données restaurées (lors des tests) étaient relativement petites (quelques giga-octets) et qu'il faudra refaire des tests avec des LUN de plus grande capacité (dépassant le téraoctet de données) pour avoir une réelle idée des temps de restaurations.

Enfin, il faut préciser que RecoverPoint est prévu pour protéger des LUN dans leur globalité. Nous pouvons récupérer un dossier ou un fichier dans l'environnement de secours, mais il n'existe aucun catalogue ou référentiel concernant les fichiers ou les dossiers présents dans les différentes images. Il faut donc connaître la date et l'heure du LUN où se trouvent les éléments que l'on souhaite récupérer avant de procéder à la restauration.

5.4.3 Stabilité et fiabilité

Durant nos différentes expérimentations, RecoverPoint s'est montré particulièrement stable : aucun plantage, ni même de ralentissement ou d'erreur n'ont été constatés. Je n'ai rencontré qu'une seule anomalie liée au système d'exploitation lors de la phase de restauration (cf. 5.3.2 page 101). En revanche, la volumétrie des tests (quelques gigaoctets) ne permet pas d'affirmer que l'outil soit stable sur des volumes plus importants.

Dans la mesure où l'architecture RecoverPoint utilise des "Splitters" pour dupliquer ses flux de données, la charge supportée entre le client et la baie de stockage n'est pas doublée (comme cela peut être le cas avec la solution FalconStor CDP). Le risque de congestion des réseaux est donc réduit.

5.4.4 Expérimentation à mettre en œuvre

Les contraintes de temps et d'architecture n'ont pas permis de mener l'étude de ce produit dans sa globalité. De nombreuses expérimentations seraient nécessaires afin d'en vérifier l'ensemble des fonctionnalités. Il faudrait réaliser en autre :

- les tests de divers agents et modules : "Replication Manager", les agents Oracle, MS SQL Server et Exchange n'ont pas été testés. Ils représentent pourtant un intérêt majeur. Par exemple la prise d'image cohérente sur des arborescences de fichiers ou d'applications (Exchange, base de données).
- les tests de charges : Des tests de charges sont nécessaires afin de vérifier le comportement de la solution sur les équipements du SAN. Sur les LUN, on peut essayer d'augmenter brusquement le nombre d'écritures, de procéder à de multiples restaurations, ou tester d'autres types de modifications. Il faudrait aussi vérifier l'efficacité des réplications distantes et notamment l'utilisation de la déduplication.
- les tests des différentes architectures CLR et CDP : RecoverPoint possède plusieurs types d'architecture (cf. figure 2-12 page 39). Nos tests ont été réalisés uniquement sur une architecture de type CRR. Il conviendrait de tester les autres types d'infrastructures.
- les tests sur divers environnements virtuels et systèmes d'exploitation : seul le système d'exploitation Windows 2008 a été testé. Il conviendrait d'étendre les tests sur d'autres systèmes d'exploitation (Linux, Unix, …), mais aussi sur les environnements virtuels Hyper-V et VMWare.

LA SYNTHÈSE

6 BILAN DE L'ÉTUDE CDP

6.1 LA PROTECTION CONTINUE DES DONNÉES

6.1.1 Les orientations de la protection continue

Les solutions CDP peuvent être classées selon 3 orientations : outils de sauvegarde ; de PRA/PCA ; ou de versioning. Les recherches effectuées, ainsi que les différentes expérimentations ont permis de définir leurs principales caractéristiques (cf. tableau ci-dessous) :

Tableau XVI : Avantages et inconvénients des différents courants du CDP

	Avantages	Inconvénients
Sauvegarde	- Coût d'infrastructure faible - Optimisation des ressources de stockage et de réseaux - Rétention possible sur de longues périodes - Granularité de restauration fine (fichier)	- Reprise d'activité lente - Utilise les ressources serveur (mémoire, processeur)
Outils de PCA	- Reprise d'activité courte (RTO quelques minutes) ; - Perte de données limitée - Ressources processeurs et mémoires peu ou pas sollicitées (solution "agentless")	- Durée de conservation des données courte (quelques mois) - Consommation importante de l'espace de stockage - Infrastructure souvent onéreuse (SAN, baie de stockage) - Solutions souvent complexes à mettre en œuvre - Sollicite souvent les réseaux - Granularité de restauration peu précise (le LUN)
Versioning	- Coût faible d'infrastructure - Granularité de restauration fine (va jusqu'au fichier)	- Consomme des ressources sur le poste client (processeur, mémoire, réseau) - Destiné au partage "bureautique" avec un taux de modifications modéré

6.1.2 L'intérêt de la protection continue

L'intérêt principal de cette technologie est qu'elle permet de récupérer plusieurs versions (voir toutes en fonction de la solution) sur une période de temps donnée. Cela en fait un atout majeur pour protéger les données des défaillances matérielles, logicielles ou humaines. Elle est particulièrement intéressante sur des volumes de grande capacité (plusieurs téraoctets) pour lesquels les outils de sauvegarde conventionnels atteignent leurs limites (en ce qui concerne les temps de sauvegardes et de restauration).

Le choix entre une solution "True CDP" et "Near CDP" ne doit pas occulter les véritables enjeux : est-ce les données ou les infrastructures que l'on souhaite protéger ? Si l'on souhaite protéger des infrastructures, la solution "Near CDP" est efficace et suffisante. Dans le cas où l'on cherche à protéger des données, on doit s'interroger sur la valeur des données modifiées. Celle-ci doit être évaluée par son propriétaire en fonction du temps et du nombre d'octets modifiés. En effet, le temps n'est pas le seul facteur à prendre en considération : dans un même intervalle de temps, il peut n'y avoir aucune modification comme plusieurs dizaines de milliers. L'utilisation du "True CDP" ne peut être justifiée que si ces modifications ont suffisamment de valeur, sinon cela ne restera qu'un accessoire.

Il existe un grand nombre solutions CDP qui possèdent des attributs différents en fonction de leurs orientations. Il conviendra, en fonction du type d'architecture, de faire le choix le plus adapté en tenant compte des besoins et de l'effort financier pour y parvenir.

6.1.2.1 Serveurs applicatifs

La protection continue peut représenter un réel intérêt pour les serveurs applicatifs. En effet, toutes les applications ne permettent pas de gérer l'historique des modifications. Le CDP ajoute donc cette fonctionnalité et facilite la mise en œuvre de PCA et de PRA. Il existe une multitude de solutions pouvant répondre aux différents besoins à des prix très variables ; en fonction de la volumétrie à protéger, de l'infrastructure des réseaux et de la qualité de service désirée.

6.1.2.2 Base de données

Compte tenu des expériences réalisées, on peut se demander si le CDP représente un intérêt majeur pour les bases de données. En effet, les principaux produits, comme MS SQL Server et Oracle, proposent déjà de repositionner les bases de données à partir de leurs journaux de transactions.

Les solutions CDP, orientées PRA et PCA, disposent de données directement accessibles qui leur permettent d'être plus réactives et d'avoir un temps de reprise d'activité plus court. De plus, elles permettent de limiter l'impact sur le serveur de base de données et les réseaux lors des opérations de sauvegardes ("dump" massif sur les disques), puisque celles-ci sont réalisées au fur et à mesure.

La protection continue ne représente un intérêt que sur des bases de données très imposantes. En effet, il n'y aura pas d'intérêt à utiliser la protection continue si la restauration des données (sans le CDP) ne nécessite que quelques minutes…

6.1.2.3 Serveur de fichiers

Les serveurs de fichiers bénéficient souvent d'une protection continue. En effet les NAS comme les serveurs Windows donnent la possibilité d'enregistrer et de déporter leurs données très régulièrement. Les besoins en protection continue existants depuis plusieurs décennies, on trouve une multitude de solutions CDP permettant de répondre à ces différentes attentes: sauvegarde, PCA, versioning.

6.1.2.4 La virtualisation de serveurs

Il n'a pas été possible d'étudier le comportement des solutions CDP dans une architecture VMWare ou Hyper-V. L'intérêt résiderait peut-être sur les temps de sauvegarde et sur la rapidité de reprise d'activité, mais cela reste à confirmer grâce à une étude un peu plus poussée.

6.1.3 Synthèse des expérimentations

6.1.3.1 Les différentes solutions

L'étude des différentes solutions FalconStor CDP et EMC RecoverPoint a montré que même si ces deux produits affichent des fonctionnalités équivalentes, ils n'étaient pas nécessairement concurrents. En effet, certaines de leurs particularités font que ces produits vont s'adresser à des architectures différentes (cf. tableau XVII, ci-après).

Tableau XVII : Comparaison des solutions EMC RecoverPoint et FalconStor CDP

		Solution CDP	
		EMC RecoverPoint	FalconStor CDP
Type d'architecture	Nombre important de LUN	Compliqué à mettre en œuvre	Gestion simplifiée
	LUN de grandes capacités	Optimisé pour gérer des LUN jusqu'à 10 To	Risque de surcharge des réseaux
	Nombre d'écritures élevé	Utilisation de "splitter" pour ne pas surcharger le SAN	Double le trafic sur le réseau : risque de surcharge des réseaux
	Stockage sur le SAN		
	Stockage sur réseau IP	Non géré	Protocole iSCSI sur IP
	Simplicité de mise en œuvre	Complexe, nécessitant un paramétrage: - des serveurs - des baies de stockage - de SAN - des appliances RP	Simple, paramétrage s'effectuant depuis le serveur à protéger ou l'appliance…
	Coût	Nécessite des infrastructures onéreuses	Prix de l'appliance + Coût par téraoctet

Au vu de cette comparaison, la solution FalconStor sera plus intéressante (notamment sur le plan financier) pour des infrastructures ne demandant pas trop d'écritures, alors qu'EMC RecoverPoint sera beaucoup plus fiable et optimisée lorsque les besoins seront plus conséquents (LUN de plusieurs téraoctets). En d'autres termes, FalconStor CDP sera plus adapté aux petites et moyennes entreprises, alors que RecoverPoint offrira des prestations qui répondront plus aux grandes entreprises telles qu'Euro Information…

6.1.3.2 Les enseignements des expérimentations

Durant les différentes expérimentations, j'ai constaté qu'il était important de réaliser une étude sur les besoins réels de la protection à mettre en place. Ceci afin de déterminer la solution CDP la plus adaptée. Il faut donc estimer l'activité moyenne des disques afin de définir quels sont les besoins en stockage. Cette étape est importante, car en cas d'erreur, la fenêtre de protection risque de ne pas être suffisamment longue.

Il faut aussi prendre en considération le fonctionnement de la protection continue choisie, car cela influe sur les serveurs à protéger, mais aussi sur les infrastructures environnantes (réseaux IP et réseaux de stockage). En effet, le trafic généré par le CDP peut être doublé et amené à saturer les équipements réseau (serveurs et switchs).

On peut également relever que la protection continue est susceptible de protéger un domaine très vaste d'architectures informatiques (messagerie, virtualisation, NAS, base de données, etc. …) qu'une personne seule ne peut totalement maîtriser. La constitution d'une équipe ayant la maîtrise de ces environnements serait souhaitable pour réaliser les prochaines expérimentations.

6.2 L'ORGANISATION DE L'ÉTUDE

6.2.1 Les différentes recherches du projet

Le travail de recherche s'est organisé en plusieurs étapes :

- la recherche des différentes documentations traitant du sujet CDP ;
- la recherche des solutions de protection continue ;
- l'étude de l'administration des équipements du stockage et des outils de sauvegardes .

6.2.1.1 Documentation CDP

Le travail de recherche de documentation sur la protection continue n'a représenté qu'une infime partie du travail de recherche. En effet, ce point avait été étudié en amont du projet. Toutefois, la découverte de certains documents de la littérature (anglo-saxonne et française) et le rapport Garner sont venus complémenter les informations précédemment trouvées sur Internet, avec un regard beaucoup plus posé sur les vrais enjeux de cette technologie.

6.2.1.2 Produits et solutions CDP

La recherche de produits a été réalisée au travers de lectures d'ouvrages ou de pages web traitant du sujet. Tout ceci a permis de récupérer une grande masse d'informations afin d'obtenir une idée plus précise sur les différentes fonctionnalités de ces technologies. Une fois ce travail de référencement effectué, les premiers tests ont été réalisés sur les produits les plus simples et qui ne nécessitaient pas de grosses infrastructures.

Certaines solutions assez complexes (FalconStor, Assigra, R1Soft, EMC RecoverPoint, Simpana Cincom,…) ont nécessité une mise en relation avec des équipes techniques et commerciales. Le but était d'obtenir des informations complémentaires sur le fonctionnement de leurs produits, et de demander, si nécessaire, une présentation plus concrète. Une démonstration réelle permet de mieux appréhender les outils en termes d'ergonomie et de fonctionnalités. Cela a permis, entre autres, d'évaluer certains produits (ASIGRA, FalconStor, R1Soft) et de limiter la sélection pour approfondir les recherches.

6.2.1.3 Le paramétrage des équipements du SAN

La mise en œuvre de solutions CDP nécessite un minimum de connaissances sur les notions de stockage : le fonctionnement des outils de sauvegardes, des baies, des équipements de routage du réseau de stockage, sont autant d'éléments indispensables pour comprendre et paramétrer les différentes architectures. Cet apprentissage a pu être réalisé au travers de lectures d'ouvrages (présents dans la bibliographie), mais aussi, et surtout, grâce au temps que les membres de mon équipe ont passé à m'enseigner les fondamentaux. À l'aide de ces compétences nouvellement acquises, j'ai pu procéder aux paramétrages des différentes infrastructures de tests FalconStor CDP et EMC RecoverPoint.

6.2.2 Mise en œuvre et expérimentations

La mise en œuvre des équipements représente une part importante de ce projet. Hormis le montage et le câblage physique des équipements, aucune opération de configuration et d'installation de logiciels n'a été sous-traitée.

L'acquisition de matériel, ainsi que son paramétrage, auront été particulièrement longs. Il aura fallu plus de 7 mois pour y parvenir. De nombreuses difficultés ont été rencontrées :

- lors des commandes des équipements : 6 mois d'attentes pour recevoir les 4 serveurs ;
- lors des demandes de machines virtuelles de tests ;
- lors des demandes de câblage réseau : problème d'identification et de localisation des switches au sein des centres de données ;
- lors du déploiement des systèmes d'exploitation : le kit d'installation Euro Information n'était pas compatible avec ces nouveaux serveurs. Plusieurs équipes d'Euro Information ont travaillé à son adaptation.

Beaucoup de ces problèmes auraient pu être évités avec une meilleure connaissance des différentes équipes et de l'environnement Euro Information.

Le paramétrage des serveurs a été réalisé sur deux sites localisés en région parisienne (à Val de Fontenay et à Osny sous-bois). Afin de limiter le nombre des équipements, j'ai partagé les mêmes serveurs pour réaliser les expérimentations des différentes solutions CDP. J'ai d'abord réalisé les tests de FalconStor CDP, avant de paramétrer les équipements pour étudier la solution RecoverPoint. Cette façon de procéder m'a amené à réduire le temps d'expérimentation de chacun des produits. De ce fait, certaines anomalies ou fonctionnalités n'ont pu être approfondies.

6.2.3 Les difficultés rencontrées

6.2.3.1 Le coût des équipements

Les technologies de protection continue s'organisent souvent autour d'infrastructures évoluées et onéreuses (baies de disques, SAN ; NAS, ESX, …). Ces contraintes m'ont quelque peu obligé à réaliser nos configurations et nos tests dans un environnement de production déjà pourvu en équipements et à n'acheter que du matériel qui pouvait être réutilisable sur d'autres projets.

L'étude des coûts dans le contexte Euro Information est difficile à estimer. La taille du parc informatique est telle que le service logistique peut négocier des accords avec les principaux fournisseurs afin d'obtenir des prix relativement bas (qui restent confidentiels).

6.2.3.2 Sécurisation de la production

Les normes de sécurité sont particulièrement rigoureuses. Les tests et expérimentations ne sont que tolérés et doivent être soigneusement argumentés. Dans la mesure où des équipements mutualisés ("switches", réseaux, baies...) sont utilisés, on ne peut prendre le risque de les mettre en péril. Le stockage et les réseaux sont des organes vitaux des centres des données. Le moindre problème impacte l'ensemble des équipements. Dans ces conditions, il n'a pas été possible de réaliser des tests de performance...

6.2.3.3 Structure segmentée des équipes d'Euro Information

L'informatique du groupe est divisée en une multitude d'équipes informatiques ayant chacune un rôle bien défini (administration des bases de données, des serveurs Unix; des HyperV ; des ESX, des messageries, etc. …). Cette organisation augmente le niveau de sécurité puisqu'une personne seule ne peut intervenir sur l'ensemble des équipements. Cependant, dans le cadre d'études de solutions impactant plusieurs domaines, il est difficile de mobiliser des ressources dans chacune de ces équipes.

Malgré les réunions d'information qui ont été organisées, aucune équipe n'a pu dégager de temps pour réaliser ces expérimentations. Cela a fortement limité le champ de mes investigations, notamment dans les domaines : bases de données et hyperviseurs (HyperV, ESX).

6.2.3.4 Actualité et décision d'entreprise.

Fin de commercialisation de Netbackup Realtime

La décision d'arrêter la commercialisation de Netbackup Realtime, annoncée par Symantec en juin 2012, m'a contraint à modifier mes objectifs en tentant d'expérimenter un outil de substitution. Je me suis donc tourné vers Replication Director, conseillé par Symantec pour remplacer Netbackup Realtime. Après avoir étudié cet outil, je me suis rendu compte qu'il présentait de nombreuses contraintes et aucun intérêt pour l'entreprise. Il m'a donc fallu revoir mon étude afin d'étudier de manière plus poussée d'autres solutions qui semblaient correspondre aux besoins de l'entreprise (principalement RecovertPoint, FalconStor CDP, Netbackup/NetApp OSSV).

Projet RecoverPoint (Réquisitions judiciaires pour NRJ Mobile)

En mai 2012, il a été demandé à l'équipe Storage Open dont je fais partie, de proposer une infrastructure capable de sécuriser une base de données de plusieurs téraoctets de données. La solution RecoverPoint semblait tout à fait correspondre à la protection d'une volumétrie si importante. J'ai donc présenté un dossier s'appuyant sur cette technologie.

La mise en place de cette nouvelle infrastructure au sein d'Euro Information aurait permis d'effectuer les tests sur des équipements dédiés, non soumis aux contraintes de production. Cela aurait été idéal pour expérimenter les différentes fonctionnalités de ce produit.

Ce projet a finalement été confié à l'équipe "stockage" du Mainframe. J'ai toutefois souhaité poursuivre mon étude de cette solution malgré des conditions moins favorables : les équipements disponibles étaient déjà en production et fortement sollicités. De ce fait, je n'ai pas pu réaliser les tests de performance, car le risque d'impacter la production était trop grand.

6.2.4 Tableaux de bord

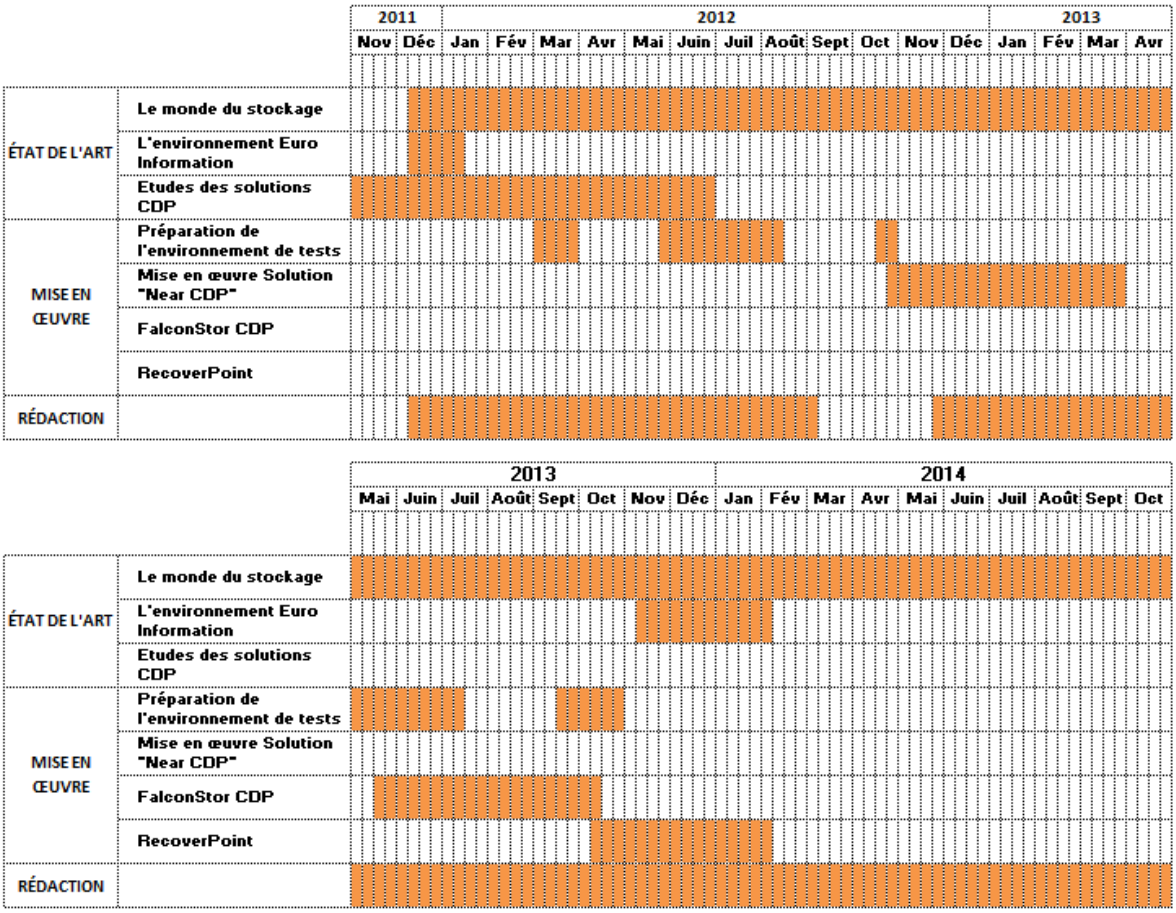


Figure 6-1 : Organisation du mémoire

Cette étude, qui devait initialement s'achever en octobre 2012, aura finalement duré près de 3 ans. Ne pouvant effectuer cette étude correctement sans en maîtriser les notions élémentaires de stockage, il m'a fallu me former afin d'en comprendre les véritables enjeux. Cette phase d'apprentissage indispensable m'a particulièrement pris du temps puisqu'à cette époque j'alternais entre deux fonctions : celle de responsable informatique au sein de Filaction et celle d'informaticien dans l'équipe "Storage Open". Pour cette dernière, j'ai eu en charge des dossiers qui auront été d'autant plus chronophages que je débutais dans ce domaine. J'ai également rencontré quelques difficultés dans la mise en œuvre des différentes expérimentations que je détaille dans la section 6.2.3.3 (page 126).

CONCLUSION

Beaucoup d'éditeurs de logiciels ont été séduits par ce nouveau concept de protection continue. Celui-ci possède de nombreux avantages, tels que : la réduction des fenêtres de sauvegardes, un temps de reprise d'activité plus court et un historique de l'état des données suffisamment complet pour garantir une perte minimale d'information en cas d'incident. Les technologies et approches utilisées par les éditeurs ont donné naissance à une multitude d'outils qui peuvent être classés selon 3 orientations (outils de sauvegarde, outils de "versioning" ou outils de PCA) possédant chacun des avantages et des inconvénients.

L'utilisation de la protection continue peut impliquer des contraintes assez lourdes : surcharge des réseaux, surconsommation d'espace de stockage, de mémoire ou de CPU. Afin d'éviter ces problèmes, il est indispensable d'étudier le profil des données à protéger (taux de modification et fréquence) ainsi que le mode de fonctionnement de la solution CDP. Ceci afin d'en déterminer les besoins et d'effectuer un paramétrage le plus optimisé possible. Cela implique également d'exercer un suivi constant des infrastructures afin de déceler les éventuelles dérives qui pourraient survenir, par exemple, lors d'un changement de profil des modifications des données.

Dans le cas d'une entreprise (telle qu'Euro Information) possédant de nombreuses infrastructures et de très nombreuses données sensibles à protéger, la protection continue s'avère être aujourd'hui la technologie la plus adaptée. Ses rapidités de sauvegarde et surtout de restauration (notamment dans le cas de solutions orientées PCA) en font un moyen de protection particulièrement efficace que les outils traditionnels n'arrivent pas à concurrencer. En effet, ils ne permettent pas de protéger correctement les volumes de grandes capacités : les outils de sauvegardes sont trop lents (en sauvegarde et en restauration) et les réplications ne permettent pas de se prémunir contre la corruption…

Cette technologie représente donc pour Euro Information un atout indispensable, répondant aussi bien aux besoins de protection des volumétries importantes qu'aux besoins très élevés (supérieurs à 99%)°de disponibilité des services. C'est pour toutes ces raisons qu'Euro Information a déjà déployé plusieurs infrastructures RecoverPoint (pour Exchange et d'autres environnements).

Le CDP s'intègre à des architectures très variées que je n'ai pas pu tester. Toutefois, il pourrait représenter un intérêt pour les bases de données, les machines virtuelles et les NAS. Il conviendrait d'étudier ces différentes possibilités. Son utilisation pourrait en effet se traduire par un lissage des flux réseaux et éviter ainsi la saturation des équipements réseaux pendant les opérations de sauvegardes (ex : "dump" des bases de données).

La forte croissance des besoins en stockage, et l'attente toujours plus grande en fiabilité, favorisent le déploiement de ce type de protection. Même s'il existe encore quelques contraintes, celles-ci devraient diminuer parallèlement à l'évolution des algorithmes et des technologies. Les solutions CDP pourraient, d'ici une décennie, devenir un standard des outils de sauvegarde ou de stockage…

ANNEXES

ANNEXE 1 : RPO et RTO

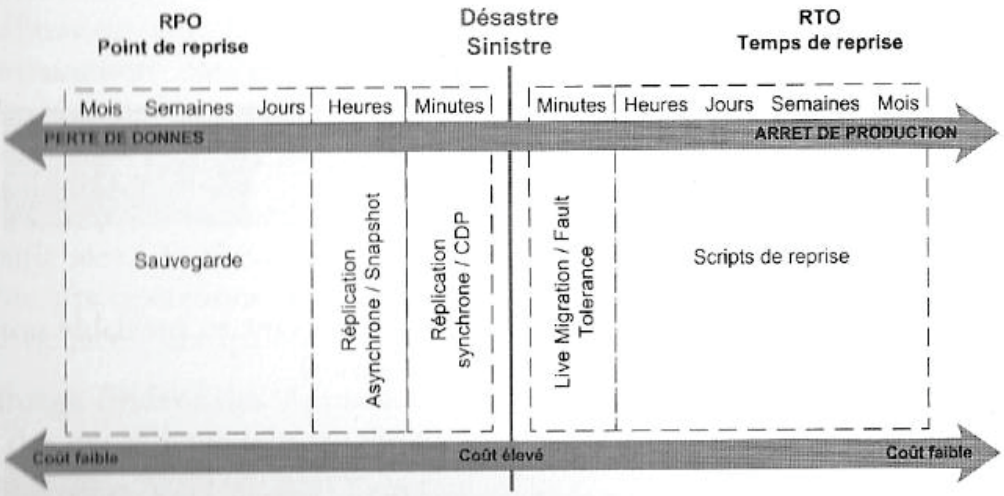
Reestablishment Point Objective et Reestablishment Time Objective

Ci-dessous, un extrait du livre de Mr GEARGEOT C . [STORAGEF03,pages 94 et 95]:

E.10 Les termes RPO et RTO

N'importe quelle entreprise a un jour réfléchi sur les conséquences d'un arrêt de production et les coûts qui en découleraient. Certaines d'entre elles pourraient se permettre un arrêt de production de trente minute tandis que d'autre ne pourraient pas se permettent de prendre plus de deux heures de données.

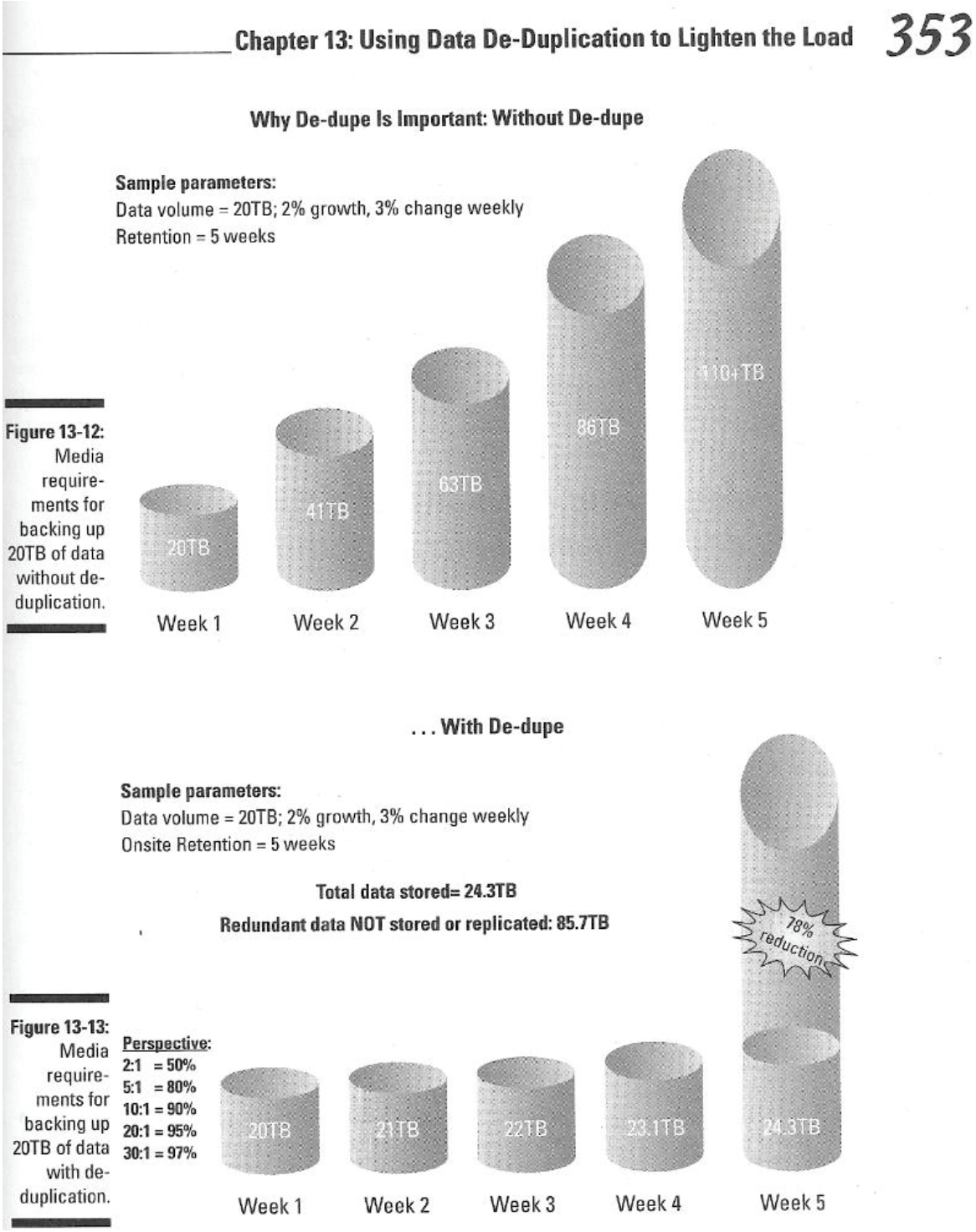
De ces exigences ont émergé des termes appelés Plan de Reprise d'Activité (PRA) ou de continuité d'activité (PCA) qui sont intimement associés aux notions de RTO (Recovery Time Objective) et RPO (Recovery Point Objective). La première notion correspond à un temps maximal pour reprendre l'activité tandis que la deuxième exprime le delta temps entre la perte maximale de données tolérée au moment du sinistre et au moment où l'activité redémarre, soit la perte de données maximale acceptable.



Bien entendu, la situation rêvée de n'importe quelle entreprise est d'avoir une valeur la plus proche possible du zéro pour le RTO et le RPO. **Plus la valeur désirée est proche du zéro, plus les coûts associés seront élevés.** En fonction des valeurs désirées, le schéma suivant vous indiquera les moyens à mettre en œuvre.

ANNEXE 2 : La déduplication

Ci-dessous, un extrait du livre "Storage Area Networks for Dummies" [STORAGEA01,page 353]:



ANNEXE 3 : Le "zoning"

Ci-dessous, un extrait du livre "Storage Area Networks for Dummies" [STORAGEA01,pages 126-127]:

TIP

You can create as many zones as you want in a fabric. You can group different zones into as many zone configurations as you want, but only one zone configuration can be active in the fabric at a time.

Types of zoning

Two types of zones are available in a SAN (detailed in the upcoming subsections):

- **Soft zoning:** Zones are identified by World Wide Name
- **Hard zoning:** Zones are identified by physical switch port

Soft zoning

Soft zoning is a method of grouping individual World Wide Names (WWNs) in the fabric into a zone set. *World Wide Names* are the 64-bit address assigned to every object connected to a switched fabric. (See Chapter 3 for more on WWNs.) Instead of using the physical-port information to create members of a zone set, you use the WWN address(es) of the device(s) connected to the port. (See Figure 5-30.)

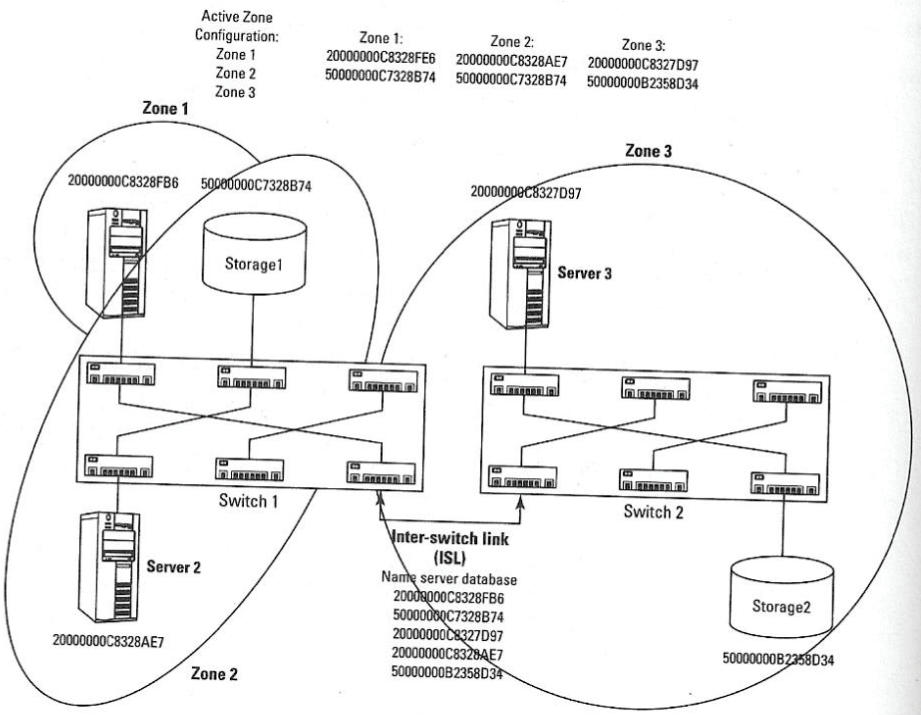


Figure 5-30: Soft zoning, using World Wide Names.

WWN zoning (soft zoning) is more flexible than port zoning (hard zoning) because the zone information is based on the device's address instead of the port on the switch that it's connected to. If a switch port goes bad and you move the device connected to that port to a different port, you need to change the zone information to reflect the changed port before the device connected to the new port will work again in the fabric. By using WWN zoning, the address will have moved with the device, so no zone changes are needed.

Hard zoning

Hard zoning is a method of grouping individual physical switch ports in a switched fabric together into a *zone* that only allows communication between physical ports on the switches. (See Figure 5-31.) Only the physical ports in the zone can communicate with each other. No other ports in the fabric can communicate with those ports, and members of that zone set cannot communicate with any other ports in the fabric.

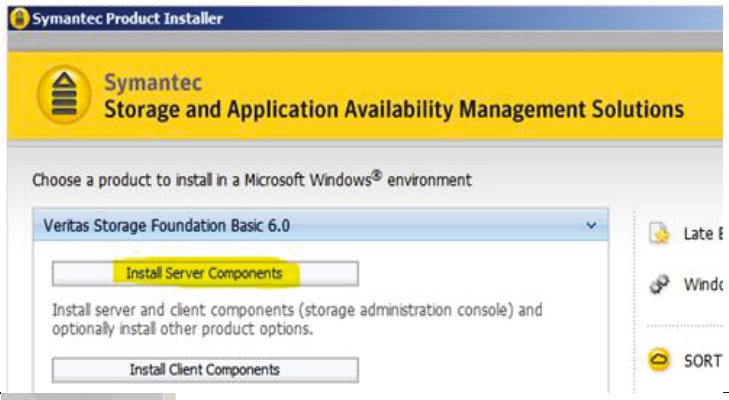
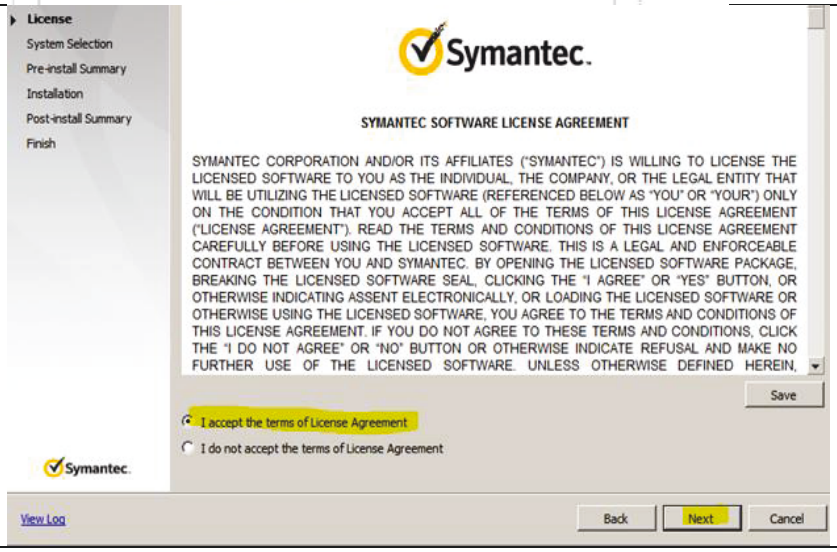
Zone members can communicate only with other members of their zone. A zone set can accommodate multiple zones; switch ports can be members of multiple zone sets. If a switch port is made a member of multiple zone sets, it can communicate with the ports of all the zone sets that it has membership with. The same holds true for soft zone members (see the preceding section).

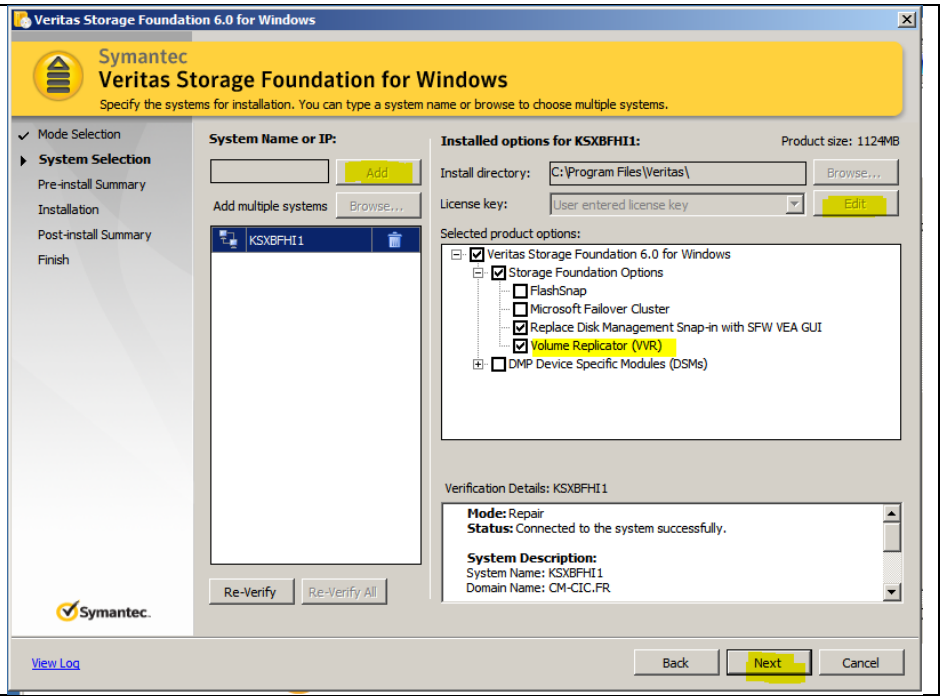
TIP

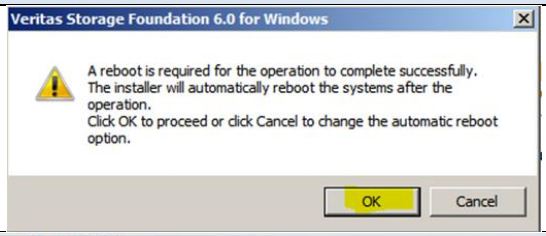
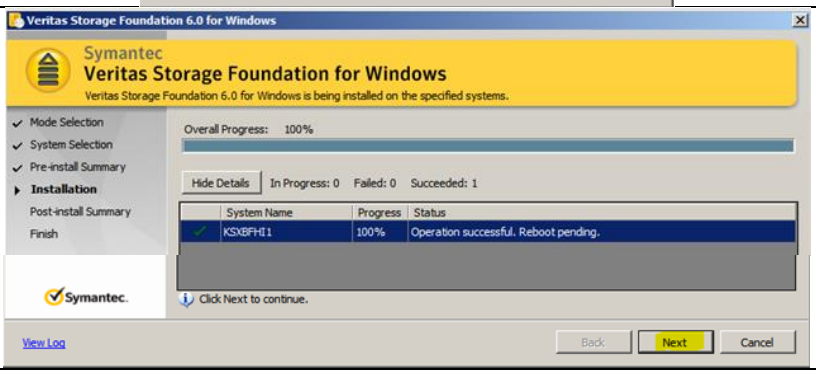
Hard zoning at the level of physical ports is the most secure method of zoning.

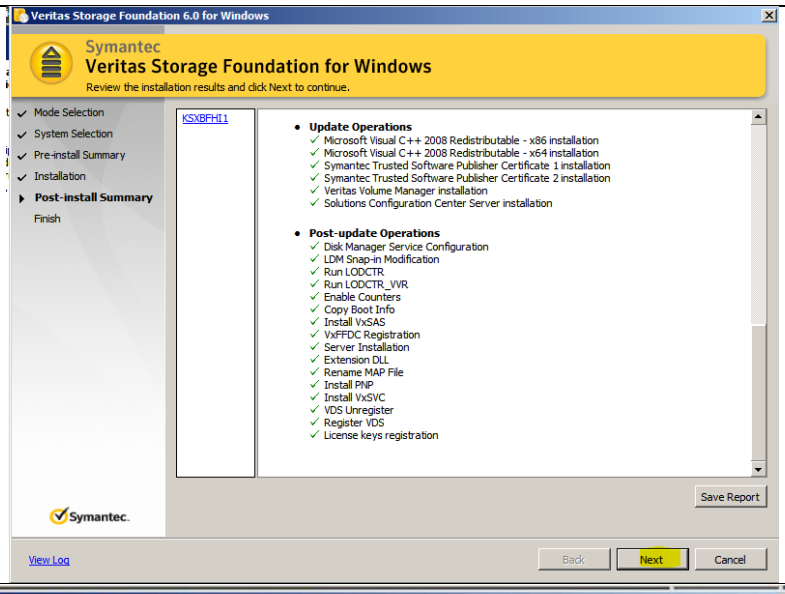
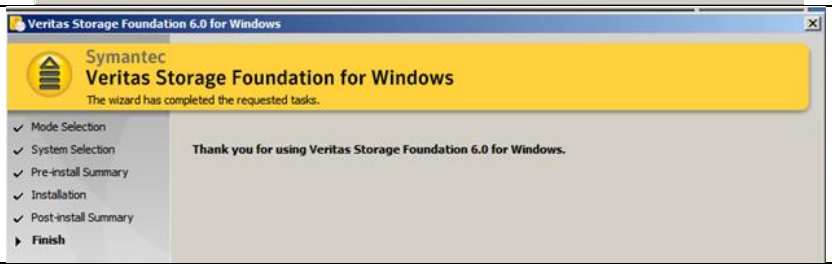
You can mix domain and port names along with WWNs in the same zone, but after you do, all the ports revert to soft zoning. (See Figure 5-32.)

ANNEXE 4 : Procédure d'installation Storage Foundation

ACTIONS	ILLUSTRATIONS
☞ Lancer la commande : "netsh int tcp set global chimney=disabled"	
☞ Cliquer sur : "Install Server Components"	
☞ Cliquer sur : "I accept the terms of license Agreement" ☞ Puis Cliquer sur :"Next"	

☞ Ajouter le serveur KSXBFHI1 ☞ Ajouter la clé de licence ☞ Cocher l'option : "Volume Replicator(VVR)" ☞ Cliquer sur "Next"	

ACTIONS	ILLUSTRATIONS
☞ Cliquer sur "OK"	
☞ Cliquer sur "Next"	

☞ Cliquer sur "Next"	
☞ Cliquer sur "Finish"	

ANNEXE 5 : Configuration Policy VSS Netbackup

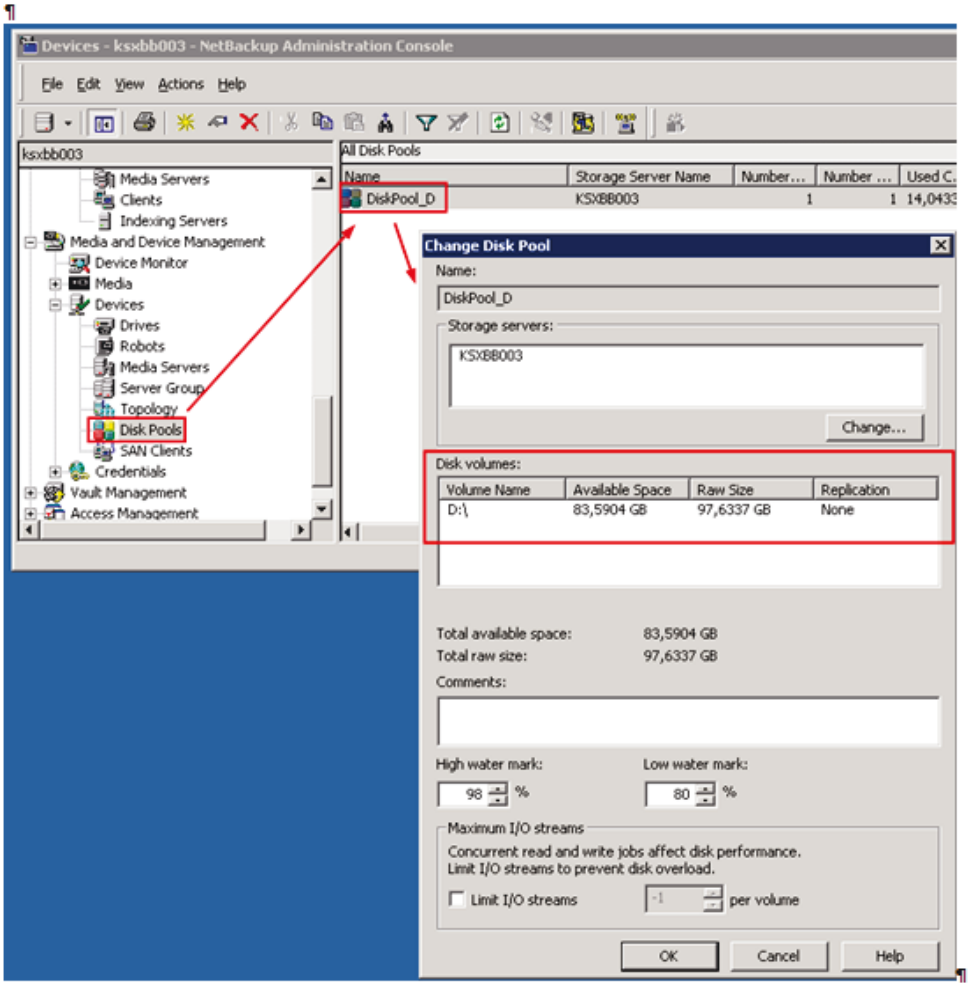
Extrait de la documentation rédigée par un membre de l'équipe Storage (3O20):

Gestion de snapshots VSS Windows → → version 1.0

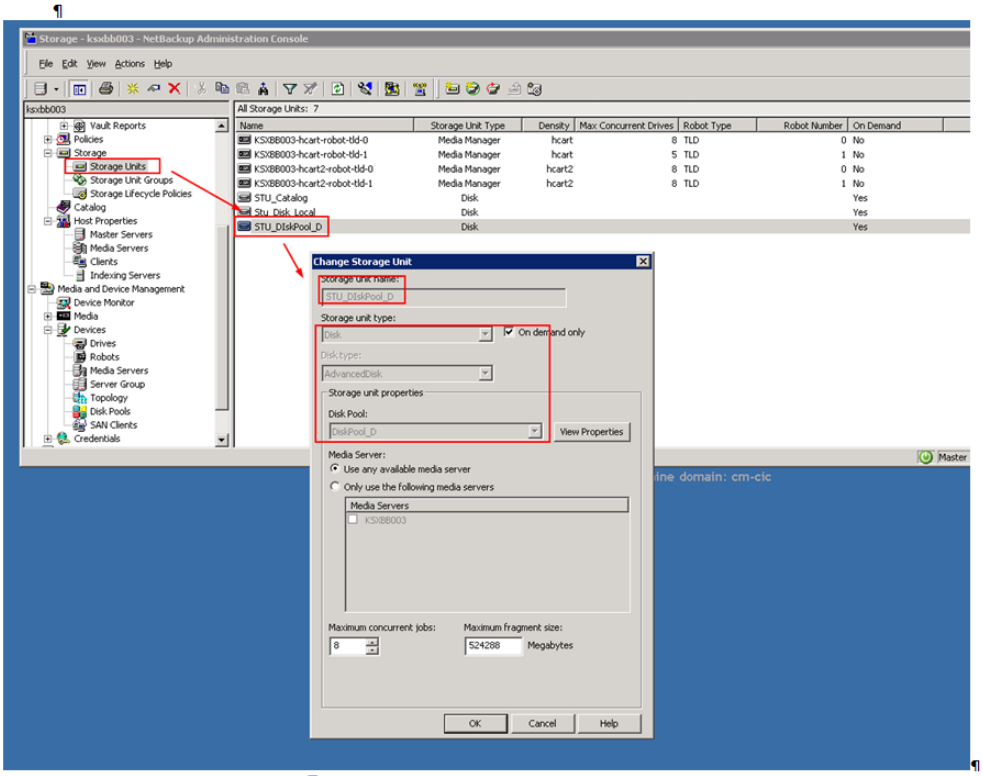
3.2. Configuration NetBackup (effectué sur KSXBB003)

3.2.1. Création d'un Disque Pool

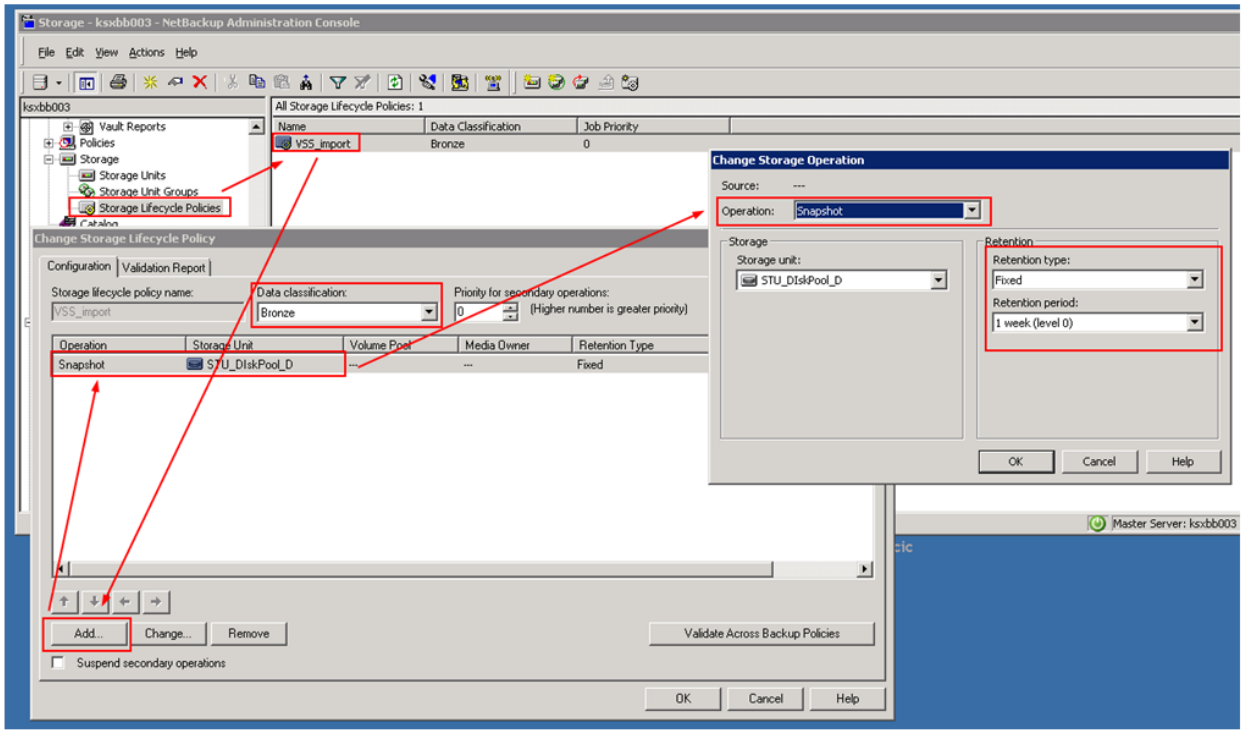
Il faut créer un Disque Pool à travers la Console d'Admin NBU → DiskPool_D



3.2.2. Création d'une StorageUnit disque : STU_DiskPool_D



3.2.3. Création d'une SLP – Storage Life Cycle Policy : VSS_import



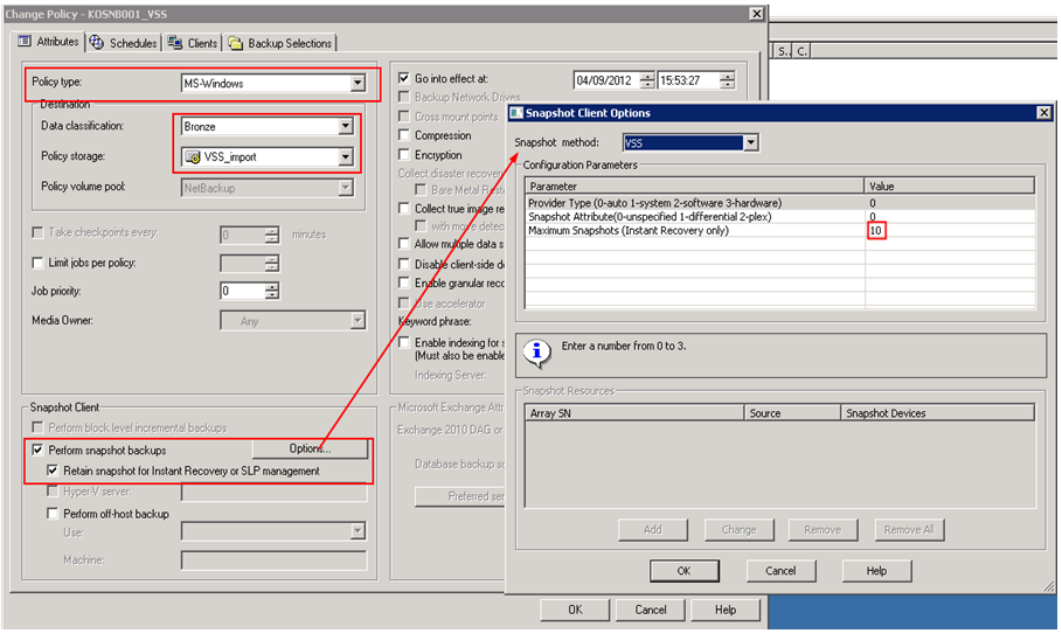
A minima, pour que cela fonctionne, il faut créer une opération de type Snapshot.
En second lieu, il est possible d'ajouter d'autres opérations associées à ce Snapshot comme par exemple l'import ou la réplication.

3.2.4. Création d'une Policy de type Windows : KOSNB001_VSS

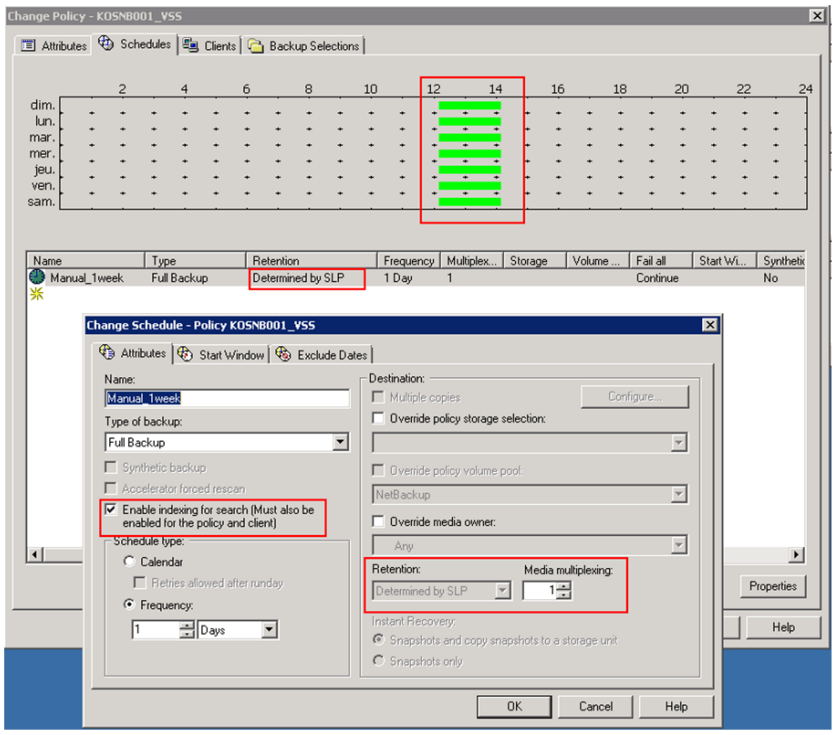
Il faut créer une Policy de type MS-Windows, en positionnant :

- Retain snapshots for Instant Recovery or SLP Managment
- Perfom snapshot backups , avec la method VSS
- On y décrit le nombre de Snapshots que l'on desire conserver

  ⇨ Ce nombre doit être cohérent avec la rétentino en place dans la SLP
  ⇨ Si SLP dit rétention=1 week, et 1 Snapshot / jour, dans ce cas-là, il faut positionner le Maximum Snapshots > 7



Et de son SCHEDULE ...



ANNEXE 6 : Management liaison OSSV

1. Création d'un OSSV vers le NAS

1.1 Activation de la liaison initiale

snapvault start -o compression=on -S<Host primlaire>:<Path> <vfiler secondaire>: /vol/<volume groupe>/<Qtree>

Exemple:

"snapvault start -o compression=on -SKSXBFHI1:G:
UNASEI1V:/vol/KSXBFHI1_PRA/PublicLyon_P002_KSXBFHI1_G"

1.2 Planification des snapshots (jour; mois; semaine)

Horaire :
snapvault snap sched -x -o preserve=default,warn=0 **<Volume groupe>** sv_hourly **<Nb images concervées>**@<tranche horaire>

Exemple : vfiler run unasei1v snapvault snap sched -x -o preserve=default,warn=0 KSXBFHI1_PRA sv_hourly 8@8-20

Quotidien :
snapvault snap sched -x -o preserve=default,warn=0 **<Volume groupe>** sv_daily **<Nb images concervées>**@**<heure exécution>**@**<jours exécutions>**

Exemple : snapvault snap sched -x -o preserve=default,warn=0 KSXBFHI1_PRA sv_daily 15@22@mon-sat

Hebdomadaire :
snapvault snap sched -x -o preserve=default,warn=0 **<Volume groupe>** sv_weekly **<Nb images concervées>@<heure execution>**@**<jours exécutions>**

Exemple : vfiler run unasei1v snapvault snap sched -x -o preserve=default,warn=0 KSXBFHI1_PRA sv_weekly 5@23@sat

2. Vérification de l'état de liaisons

- Snapvault status

Récupère l'état de toutes les liaisons OSSV

```
D:\NetApp\IBM\snapvault\bin>snapvault status
Snapvault primary is ON
Source          Destination                          State   Lag        Status
KSXBFHI1:H:\    UNASEI1V:/vol/KSXBFHI1_PRA/qtree_HIPU003  Source  -          Transferring  (6306 MB done)
KSXBFHI1:G:\    UNASEI1V:/vol/KSXBFHI1_PRA/qtree_HIPU002  Source  04:03:31   Idle
```

Ici, la première est en cours d'actualisation, la seconde est déjà actualisée (début de la dernière synchronisation il y a 4h)

☞ Snapvault status -l

Récupère la description détaillée de l'état de toutes les liaisons

```
D:\NetApp\IBM\snapvault\bin>snapvault status  -l
Snapvault primary is ON

Source:                          KSXBFHI1:H:\
Destination:                     UNASEI1V:/vol/KSXBFHI1_PRA/qtree_HIPU003
Status:                          Transferring
State:                           Source
Lag:                             -
Mirror Timestamp:                -
Base Snapshot:                   -
Current Transfer Type:           -
Contents:                        -
Last Transfer Type:              -
Last Transfer From:              -
Bytes transferred so far:        960 MB
Transfer Time Elapsed:           01:09:28
Current Transfer Throttle:       Unthrottled
Total files to transfer:         4488228
Total files transferred:         35
Current File Size:               116736
Current File Progress:           0
Current File Name:               H:\DOMAINE_M200\ModSle CR de r'union.doc
Transfer Error ID:               -
Transfer Error Message:          -
Compression Ratio:               2,2:1

Source:                          KSXBFHI1:G:\
Destination:                     UNASEI1V:/vol/KSXBFHI1_PRA/qtree_HIPU002
Status:                          Idle
State:                           Source
Lag:                             03:33:54
Mirror Timestamp:                -
Base Snapshot:                   -
Current Transfer Type:           -
Contents:                        -
Last Transfer Type:              -
Last Transfer From:              -
Last Transfer Size:              38 GB (Compression=37%)
Last Transfer Duration:          03:15:50
Total files to transfer:         209470
Total files transferred:         209470
Current File Size:               -
Current File Progress:           -
Current File Name:               -
Transfer Error ID:               -
Transfer Error Message:          -

D:\NetApp\IBM\snapvault\bin>_
```

- Transfert de données en cours
- 960 Mo déjà envoyé
- Compression moyenne de 2.2

[Status:Idle]: Les données sont à jour s

[Last Transfer Size]:38 Go (compression 37%)

[Lag]: Dernière actualisation à 3h33min 54s

3. Suppression d'une liaison

☞ Sur le primaire (Serveur Windows ou Linux)

snapvault **release** g:\ UNASEI1V:/vol/KSXBFHI1_PRA/PublicLyon_P002_KSXBFHI1_G

☞ Sur le secondaire(NAS)

snapvault **stop** UNASEI1V:/vol/KSXBFHI1_PRA/PublicLyon_P002_KSXBFHI1_G "

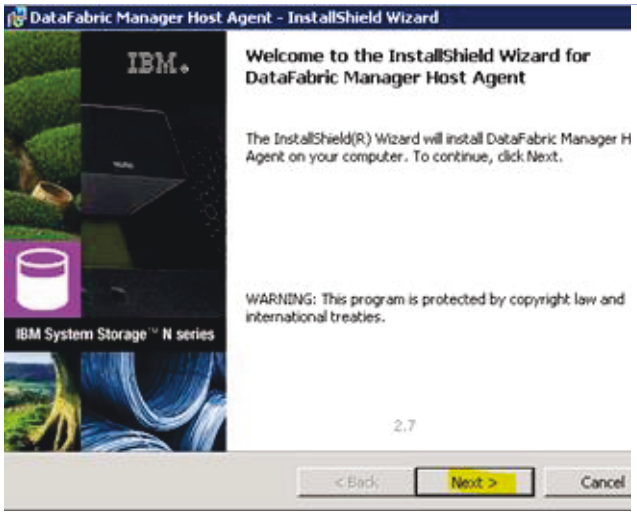
Résultat de la commande :

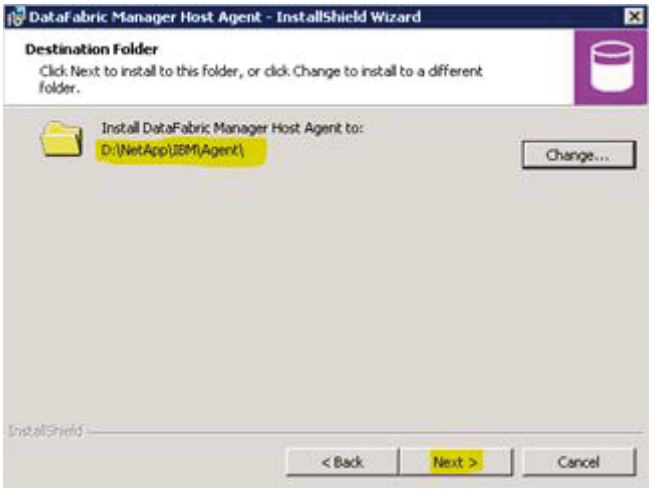
Stopping /vol/KSXBFHI1_PRA/PublicLyon_P002_KSXBFHI1_G is permanent.
The secondary qtree will be deleted.
Further incremental updates will be impossible.
Data already stored in snapshots will not be deleted.
This may take a long time to complete.
Are you sure you want to do this? **Y**
Protection to /vol/KSXBFHI1_PRA/PublicLyon_P002_KSXBFHI1_G has been stopped and the qtree deleted.

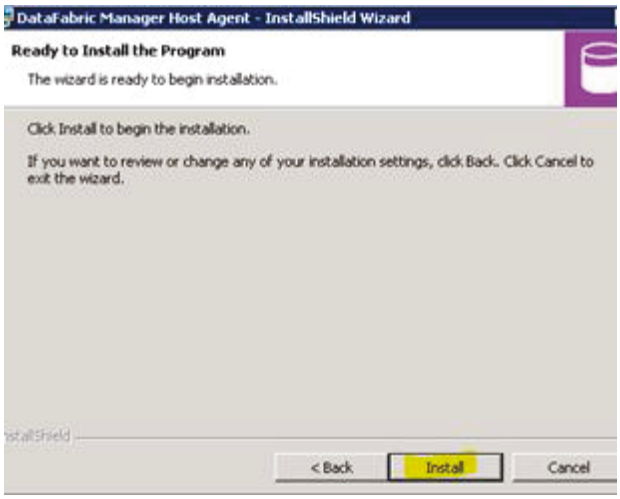
ANNEXE 7 : Installation DFM Host Agent

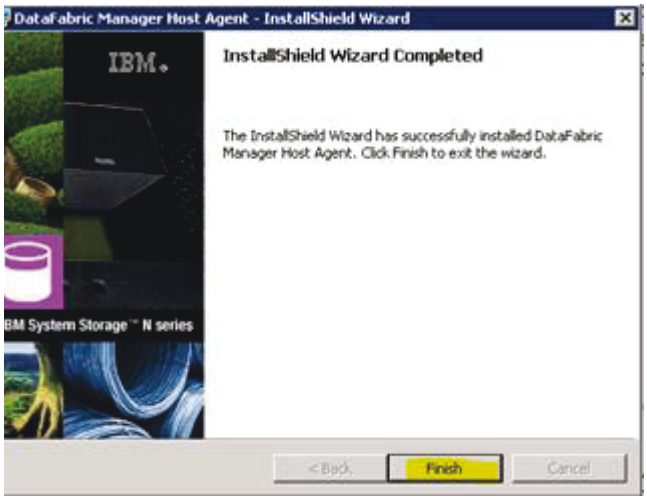
1. MISE EN ŒUVRE SUR LE CLIENT WINDOWS

Sur KSXBFHI1, lancer: D:\Install\Host_Agent\agentsetup-2-7-win32_from_IBM.exe

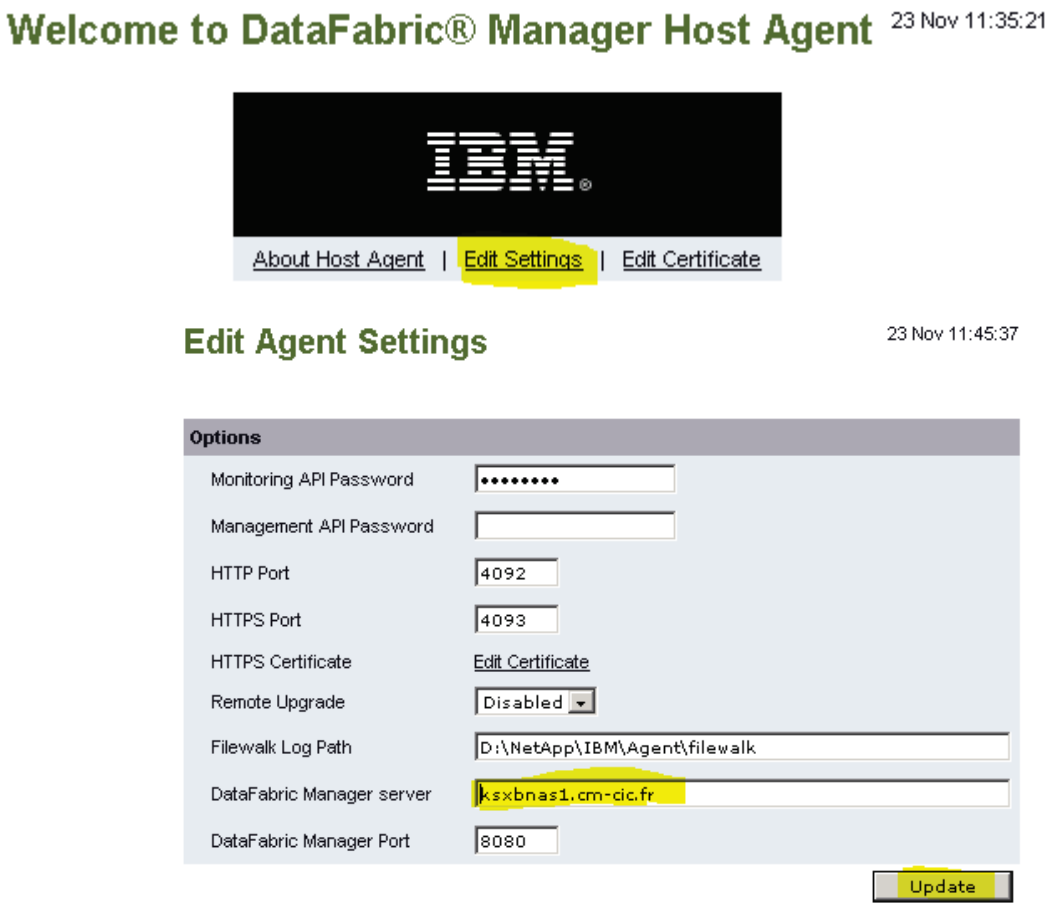


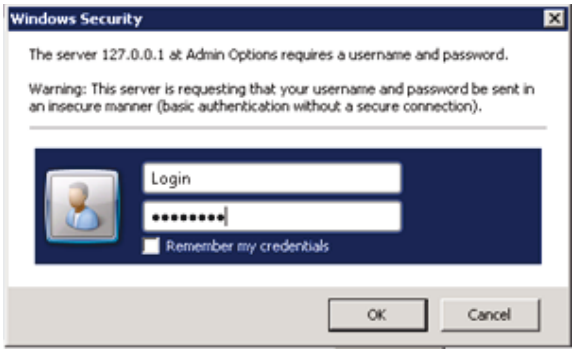




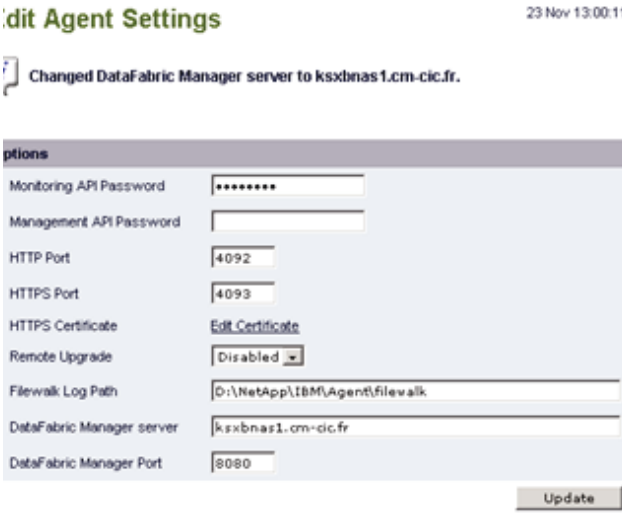


ANNEXE 8 : Paramétrage DFM Host Agent



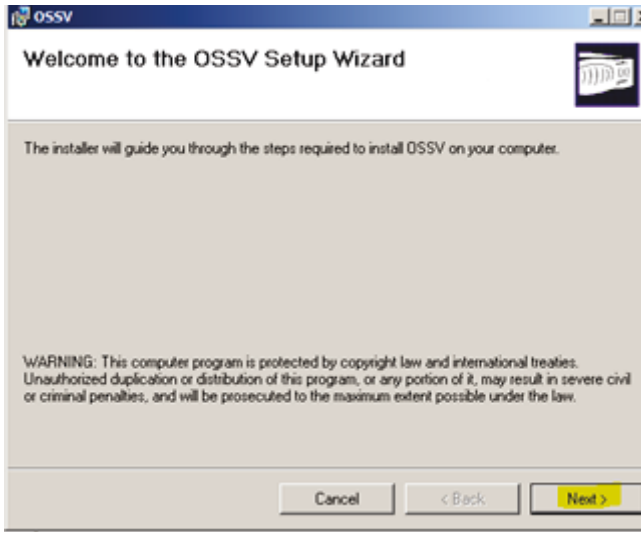


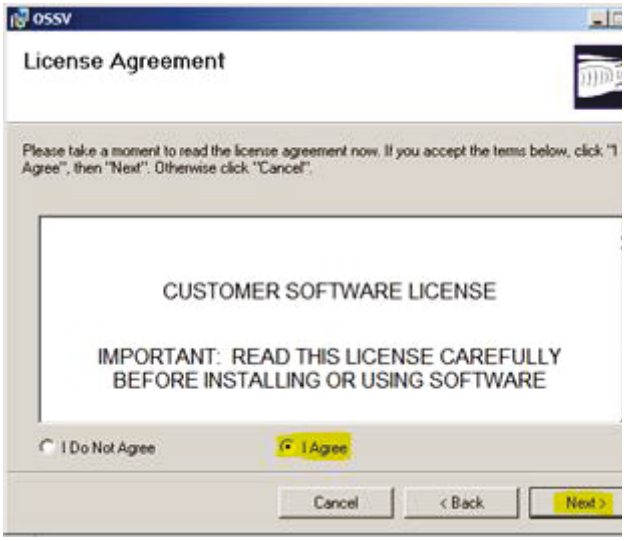
→Utiliser le compte 2

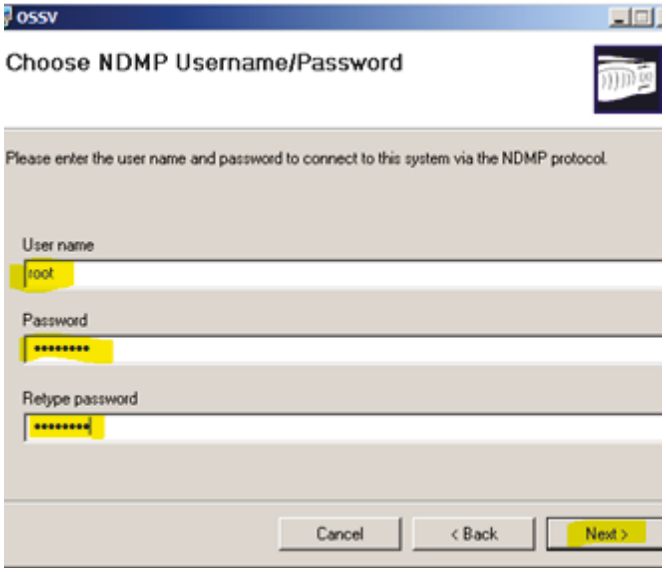


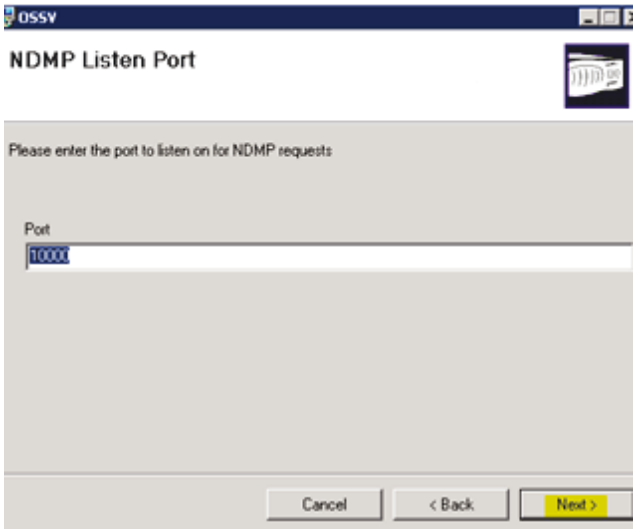
ANNEXE 9 : Installation du plug-in OSSV

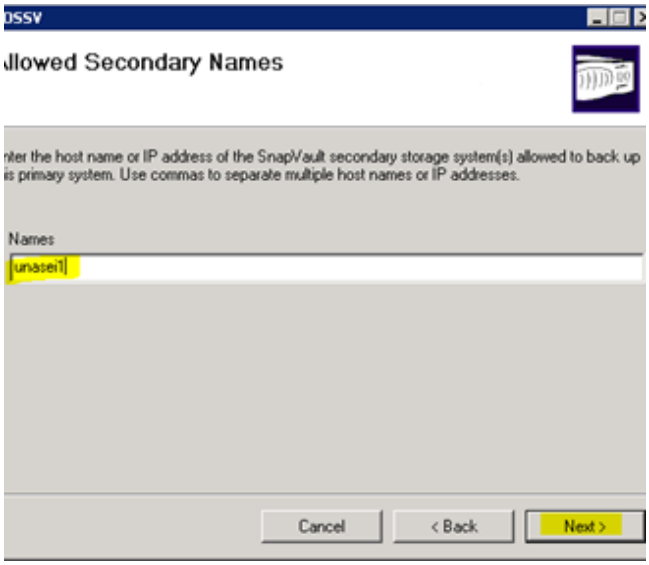
Sur KSXBFHI1, lancer D:\Install\OSSV\ossv\Setup.exe

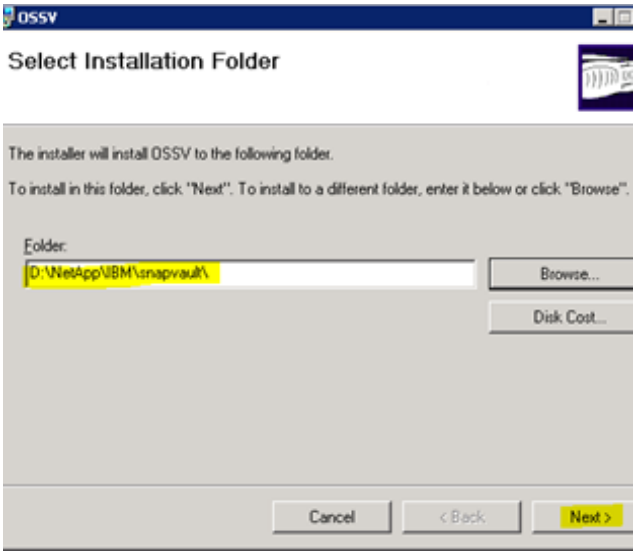


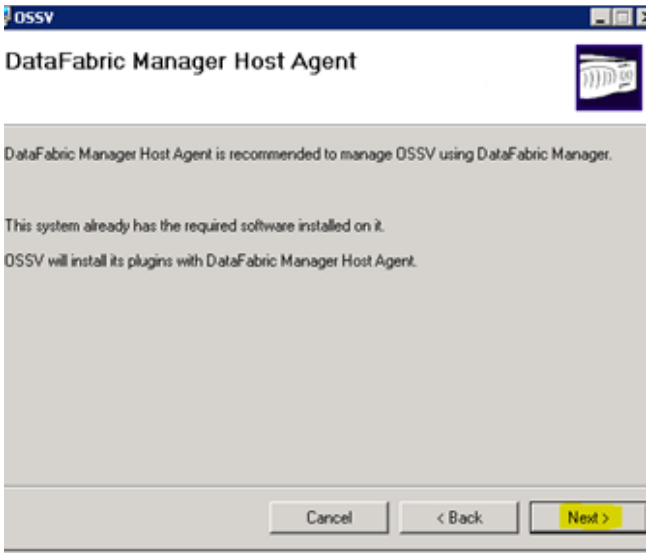


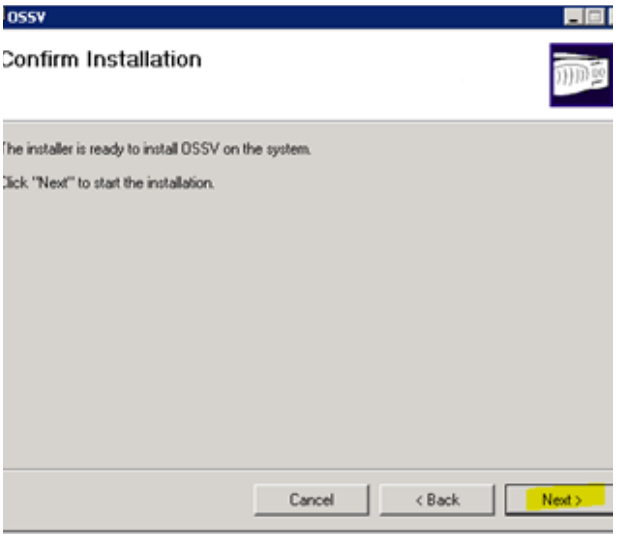


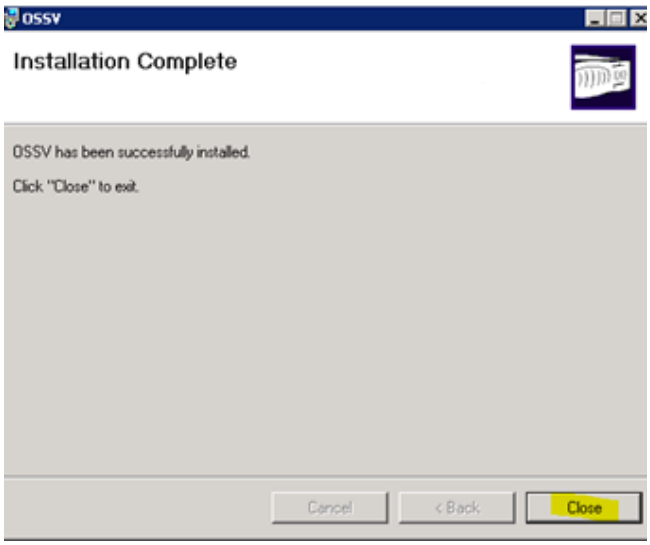



OSSV
llowed Secondary Names
nter the host name or IP address of the SnapVault secondary storage system(s) allowed to back up
is primary system. Use commas to separate multiple host names or IP addresses.
Names
unasei1
Cancel
< Back
Next >


OSSV
Select Installation Folder
The installer will install OSSV to the following folder.
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".
Folder:
D:\NetApp\IBM\snapvault\
Browse...
Disk Cost...
Cancel
< Back
Next >


OSSV
DataFabric Manager Host Agent
DataFabric Manager Host Agent is recommended to manage OSSV using DataFabric Manager.
This system already has the required software installed on it.
OSSV will install its plugins with DataFabric Manager Host Agent.
Cancel
< Back
Next >


OSSV
Confirm Installation
The installer is ready to install OSSV on the system.
Click "Next" to start the installation.
Cancel
< Back
Next >


OSSV
Installation Complete
OSSV has been successfully installed.
Click "Close" to exit.
Cancel
< Back
Close

ANNEXE 10 : Tests du plugin OSSV

```
D:\NetApp\IBM\snapvault\bin>vinstallcheck
'vinstallcheck' is not recognized as an internal or external command,
operable program or batch file.

D:\NetApp\IBM\snapvault\bin>svinstallcheck
SnapVault home directory: 'D:/NetApp/IBM/snapvault'
SnapVault database directory: 'D:\NetApp\IBM\snapvault\db'
SnapVault temporary directory: 'D:\NetApp\IBM\snapvault/tmp'
SnapVault Database and Temporary directories have 61% space left
(25824Mb)
SnapVault service is running
SnapVault listener is running
Snapvault NDMP interface on port 10000:
   Vendor     : Netapp
   Product    : SnapVault
   Version    : 3_0_1_2011FEB22_x64_IBM-RC
   Host       : KSXBFHI1
   Host Id    : 28A74F16DB1327E71013C14351A51E25
   OS Type    : Windows 2008
   OS Version : 6.1
   IPV6       : Ndmp Server is responding correctly
   IPV4       : Ndmp Server is responding correctly
Snapvault QSM interface on port 10566:
   IPV6       : QSM Server is responding correctly
   IPV4       : QSM Server is responding correctly
Validating filesystems:
   Drive 'A:\' is removable, unsuitable for backup
   Drive 'C:\' is suitable for backup
   Drive 'D:\' is suitable for backup
   Drive 'F:\' is suitable for backup
   Drive 'G:\' is suitable for backup
   Drive 'H:\' is suitable for backup
   Drive 'Z:\' is a CDROM, unsuitable for backup
   Mount Point 'D:\Vol\VFUF50_002\DONUTIL\PUBLIC\' is suitable for
backup
   Mount Point 'D:\Vol\VFUF50_018\DONUTIL\PUBLIC\' is suitable for
backup
   Mount Point 'D:\Vol\VFUF50_051\DONUTIL\PUBLIC\' is suitable for
backup
DataFabric Manager Host Agent is installed on this system.
   Install Location : D:\NetApp\IBM\Agent\
   Version :    DataFabric Manager Host Agent version 2.7 (2.7.0.2203)
   Agent Core Library version 2.7 (2.7.0.2203)
   Status : Running
ChangeLog Filter Driver is installed and is unloaded.

Check Succeeded
```

ANNEXE 11 : Matrice Compatibilité FalconStor CDP

FalconStor NSS/CDP Clients

The following is a list of operating systems that have been certified to run FalconStor NSS/CDP clients:

Platform	Certified Versions
FalconStor NSS/CDP Client using Fibre Channel protocol	
AIX	- AIX 4.3.3.x - AIX 5.1 - AIX 5.2 - AIX 5.3 - AIX 6.1 - AIX 7.1 - Virtual I/O Server 2.2 - Requires FalconStor DynaPath for failover.
Citrix XenServer	- XenServer 4.1.0 / 5.0.0 / 5.5.0 / 5.6.0 / 6.1 - Certified as "Citrix Ready"
HP-UX	- HP-UX 11.00, HP-UX 11i, HP-UX 11iv2 - Requires FalconStor DynaPath for failover. - HP-UX 11iv3 - Uses native multipathing software instead of FalconStor DynaPath
HP Tru64 UNIX	5.1.A with Compaq KGPSA-CX FC Adapter (FW rev 6.0) or Compaq KGPSA-C FC Adapter (FW rev 6.0)
Linux	- Linux 2.4 and 2.6 kernels from Red Hat distributions - Linux 2.4, 2.6, and 3.0 from SUSE distributions - Uses FalconStor DynaPath, if available, or Linux native multipathing software, for failover
Macintosh	9.1 or OSX with ATTO ExpressPCI FC SW HBA.
NetWare	- NetWare 6.5 with SP 1
SCO OpenServer	SCO OpenServer 5
SGI IRIX	IRIX v6.5 with Irix v6.5.7f or QLogic 2200 (the Fibre Channel driver is bundled with the IRIX operating system)
Solaris	**SPARC:** - Solaris 10 - Solaris 9 Generic with kernel patch level 112233-04 - Requires FalconStor DynaPath for failover. **Intel:** - Solaris 10 - Solaris 9 Generic with kernel patch level 112233-04
VMware vSphere 4	- CDP/NSS 6.15 with clients running ESX 4.1, 4.0 and ESXi 4.1 - ESXi 4.1 storage arrays and storage gateways (SVD) certified as "VMware Ready"
VMware vSphere 5	- CDP/NSS 6.15 with clients running ESXi 5.1/5.0 without VAAI - CDP/NSS 7.00 with clients running ESXi versions 5.5, 5.1 (including update 1), 5.0 (including updates 3, 2, and 1) - CDP/NSS 7.50 with clients running ESXi version 5.5, 5.1 (including update 1) - ESXi 5.5/5.1/5.0 storage arrays and storage gateways (SVD) certified as "VMware Ready" for CDP/NSS 7.00 and 6.15

VMware vCenter Site Recovery Manager (SRM) v4	FalconStor Storage Replication Adapter (SRA) v1.10 build 111 certified for VMware vCenter Site Recovery Manager 4.0
VMware vCenter Site Recovery Manager (SRM) v5	FalconStor Storage Replication Adapter (SRA) v5.0 build 5023 certified for VMware vCenter Site Recovery Manager 5.0
Windows 2003	- Windows Server 2003 (32-bit and 64-bit) - Windows Server 2003 R2 (32-bit and 64-bit) - Requires FalconStor DynaPath for MPIO and failover
Windows 2008	- Windows Server 2008 (32-bit and 64-bit) - Windows Server 2008 R2 (64-bit) - Windows Server 2008 with Hyper-V (64-bit) - Windows Server 2008 R2 with Hyper-V (64-bit) - Requires FalconStor DynaPath for MPIO and failover
Windows 2012	- Windows Server 2012 - Windows Server 2012 R2 - Windows Server 2012 with Hyper-V - Windows Server 2012 R2 with Hyper-V - Requires FalconStor DynaPath for MPIO and failover
FalconStor NSS/CDP Client using iSCSI protocol	
AIX	- 4.3.3.x - 5.2 - 5.3 - 6.1
Citrix XenServer	- XenServer 4.1.0 / 5.0.0 / 5.5.0 / 5.6.0 / 6.1 - Certified as "Citrix Ready"
HP-UX	B.11.11
Linux	Linux 2.4 and 2.6 kernels from Red Hat and SUSE distributions
NetWare	- NetWare 6.5 with SP 1a
Solaris SPARC	- Solaris 10 - Solaris 9
VMware vSphere 4	- CDP/NSS 6.15 with clients running ESX 4.0, 4.1, and ESXi 4.1 - ESXi 4.1 storage arrays and storage gateways (SVD) certified as "VMware Ready"
VMware vSphere 5	- CDP/NSS 6.15 with clients running ESXi 5.1/5.0 without VAAI - CDP/NSS 7.00 with clients running ESXi versions 5.5, 5.1 (including update 1), 5.0 (including updates 3, 2, and 1) - CDP/NSS 7.50 with clients running ESXi version 5.5, 5.1 update 1, 5.1 - ESXi 5.5/5.1/5.0 storage arrays and storage gateways (SVD) certified as "VMware Ready" for CDP/NSS 7.00 and 6.15
VMware vCenter Site Recovery Manager (SRM) v4	FalconStor Storage Replication Adapter (SRA) v1.10 build 111 certified for VMware vCenter Site Recovery Manager 4.0
VMware vCenter Site Recovery Manager (SRM) v5	FalconStor Storage Replication Adapter (SRA) v5.0 build 5023 certified for VMware vCenter Site Recovery Manager 5.0
Windows XP Professional	With SP 1 or above
Windows 2003	- Windows Server 2003 (32-bit and 64-bit) - Windows Server 2003 R2 (32-bit and 64-bit)
Windows 2008	- Windows Server 2008 (32-bit and 64-bit) - Windows Server 2008 R2 (64-bit) - Windows Server 2008 with Hyper-V (64-bit) - Windows Server 2008 R2 with Hyper-V (64-bit)
Windows 2012	- Windows Server 2012 - Windows Server 2012 R2 - Windows Server 2012 with Hyper-V - Windows Server 2012 R2 with Hyper-V

FalconStor CDP Client Protection

Platform	Requires
AIX	FalconStor FileSafe or AIX Logical Volume Manager
HP-UX	FalconStor FileSafe or HP-UX Logical Volume Manager
Oracle Linux	- DiskSafe does not support Oracle Unbreakable Enterprise Linux kernel (not RHEL compatible) - DiskSafe does support Oracle Enterprise Linux Kernel (RHEL binary compatible)
Red Hat Linux	FalconStor DiskSafe, FalconStor FileSafe, or Linux Volume Manager 2 (LVM2)
Solaris	FalconStor FileSafe or Solaris Volume Manager (SVM)
SUSE Linux	FalconStor DiskSafe, FalconStor FileSafe, or Enterprise Volume Management System (EVMS)
VMware vSphere	FalconStor DiskSafe running in a virtual machine or using a direct connection for data recovery with ESXi 5.5, ESXi 5.1 (including update 1), 5.0 (including updates 3, 2, and 1), 4.0
Windows	FalconStor DiskSafe, FalconStor FileSafe

ANNEXE 12 : Installation Appliance FalconStor CDP

ACTIONS	ILLUSTRATIONS
Pré installation	
Affichage des disques Lancement fdisk : ☞ sudo fdisk /dev/sda" Liste des partitions ☞ taper "p" puis "↵ "	[harfouka2@stoeitc1 ~]$ sudo fdisk /dev/sda WARNING: DOS-compatible mode is deprecated. It's strongly recommended switch off the mode (command 'c') and change display units to sectors (command 'u'). Command (m for help): p Disk /dev/sda: 599.9 GB, 599932844032 bytes 255 heads, 63 sectors/track, 72937 cylinders Units = cylinders of 16065 * 512 = 8225280 bytes Sector size (logical/physical): 512 bytes / 512 bytes I/O size (minimum/optimal): 262144 bytes / 524288 bytes Disk identifier: 0x9d4636f9 Device Boot Start End Blocks Id System /dev/sda1 * 1 33 262144 83 Linux Partition 1 does not end on cylinder boundary. /dev/sda2 33 72938 585608192 8e Linux LVM Partition 2 does not end on cylinder boundary.
Suppression de la 1ère partition: ☞ taper "d" puis "↵ " ☞ taper "1" puis "↵ " Suppression de la 2e partition: ☞ taper "d" puis "↵ " Lister les partitions : ☞ taper "p" puis "↵ " Enregistrer les modifications : ☞ taper "w" puis "↵ "	Command (m for help): d Partition number (1-4): 1 Command (m for help): d Selected partition 2 Command (m for help): p Disk /dev/sda: 599.9 GB, 599932844032 bytes 255 heads, 63 sectors/track, 72937 cylinders Units = cylinders of 16065 * 512 = 8225280 bytes Sector size (logical/physical): 512 bytes / 512 bytes I/O size (minimum/optimal): 262144 bytes / 524288 bytes Disk identifier: 0x9d4636f9 Device Boot Start End Blocks Id System Command (m for help): w The partition table has been altered! Calling ioctl() to re-read partition table. WARNING: Re-reading the partition table failed with error 16: Device or busy. The kernel still uses the old table. The new table will be used at the next reboot or after you run partprobe(8) or kpartx(8) Syncing disks.

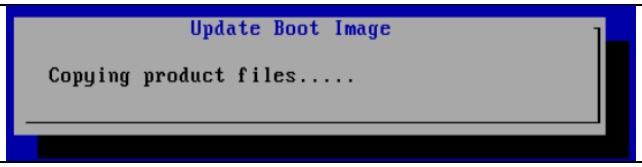
Montage du disque de démarrage FalconStor CDP : ☞ Sélectionner "Virtual Drives" ☞ puis "Image File "	
☞ Sélectionner le fichier de démarrage ☞ Cliquer sur "ouvrir"	
Redémarrer le serveur Sudo reboot	

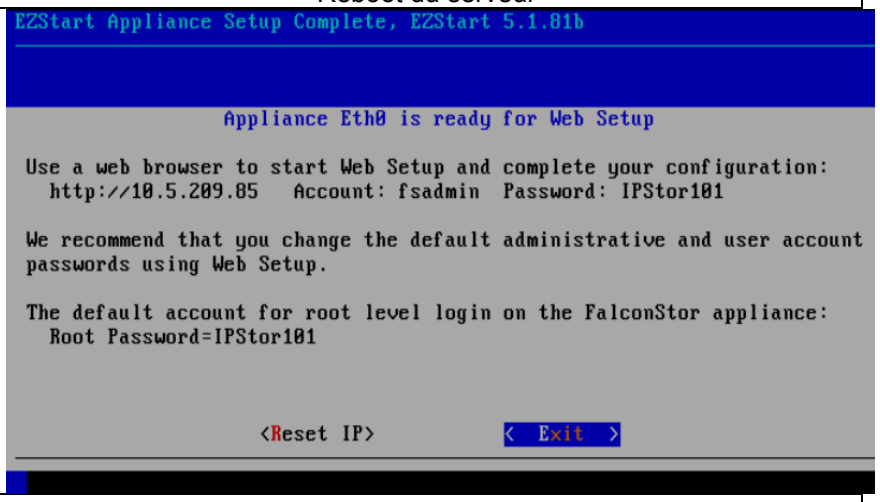
Installation	
Le serveur démarre sur le disque d'installation FalconStor CDP	FalconStor EZStart Installation Utility v5.1.81 Loading.....
☞ Cliquer sur "OK"	Power Switch Virtual Drives Keyboard Help FalconStor EZStart 5.1.81b - Installation Utility Installation Summary This utility performs the following action: Installation Operating System : Enterprise Linux 5U7 Product : CDP V7.00 B7088 Package : IPStor Select <OK> to continue, or select <Cancel> to abort the operation. Press [Tab] to switch and [Enter] to select. < OK > <Cancel>
☞ Cliquer sur "OK"	Detect Controllers Detecting SCSI and Ethernet controllers. Please stand by..... Power Switch Virtual Drives Keyboard Help FalconStor EZStart 5.1.81b - Installation Utility Detect Hardware The following hardware has been detected: Manufacturer : HP Model : ProLiant DL360p Gen8 Storage Controller : 1. Hewlett-Packard Company Device 323b (1 Adapter) This utility extracts the boot image onto the first controller. Select <OK> to continue. < OK >

☞ Cliquer sur "OK"	Detect Drives Detecting the boot drive and partitions. Please stand by..... Detect RAID Configuration An existing RAID configuration has been detected. Select <OK> to install the boot image on the detected LUN. Select <Cancel> to abort the installation. < OK > <Cancel>
☞ Cliquer sur "Yes"	Change Host Name The default host name is "FS5U7HPCDP064" Do you want to change the host name? Press [Tab] to switch and [Enter] to select. < Yes > < No >
☞ Définition du nom du serveur	Change Host Name The default host name is "FS5U7HPCDP064" Enter new host name and select OK or Cancel to keep default host name Press [Tab] to switch and [Enter] to select. stoeitc1 < OK > <Cancel>
☞ Cliquer sur "Yes"	Configure Network Settings Eth0 Do you want to change eth0 IP address? Select <No> to keep using the default IP address. Press [Tab] to switch and [Enter] to select. < Yes > < No >

☞ Définir l'adresse IP du serveur	Configure Eth0 IP Enter a new IP for eth0 in the format xxx.xxx.xxx.xxx and select OK to confirm. Cancel to keep using the default IP address. Press [Tab] to switch and [Enter] to select. 10.5.209.85_ < OK > <Cancel>
☞ Définir les paramètres réseau	Verify eth0 Network Parameters Select Save and <OK> to confirm your changes. Select <Abort> to keep the default eth0 IP address Use [UP/DOWN] arrow keys to select a parameter to modify, [Enter] to select the menu option. Save — Save changes IP-Change — 10.5.209.85 Netmask-Change — 255.255.255.0 Gateway-Change — 10.5.209.1 < OK > <Abort>
☞ Cliquer sur "No"	Storage Cluster Interlink (SCI) Port Settings ifcfg-sci0 Two network ports must be dedicated for the Storage Cluster Interlink (SCI) between servers in the new high availability scheme, which provides faster failover and recovery. The SCI must be on an isolated subnet. Do you want to change ifcfg-sci0 IP address? Select <No> to keep using the default IP address. Press [Tab] to switch and [Enter] to select. < Yes > < No >
☞ Cliquer sur "Cancel"	Power Switch Virtual Drives Keyboard Help Configure Network Settings Configure IPMI Management Port IP Address Intelligent Platform Management Interface configuration Enter a new IPMI address for Management port in the format xxx.xxx.xxx.xxx and select <OK> to confirm. Select <Cancel> to use the default or current IP address (10.5.24.27). Note: This IP address must be different than eth0. Current eth0 IP address: 10.5.209.85. Press [Tab] to switch and [Enter] to select. < OK > <Cancel>

☞ Cliquer sur "Europe" ☞ Cliquer sur "OK"	Select a Location Select one of the following locations. Use the [UP/DOWN] arrow keys to change your selection. Select <OK> to confirm your selection. Select <Next> for the other locations. 0 Current time zone (America/New_York) 1 US --> 2 America --> 3 Europe --> 4 Canada --> 5 Indian Ocean --> 6 Pacific Ocean --> 7 Africa --> 8 Arctic Ocean --> 9 Asia --> 10 Atlantic Ocean --> 11 Australia --> < OK > < Next >
☞ Sélectionner "Copenhagen" ☞ Cliquer sur "OK"	Select a Time Zone Region Select one of the following time zone regions. Use the [UP/DOWN] arrow keys to change your selection. Select <OK> to confirm your selection. Select <Next> for the other time zone regions. 0 Amsterdam 1 Andorra 2 Athens 3 Belfast 4 Belgrade 5 Berlin 6 Bratislava 7 Brussels 8 Bucharest 9 Budapest 10 Chisinau 11 Copenhagen Main Menu < OK > < Next >
	Extract Boot Image The boot image is being extracted from the USB key to the boot drive on the appliance. This may take a few minutes. 100% Verify Boot Image Verifying the boot image..... Update Boot Image Copying Web Setup.....

<table>
<tr><td></td><td> 
</td></tr>
<tr><td></td><td>Reboot du serveur</td></tr>
<tr><td>☞ Noter les identifiants de connexion

☞ Cliquer sur "Exit"</td><td> 
</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Vérifications</td></tr>
<tr><td></td><td></td></tr>
<tr><td>☞ Connectez-vous sur l'appliance en tant que "root"

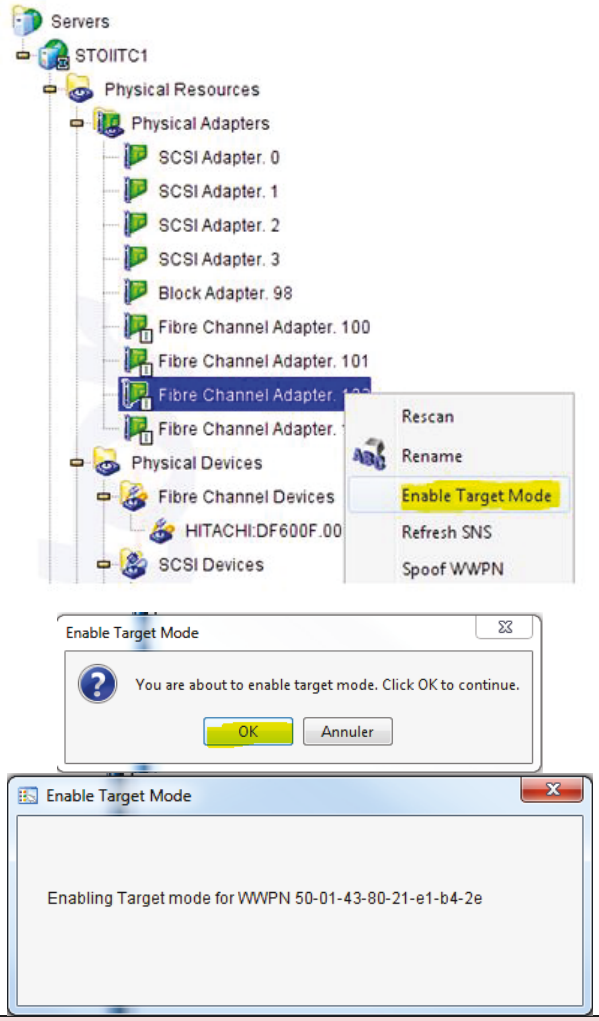
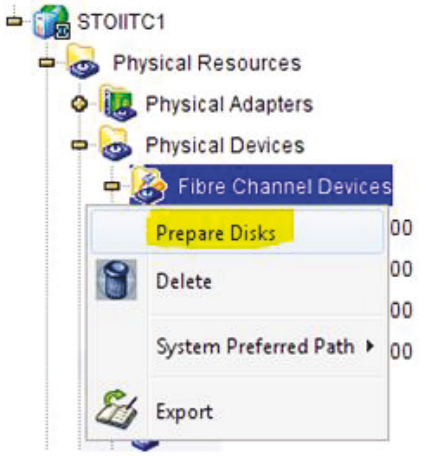
☞ Lancer la commande : "ipstor status"

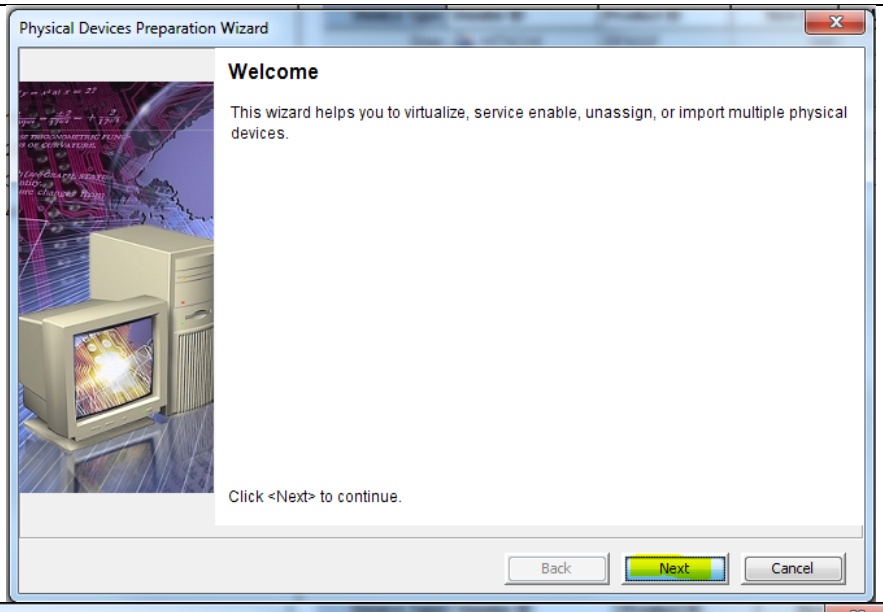
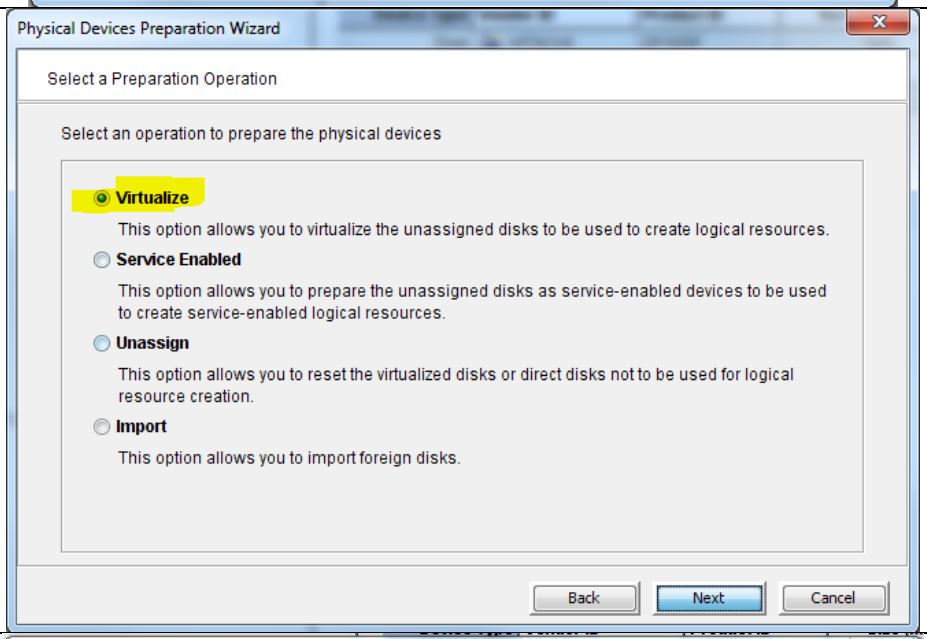
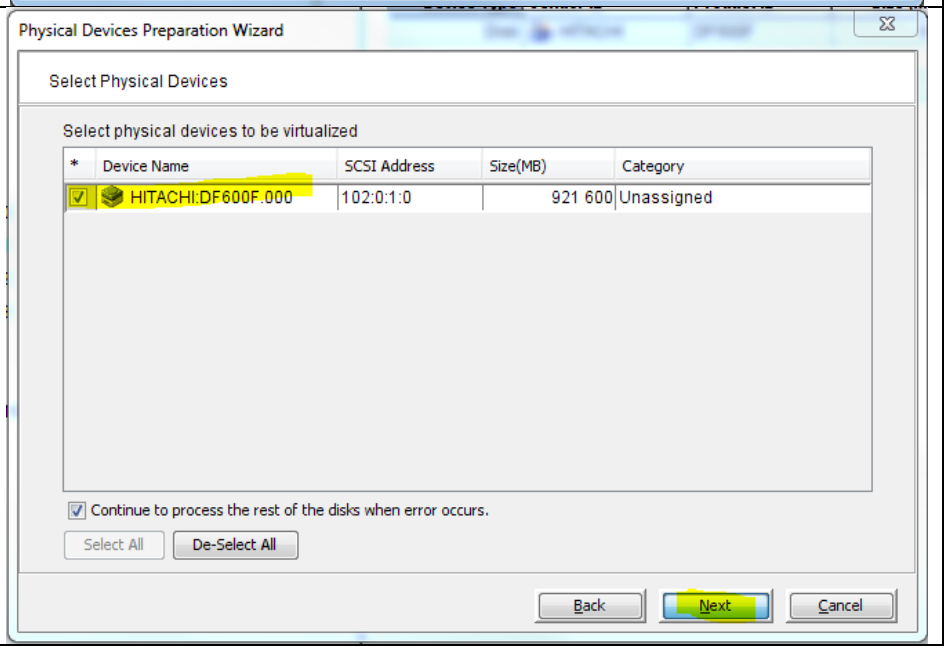
☞ Vérifier que tous les modules soient dans l'état "RUNNING"</td><td>

```
Usage: /usr/local/ipstor/bin/ipstor <start|stop|restart|status>
[root@stoeitc1 ~]#
[root@stoeitc1 ~]#
[root@stoeitc1 ~]#
[root@stoeitc1 ~]# ipstor status

FalconStor IPStor Server  version 7.00 (Build 7088)

Status of IPStor SNMPD Module                          [RUNNING]
Status of IPStor Configuration Module                  [RUNNING]
Status of IPStor Base Module                           [RUNNING]
Status of IPStor HBA Module                            [RUNNING]
Status of IPStor Authentication Module                 [RUNNING]
Status of IPStor Block Device Module                   [RUNNING]
Status of IPStor Server (FSNBase) Module               [RUNNING]
Status of IPStor Server (Application)                  [RUNNING]
Status of IPStor Server (Upcall) Module                [RUNNING]
Status of IPStor Target Module                         [RUNNING]
Status of IPStor Communication Module                  [RUNNING]
Status of IPStor CLI Proxy Module                      [RUNNING]
Status of IPStor Logger Module                         [RUNNING]
Status of IPStor Central Client Manager Module         [RUNNING]
Status of IPStor Self Monitor Module                   [RUNNING]
[root@stoeitc1 ~]#
```

</td></tr>
</table>

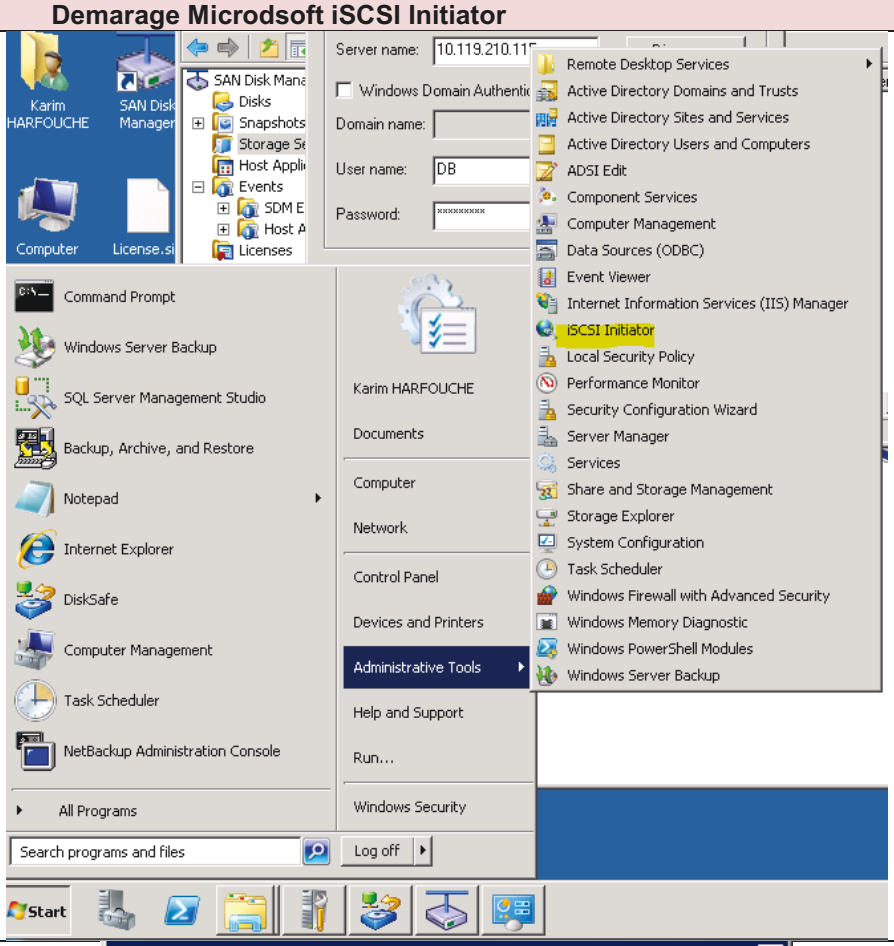
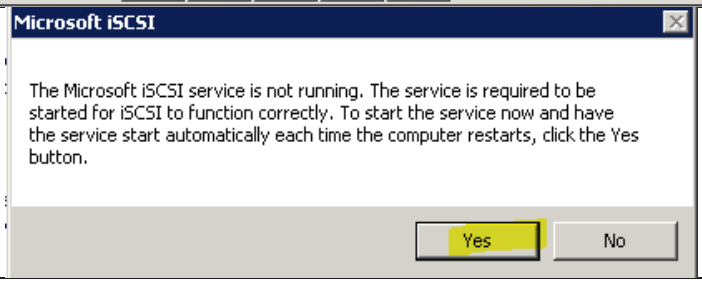
ANNEXE 13 : Paramétrage Appliance FalconStor

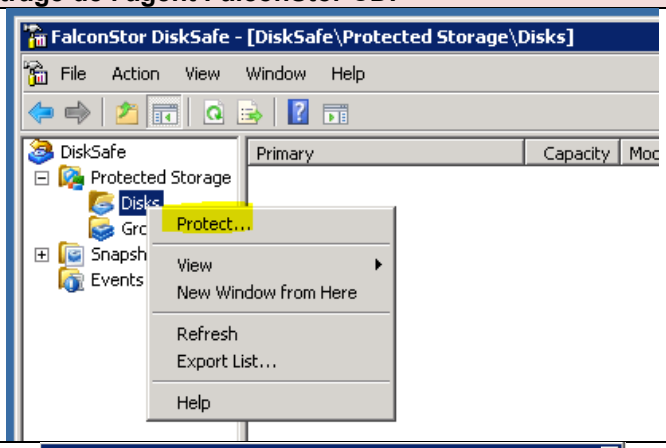
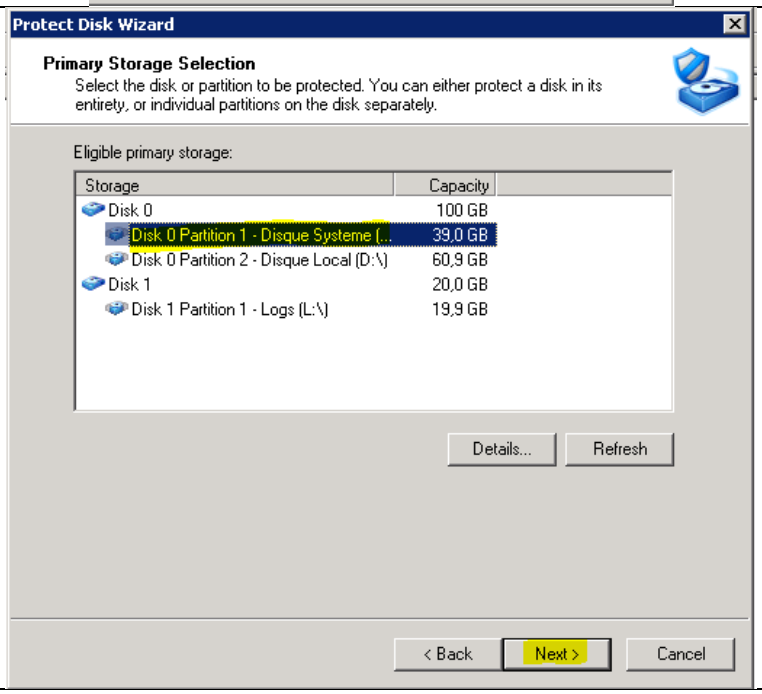
ACTIONS	ILLUSTRATIONS
Activer les ports SAN mode cible : ☞ "Clic droit" sur "FC Adapter" ☞ Cliquer sur "OK" Répéter l'opération sur les autres ports FC	
Préparation du storage	
☞ Faire un "Clic droit" sur "Fibre Channel Devices" ☞ Sélectionner "Prepare Disks"	

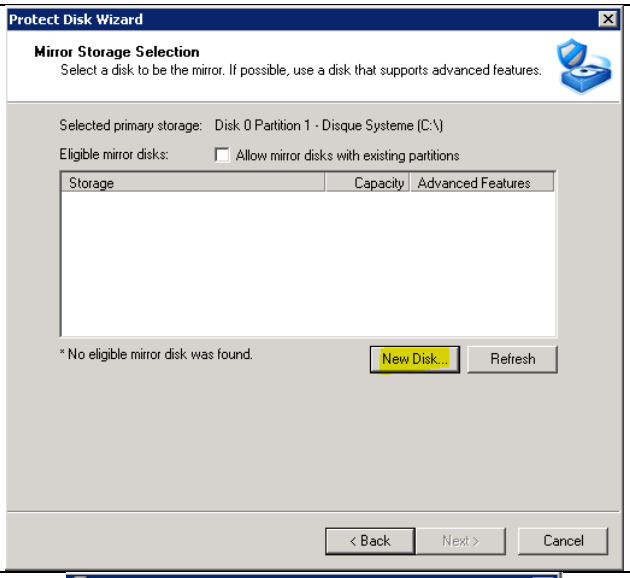
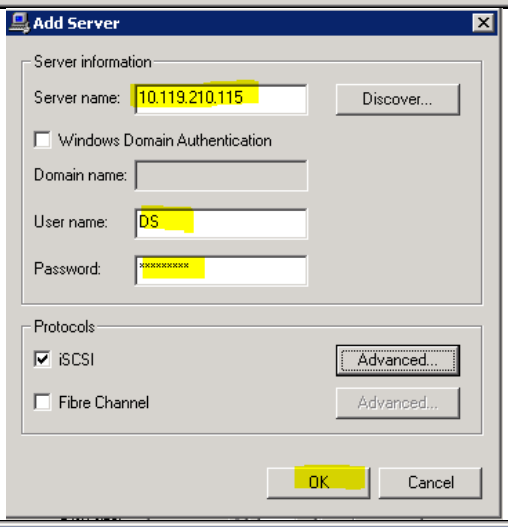
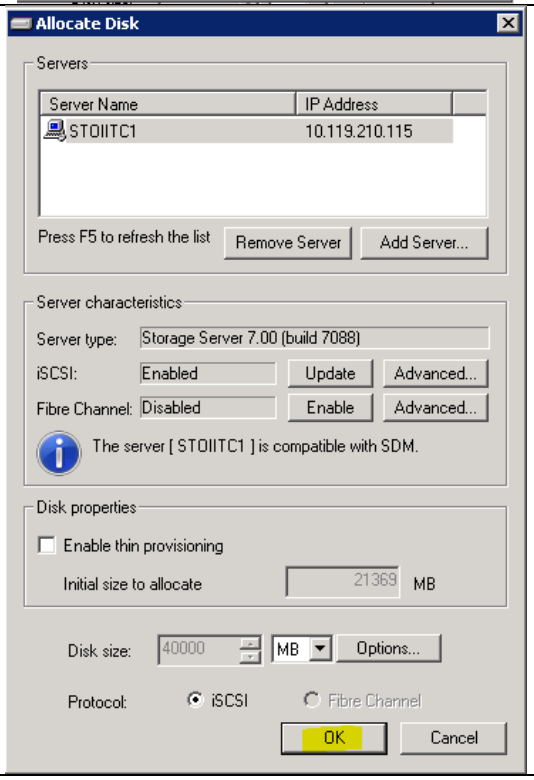
☞ Cliquer sur "Next"	
☞ Sélectionner "Virtualize" ☞ Cliquer sur "Next"	
☞ Sélectionner le LUN disponible ☞ Cliquer sur "Next"	

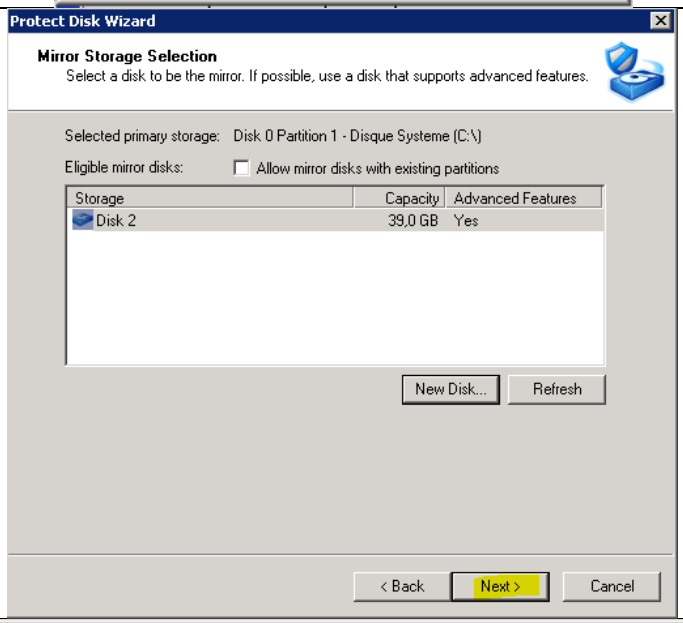
☞ Cliquer sur "Finish"	Physical Devices Preparation Wizard Prepare Disks Selected physical devices for disk preparation. Device Name: HITACHI:DF600F.000 — SCSI Address: 102:0:1:0 — Size(MB): 921 600 — Category: Unassigned **The selected physical devices will be virtualized. If error occurs, the operation will continue.** Click <Finish> to start disk preparation. Back — Finish — Cancel
☞ Saisir "YES" ☞ Cliquer sur "OK"	Physical Devices Preparation Wizard **WARNING!** Valid partition table exists on the following disks. Continuing with this operation will result in irreversible loss of data. Type YES and click OK if you are absolutely sure you wish to proceed. - 102 : 0 : 1 : 0 Type YES to confirm: YES OK — Cancel
☞ Cliquer sur "OK"	Physical Devices Preparation Status Physical devices have been virtualized. Device Name: HITACHI:DF600F.000 — SCSI Address: 102:0:1:0 — Size(MB): 921 593 — Status: Successful OK
Le LUN apparaît dans la rubrique "Fibre Channel Devices".	Physical Devices Fibre Channel Devices HITACHI:DF600F.000 (102:0:1:0) SCSI Devices

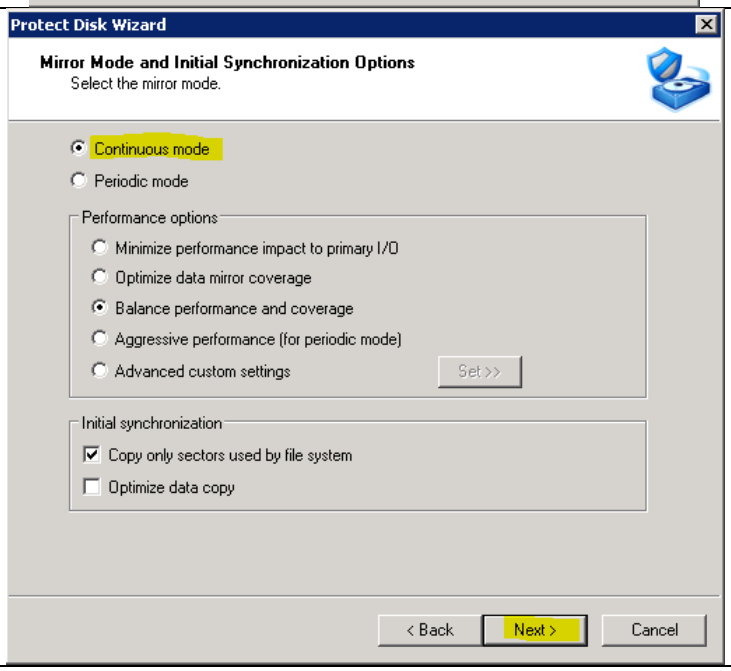
ANNEXE 14 : Procédure Installation FalconStor Windows Agent

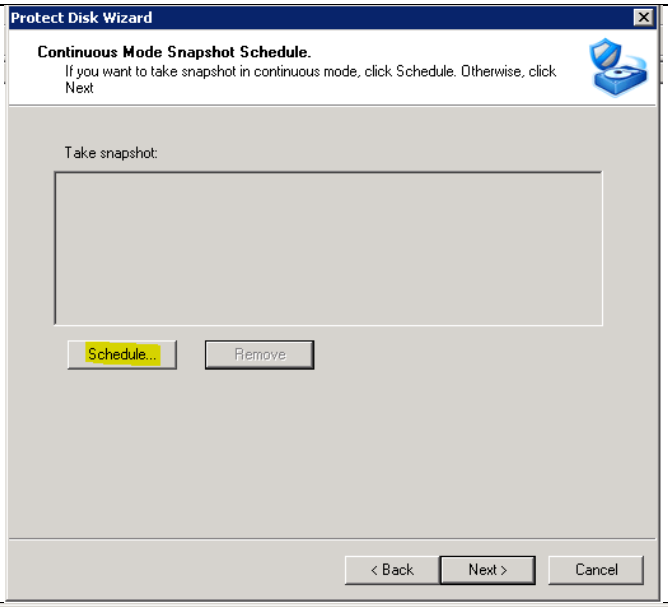
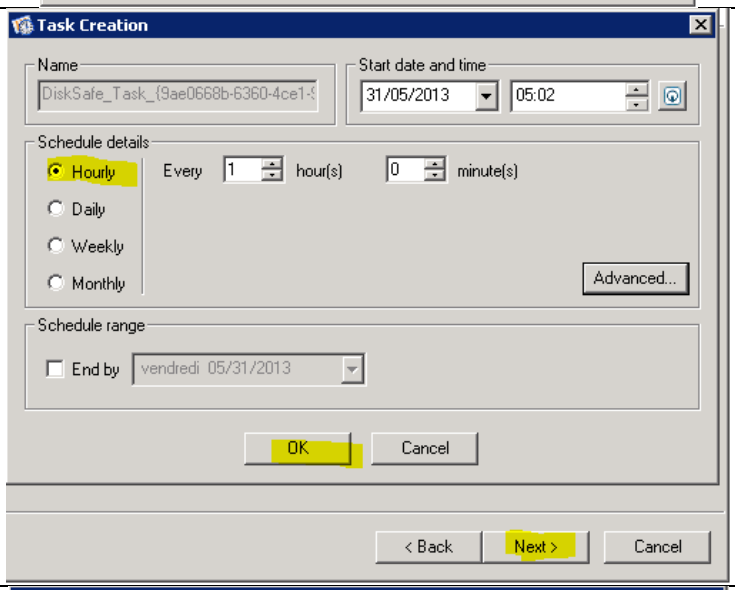
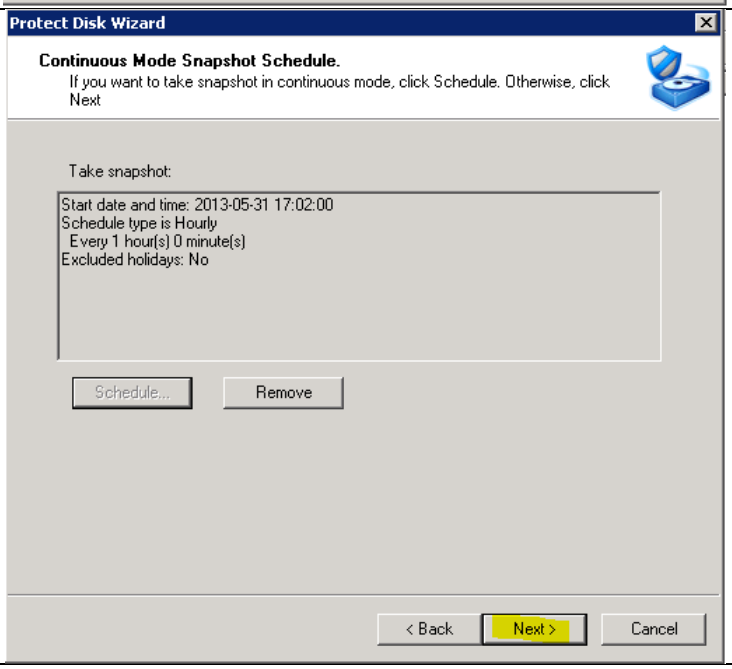
ACTIONS	ILLUSTRATIONS
Demarage Microdsoft iSCSI Initiator	
☞ Cliquer sur : "Start" ☞ Cliquer sur : "Administrative Tools" ☞ Cliquer sur : " iSCSI Initiator "	
☞ Cliquer sur "Yes"	

Paramétrage de l'agent FalconStor CDP	
☞ Faire un "Clic droit" sur : "Disks" ☞ Cliquer sur "Protect"	
☞ Cliquer sur "Next"	
☞ Sélectionner le disque à protéger ☞ Cliquer sur "Next"	

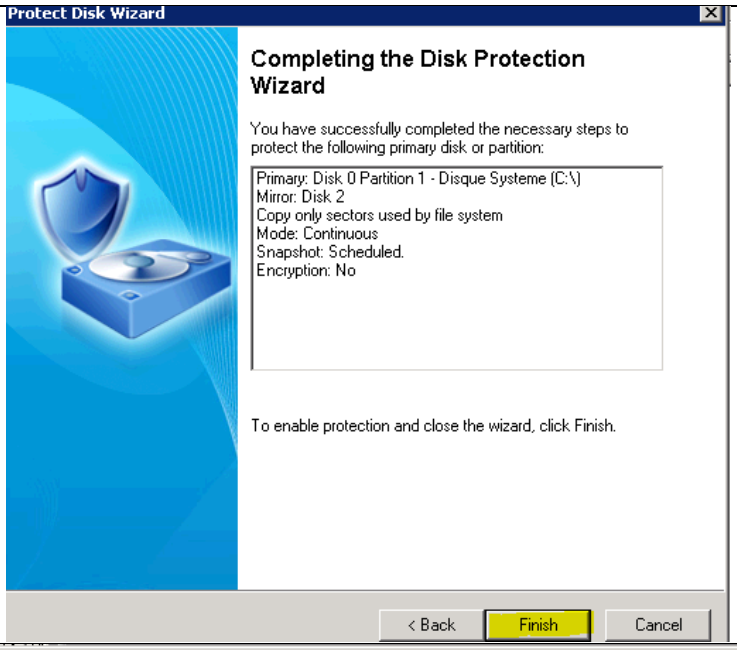
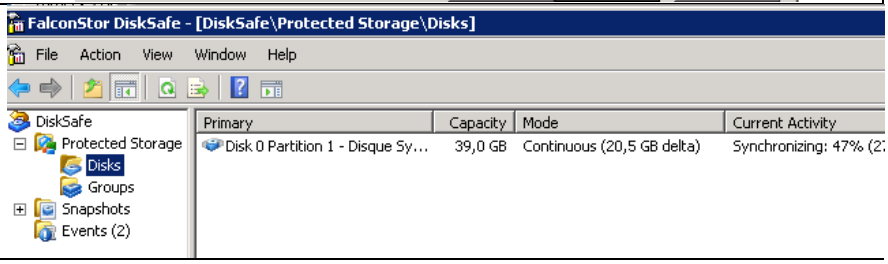
☞ Cliquer sur "New Disk"	
Connexion de l'agent DiskSafe à l'IpStor ☞ Saisir l'adresse IP de "IPStor" ☞ Saisir les identifiants de connexion de l'IPStor ☞ Cocher la case "iSCSI" ☞ Cliquer sur "OK"	
☞ Cliquer sur "OK"	

<table>
<tr><td></td><td>
</td></tr>
<tr><td>☞ Cliquer sur "Next"</td><td> 
</td></tr>
<tr><td>☞ Cliquer sur "Continuous mode"

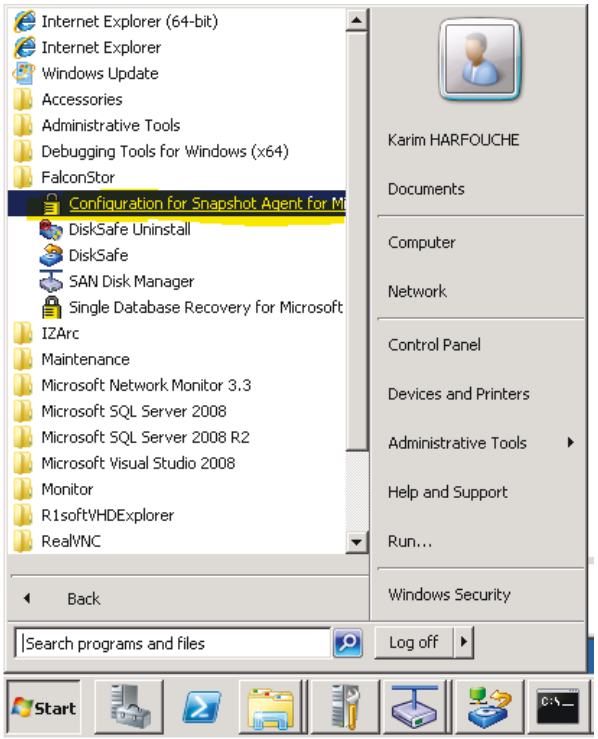
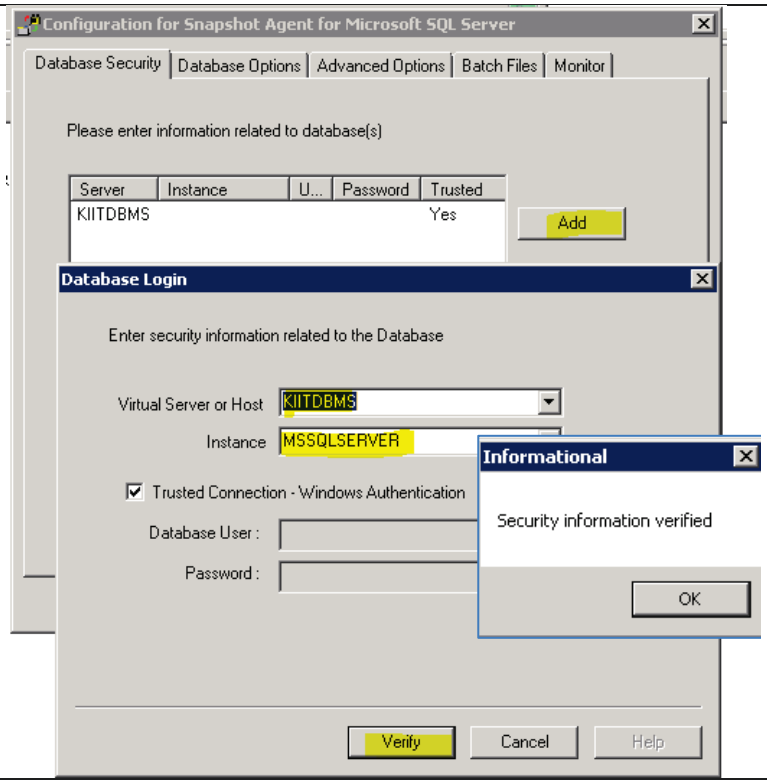
☞ Cliquer sur "Next"</td><td> 
</td></tr>
</table>

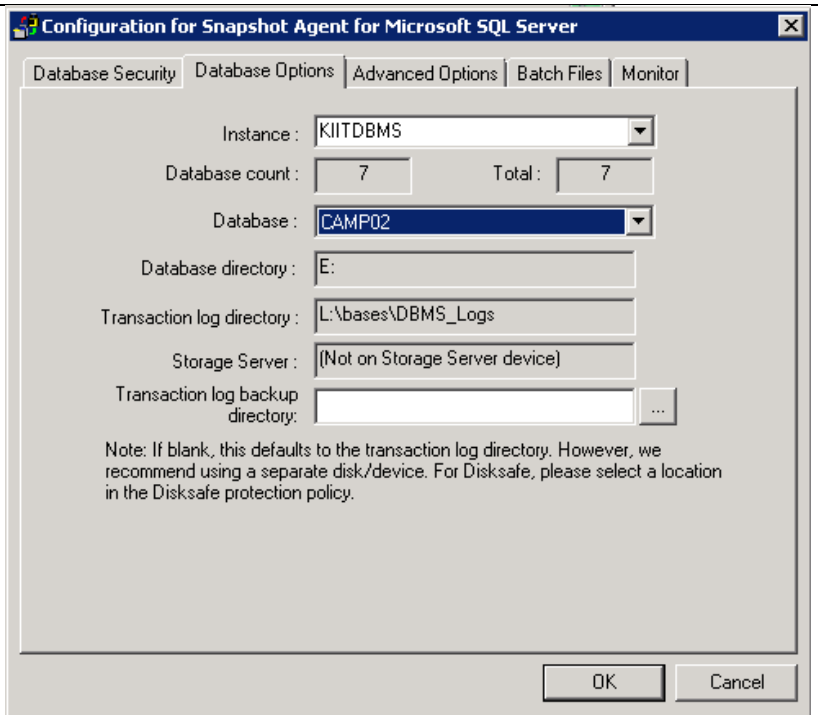
☞ Cliquer sur "Schedule"	
☞ Sélectionner sur "Hourly" ☞ Cliquer sur "OK"	
☞ Cliquer sur "Next"	

☞ Cliquer sur "Next"	Protect Disk Wizard **Advanced Synchronization Options** Specify advanced synchronization options here or click Next to accept the default settings. ☐ Optimize data copy during synchronizations ☐ Limit I/O throughput generated (KB/s): ☑ If synchronization fails, retry for every: 1 min ☐ Perform synchronization when the new/changed data exceeds (MB) ☐ Suspend I/O when mirror disk throughput deteriorates Acceptable throughput (KB/s): Set >> Deterioration threshold to suspend I/O: 1% ☐ Encrypt mirror disk Encryption key: Change... Number of outstanding I/Os for synchronization 1 < Back Next > Cancel
☞ Cliquer sur "OK"	**Advanced Snapshot Retention** Specify the day or time of the snapshot to retain for each level. For multiple snapshots taken within an hour, keep the snapshot nearest to this minute: 0 (0 ~ 59) For multiple snapshots taken within a day, keep the snapshot nearest to this hour: 0 (0 ~ 23) For multiple snapshots taken within a week, keep the snapshot nearest to this day of the week: Saturday For multiple snapshots taken within a month, keep the snapshot nearest to this day of the month: 31 (1 ~ 31) OK
☞ Cliquer sur "Next"	Protect Disk Wizard **Advanced Snapshot Options** Change default snapshot options and specify a Snapshot Retention Policy, or select Next to accept the default settings. ☐ Take a temporary snapshot before each synchronization to recover the mirror in case of failure. The temporary snapshot is automatically deleted after successful synchronization ☑ Invoke snapshot agents every 1 scheduled snapshot(s) Snapshot Retention Policy Determine which snapshots to keep over time. ○ Keep the latest 255 snapshots ◉ Keep a specified number of snapshots for each level Hours 24 Days 14 Weeks 4 Months 1 Advanced < Back Next > Cancel

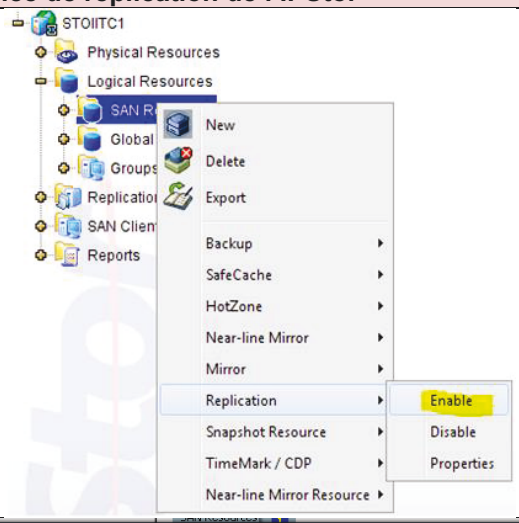
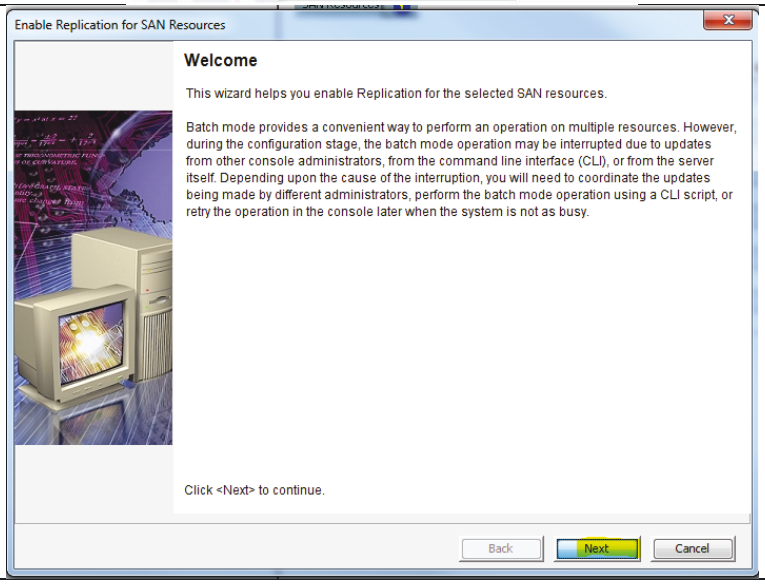
☞ Cliquer sur "Finish"	
La protection du disque est en place et se synchronise…	

ANNEXE 15 : Paramétrage de l'agent FalconStor pour Microsoft SQL Server

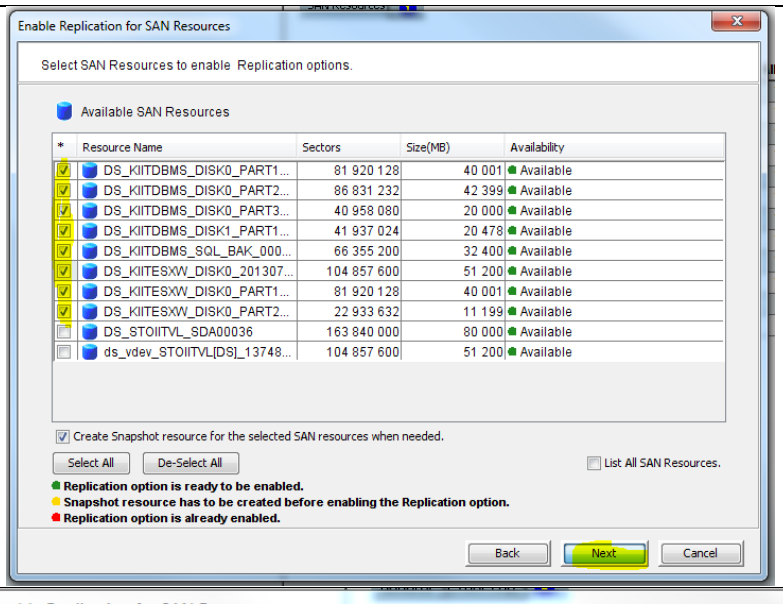
ACTIONS	ILLUSTRATIONS
Paramétrage	
Lancement de l'application de configuration ☞ Cliquer sur "Start" ☞ Cliquer sur "Configuration for Snapshot Agent for Microsoft SQL Server"	
☞ Saisir le nom du serveur MS SQL ☞ Indiquer le nom de l'instance SQL ☞ Cocher la case : "Trusted Connection" ☞ Cliquer sur "Verify" ☞ Cliquer sur "OK" pour fermer la fenêtre	

☞ Vérifier les paramètres de la base de données dans l'onglet "Database Options"	

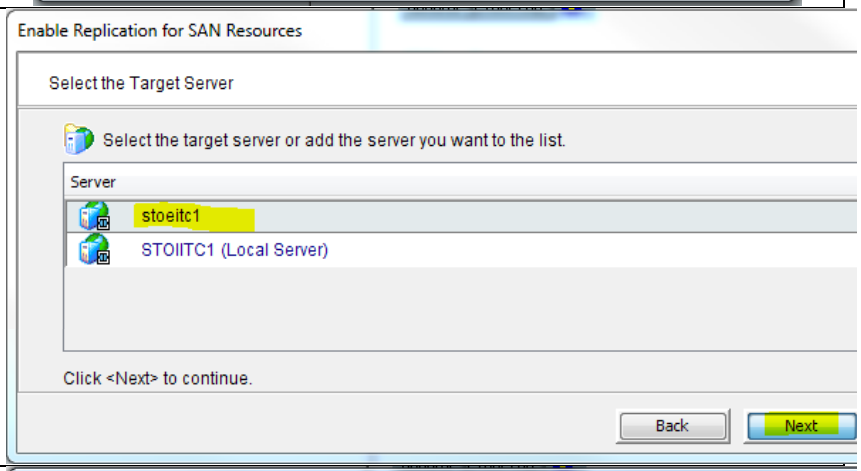
ANNEXE 16 : Procédure Paramétrage Replication FalconStor

ACTIONS	ILLUSTRATIONS
Activation du service de réplication de l'IPStor	
☞ Cliquer sur "SAN Ressource" ☞ Cliquer sur "Enable" dans la section "Replication"	
☞ Cliquer sur "Next"	

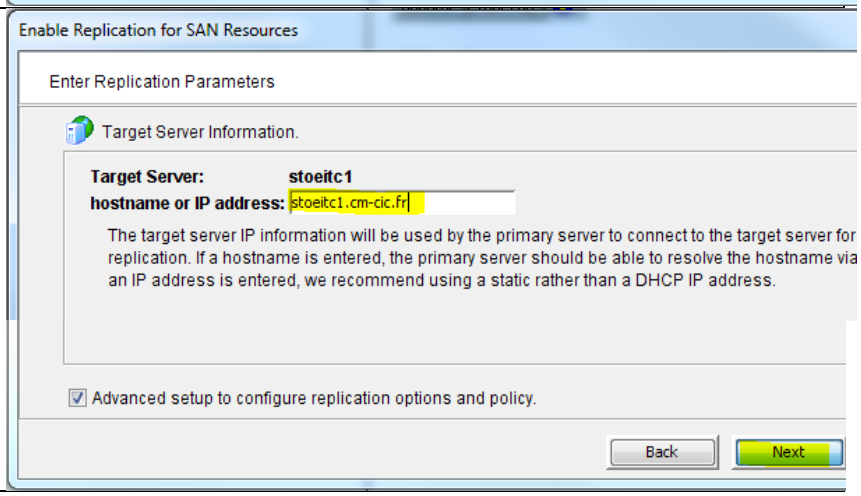
- Sélectionner les LUN à répliquer"
- Cliquer sur "Next"



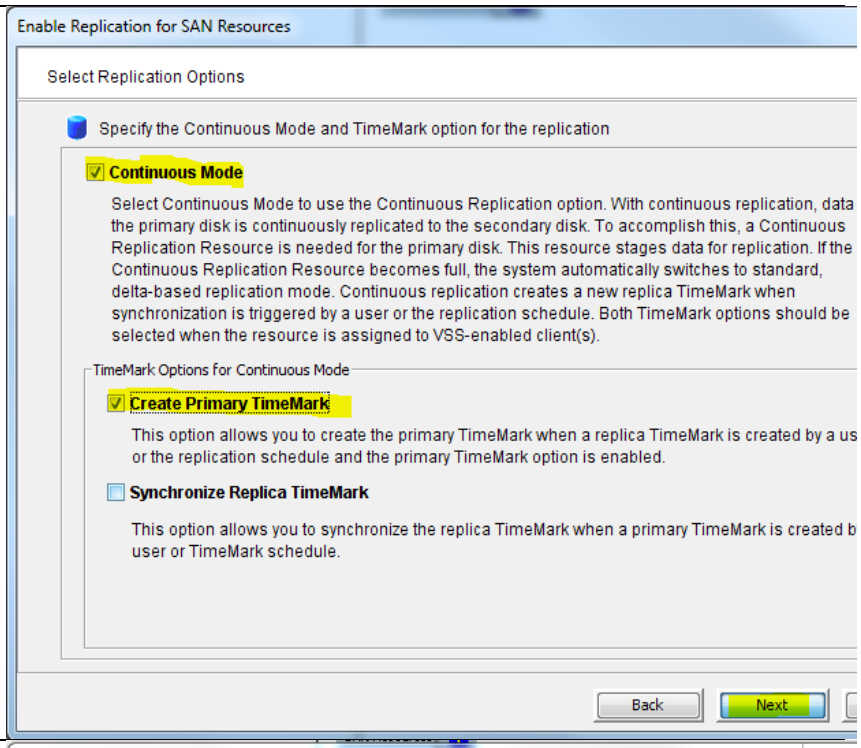
- Sélectionner l'appliance FalconStor CDP cible
- Cliquer sur "Next"



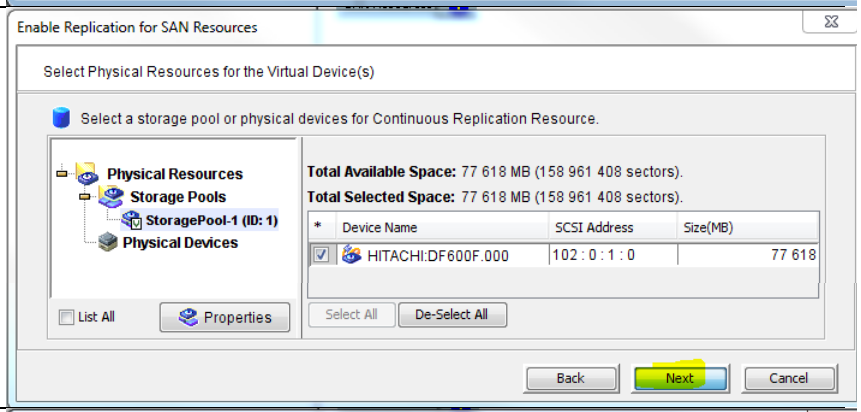
- Saisir le nom complet de l'appliance cible
- Cliquer sur "Next"



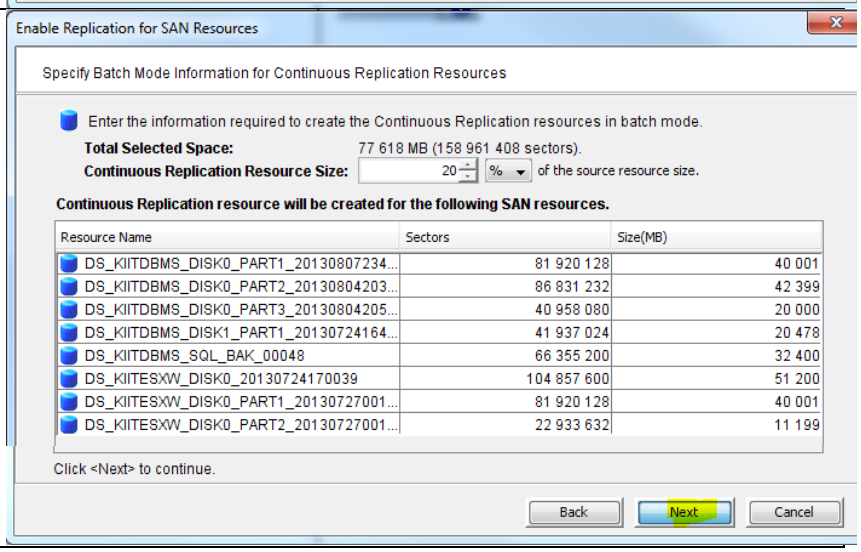
- Cocher "Continuous Mode"
- Forcer la première réplication en cochant "Create Primary TimeMark"
- Cliquer sur "Next"

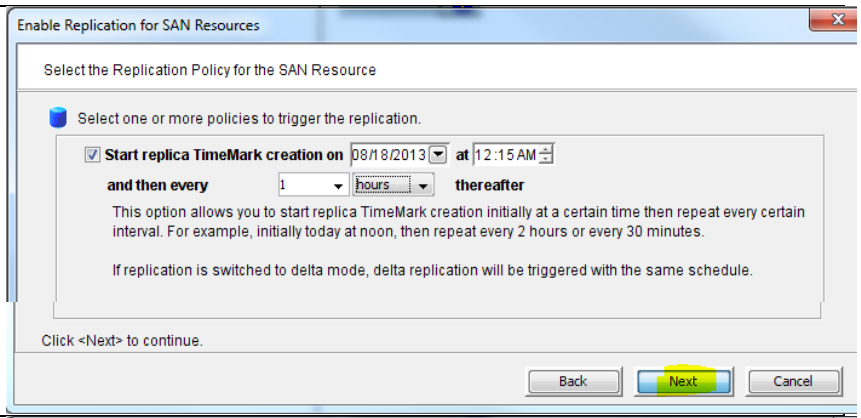
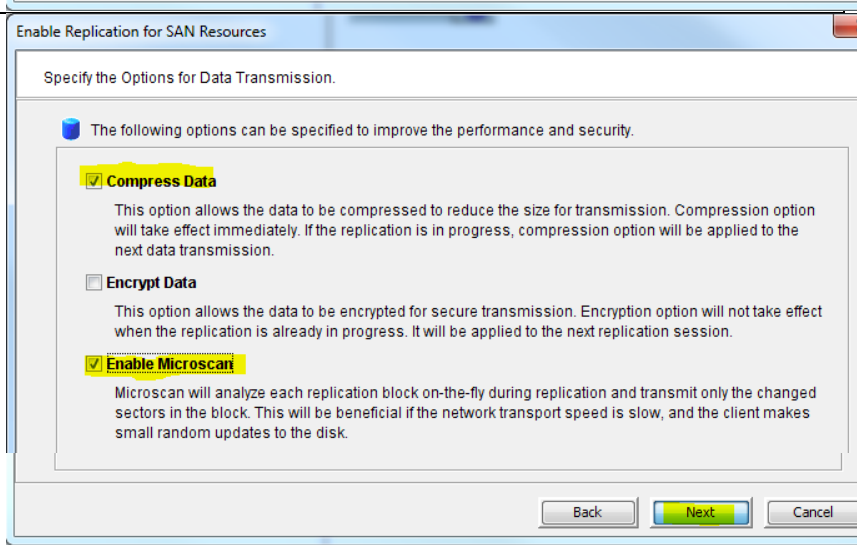
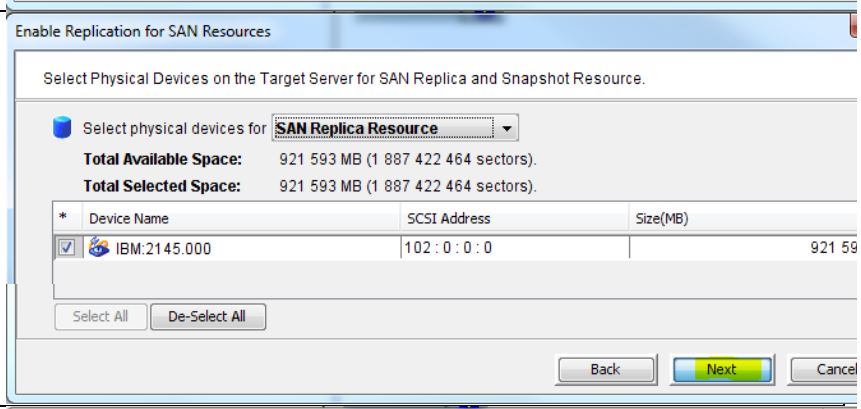
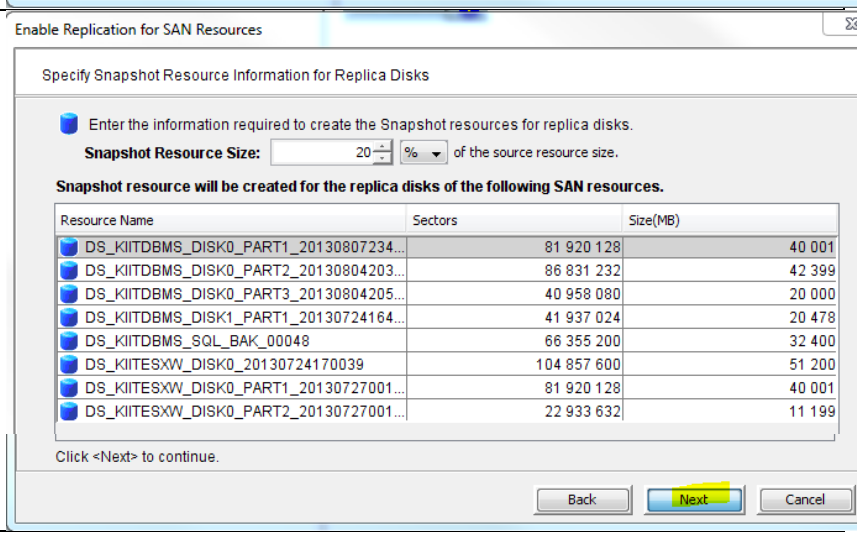


- Cliquer sur "Next"



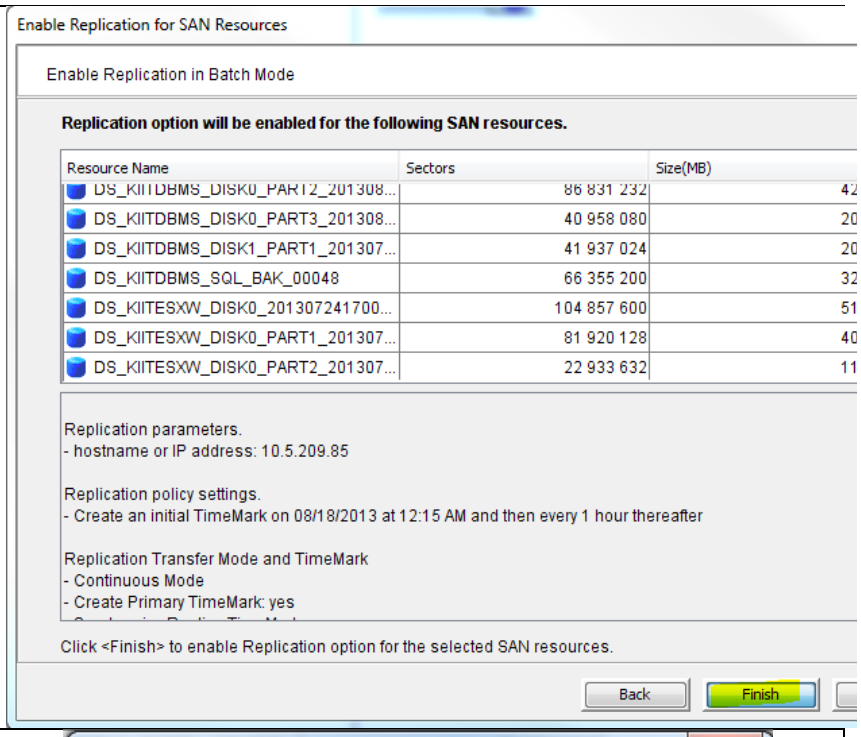
- Cliquer sur "Next"

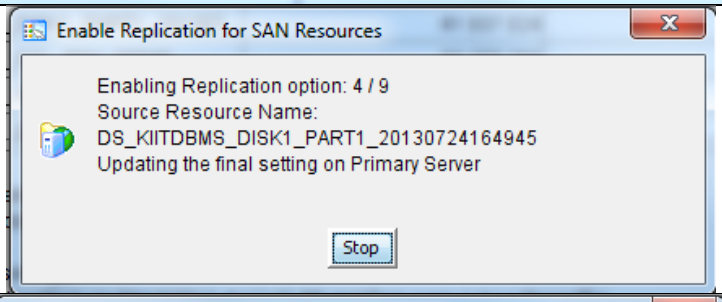


☞ Cliquer sur "Next"	
☞ Cocher la case : "Compress Datat" ☞ Cocher la case "Enable Microscan" ☞ Cliquer sur "Next"	
☞ Cliquer sur "Next"	
☞ Cliquer sur "Next"	

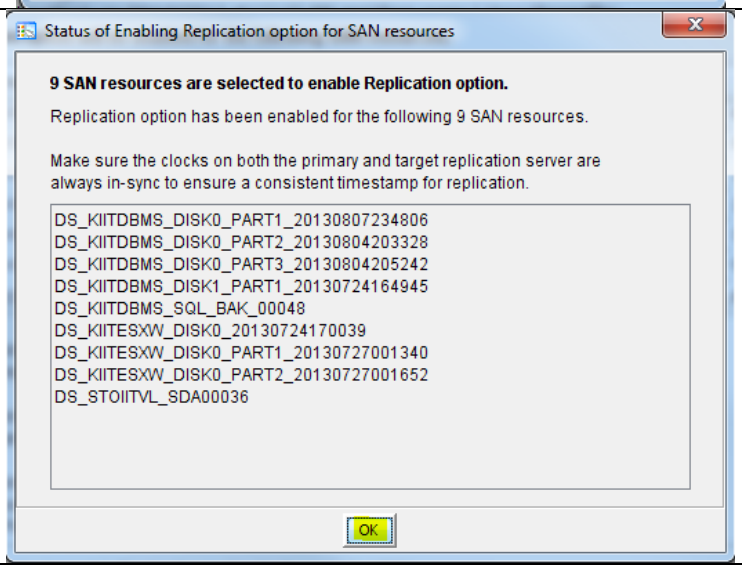
☞ Cliquer sur "Next"	Enable Replication for SAN Resources Select Storage Policy for the Snapshot Resource of the SAN Replica Disks Select the storage policy to be triggered when the space is running low. **Specify a threshold as a percentage of the space used (1%-99%)** 50 % Set the threshold to indicate when more space for the snapshot resource is needed. The system will either delete the earlier TimeMarks to free up the space or stop writing data, depending on the policy selected on the next screen. If the automatic expansion option below is specified, the threshold is used to trigger the automatic expansion before applying the policy. ☑ **Automatically allocate more space for the Snapshot Resource.** Allocate additional space according to the following settings for the Snapshot Resource when space usage reaches the threshold. **Increment the space by** 10 % **Maximum size allowed for the Snapshot Resource** 0 % (The maximum size is set as a limit for the automatic expansion. Specify 0 if you do not want to set the limit. Otherwise, specify a percentage greater than 100% of the size of the snapshot resource.) Back Next Canc
☞ Sélectionner l'option "Always maintain write operations" ☞ Cocher la case "Enable Microscan" ☞ Cliquer sur "Next"	Enable Replication for SAN Resources Set Snapshot Resource Policy for the Replica Disks of the selected SAN Resources. Set Snapshot Resource Policy Select the policy to use when a Snapshot Resource has no space available and cannot expand or has a disk failure. ○ **Preserve all TimeMarks** This option will stop writing data to the source Resource if there is no space available on the Snapsl Resource or if there is a disk failure, in order to preserve all TimeMarks. ○ **Preserve recent TimeMarks** This option will delete older TimeMarks to free up space if there is no space available on the Snapsh Resource. If there is a disk failure,this option will stop writing data to the source Resource in order to preserve recent TimeMarks. ◉ **Always maintain write operations** This option will delete older TimeMarks to free up space if there is no space available on the Snapsh Resource. If there is a disk failure, this option will disable the Snapshot Resource and all TimeMarks be deleted in order to maintain write operations to the source Resource. ☑ **Enable Microscan** Microscan will analyze the data block during "copy-on-first-write". Only the changed data will be copi which will eliminate unnecessary writes. Back Next

☞ Cliquer sur "Finish"

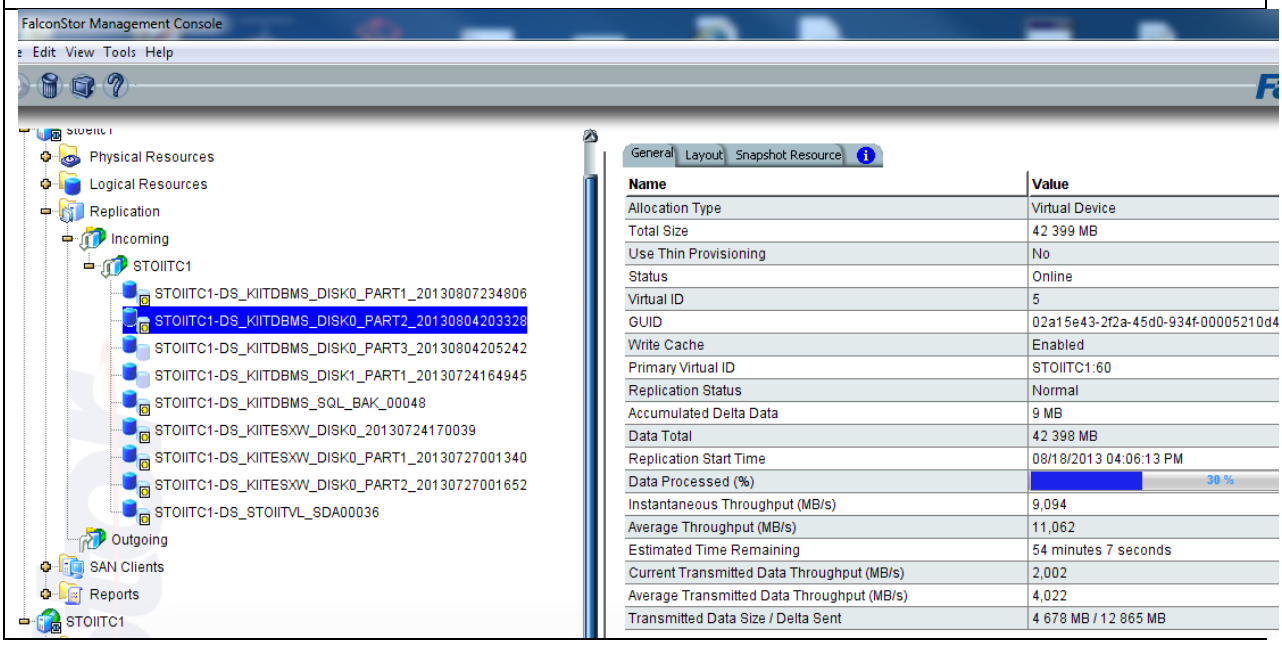




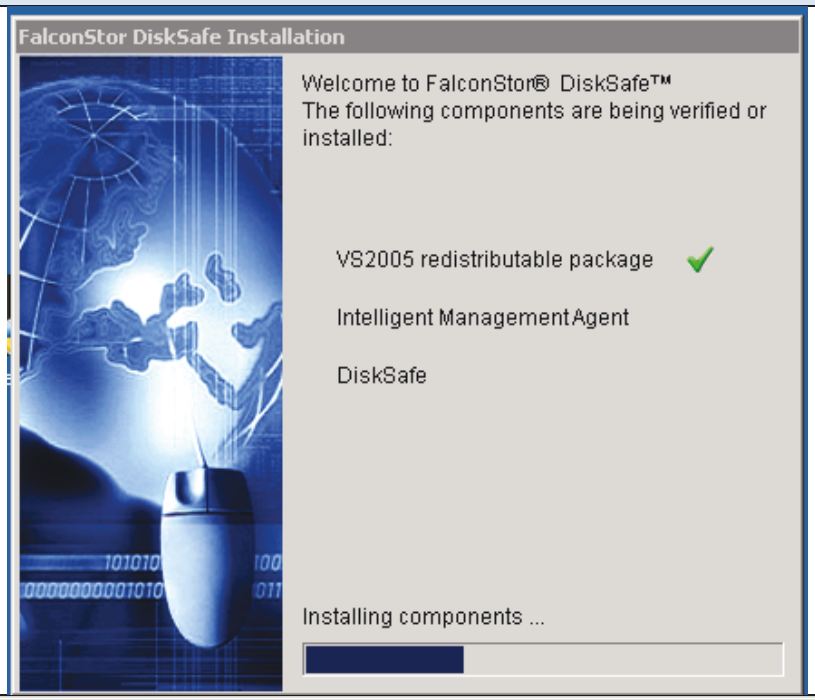
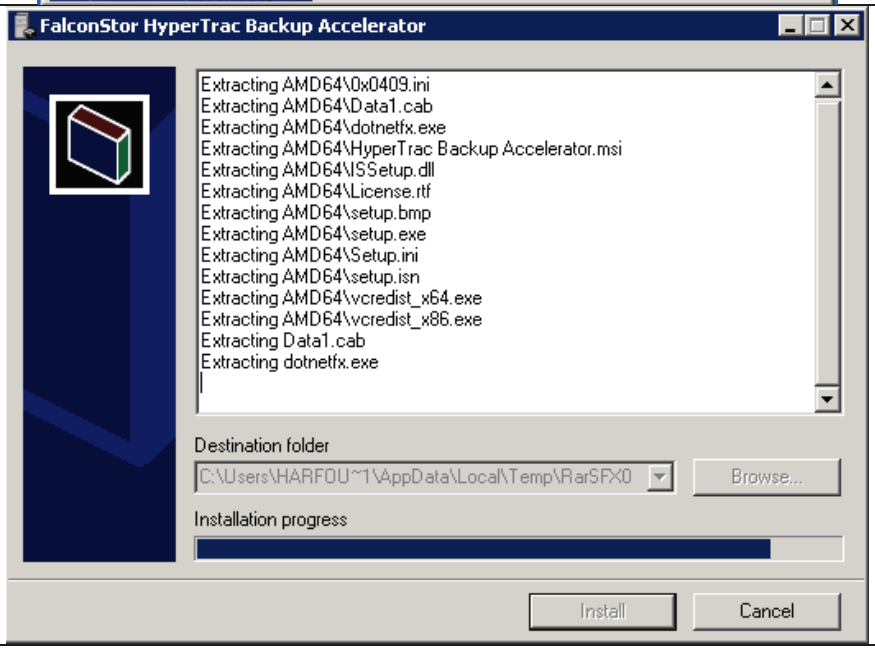
☞ Cliquer sur "OK"

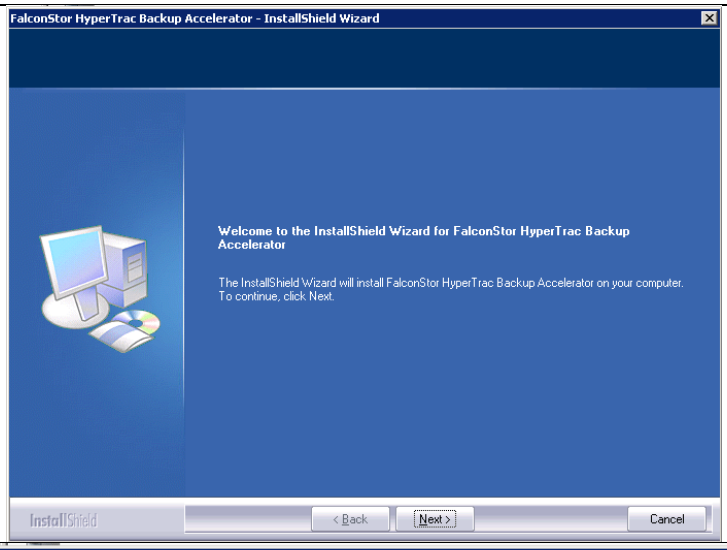
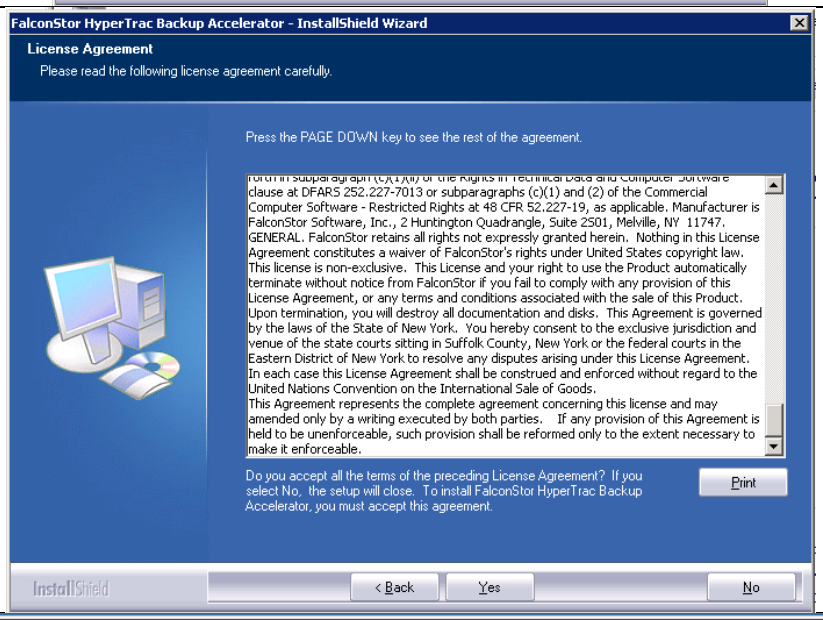
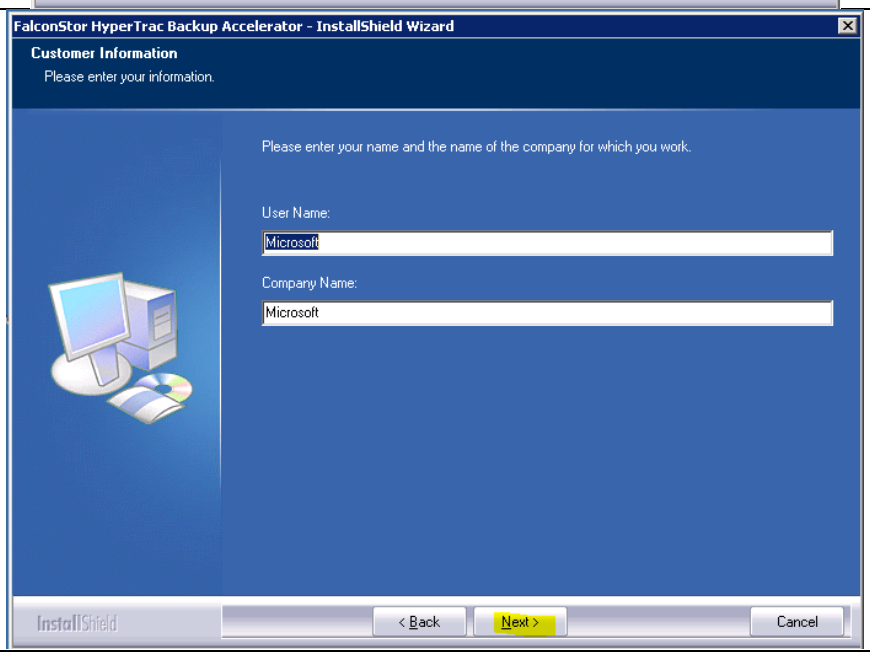


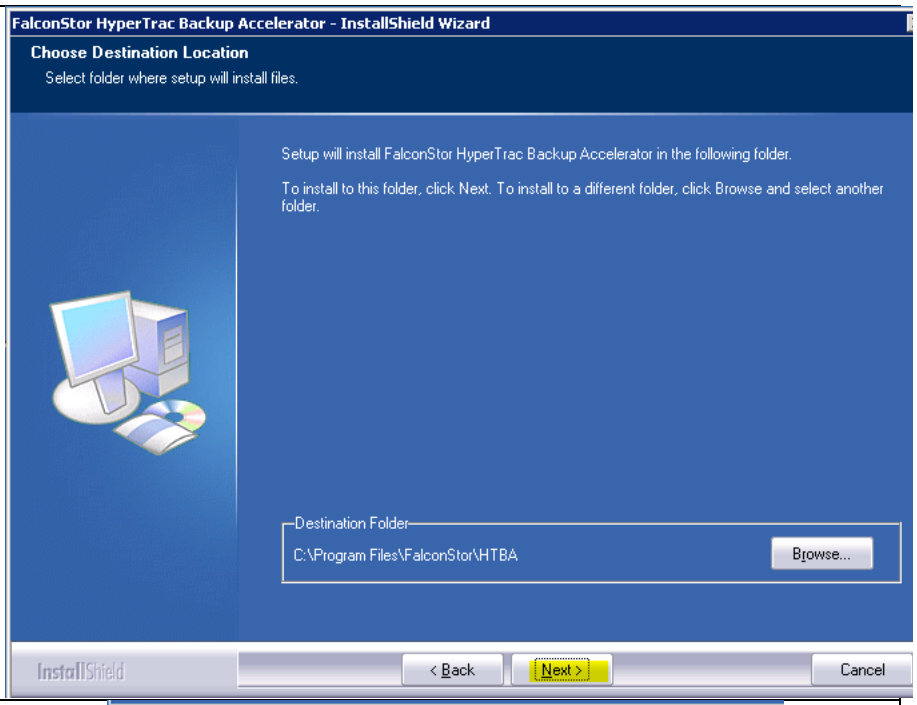
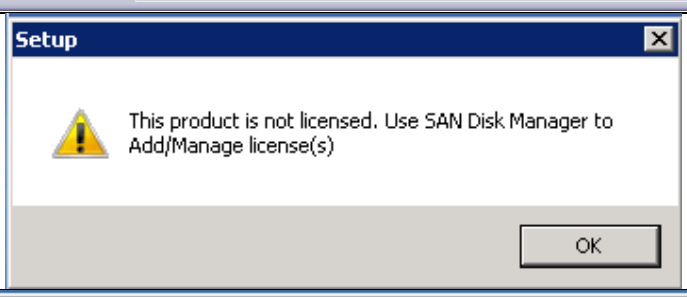
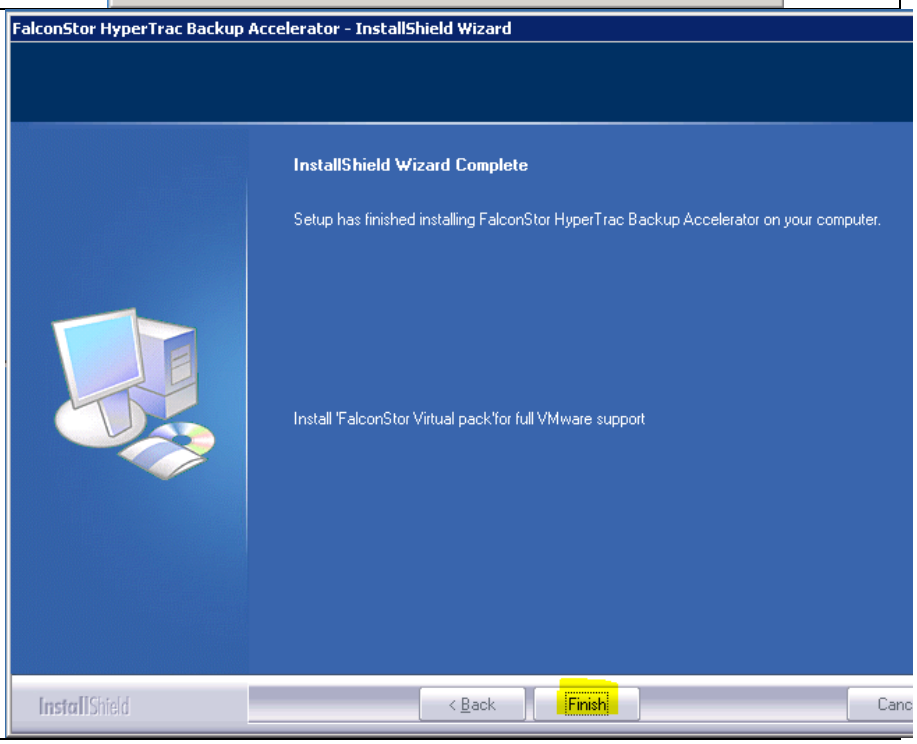
Vérification



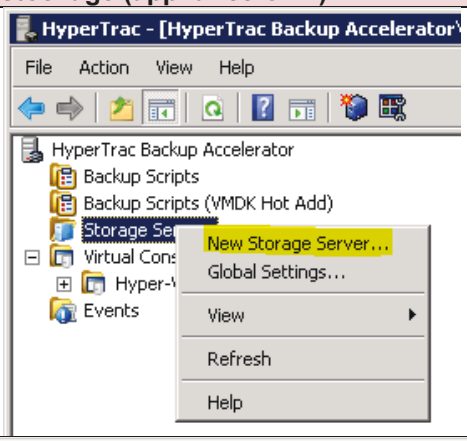
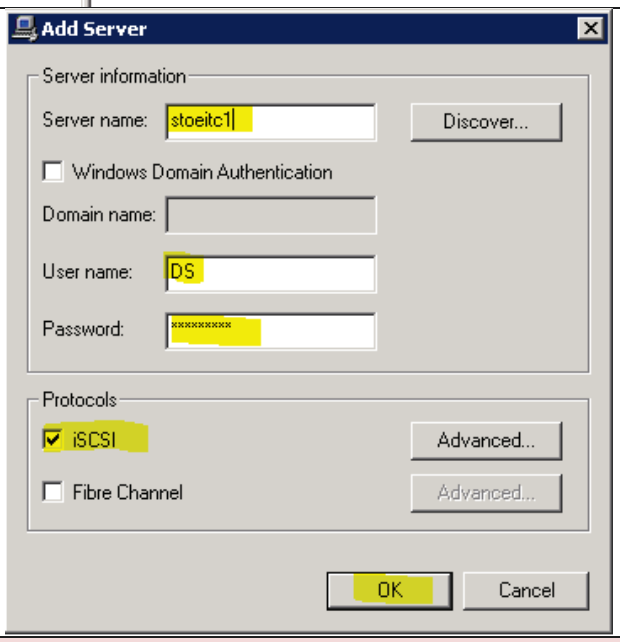
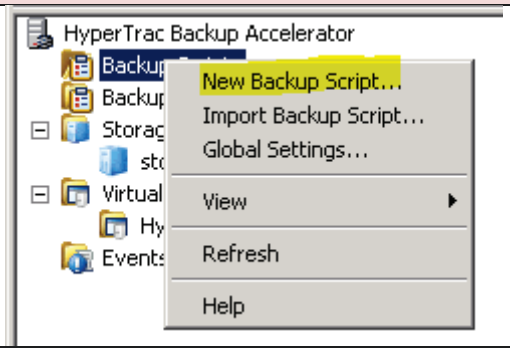
ANNEXE 17 : Installation HyperTrac

ACTIONS	ILLUSTRATIONS
☞ Lancer le programme "Installatation Intelligent Managment Agent"	
Lancement du programme d'installation	

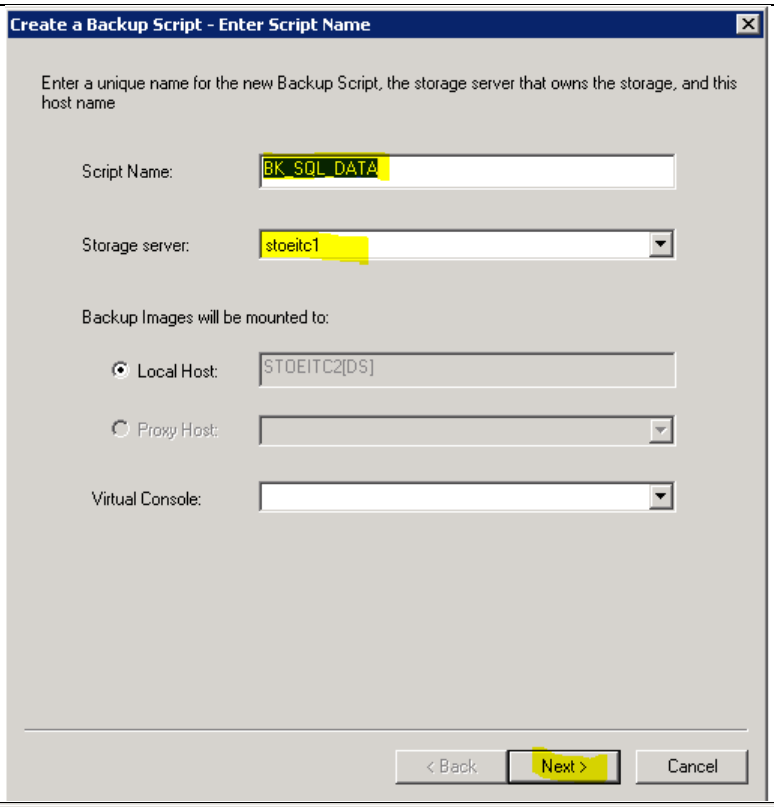
☞ Cliquer sur "Next"	
☞ Cliquer sur "Yes"	
☞ Cliquer sur "Next"	

☞ Cliquer sur "Next"	
☞ Cliquer sur "OK"	
☞ Cliquer sur "Finish"	

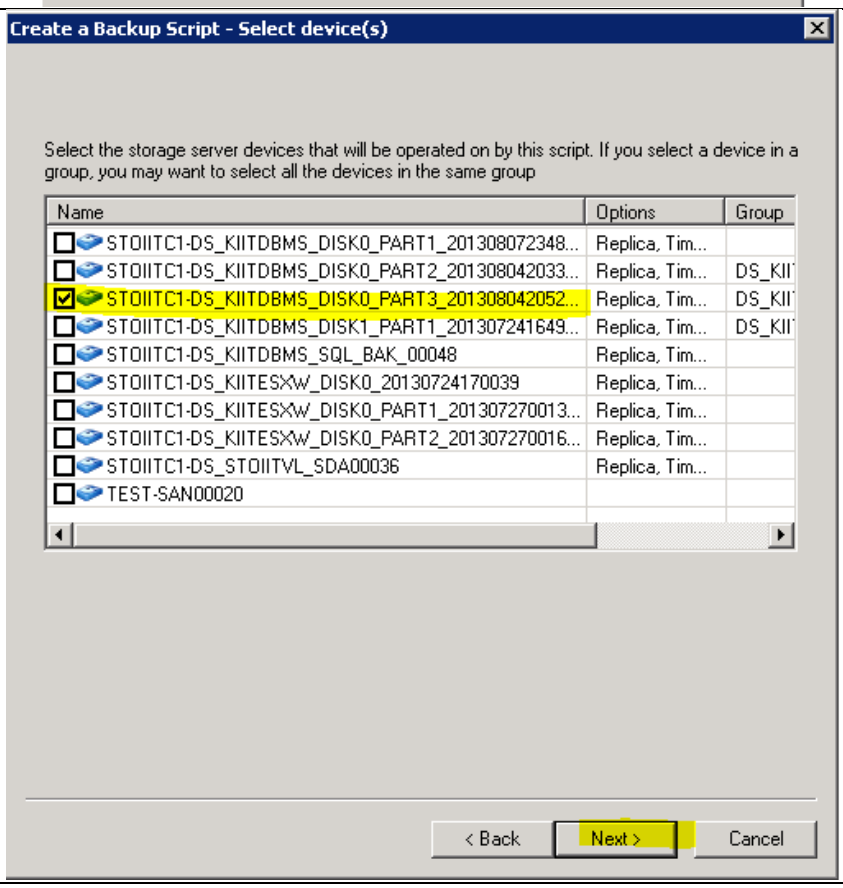
ANNEXE 18 : Paramétrage HyperTrac

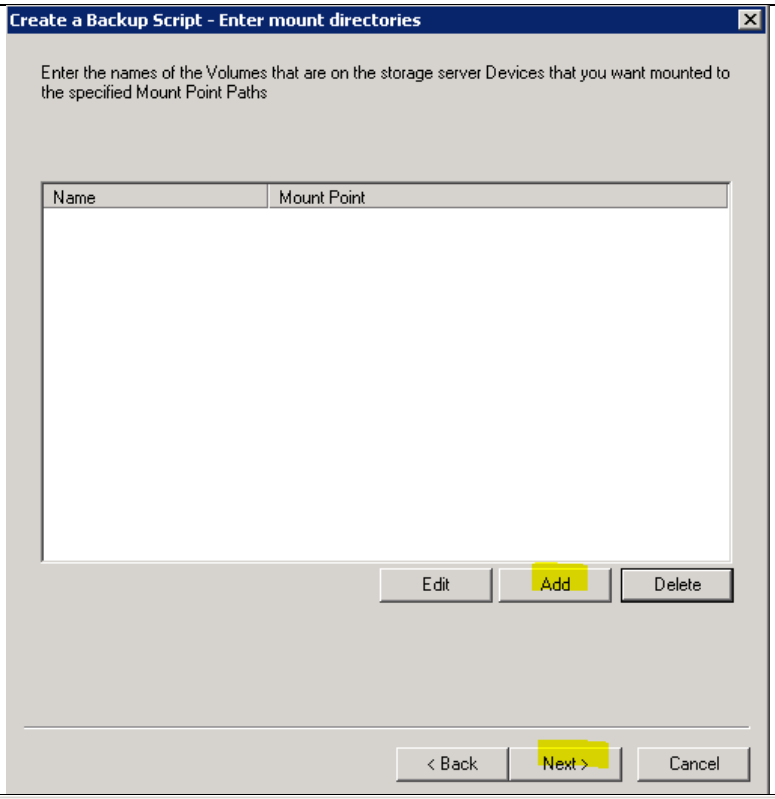
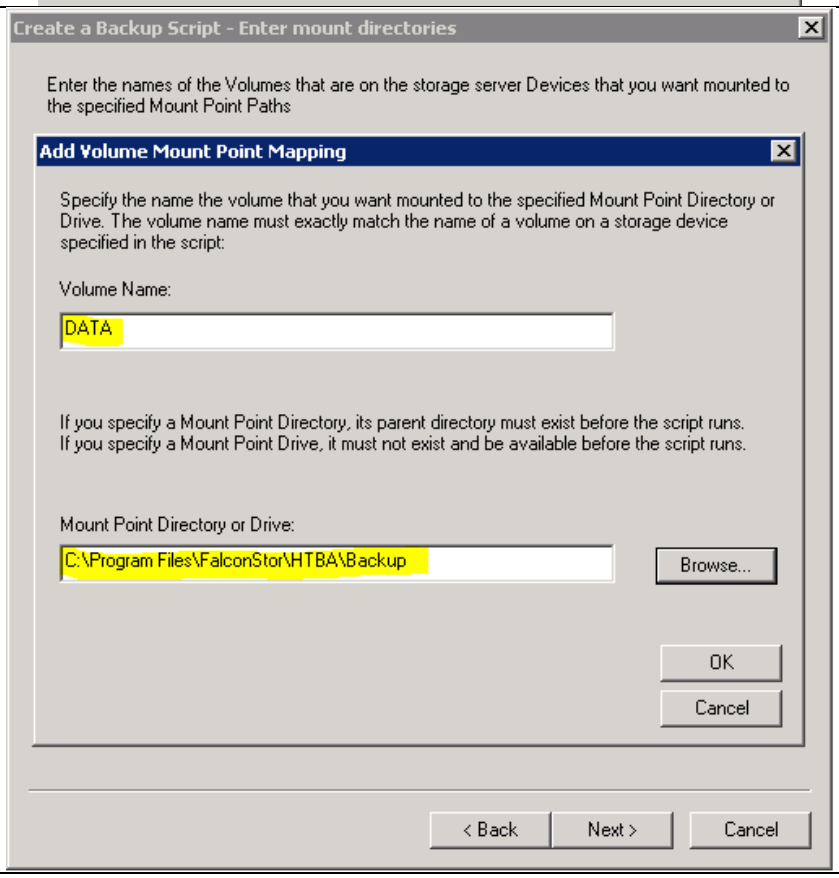
ACTIONS	ILLUSTRATIONS
Ajout du serveur de stockage (appliance CDP)	
☞ Faire un "Clic droit" sur "Storage Server" ☞ Sélectionner "New Storage server…"	
☞ Renseigner les informations : - Server name (Appliance CDP) - User name (Compte administrateur CDP) - Password ☞ Activer le protocole "iSCSI" en cochant la case ☞ Cliquer sur "OK"	
Création d'un Jobs	
☞ Faire un "Clic droit" sur "Backup Scripts" ☞ Sélectionner "New Backup Script…"	

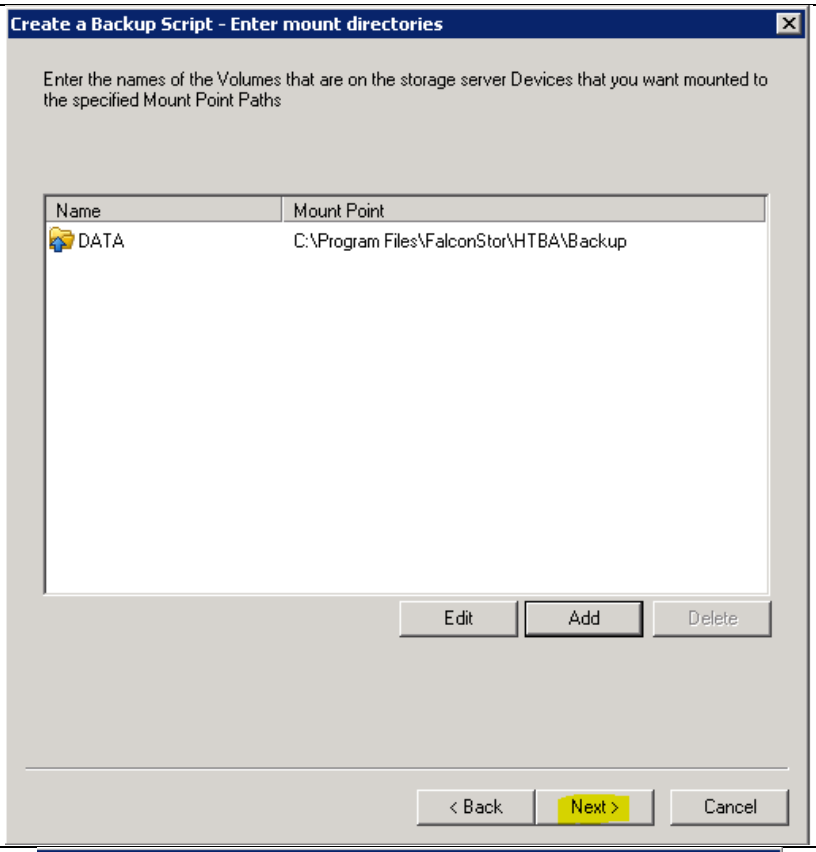
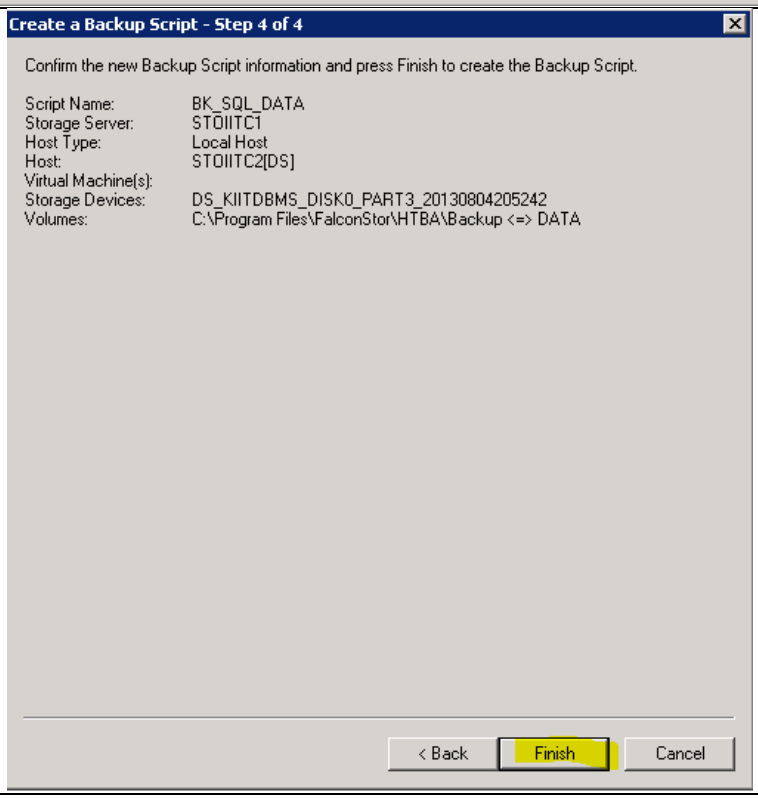
- Définir le nom du script
- Définir le serveur de stockage FalconStor CDP
- Cliquer sur "Next"



- Choisir les LUN à sauvegarder
- Cliquer sur "Next"



☞ Ajouter un point de montage en cliquant sur "Add"	
☞ Saisir le nom du volume ☞ Sélectionner un point de montage ☞ Cliquer sur "OK"	

☞ Cliquer sur "Next"	
☞ Cliquer sur "Finish"	

ANNEXE 19 : FalconStor expérience n°1 (Backup)

Analyse du comportement de FalconStor CDP sur lecteur de sauvegarde de la base de données MS SQL Server

KIITDMS
C:\ Disque Système
D:\ Disque Applicatifs
E:\ fichier de données (DATA) MS SQL Serveur
L:\ fichiers de transactions (LOG) MS SQL Serveur
M:\Lecteur de sauvegardes MS SQL Serveur

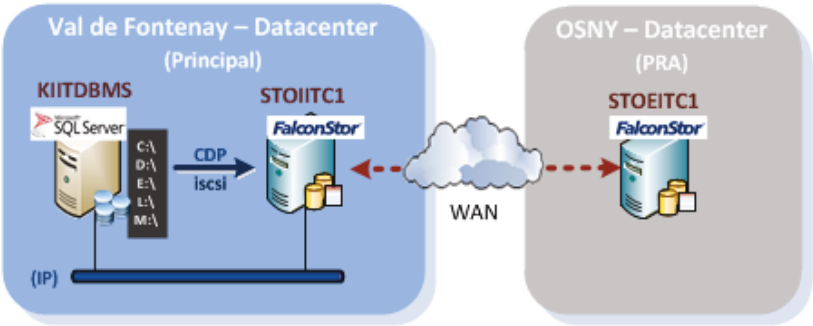


Tableau XVIII : Récapitulatif des différentes phases de l'expérimentation

N°	Dates / heures	Actions réalisées	Taille (Mo)	Nb lignes
1	22/08/2012 18:45	Ajout de la table DELETE_ME_2	9 931	12 665 766
2	22/08/2012 19:29	Ajout de la table DELETE_ME_3	340	561 756
3	22/08/2012 20:01	Demande de prise d'image (M:\)		
4	22/08/2012 20:10	Suppression des tables DELETE_ME_2 et DELETE_ME_3	10 271	13 227 522
5	22/08/2012 20:25	Sauvegarde de la base de données vers "M:"		
6	22/08/2012 20:38	Élagage de la base de données		
7	22/08/2012 20:40	Suppression du fichier de sauvegarde sur "M :"		

ÉTAPE 0 : Initialisation

Au début des tests, le lecteur logique M ne contient qu'un fichier :

CAMP02_Full.bak	22/08/2013 18:39	BAK File	8 158 630 KB

L'espace alloué aux snapshots est vide :

Tableau XIX : Étape 0 - Ressources allouées au stockage secondaire (FalconStor) du lecteur M

Used Size	192.0 KB
Size Before Reaching Threshold	19.439 GB
Usage Percentage	0 %

Le journal ne présente que deux lignes :

- la première est créée lors de l'activation de la protection du LUN ;
- la seconde lorsque que le CDP a été activé.

Tableau XX : Étape 0 – Détail des snapshots du lecteur M

	Timestamp	Used Size	Comment	Priority	Quiescent	TimeView Data	Status
1	08/22/2013 18:56:01	64.0 KB	DEBUT DU TEST	Medium	Yes	none	N/A
2	08/22/2013 18:59:29	128.0 KB	@initcdpsnapAug 22 18:59:29	Medium	Yes	none	N/A

ÉTAPE 1 : Création de la table "DELETE_ME_2"

À l'aide d'une requête SQL, j'ai ajouté une table. L'opération reste sans effet jusqu'à ce que MS SQL Serveur lance son job de sauvegarde et commence à écrire dans le fichier "CAMP02_Full.bak" à 19h15.

À ce moment, les modifications sont enregistrées dans le journal CDP et les données modifiées sont affectées à la dernière prise d'image.

À 19h20 la prise d'image se déclenche, et l'espace alloué aux snapshots augmente jusqu'à dépasser les 9 Go (environ la taille de l'ajout sur le disque).

Tableau XXI : Étape 1 - Ressources allouées au stockage secondaire (FalconStor) du lecteur M

Used Size	9.61 GB
Size Before Reaching Threshold	9.829 GB
Usage Percentage	24 %

Les données acquises après la prise d'image sont affectées aux snapshots suivants :

Tableau XXII : Étape 1 – Détail des snapshots du lecteur M

	Timestamp	Used Size	Comment	Priority	Quiescent	TimeView Data	Status
1	08/22/2013 18:56:01	64.0 KB	DEBUT DU TEST	Medium	Yes	none	N/A
2	08/22/2013 18:59:29	8.35 GB	@initcdpsnapAug 22 18:59:29	Medium	Yes	none	N/A
3	08/22/2013 19:20:00	1.26 GB	Scheduled_20130822192000	Medium	Yes	none	N/A

ÉTAPES 2 et 3 : Création de la table "DELETE_ME_3" et demande de prise d'image (M:\)

J'ajoute une nouvelle table beaucoup moins conséquente (340 Mo et 561 756 enregistrements). Tout comme lors de l'ajout de la précédente table, je ne constate alors aucun changement.

Afin de dissocier les différentes créations de tables, une demande de prise d'image est alors effectuée à 20h01. Tout comme lors de l'initialisation (étape 0), un snapshot vide (128 Ko) est créé et aucun effet n'est constaté avant le lancement du job de sauvegarde de Microsoft SQL Serveur à 20h15.

Tableau XXIII : Étape 3 – Détail des snapshots

	Timestamp	Used Size	Comment	Priority	Quiescent	TimeView Data	Status
1	08/22/2013 18:56:01	64.0 KB	DEBUT DU TEST	Medium	Yes	none	N/A
2	08/22/2013 18:59:29	8.35 GB	@initcdpsnapAug 22 18:59:29	Medium	Yes	none	N/A
3	08/22/2013 19:20:00	1.265 GB	Scheduled_20130822192000	Medium	Yes	none	N/A
4	08/22/2013 20:01:24	28.623 MB	Ajout tale DELETE_ME_3	High	Yes	none	N/A

La taille de la dernière empreinte est modifiée et l'augmentation de la taille du fichier est répercutée sur le disque de l'appliance FalconStor CDP.

Tableau XXIV : Étape 3 - Ressources allouées au stockage secondaire (FalconStor) du lecteur M

Used Size	9.643 GB
Size Before Reaching Threshold	9.796 GB
Usage Percentage	24 %

Remarque : Bien que la taille de la table soit de 340 Mo (selon MS SQL Serveur), elle ne représente plus qu'une petite trentaine de Mo lorsqu'elle est extraite (cf. encadré rouge du tableau XX).

ÉTAPE 4 : Suppression des tables "DELETE_ME_2" et "DELETE_ME_3"

Cette opération n'a aucune conséquence sur le système de stockage. Aucune modification n'est donc constatée.

ÉTAPE 5 : Sauvegarde de la base de données vers "M:"

Pour réaliser cette opération, on génère un fichier de transaction (que l'on a paramétré sur le lecteur étudié) à partir de Microsoft SQL Server en lui demandant la suppression des journaux de transactions ("Dump Database").

L'exécution du job de sauvegarde, réalisée après la prise d'image (entre 20h25 et 20h31), a généré un fichier d'une dizaine de Go. Comme dans les deux précédents ajouts, une augmentation de l'espace de stockage utilisé et l'accroissement du volume de la dernière prise d'image sont constatés.

Tableau XXV : Étape 5 - Ressources allouées au stockage secondaire (FalconStor) du lecteur M

Used Size	18.174 GB
Size Before Reaching Threshold	9.266 GB
Usage Percentage	33 %

Tableau XXVI : Étape 5 – Détail des snapshots du lecteur M

	Timestamp	Used Size	Comment	Priority	Quiescent	TimeView Data	Status
1	08/22/2013 18:56:01	64.0 KB	DEBUT DU TEST	Medium	Yes	none	N/A
2	08/22/2013 18:59:29	8.35 GB	@initcdpsnapAug 22 18:59:29	Medium	Yes	none	N/A
3	08/22/2013 19:20:00	1.265 GB	Scheduled_20130822192000	Medium	Yes	none	N/A
4	08/22/2013 20:01:24	28.623 MB	Ajout tale DELETE_ME_3	High	Yes	none	N/A
5	08/22/2013 20:20:00	10.28 GB	Scheduled_20130822202000	Medium	Yes	none	N/A

ÉTAPE 6 : Élagage de la base de données

Cette étape n'a aucune influence sur l'environnement étudié. Seuls les fichiers de la base de données (journaux et données) sont concernés.

ÉTAPE 7 : Suppression du fichier de sauvegarde sur "M :"

Cette suppression de fichier intervient entre 2 prises d'images. Lors de son exécution (à 20h40), aucun changement n'est constaté. L'espace de stockage et l'empreinte prise à 20h20 restent inchangées (10.28 Go).

Tableau XXVII : Étape 7 - Ressources allouées au stockage secondaire (FalconStor) du lecteur M

Used Size	18.174 GB
Size Before Reaching Threshold	9.266 GB
Usage Percentage	33 %

ANNEXE 20 : FalconStor expérience n°2 (Restauration)

Restauration à partir des prises d'images CDP

Tableau XXVIII : Les étapes de l'expérimentation de restauration d'une base de données MS SQL Serveur

N°	Date /heures	Action Réalisé
1	14/10/2013 16:35	Suppression de la table DELETE_ME_4
2	14/10/2013 17:00	Arrêt de la base de données CAMP02
3	14/10/2013 18:42	Restauration de la base de données
4	14/10/2013 19:05	Redémarrage de la base de données CAMP02
5	14/10/2013 19:25	Démontage des images de restauration

ÉTAPE 1 : Suppression d'une table

J'ai supprimé la table DELETE_ME_4, composée de 2 382 012 enregistrements et occupant une place de 1 478 Mo, en lançant la commande SQL sur la base de données CAMP02 :

```
Drop table DELETE_ME_4
```

ÉTAPE2 : Arrêt de la base de données "CAMP02"

L'objectif de cette étape est d'arrêter la base de données afin de permettre le remplacement de ses fichiers de données et de transactions.

L'opération a été réalisée depuis la console d'administration MS SQL Server Management Studio (cf. figure ci-après) :

- en réalisant un "clic roit" sur la base de données CAMP02 ;
- puis en allant dans le sous-menu "Tasks" ;
- et enfin, en sélectionnant "Take Offline".

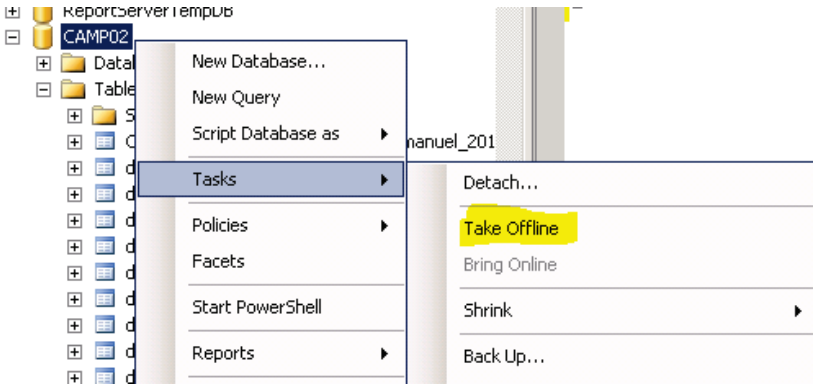


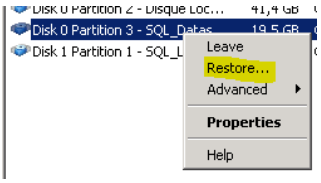
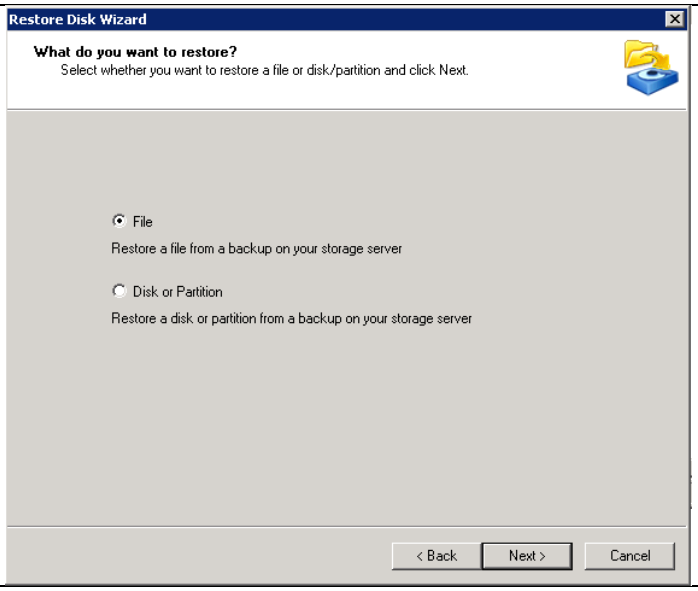
Figure A20-1 : Arrêt d'une base de données MS SQL Server

ÉTAPE 3 : Restauration de la base de données "CAMP02"

La restauration de la base de données sera réalisée en 2 phases :

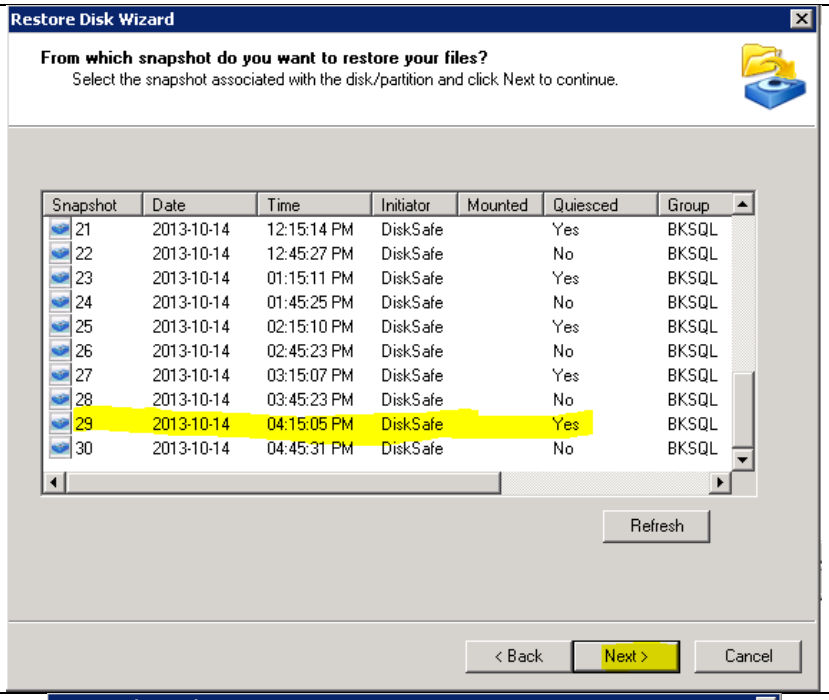
- Restauration du fichier de données "CAMP02.mdf" :
  - Présentation au serveur du LUN contenant les données ;
  - Remplacement des fichiers de la base de données.
- Restauration du fichier de données "CAMP02.ldf" :
  - Présentation au serveur du LUN contenant les données ;
  - Remplacement des fichiers de la base de données.

Procédure de restauration de la base de données "CAMP02" :

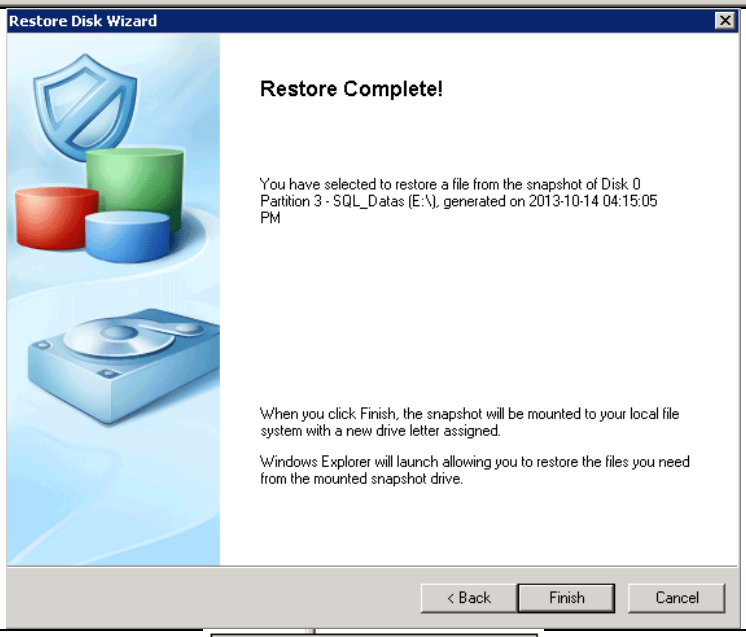
ACTIONS	ILLUSTRATIONS
Restauration du fichier de données de la base CAMP02 ("CAMP02.mdf")	
☞ Sélectionner le disque (lecteur logique "E :\") contenant le fichier de données "CAMP02.mdf" ☞ "Clic droit" puis "Restore"	
☞ Choisir "File" ☞ Puis, cliquer sur "Next"	

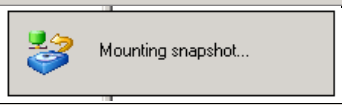
☞ Sélectionner l'image qui a été prise à 16H15, c'est à dire avant la suppression de la table (16H35).

Attention, il faudra sélectionner la version du LUN contenant le fichier de transactions "CAMP02.ldf" correspondant à la même date.

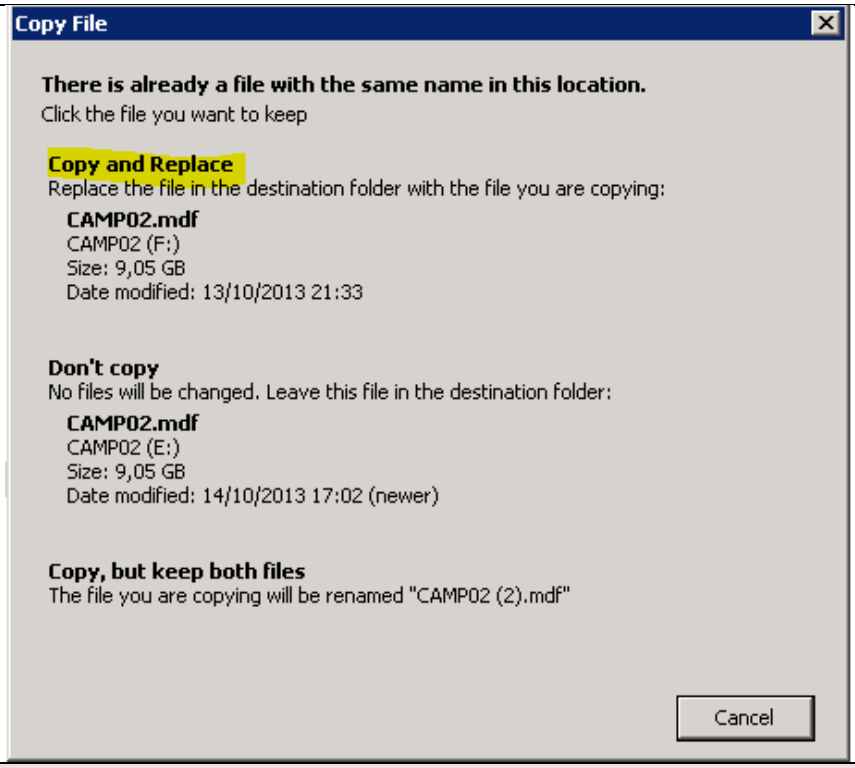
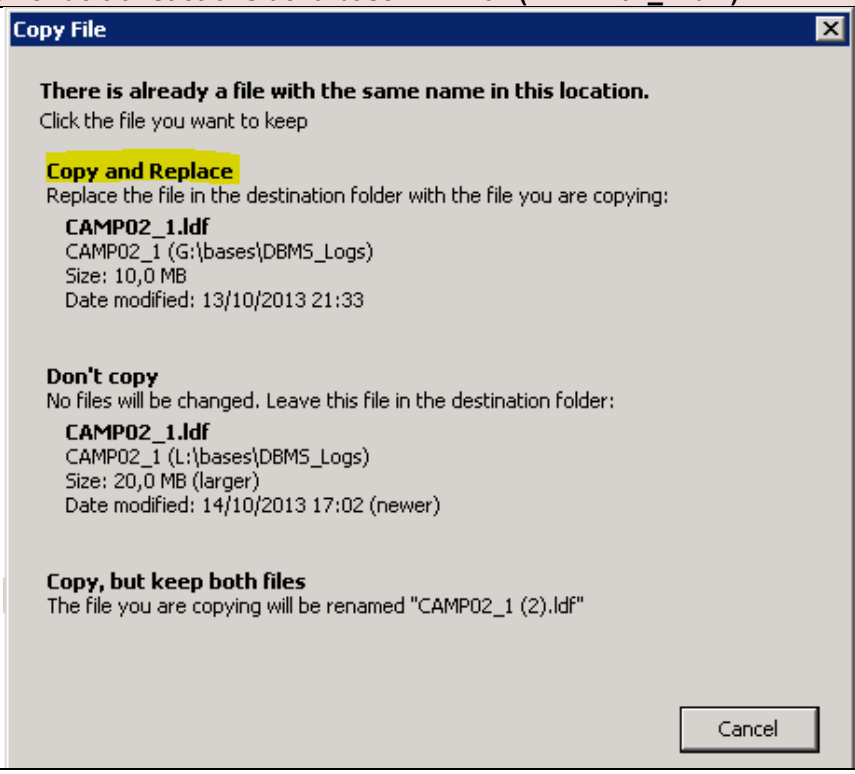


☞ Cliquer sur "Finish"





Un nouveau lecteur devient visible : (le "F:")

☞ Cliquer sur "Copy and Replace"	
Restauration du fichier de transactions de la base CAMP02 ("CAMP02_1.ldf")	
J'ai procédé à la même opération avec le lecteur logique "L:\" et le fichier "CAMP02.ldf"	

Remarque : J'ai attendu que les copies soient achevées avant de passer à l'étape suivante.

ÉTAPE 4 : Redémarrage de la base de données "CAMP02"

Tout comme l'opération d'arrêt de la base de données, je me suis servi de la console d'administration MS SQL Server Management Studio (cf. figure ci-dessous) pour relancer la base de données "CAMP02" précédemment restaurée :

- en réalisant un clic "droit" sur la base de données CAMP02 ;
- puis en allant dans le sous-menu "Tasks" ;
- et enfin, en sélectionnant "Bring Online".

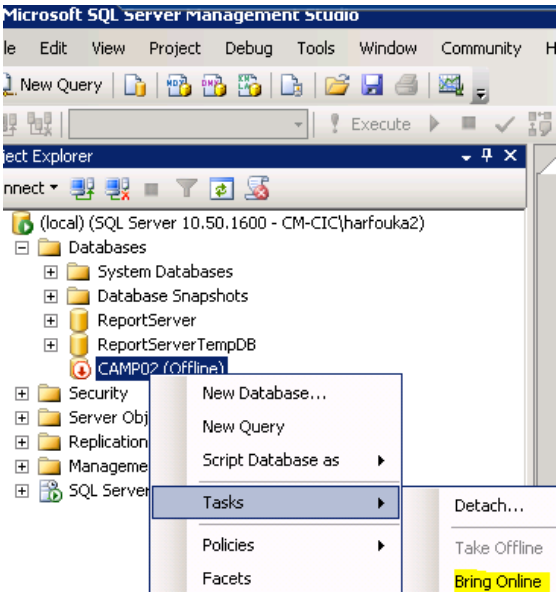


Figure A20-2: Démarrage de la base "CAMP02"

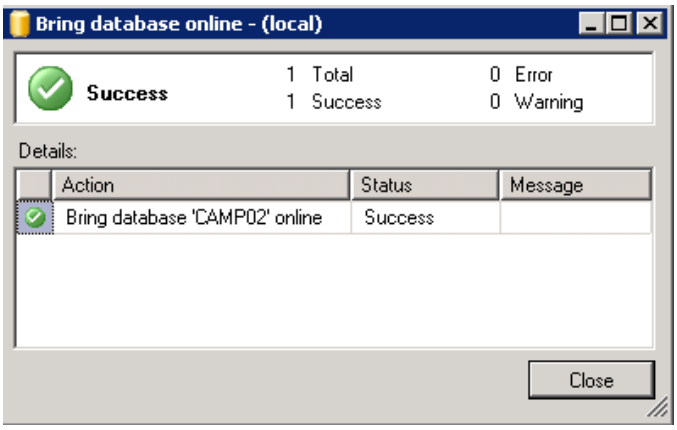


Figure A20-3 : Résultat du démarrage de la base "CAMP02"

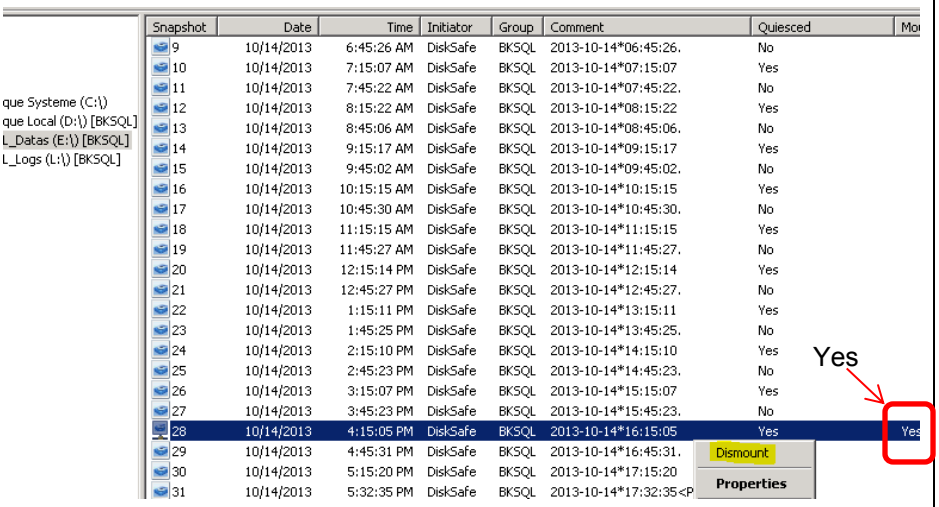
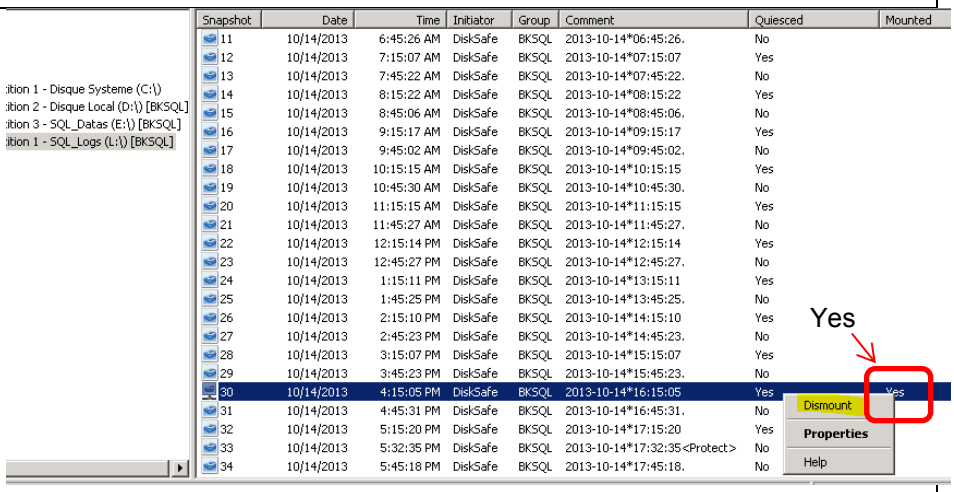
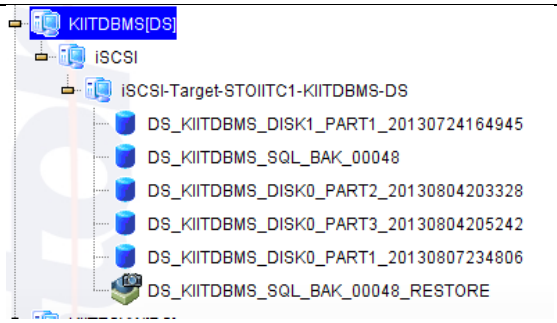
Remarque : La base de données CAMP02 est désormais accessible et la table "DELETE_ME_4" a été récupérée avec tous ses enregistrements.

ÉTAPE 5 : Démontage des snapshots de restauration

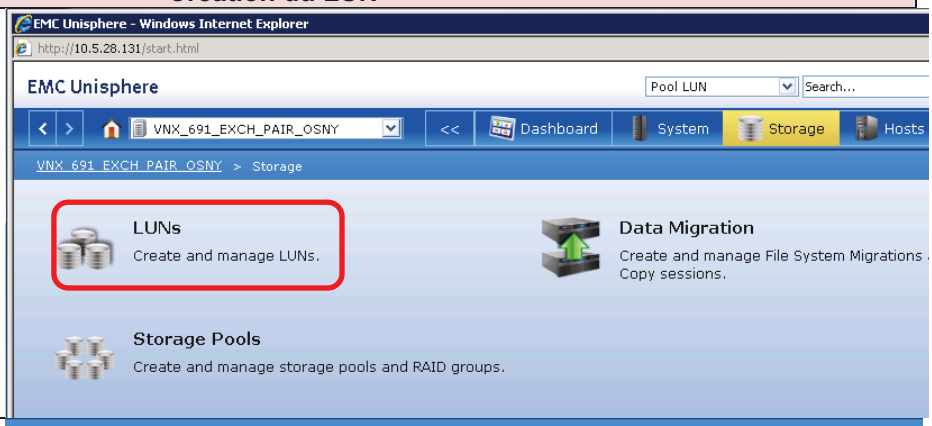
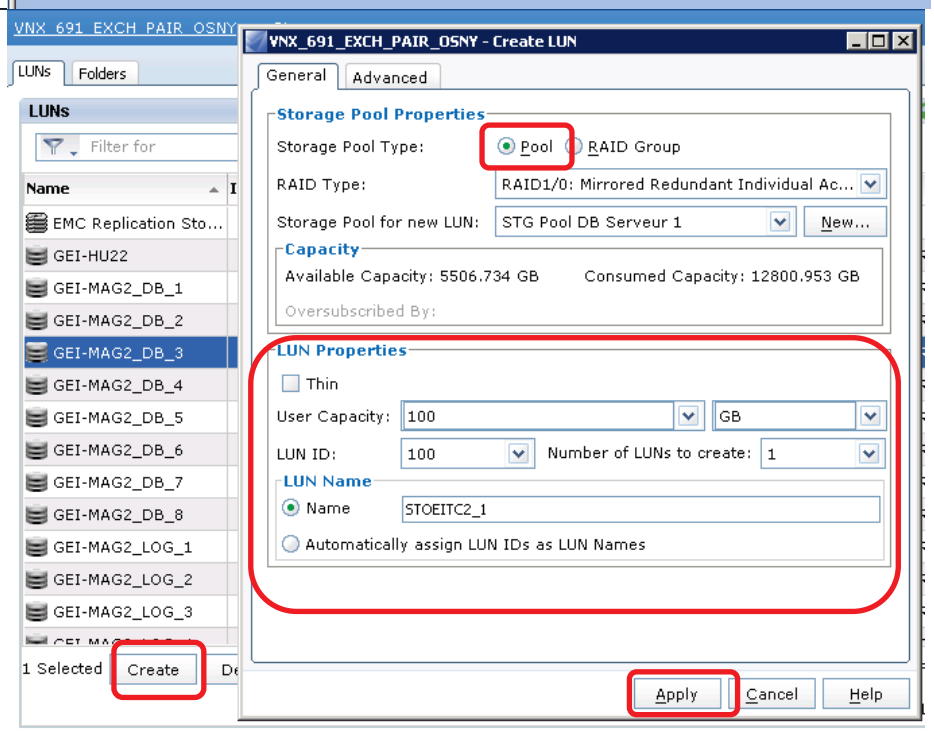
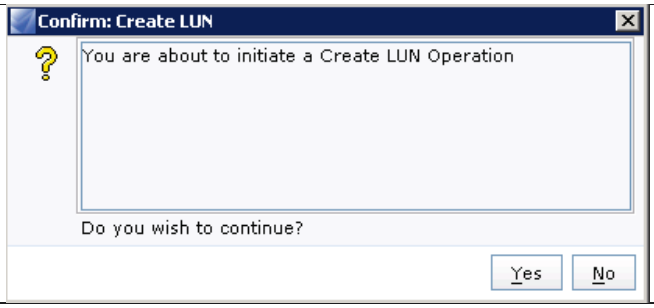
Lors des précédentes étapes de restauration, les LUN sont restés présentés au serveur SQL (cf. figure A20-4).

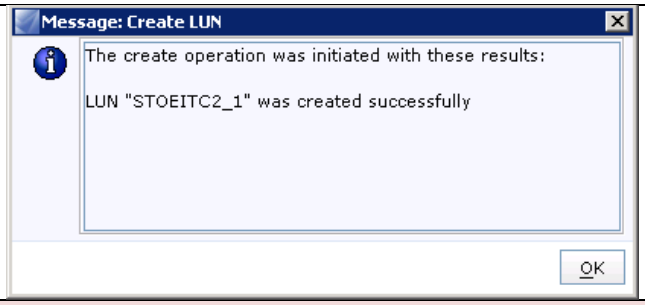
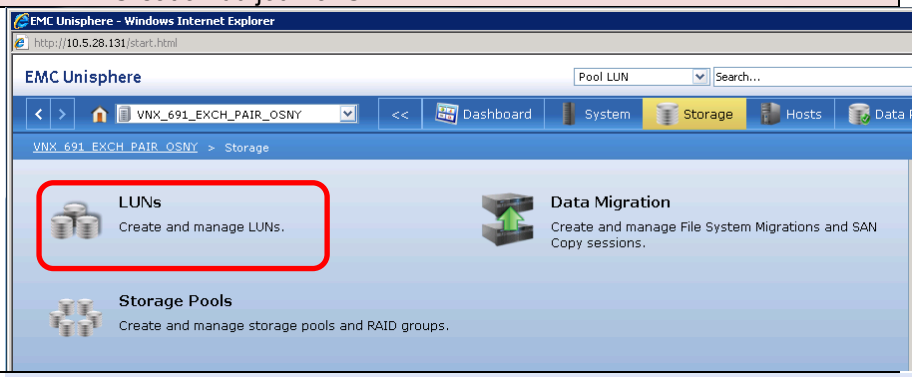
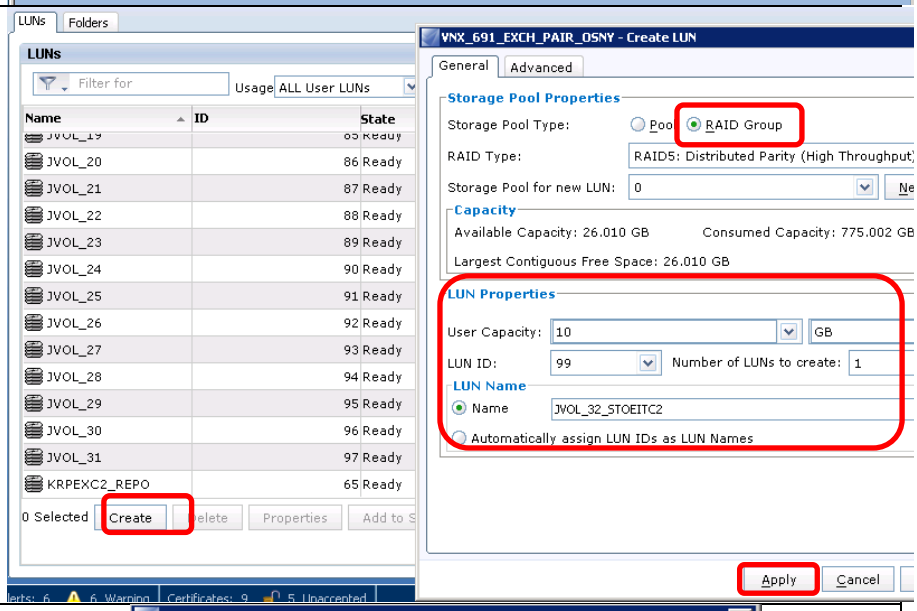
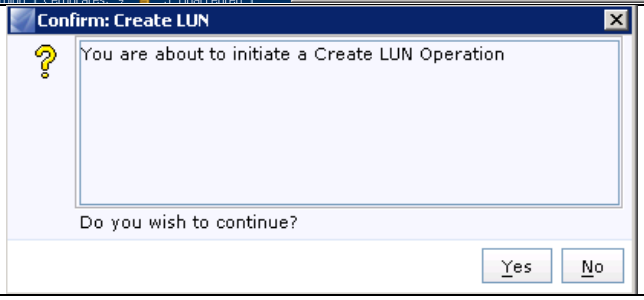
Figure A20-4 : Liste des LUN présentés au serveur KIITDBMS par l'IPStor

Il faut donc les démonter, soit à partir de la console IPStor, soit à partir de la console DiskSafe du serveur.

ACTIONS	ILLUSTRATIONS
Démontage des snapshots de restauration	
Dans la console DiskSafe (section Snapshots/Disks) : ☞ Rechercher les disques montés (yes) ☞ Clic "droit" ☞ cliquer sur "Dismount"	
Il faut ensuite réaliser la même opération pour le disque des journaux (le lecteur "L:") .	
Sous la console IPStor, on remarque que les 2 images ont bien été supprimées.	

ANNEXE 21 : Paramétrage des baies VNX

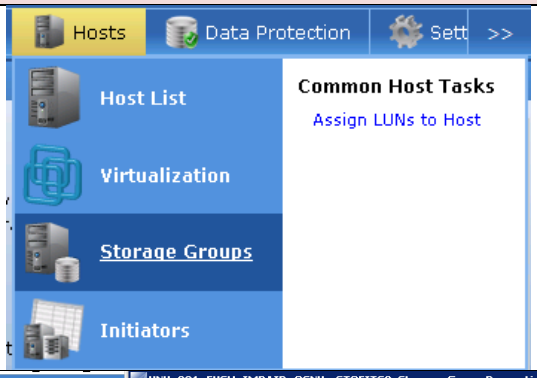
ACTIONS	ILLUSTRATIONS
Création du LUN	
Dans l'interface de la baie, cliquer sur "LUNs"	
☞ Cliquez sur "Create" ☞ Changer le storage pool type en "Pool" ☞ Définir la taille et le nom du LUN ☞ Cliquer sur "Apply"	
☞ Cliquer sur "Yes"	

☞ Cliquer sur "OK"	
Création du journal CDP	
Dans l'interface de la baie, cliquez sur "LUNs"	
☞ Cliquez sur "Create" ☞ Définir le "storage pool type" en "RAID Group" ☞ Définir la taille et le nom du LUN ☞ Cliquer sur "Apply"	
☞ Cliquer sur "Yes"	

Présentation des LUNs au serveur

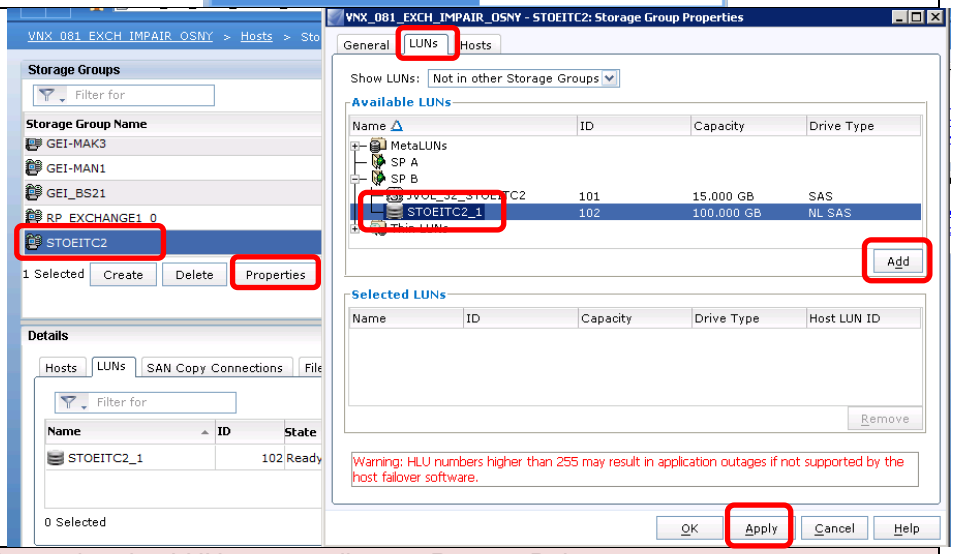
Dans l'interface de la baie :

- Cliquer sur "Hosts"
- Cliquer sur "Storage Groups"



Dans l'interface de la baie :

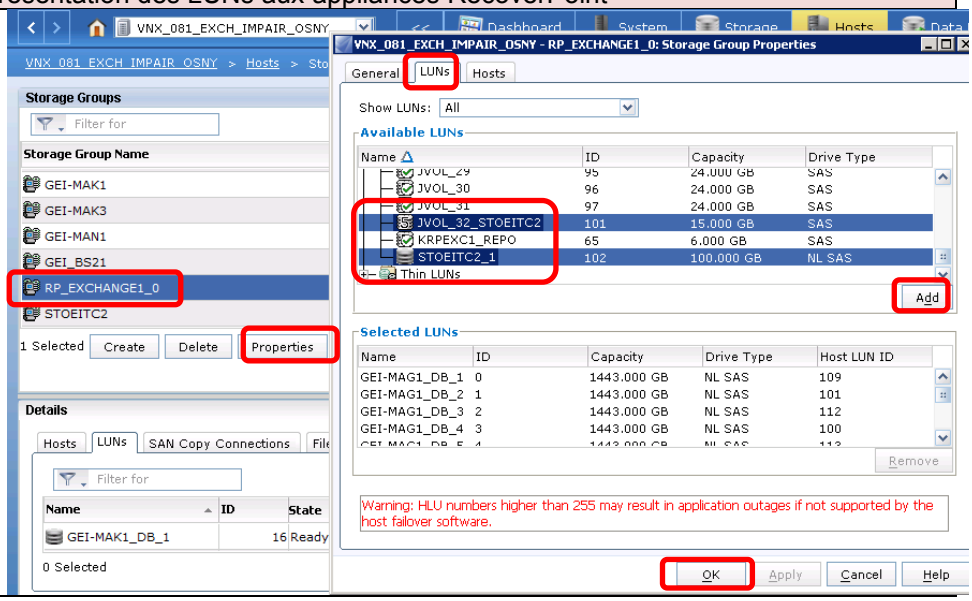
- Sélectionner le groupe "STOEITC2"
- Cliquer sur "Properties"
- Cliquer sur l'onglet "LUNs"
- Sélectionner le LUN à ajouter "STOEITC2_1"
- Cliquer sur "Add"
- Cliquer sur "Apply"



Présentation des LUNs aux appliances RecoverPoint

Dans l'interface de la baie :

- Sélectionner le groupe "RP_EXCHANGE1_0"
- Cliquer sur "Properties"
- Cliquer sur l'onglet "LUNs"
- Sélectionner le LUN à ajouter "STOEITC2_1" et les journaux RP "JVOL_32_STOEITC2"
- Cliquer sur "Add"
- Cliquer sur "Apply"

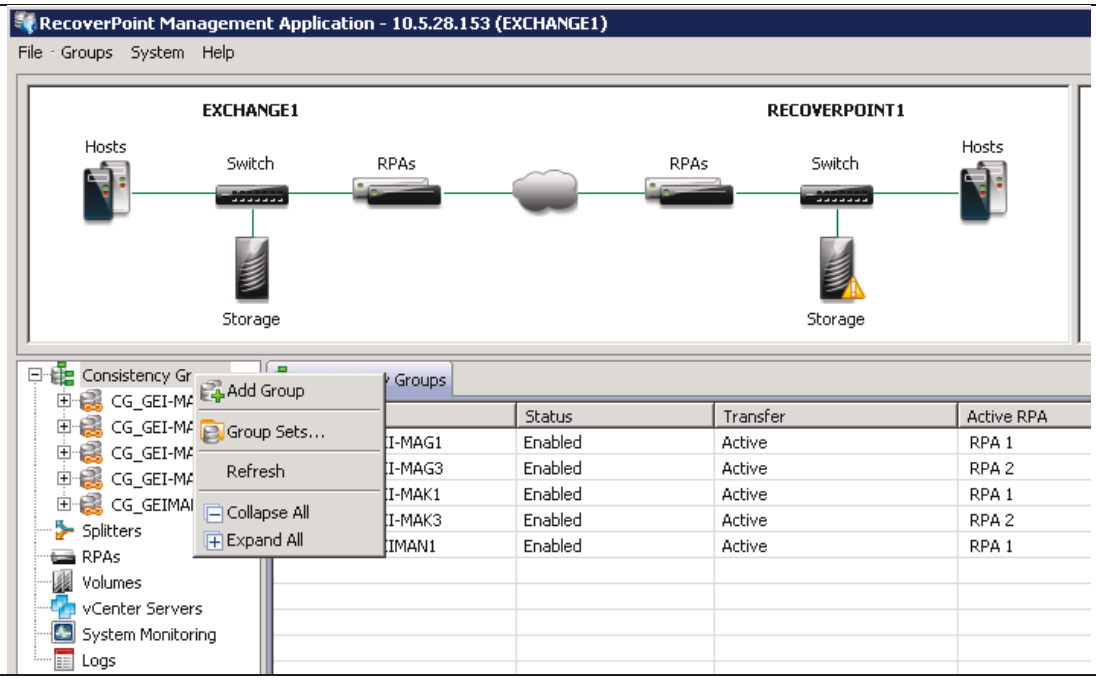


Procéder à la même opération sur la baie secondaire	

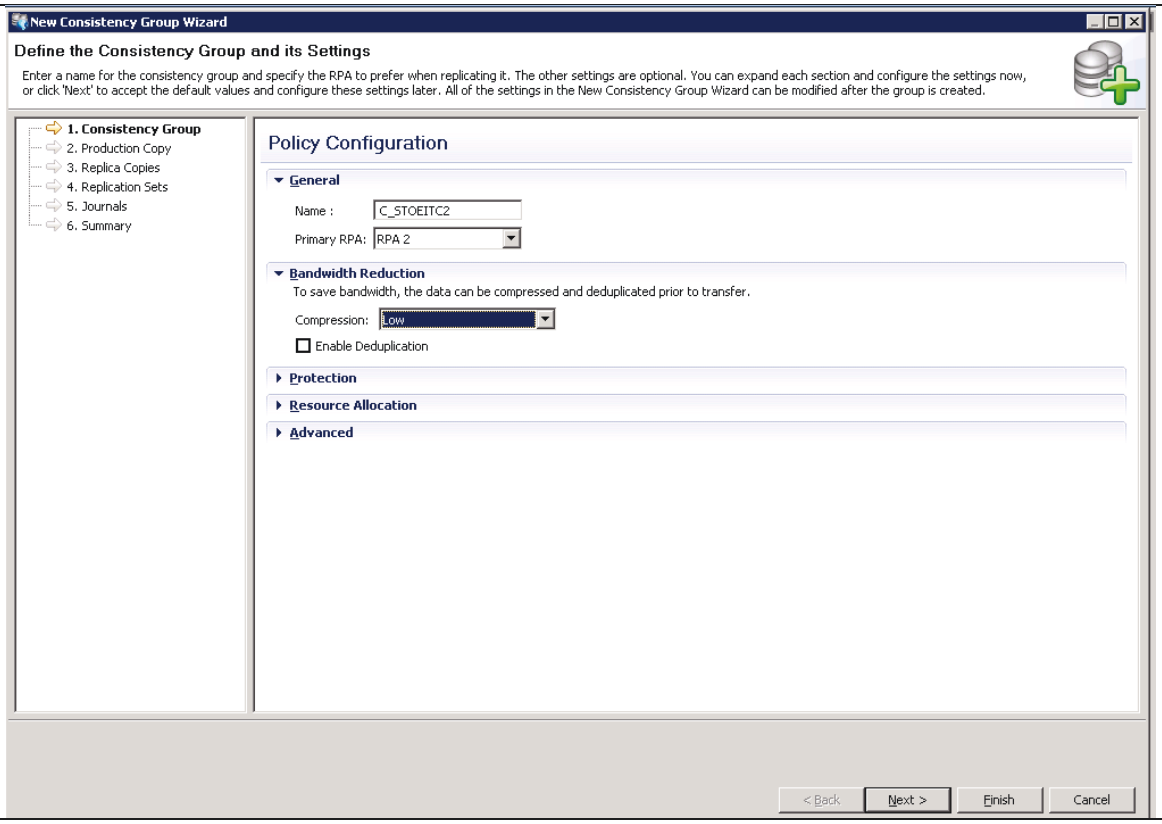
ANNEXE 22 : Paramétrage RecoverPoint

Dans la console d'administration des appliances RecoverPoint

- Faire une "Clic droit" sur "Consistency Group"
- Sélectionner "Add Group"



- Renseigner les champs
- Cliquer sur "Next"



- Renseigner les champs

☞ Cliquer sur "Next"

New Consistency Group Wizard

Define the Production Copy and its Settings

Enter a name for the production copy (the data to protect). If there are two sites in your configuration, specify the site at which the production copy is located in the Production Site field. The other settings are optional. You can expand each section and configure the settings now, or click 'Next' to accept the default values

1. Consistency Group
2. **Production Copy**
3. Replica Copies
4. Replication Sets
5. Journals
6. Summary

Production Site: EXCHANGE1

Policy Configuration

General

Name: STOEITC2_Prod

Journal Compression: None

Protection

Journal

Maximum Journal Lag:

Unlimited

Limited 0 MB

Proportion of journal allocated for image access log (20%-80%): 20

Journal size limit (GB): 5000

Advanced

Host OS: Windows

Reservations Policy: Auto

Fail-all variant Auto

Allow distribution of snapshots that are larger than capacity of journal volumes.

< Back | Next > | Finish | Cancel

☞ Renseigner les champs
☞ Cliquer sur "Next"

1. Consistency Group
2. Production Copy
3. **Replica Copies**
4. Replication Sets
5. Journals
6. Summary

Create Local Copy at EXCHANGE1

Policy Configuration

General

Name:

Journal Compression: None

Protection

Journal

Create Remote Copy at RECOVERPOINT1

Policy Configuration

General

Name: STOEITC2_BKP

Journal Compression: None

Protection

Journal

Advanced

Host OS: Windows

Reservations Policy: Auto

Fail-all variant Auto

Allow distribution of snapshots that are larger than capacity of journal volumes.

☞ Sélectionner le LUN source (à protéger)

☞ Cliquer sur "Next"

New Consistency Group Wizard

Select the Production Volumes for which to Create Replication Sets

Click 'Rescan' to update the list of available volumes at EXCHANGE1. Select the production volumes to replicate.
Click 'Next' to add the selected volumes to STOEITC2_Prod and begin configuring a replication set for each production volume. A replication set consists of one production volume, and one

1. Consistency Group
2. Production Copy
3. Replica Copies
4. **Replication Sets**
5. Journals
   5. 1. Production
   5. 2. Remote
6. Summary

Volumes at EXCHANGE1 that can be Added to Replication Set 1

Filter volumes by: Product | type filter text

Size	Vendor	Product	Name	UID
15.0GB	DGC	RAID 5	JVOL_32_STOEITC...	60,06,01,60,c3,60,2d,00,8a,0a,20,5a,ed,55,e
100GB	DGC	VRAID	STOEITC2_001 (102)	60,06,01,60,c3,60,2d,00,92,9a,c2,94,fc,58,e3

☞ Sélectionner le LUN cible
☞ Clic sur "Next"

New Consistency Group Wizard

Add Volume from RECOVERPOINT1 to Replication Set 1

Click 'Rescan' to update the list of available volumes at RECOVERPOINT1. Select the volume to use for the recovery of the specified production volume. For best performance during failo
select a volume that is the same size as the production volume. Click 'Next' to add the selected volume to the replication set of the production volume.

1. Consistency Group
2. Production Copy
3. Replica Copies
4. **Replication Sets**
   4. 1. Set 1
   4. 2. Summary
5. Journals
   5. 1. Production
   5. 2. Remote
6. Summary

Production Volume of Replication Set 1

Size	Vendor	Product	Name	UID
100GB	DGC	VRAID	STOEITC2_001 (102)	60,06,01,60,c3,60,2d,00,92,9a,c2,94,fc,58,e3,11

Volumes at RECOVERPOINT1 that can be Added to Replication Set 1

Filter volumes by: Product | type filter text

Size	Vendor	Product	Name	UID
100GB	DGC	VRAID	STOEITC2_1 (152)	60,06,01,60,33,00,2e,00,fa,5f,59,2d,ee,55,e3,11

1 volume(Volumes smaller than the production volume are not displayed)

Volume Details

Attached Splitters

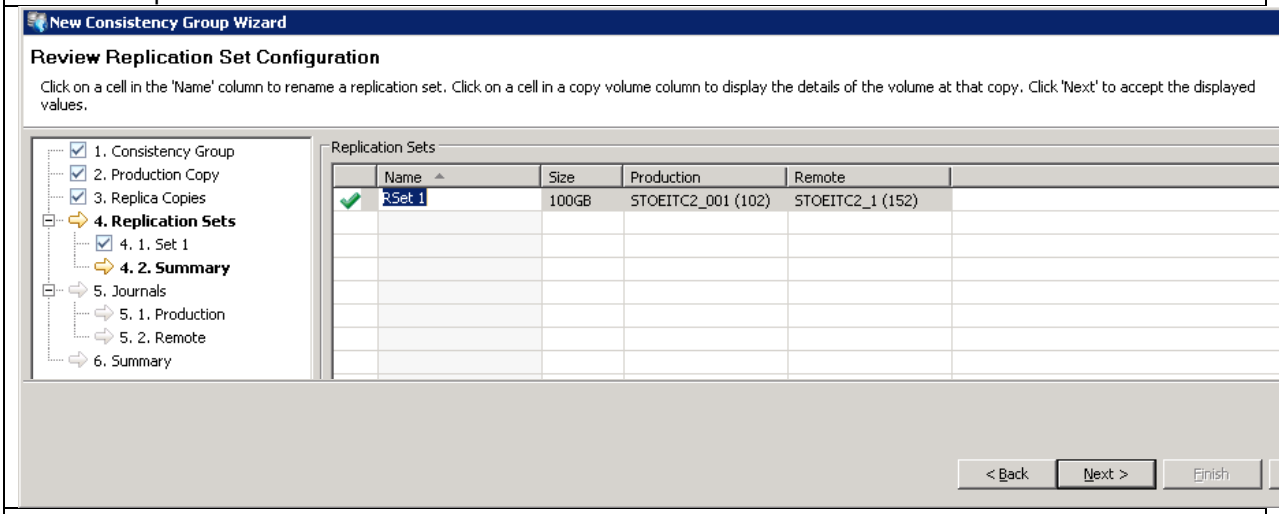
Status	Name
✓	CKM00112...
✓	CKM00112...

Paths from RPAs

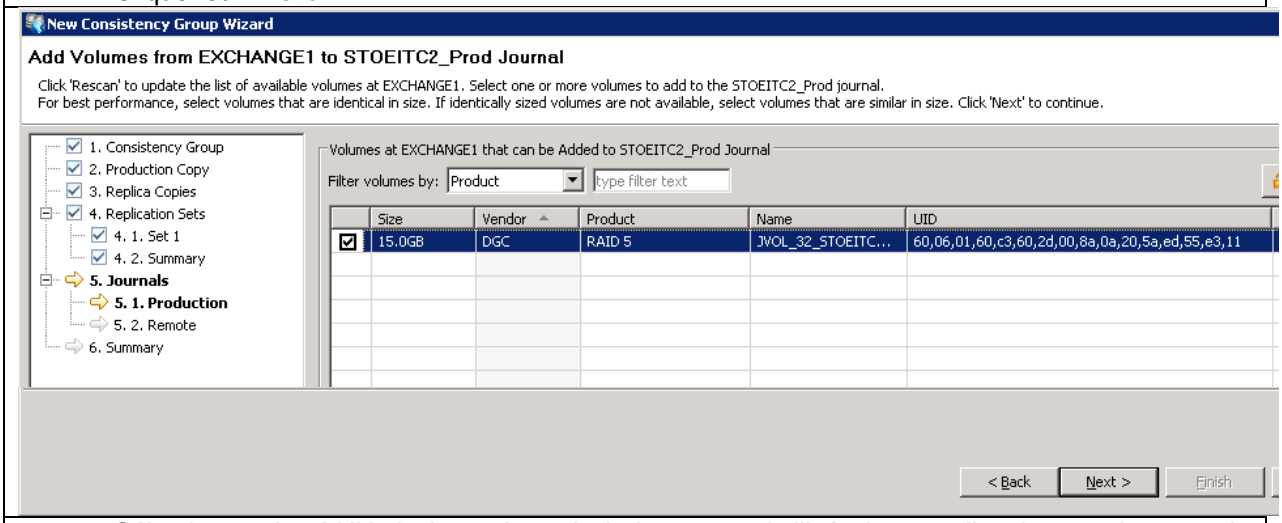
RPA	Port	WWN	Controller	Serial #	LUN
RPA 1	1	500601613ea01cd6	SP-A	CKM00112400080	32
RPA 1	1	500601693ea01cd6	SP-B	CKM00112400080	32
RPA 1	0	500601603ea01cd6	SP-A	CKM00112400080	32

< Back | Next > | Finish

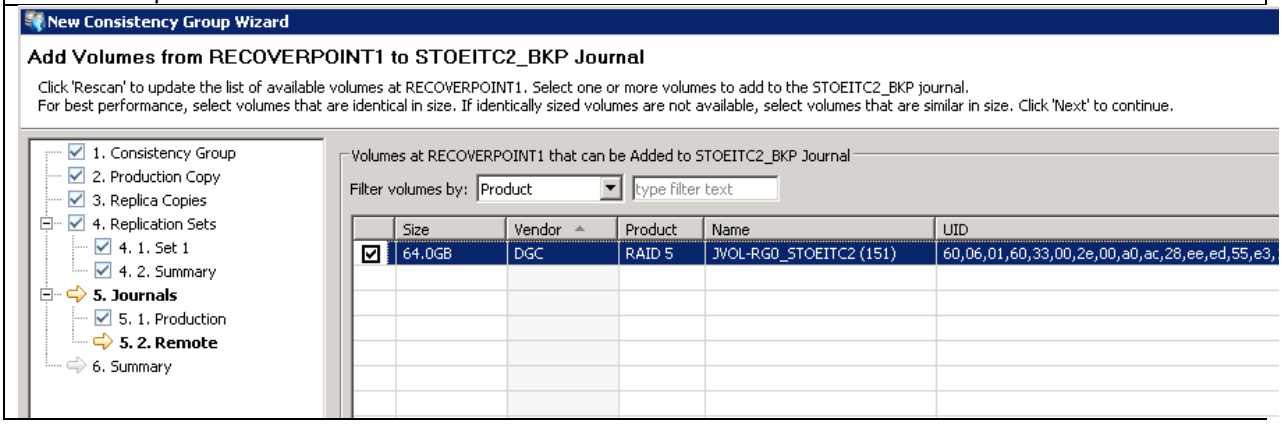
- Vérifier que les LUN ont été correctement définis
- Cliquer sur "Next"



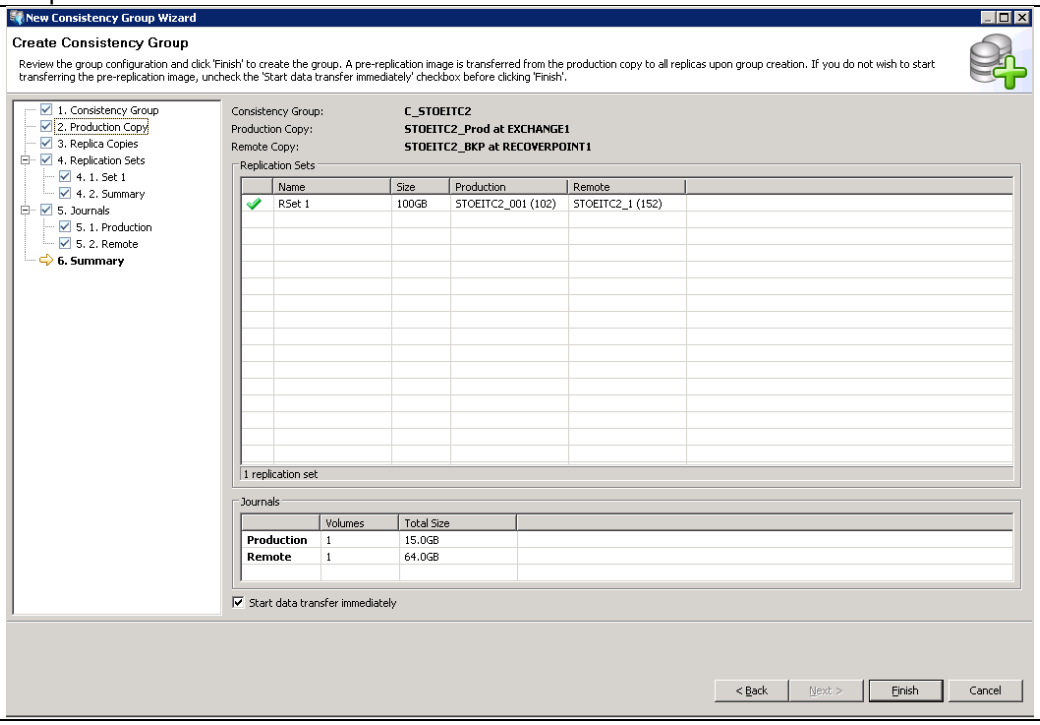
- Sélectionner les LUN du journal sur la baie source (active lorsque l'on inverse le sens de réplication)
- Cliquer sur "Next"



- Sélectionner les LUN du journal sur la baie source (utilisés lorsque l'on inverse le sens de réplication)
- Cliquer sur "Next"



- Sélectionner les LUN du journal sur la baie secondaire
- Cliquer sur "Next"



ANNEXE 23 : Restauration RecoverPoint

Tableau XXIX : Séquencement de l'expérimentation

N°	Date /heures	Actions réalisées	Taille (Mo)	Temps
1	16/01/2014 10:20	Prise d'une image témoin : "TST-INIT-00"		10 s
2	16/01/2014 10:25	Ajout de données sur le serveur STOEITC2	1.84 Go	3 min
3	16/01/2014 10:30	Prise d'une image la suppression des données : "AVANT-SUP-01"		10 s
4	16/01/2014 10:35	Suppression de tous les fichiers et dossiers sur STOEITC2	- 1.84 Go	35 s
5	16/01/2014 10:45	Restauration de l'image "AVANT-SUP-01" sur STOEITC1 (Serveur PRA)	1.84 Go	1 min
6	16/01/2014 11:17	Ajout d'un fichier témoin sur STOEITC1		30 s
7	16/01/2014 11:35	Recopie de la LUN vers le serveur de Production (STOEITC2)		1 min
8	16/01/2014 11:51	Réactivation de la réplication vers le site de PRA		30 s

ÉTAPE 1 : Prise d'image

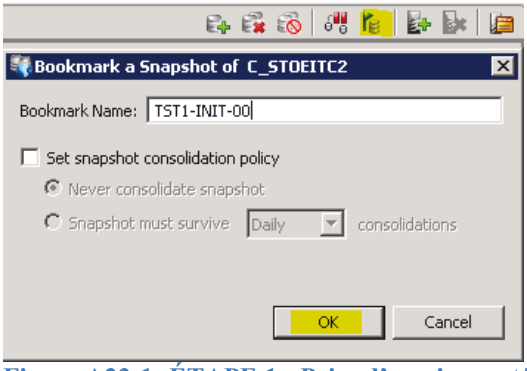


Figure A23-1: ÉTAPE 1 - Prise d'une image témoin

L'action est réalisée en quelques secondes en respectant la procédure donnée au chapitre 5.3.1.1 (page 109).

ÉTAPE 2 : Ajout de données

Sur le disque protégé, j'ai ajouté 1.84 Go de données dans le répertoire "E:\Nouvelles Données".

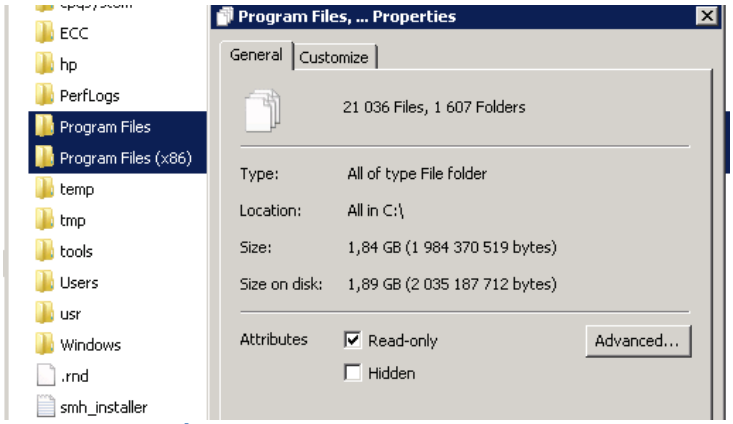
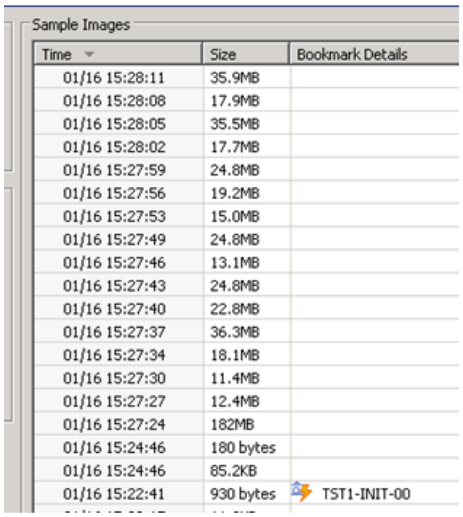


Figure A23-2 : ÉTAPE 2 – Ajout de données sur le disque primaire

Lors de l'exécution de cette action, on constate des modifications dans les journaux RecoverPoint :

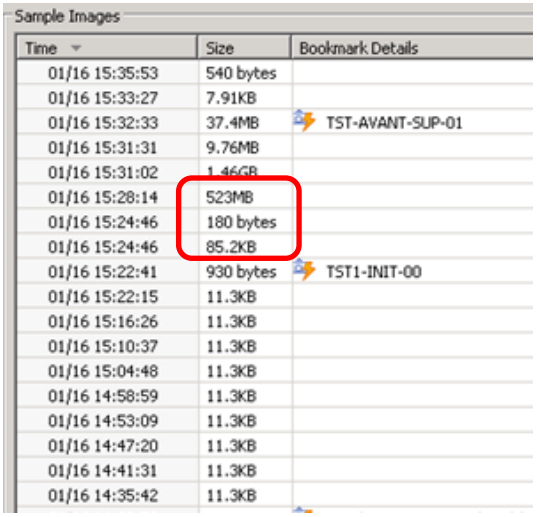
- les écritures sont journalisées et forment différentes images de plusieurs dizaines de mégaoctets (cf..figure A23-3) ;
- les images sont ensuite regroupées afin d'améliorer la lisibilité (cf. figure A23-4). Cela diminue le nombre d'images tout en augmentant leur taille.



Sample Images

Time	Size	Bookmark Details
01/16 15:28:11	35.9MB	
01/16 15:28:08	17.9MB	
01/16 15:28:05	35.5MB	
01/16 15:28:02	17.7MB	
01/16 15:27:59	24.8MB	
01/16 15:27:56	19.2MB	
01/16 15:27:53	15.0MB	
01/16 15:27:49	24.8MB	
01/16 15:27:46	13.1MB	
01/16 15:27:43	24.8MB	
01/16 15:27:40	22.8MB	
01/16 15:27:37	36.3MB	
01/16 15:27:34	18.1MB	
01/16 15:27:30	11.4MB	
01/16 15:27:27	12.4MB	
01/16 15:27:24	182MB	
01/16 15:24:46	180 bytes	
01/16 15:24:46	85.2KB	
01/16 15:22:41	930 bytes	TST1-INIT-00

Figure A23-3 : ÉTAPE 2 : Snapshots avant regroupement



Sample Images

Time	Size	Bookmark Details
01/16 15:35:53	540 bytes	
01/16 15:33:27	7.91KB	
01/16 15:32:33	37.4MB	TST-AVANT-SUP-01
01/16 15:31:31	9.76MB	
01/16 15:31:02	1.46GB	
01/16 15:28:14	523MB	
01/16 15:24:46	180 bytes	
01/16 15:24:46	85.2KB	
01/16 15:22:41	930 bytes	TST1-INIT-00
01/16 15:22:15	11.3KB	
01/16 15:16:26	11.3KB	
01/16 15:10:37	11.3KB	
01/16 15:04:48	11.3KB	
01/16 14:58:59	11.3KB	
01/16 14:53:09	11.3KB	
01/16 14:47:20	11.3KB	
01/16 14:41:31	11.3KB	
01/16 14:35:42	11.3KB	

Figure A23-4: ÉTAPE 2 : Snapshots après regroupement

ÉTAPE 3 et 4 : Prise d'image et suppression de données

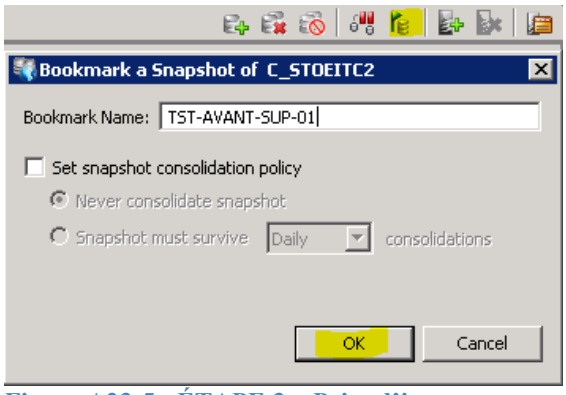


Figure A23-5 : ÉTAPE 3 – Prise d'image

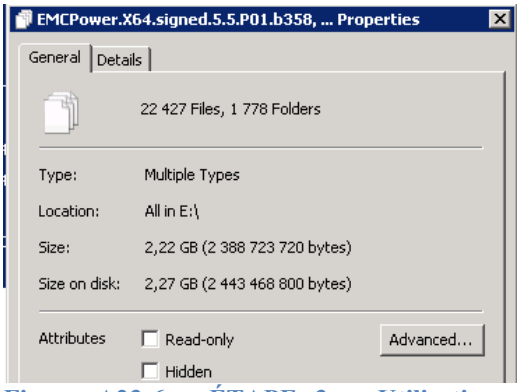


Figure A23-6 : ÉTAPE 3 – Utilisation du

J'ai effacé l'ensemble des fichiers et répertoires du lecteur E : (protégé par RecoverPoint). L'ensemble comportait près de 2.3 Go de données.

ÉTAPE 5 : Restauration sur le serveur PRA

En état de fonctionnement dit "normal", les données modifiées sur le serveur de production sont transmises sur le système de stockage secondaire. Afin de le protéger, et qu'il ne soit pas corrompu par le serveur de PRA, ce dernier n'a pas accès à ce stockage.

En fonction de l'état du système, les accès aux stockages changent d'état. Les lignes pointillées vertes permettent de visualiser les équipements qui y sont connectés (cf. figure A23-7).

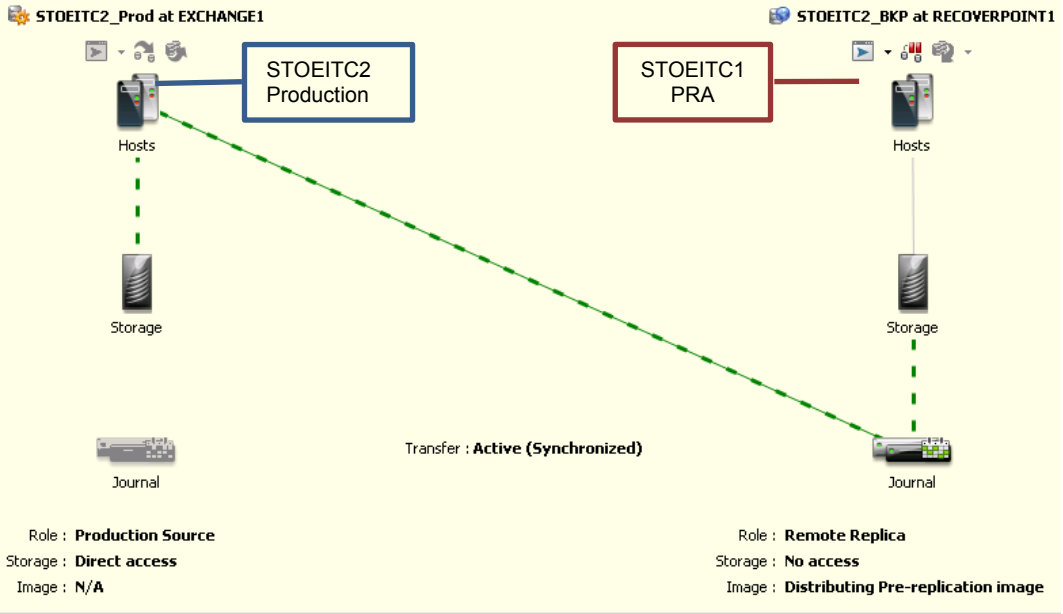


Figure A23-7 : ÉTAPE 5 – Prise d'image

La phase de restauration est organisée en plusieurs sous-étapes :

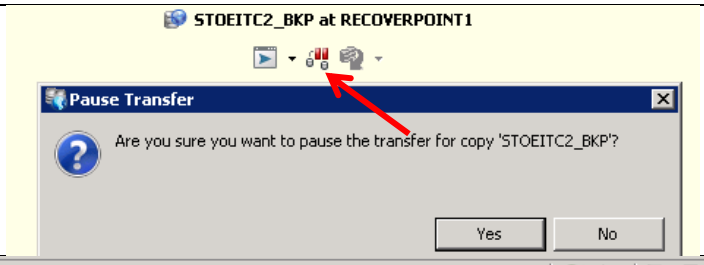
- ☞ l'arrêt de la réplication vers le PRA ;
- ☞ le montage de l'image "TST-AVANT-SUP-01" ;
- ☞ la vérification du contenu du LUN.

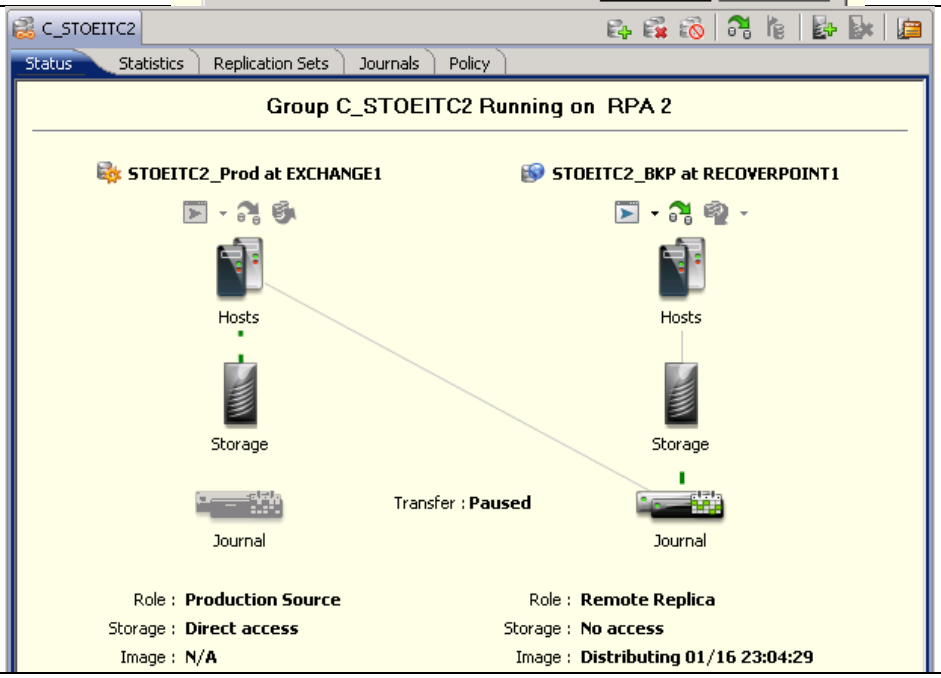
La procédure qui a été appliquée pour récupérer les données sur le serveur de PRA (STOEITC1) est décrite ci-après :

Restauration sur le serveur PRA

Arrêt de la réplication :

- ☞ Cliquer sur "Pause Transfer"
- ☞ Cliquer sur "Yes"

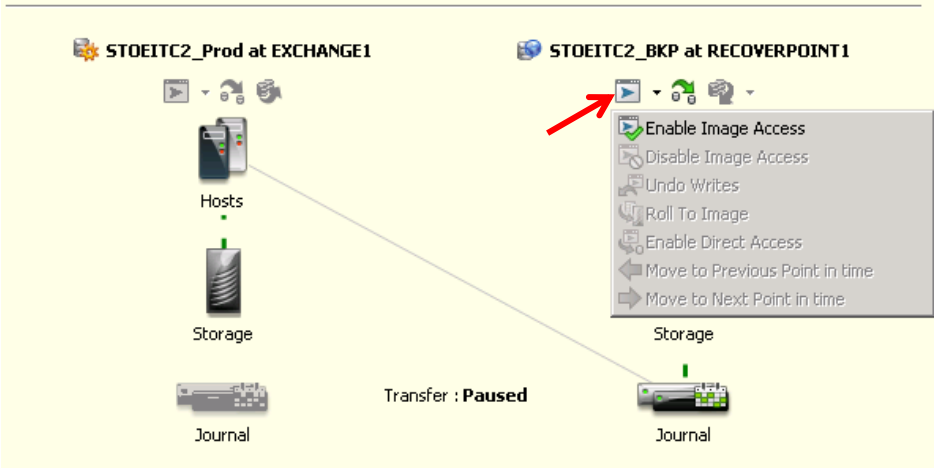




- ➢ Les données ne sont plus répliquées vers le serveur PRA
- ➢ Le serveur PRA(STOEITC1) n'a toujours pas accès aux données

Montage de L'image

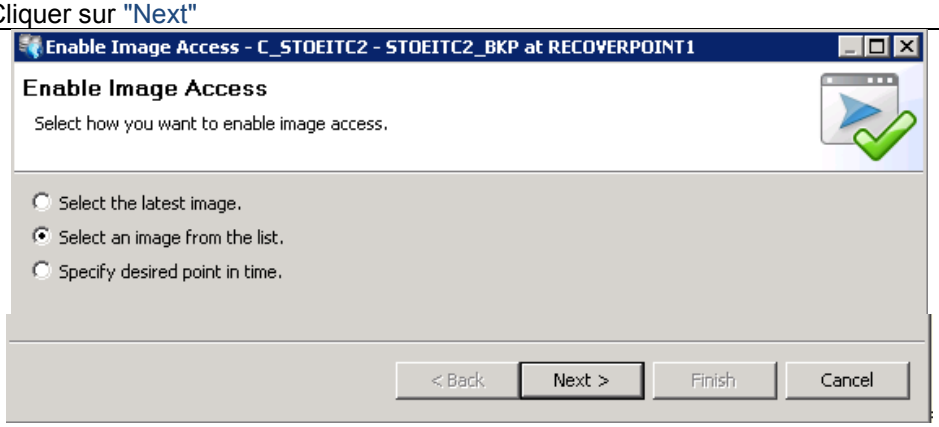
- ☞ Cliquer sur "Enable Image Access"



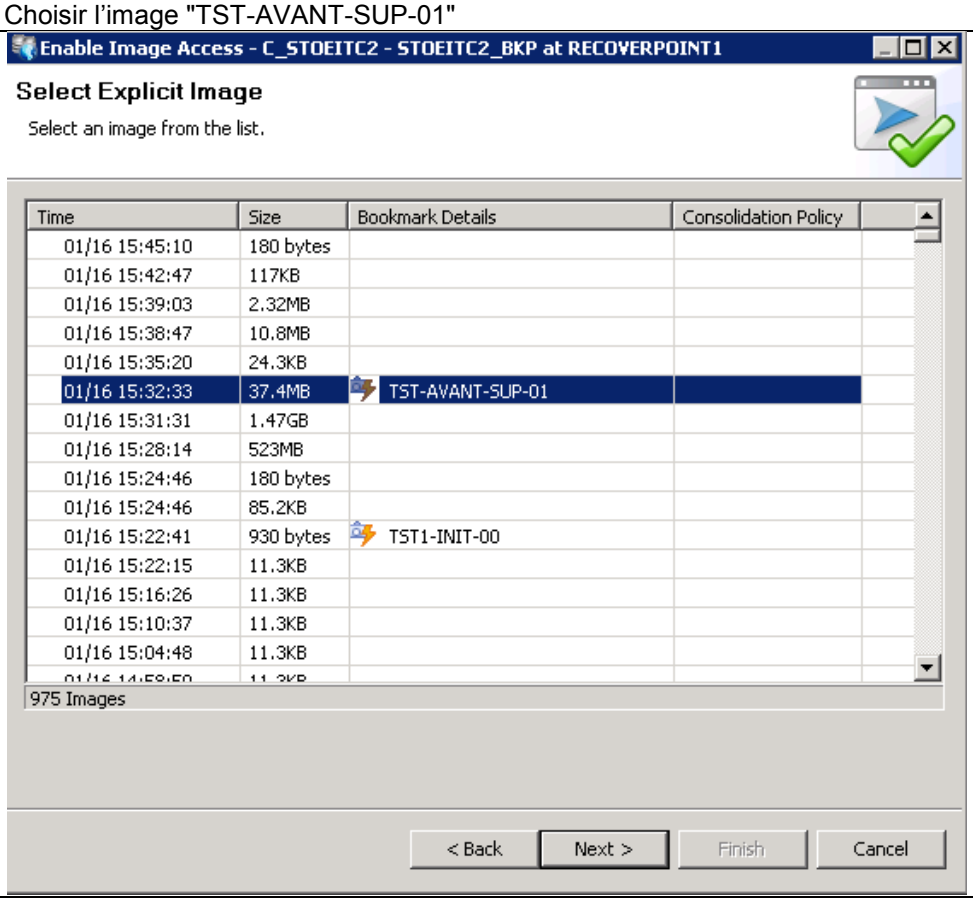
*

- ☞ Choisir "Select an image from the list"

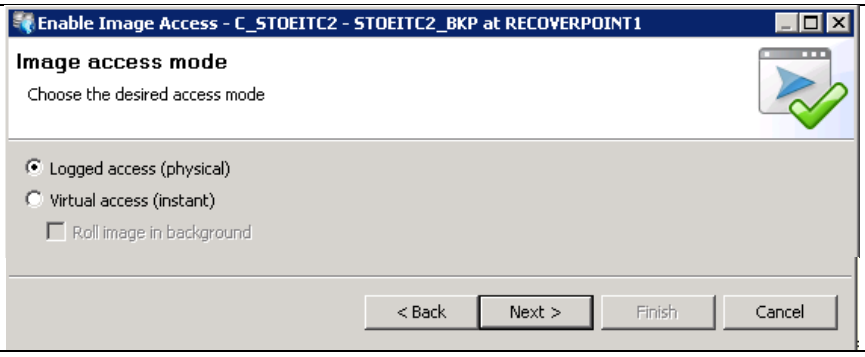
☞ Cliquer sur "Next"



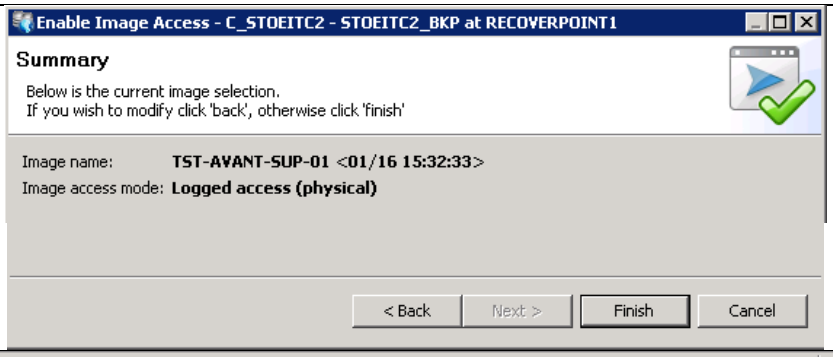
☞ Choisir l'image "TST-AVANT-SUP-01"

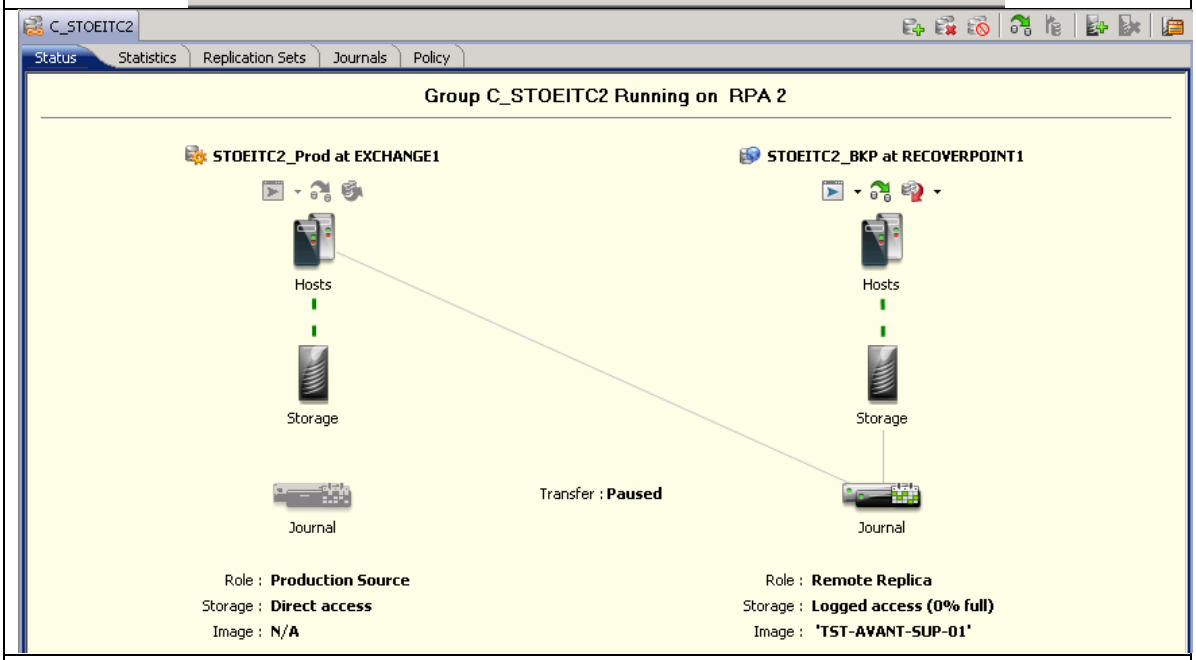


☞ Choisir l'image "Logged access (physical)"
☞ Cliquer sur "Next"



☞ Cliquer sur "Finish"





Remarque :

- Les serveurs de production et de PRA ont désormais accès à leur propre stockage.
- Le LUN est bien présenté au serveur PRA (STOEITC1), mais celui-ci n'en est pas forcément informé…

Effectivement, lors de l'exécution du scénario, les informations affichées dans l'explorateur Windows du serveur STOEITC1 (Serveur PRA) étaient inexactes : il manquait le répertoire "E:\Nouvelles Données" (cf. figure A23-8) qui avait été ajouté lors de l'étape 2.

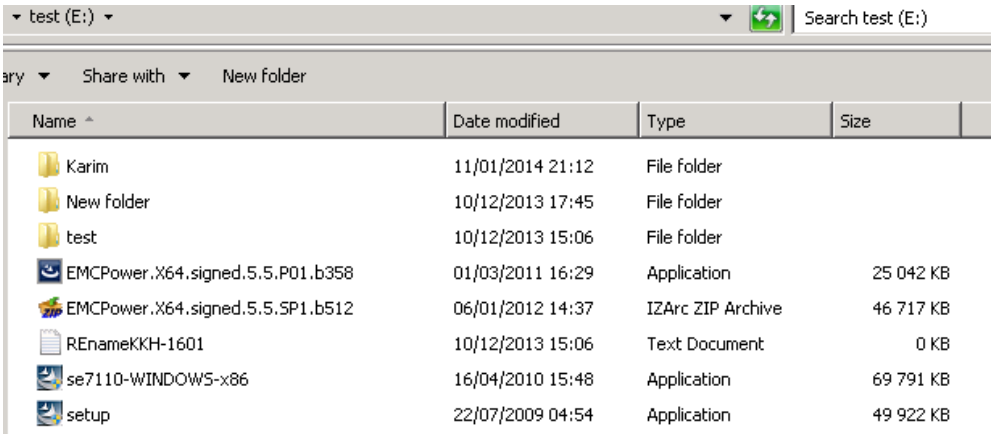


Figure A23-8 : Contenu de l'explorateur après la présentation

Pour corriger cette anomalie, il a fallu forcer un rafraîchissement des disques du serveur à l'aide de la console "Server Manager" du serveur STOEITC1.

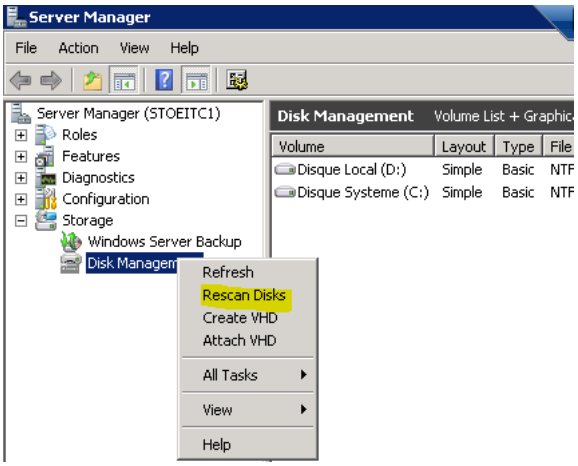


Figure A23-9:"Rescan" des disques (Server Manager)

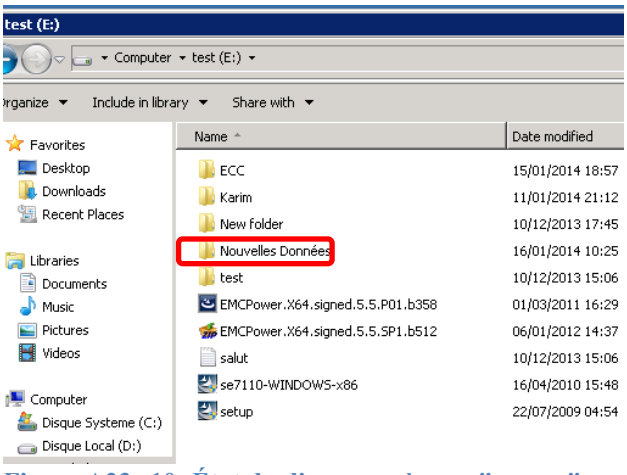


Figure A23--10: État du disque après son "rescan"

ÉTAPE 6 : Ajout d'un fichier sur le serveur PRA

L'objectif de cette étape est de vérifier que l'on peut modifier une image restaurée avant de la mettre en production.

Lorsque j'ai essayé d'ajouter un fichier, l'accès m'a été refusé. Après quelques recherches,j'ai effectivement constaté au travers de la console d'administration du serveur que le disque était en "lecture seul" (cf. figure A23-10). Pour remédier à ce problème, j'ai été contraint de le déconnecter, puis de le reconnecter. Suite à ces modifications, j'ai pu créer le fichier témoin :"20140116_11-15-00.txt"(cf. figure A23-11).

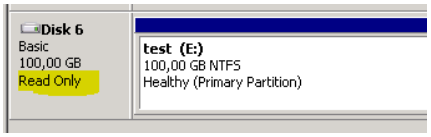


Figure A23-10: Disque E: en lecture seule

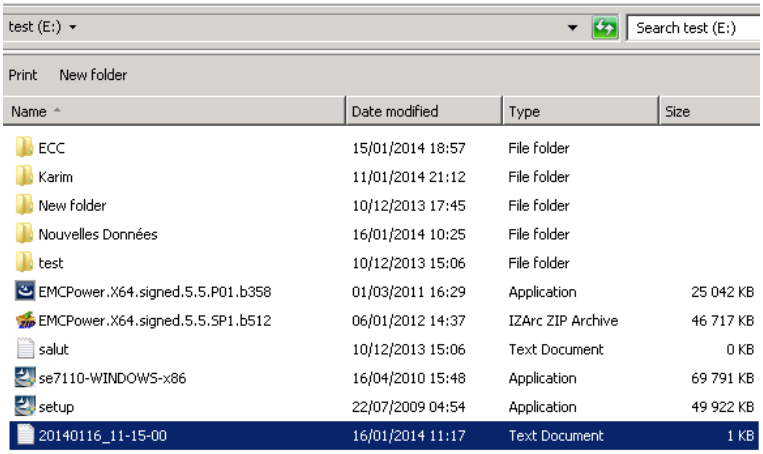


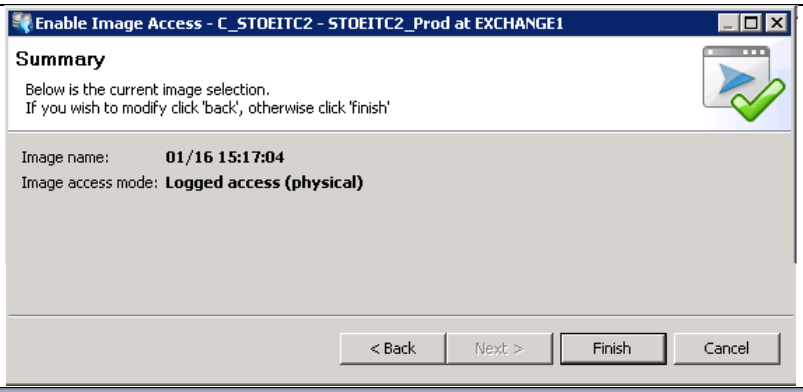
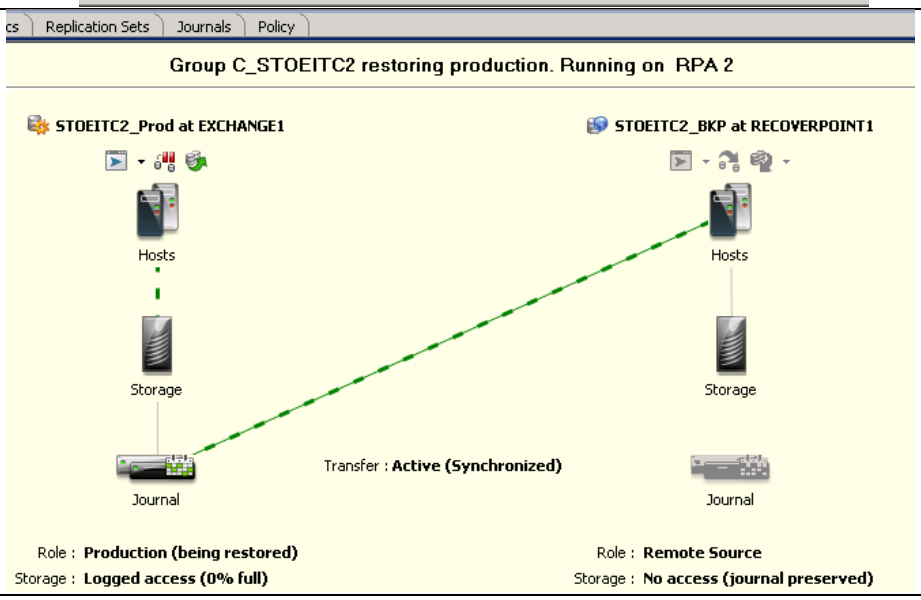
Figure A23-11:STOEITC1("E :") après la création du fichier témoin

ÉTAPE 7 : Restauration vers le serveur de production

La procédure ci-dessous montre comment inverser le sens de réplication afin d'actualiser les LUN de production et rendre le serveur de production de nouveau opérationnel.

ACTIONS	ILLUSTRATIONS
Actualiser les données du serveur de production	
☞ Cliquer sur "Failover Actions" ☞ Cliquer sur "Recover Production"	Replication Sets / Journals / Policy Group C_STOEITC2 Running on RPA 2 STOEITC2_Prod at EXCHANGE1 — Hosts — Storage — Journal STOEITC2_BKP at RECOVERPOINT1 — Hosts — Storage — Journal Failover to STOEITC2_BKP Recover Production Transfer : **Paused** Role : **Production Source** / Storage : **Direct access** / Image : **N/A** Role : **Remote Replica** / Storage : **Logged access (0% full)** / Image : **'TST-AVANT-SUP-01'**
☞ Cliquer sur "Yes"	**Recover Production** Do you wish to perform production restore? ☑ Start transfer from STOEITC2_BKP? Yes / No
☞ Cliquer sur "Yes"	**Warning** Host access to storage in remote copy will be blocked. Do you wish to continue? Yes / No
Le système initialise la restauration.	STOEITC2_Prod at EXCHANGE1 — Hosts — Storage — Journal STOEITC2_BKP at RECOVERPOINT1 — Hosts — Storage — Journal Transfer : **Paused by system** Role : **Production (being restored)** / Storage : **Direct access** / Image : **N/A** Role : **Remote Source** / Storage : **Enabling logged access** / Image : **'TST-AVANT-SUP-01'**

Le stockage de production est synchronisé. Les stockages ne sont plus accessibles ni par le serveur de production, ni par le serveur de PRA.	STOEITC2_Prod at EXCHANGE1 / STOEITC2_BKP at RECOVERPOINT1 Hosts / Hosts Storage / Storage Journal / Transfer : **Active (Synchronized)** / Journal Role : **Production (being restored)** / Role : **Remote Source** torage : **No access** / Storage : **No access (journal preserved)** Image : **Distributing 01/16 15:04:53** / Image : **N/A**
Activation du stockage sur le serveur de production	
☞ Cliquer sur "Image Access" ☞ Cliquer sur "Enable Image Access"	STOEITC2_Prod at EXCHANGE1 / STOEITC2_BKP at RECOVERPOINT1 Enable Image Access Disable Image Access Undo Writes Roll To Image Enable Direct Access Move to Previous Point in time Move to Next Point in time Hosts / Hosts Storage / Storage Journal / Transfer : **Active (Synchronized)** / Journal
☞ Choisir : "Select an image from the list" ☞ Cliquer sur "Next"	Enable Image Access - C_STOEITC2 - STOEITC2_Prod at EXCHANGE1 **Enable Image Access** Select how you want to enable image access. Select the latest image. Select an image from the list. Specify desired point in time. < Back / Next > / Finish / Cancel
☞ Choisir "Select an image from the list" ☞ Cliquer sur "Next"	Enable Image Access - C_STOEITC2 - STOEITC2_Prod at EXCHANGE1 **Image access mode** Choose the desired access mode Logged access (physical) Virtual access (instant) Roll image in background < Back / Next > / Finish / Cancel

☞ Cliquer sur "Finish"	
Le serveur de production STOEITC2 a de nouveau accès à ses données.	

Le stockage du serveur STOEITC2 retrouve ses caractéristiques initiales et son LUN restauré avec le fichier témoin que l'on a ajouté.

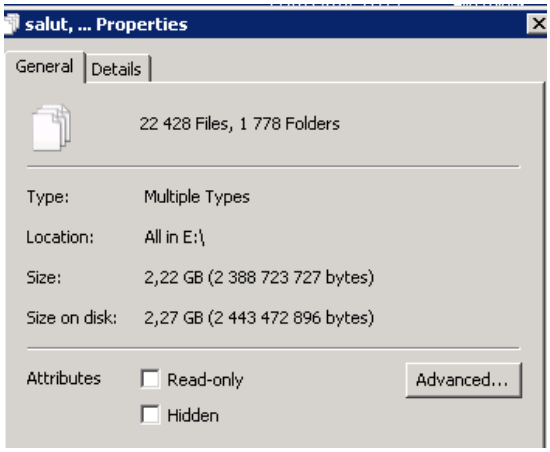


Figure A23-12: Utilisation de E : après restauration

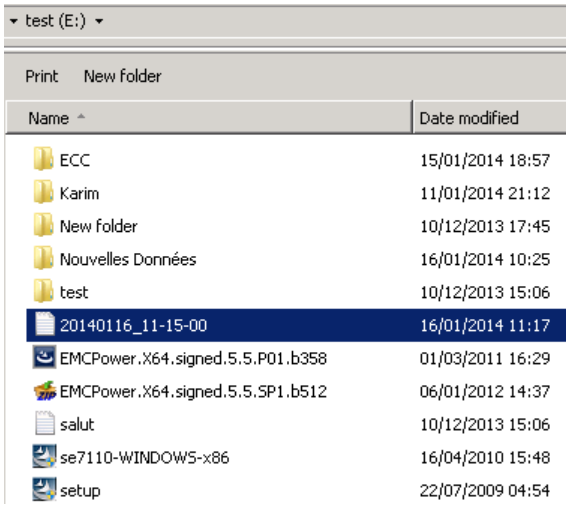
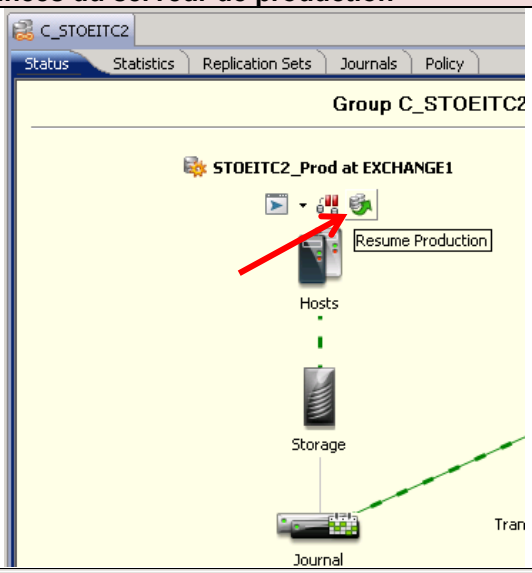
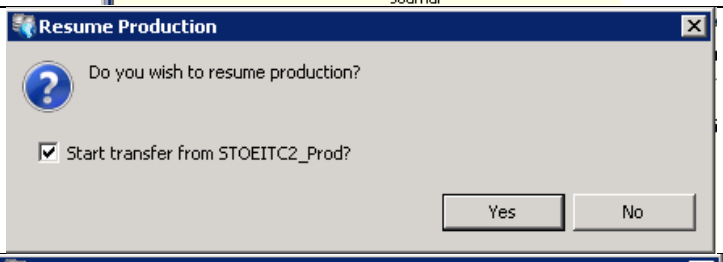
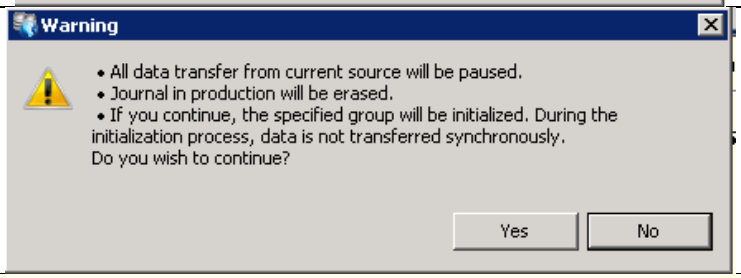
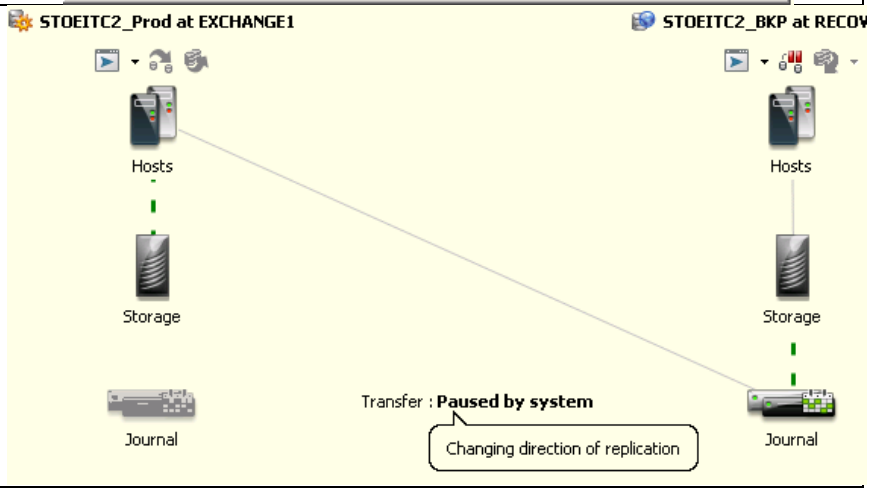


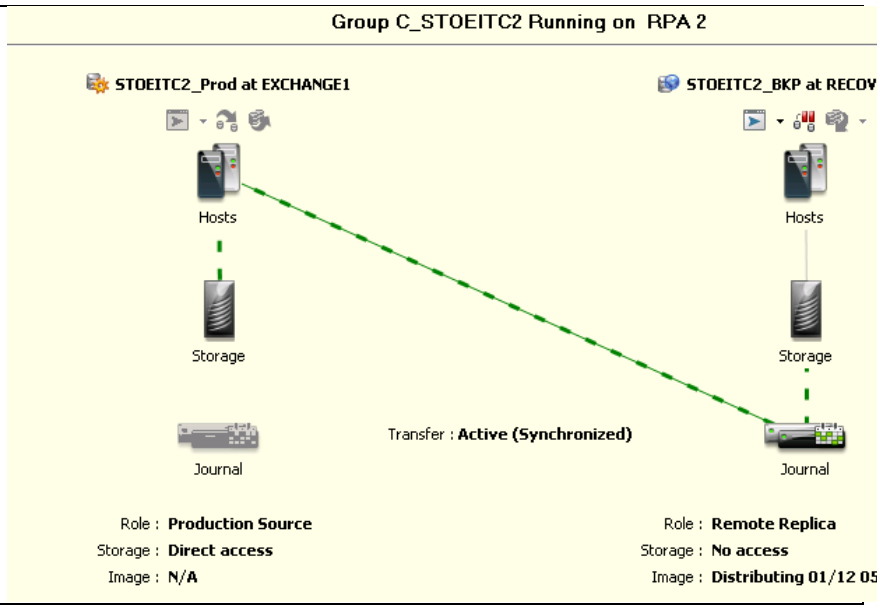
Figure A23-13 :STOEITC1 ("E :") après restauration

Remarque : À ce stade, le serveur de production est opérationnel, mais il n'est plus protégé par RecoverPoint .

ÉTAPE 7: Réactivation de la réplication vers le site de PRA

L'objectif de ces actions est de réactiver la réplication des LUN vers le site PRA

ACTIONS	ILLUSTRATIONS
Actualiser les données du serveur de production	
☞ Cliquer sur "Resume Production"	
☞ Cliquer sur "Yes"	
☞ Cliquer sur "Yes"	
Initialisation de la synchronisation	



La situation est de nouveau stable et le serveur de production est répliqué. Cette opération peut être réalisée en moins de 10 minutes, ce qui est relativement rapide.

On peut aussi remarquer que le journal contient toujours les images qui ont été prises avant le début de la restauration des LUN :

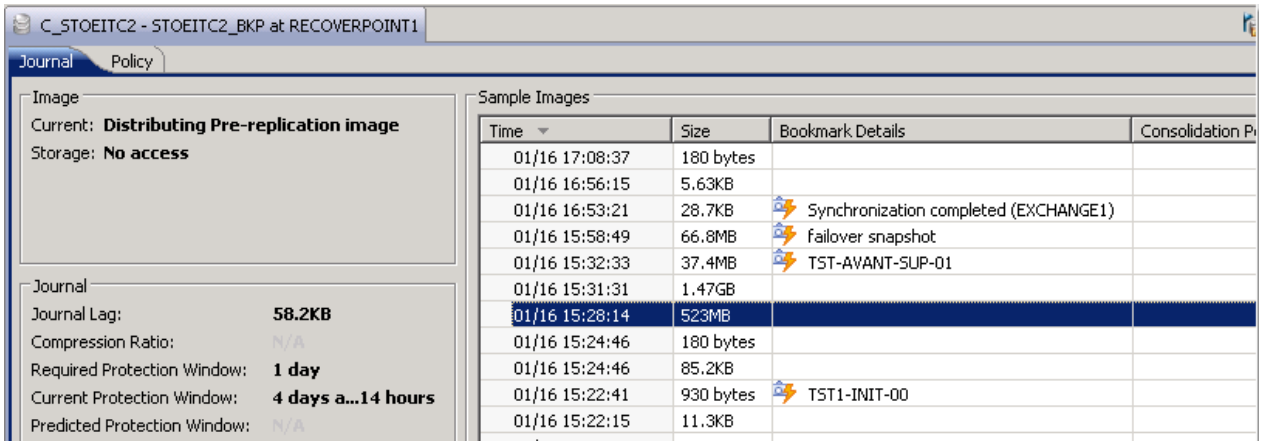


Figure A23-14 : Extrait du journal du groupe de cohérence "C_STOEITC2"

Remarque : Dans le cas d'une erreur de manipulation (activation du failover sur une version), ce journal risque d'être totalement vidé et on ne sera plus en mesure de récupérer aucune autre version. Les conséquences peuvent être très dommageables, car si une mauvaise version a été restaurée, la bonne version ne sera plus récupérable.

BIBLIOGRAPHIE

1. LE STOCKAGE

[STORAGEA01] POELKER C., NIKITIN A, 2009, "Storage Area Networks for Dummies", WILEY Publihing, Inc,438 pages

[STORAGEA02] HDS Academy,2012, ”Storage Concept - Storing and Managing Digital Data”,MANIJAK P, STEWART M., VILD Pavel, 345 pages

[STORAGEF03] GEARGEOT C., 2011, "BONNES PRATIQUES, PLANIFICATION ET DIMENSIONNEMENT DES INFRASTRCTURES DE STOCKAGE ET DE SERVEUR EN ENVIRONNEMENT VIRTUEL", Books On Demand GmbH, 136 pages

[STORAGEA04] Dave Russel,Sheila Childs,Alan Dayley, 28/01/2011, “Magic Quadrant for Entreprise Disk-Based Backup/Recovery”, Gartner RAS, 16 pages

2. LA PROTECTION CONTINUE DES DONNEES

[CDPA01] 2012,"Continuous Data Protection(CDP)", Backup for Workgroup™, Anglais, Document décrivant les principes du CDP et notamment ses avantages et inconvénients
http://www.backup-for-workgroups.com/what-is-continuous-data-protection-CDP.html

[CDPF02] 10/04/2011,STERCKMANS Nicolas, "Protection continue…",Français, Rôle que peut jouer le CDP vis-à-vis des PRA et des autres solutions de sauvegarde.
http://maitrisedelasauvegarde.com/2011/04/10/protection-continue/#more-372

[CDPF03] 9/05/2011,"Continuious Data Protection",Wikipedia, Français, Quelques lignes décrivant très brièvement le concept du CDP
http://fr.wikipedia.org/wiki/Continuous_Data_Protection

[CDPA04] 12/11/2011,"Continuious data protection",Wikipedia, Anglais, Description détaillée du concept CDP ainsi que des solutions
http://en.wikipedia.org/wiki/Continuous_data_protection

2. LES DIFFERENTES SOLUTIONS CDP

2.1. ASIGRA

[ASIGRAA01] 2012,"Asigra Web site",Asigra, Anglais,
Site internet présentant les différentes technologies et produits
http://www.asigra.com/

[ASIGRAA02] 2012,"Asigra Web site",Asigra, Anglais,
Site internet présentant les différentes technologies et produits
http://www.asigra.com/product/continuous-data-protection

2.2. NETBACKUP REALTIME

[NETBKPF01] 2011,"NetBackup RealTime",Infoniqa, Français,
Description synthétique de la solution CDP NetBackup Realtime
http://www.infoniqa.ch/index.php/fr/produits/infrastructure-et-storage-management/symantec/52-netbackuprealtime.html

[NETBKPF02] 2011,"Symantec NetBackup RealTime",Symantec,Français,
Site Internet présentant NetBackup RealTime
http://www.symantec.com/fr/fr/business/netbackup-realtime

[NETBKPA03] Symantec, "NetBackup RealTime 7.0",Daniel de Prezzo, Présentation Powerpoint en anglais du produit Netbackup Realtime, 30 pages

2.3. FALCONSTOR CDP

[FALSTOF01] 26/07/2011,STERCKMANS Nicolas,"CDP Appliance", Maitrise de la sauvegarde,Français,
Description détaillée de la solution CDP de FalconStor Continuous Data Protector
http://maitrisedelasauvegarde.com/2011/07/26/cdp-appliance/

[FALSTOA01] 2011," Instant Microsoft Application Recovery with FalconStor CDP ",FalconStor, Anglais,
Vidéo de présentation de la solution FalconStor CDP
http://www.falconstor.com/library/videos-and-podcasts/webcasts/Instant-Microsoft-Application-Recovery-with-FalconStor-CDP/10/64/1

2.4. EMC RECOVERPOINT

[EMCA01] "RecoverPoint",Wikipedia,Langue Anglais,
Description du fonctionnement du produit CDP proposé par EMC RecoverPoint
http://en.wikipedia.org/wiki/RecoverPoint

[EMCA02] 2008,Rick Walsworth," EMC RecoverPoint Overview",EMC,Anglais,
Présentation des solutions de sauvegarde EMC
https://enterpriseportalcontent.mci.com/NR/rdonlyres/7A037904-A72F-4C79-BC21-4731442BFD9A/0/SoCDREventEMCReplicationRW.pdf

[EMCA03] 2011,"EMC RECOVERPOINT FAMILY", EMC, Anglais,
Présentation des solutions EMC RevoverPoint
http://www.emc.com/collateral/software/data-sheet/h2769-recoverpoint-ds.pdf

2.5. MICROSOFT DATA PROTECTION MANAGER

[MSDPMF01] 29/09/2005,BARDY Christophe,"Microsoft et Symentec lancent leurs solutions de backup continu sur disque", Le Monde Informatique,Français,
Annonce de lancement des produits CDP de Microsoft et Symantec
http://www.lemondeinformatique.fr/actualites/commentaires-microsoft-et-symantec-lancent-leurs-solutions-de-backup-continu-sur-disque-9378.html

[MSDPMA01] 3/10/2005,MEARIAN Lucas,"Mircosoft,Symantec Ready CDP Products", ComputerWorld, Anglais,
Brève description des produits Microsoft et Symantec
http://www.computerworld.com/s/article/105118/Microsoft_Symantec_Ready_CDP_Products
http://features.techworld.com/networking/2996/microsofts-troops-advance-on-cdp/

[MSDPMF02] 2011,"System Center Data Protection Manager 2007",Microsoft,Français,
Site Internet officiel présentant de l'outil DPM
http://www.microsoft.com/france/serveur/system-center/data-protection-manager.aspx

2.6. R1SOFT

[R1SOLFTA01] Site Internet officiel de R1Soft, Anglais,
http://www.r1soft.com/

[R1SOLFTA02] 8/06/2011,,"R1Soft Introduces CDP Server Backup Solution", The hosting news, Anglais,
Document évoquant la stratégie de R1Soft pour répondre aux nouveaux besoins des outils de sauvegardes
http://www.thehostingnews.com/r1soft-introduces-cdp-server-backup-solution-18471.html

[R1SOLFTA03] 18/09/2012,,"R1Soft", The hosting news, Anglais,
Document évoquant la stratégie de R1Soft pour répondre aux nouveaux besoins des outils de sauvegardes
http://en.wikipedia.org/wiki/R1Soft

2.7. CISCO

[CISCOF01] 2011,"Une Protection SmallBusiness – Cisco Small Business", CISCO, Français,
Site Web Présentant la solution CDP de Cisco
http://www.cisco.com/web/FR/solutions/smb/products/storage/small_business_continuous_data_protection/index.html

[CISCOF02] 2009,"Solution CDP (Continuous Data Protection de Cisco",Cisco,Français,
PDF de quelques pages présentant la solution CDP de Cisco
https://www.cisco.com/offer/email/FR/19843/French_Continuous_Data_Protection_for_Files.pdf

2.8. IBM

[IBMA01] ,"IBM Tivoli Continuous Data Protection for files",IBM,Anglais,
Document présentant les avantages du CDP et de la solution d'IBM
ftp://ftp.software.ibm.com/software/tivoli/datasheets/CDP_3-1_datasheet_TID10411-USEN-00.pdf

[IBMA02] GUCER V.,BASS G., BEUTTLER W.,KUBO M., 2007, "Deployment Guide Series: Tivoli Continuous Data Protection for Files V3.1", IBM, 390 pages

2.9. COFIO AIMSTOR

[COFIOA01] 14/01/2010, CERQUERIA Tony,"CDP is a Dog -> Unless it's UNIFIED with Backup",Anglais
Mise en garde sur les risques de mise en place de solution CDP non intégrée aux outils de sauvegardes
http://blog.cofio.com/?p=70

[COFIOA02] 2011,"AIMstor CDP",Cofio,Anglais, Site Web présentant la solution AIMstor CDP de Cofio
http://www.cofio.com/AIMstor-CDP/

[COFIOA03] 22/09/2011,"Cofio Software",Wikipedia,Anglais, Présentation de l'outils AIMstor de Cofio
http://en.wikipedia.org/wiki/Cofio_Software#AIMstor

[COFIOA04] 22/09/2011,"Cofio Software",Wikipedia,Anglais, Documentation de l'outil AIMstor de Cofio
http://doc.cofio.com/r

LISTE DES FIGURES

Figure 1-1 : Présentation du groupe CM-CIC 4
Figure 1-2 : La dimension Européenne du groupe CM-CIC 5
Figure 1-3 : L'informatique du groupe CM-CIC 6
Figure 1-4 : La composition des domaines d'Euro-Information Production 6
Figure 1-5 : Sauvegardes des agences 8
Figure 1-6 : La déduplication selon AVAMAR 9
Figure 1-7 : Sauvegardes des directions générales 10
Figure 1-8 : Réplications PureDisk 10
Figure 1-9 : Architecture NetBackup Protectier 11
Figure 1-10 : Réplication des Protectiers 11
Figure 1-11 : Architecture Exchange EMC RecoverPoint 12
Figure 1-12 : Architecture des NAS Netapp 13
Figure 2-1 : Exemple de réplication synchrone 17
Figure 2-2 : Les Clusters 21
Figure 2-3 : Différences entre CDP et les autres technologies [SYMANTEC] 23
Figure 2-4 : Les orientations du CDP 25
Figure 2-5 : Exemple d'architecture CDP favorisant la reprise d'activité 28
Figure 2-6 : Architecture Netbackup Realtime 29
Figure 2-7 : Problématique corruption de données 32
Figure 2-8 : Sauvegardes sur disques - Gartner 2011 32
Figure 2-9 : Architecture Simpana 34
Figure 2-10 : ContinuousDataReplicator 35
Figure 2-11 : Architecture EMC RecoverPoint 37
Figure 2-11 : Optimisation de la liaison RecoverPoint 38
Figure 2-12 : Les réplications RecovertPoint 39
Figure 2-13 : Options d'optimisation réseaux 39
Figure 2-14 : Paramétrage des rétentions RecoverPoint 40
Figure 2-15 : Architecture Netbackup Realtime 41
Figure 2-16 Les besoins en PRA selon Symantec 42
Figure 2-17 : Architecture Tivoli CDP for files 43
Figure 2-18 L'interface de Tivoli CDP for files 44
Figure 2-20 Prix public des licences IBM CDP for files 45
Figure 2-19 : Extrait documentation [IBMA02, page 60] 45
Figure 2-21 : Architecture ASIGRA [ASIGRAA01] 46
Figure 2-22 : Les Agents ASIGRA [ASIGRAA01] 47
Figure 2-23 : Architecture FalconStor CDP 49
Figure 2-24 : Présentation de RecoverTrac 51
Figure 2-25 : Lancement d'un script de reconstruction d'une VM avec RecoverTrac 51

Figure 2-26 : Stockage NetApp 52
Figure 2-27 : Architecture MS DPM 53
Figure 2-28 : MS DPM - Création d'un groupe de protection 54
Figure 2-29 : Architecture AIMstor 55
Figure 2-30 : Interface utilisateur AIMstor 56
Figure 2-31 : R1Soft – Principe de sauvegarde 57
Figure 2-32 : Les différentes versions de R1Soft 57
Figure 2-33 : Orientation des solutions étudiées 59
Figure 3-1 : Architecture existante 61
Figure 3-2 : Architecture cible 62
Figure 3-3 : Description du nouveau serveur de fichiers 65
Figure 3-4 : Intégration de Storage Foundation dans les outils d'administration Windows 66
Figure 3-5 : Paramétrage de la politique de sauvegarde Netbackup du serveur KSXBFHI1 67
Figure 3-6 : Paramétrage de l'agent DFM 67
Figure 3-7 : Statut des liens OSSV 71
Figure 3-8 : Statut détaillé des liens OSSV 71
Figure 3-9 : Accès aux précédentes versions depuis l'explorateur Windows 72
Figure 4-1 : Architecture de tests FalconStor CDP 77
Figure 4-2 : Architecture de tests FalconStor CDP 79
Figure 4-3 : Caractéristiques de la base de données de tests 79
Figure 4-4 : Architecture HyperTrac 80
Figure 4-5 : Présentation d'un LUN à l'aide de l'interface HyperTrac 81
Figure 4-6 : Extrait de la documentation 82
Figure 4-7 : Interface graphique d'administration FalconStor CDP (DiskSafe) 83
Figure 4-8 : Accès aux propriétés des disques par l'outil (DiskSafe) 83
Figure 4-9 : La gestion des snapshots par l'interface graphique Disksafe 84
Figure 4-9 : Extrait des journaux du client Falconstor CDP (Disksafe) 84
Figure 4-10 : Filtre du journal DiskSafe 85
Figure 4-10 : Filtre du journal DiskSafe 87
Figure 4-11 : La gestion des ressources logiques 88
Figure 4-12 : La gestion des réplications (IPStor) 89
Figure 4-13 : La gestion des clients SAN (IPStor) 89
Figure 4-14 : Liste non exhaustive de rapports proposés par la console IPStor 90
Figure 4-15 : Configuration de la planification des prises d'images 90
Figure 4-16 : Gestion des rétentions de FalconStor CDP 91
Figure 4-17 : Propriétés du journal CDP de FalconStor CDP 92
Figure 4-18 : Architecture de tests d'une base MS SQL Server protégée par FalconStor CDP 92
Figure 4-19 : Caractéristiques du journal CDP 94
Figure 4-20 : Architecture de tests MS SQL Server 95
Figure 4-21 : Paramétrage des prises d'images 97
Figure 4-22 : Extrait du journal Disksafe du serveur KIITDBMS 98
Figure 4-27 : Modification du nom du disque 99
Figure 4-28 : Trace de l'exécution du job HyperTrac 101

Figure 4-29 : Erreur générée sur les serveurs Linux 102
Figure 4-30 : Exemple de rapport sur l'utilisation de l'espace de stockage 104
Figure 4-31 : Planification d'un rapport 104
Figure 4-31 : Classement des rapports 105
Figure 4-31 : Rapport de stockage (IPStor) 106
Figure 5-1 : Architecture de tests EMC RecoverPoint 110
Figure 5-1 : RecoverPoint - Procédure manuelle de prise d'images depuis la console d'administration 112
Figure 5-2 : Détail du journal du groupe de cohérence "C_STOEITC2" après une prise d'image manuelle 112
Figure 5-3 : RecoverPoint - Paramétrage de la politique de consolidation des snapshots 113
Figure 5-4 :RecoverPoint – Notion de consolidation des sanpshots 113
Figure 5-5:"Recan" des disques (Server Manager) 114
Figure 5-7 : Extrait des logs RecoverPoint 115
Figure 5-8 : Exemple de statistiques du trafic d'un groupe de cohérence 115
Figure 5-9 : Exemple de statistiques sur les performances d'un groupe de cohérence 116
Figure 6-1 : Organisation du mémoire 127
Figure A20-1 : Arrêt d'une base de données MS SQL Server 189
Figure A20-3 : Résultat du démarrage de la base "CAMP02" 193
Figure A20-2: Démarrage de la base "CAMP02" 193
Figure A20-4 : Liste des LUN présentés au serveur KIITDBMS par l'IPStor 193
Figure A23-1: ÉTAPE 1 - Prise d'une image témoin 204
Figure A23-2 : ÉTAPE 2 – Ajout de données sur le disque Primaire 204
Figure A23-4: ÉTAPE 2 : Snapshots après regroupement 205
Figure A23-3 : ÉTAPE 2 : Snapshots avant regroupement 205
Figure A23-6 : ÉTAPE 3 – Utilisation du disque E : 205
Figure A23-5 : ÉTAPE 3 – Prise d'image 205
Figure A23-7 : ÉTAPE 5 – Prise d'image 206
Figure A23-8 : Contenu de l'explorateur après la présentation 209
Figure A23-9:"Rescan" des disques (Server Manager) 210
Figure A23--10: État du disque après son "rescan" 210
Figure A23-11:STOEITC1("E :") après la création du fichier témoin 210
Figure A23-10: Disque E: en lecture seule 210
Figure A23-13 :STOEITC1 ("E :") après restauration 213
Figure A23-12: Utilisation de E : après restauration 213
Figure A23-14 : Extrait du journal du groupe de cohérence "C_STOEITC2" 215

LISTE DES TABLEAUX

Tableau I : Récapitulatif des principales solutions étudiées 58
Tableau II : Tests de performances 69
Tableau III : Temps de transferts des données de Lyon vers Strasbourg 70
Tableau IV : Tests de restaurations Netbackup VSS 70
Tableau V : Récapitulatif des différentes phases de l'expérimentation 93
Tableau VI : Étape 6 – Détail des snapshots du lecteur M 94
Tableau VII : Rappel du séquencement du test 95
Tableau VIII : Détail des snapshots du groupe de cohérence GRP_BKSQL (lecteur "D","E","L") 95
Tableau IX : Disque logique Applicatif 96
Tableau X : Disque de données MS SQL Serveurs 96
Tableau XI : Disque des journaux de la base de données 96
Tableau XII : Détail des snapshots d'un LUN Falconstor 97
Tableau XIII : Les étapes de l'expérimentation de restauration d'une base de données MS SQL Serveur 98
Tableau XIV : Descriptif du LUN qui posait problème au script HyperTrac 102
Tableau XV : Séquencement de l'expérimentation 114
Tableau XVI : Avantages et inconvénients des différents courants du CDP 120
Tableau XVII : Comparaison des solutions EMC RecoverPoint et FalconStor CDP 122
Tableau XVIII : Récapitulatif des différentes phases de l'expérimentation 185
Tableau XIX : Étape 0 - Ressources allouées au stockage secondaire (FalconStor) du lecteur M 185
Tableau XX : Étape 0 – Détail des snapshots du lecteur M 185
Tableau XXI : Étape 1 - Ressources allouées au stockage secondaire (FalconStor) du lecteur M 186
Tableau XXII : Étape 1 – Détail des snapshots du lecteur M 186
Tableau XXIII : Étape 3 – Détail des snapshots 186
Tableau XXIV : Étape 3 - Ressources allouées au stockage secondaire (FalconStor) du lecteur M 187
Tableau XXV : Étape 5 - Ressources allouées au stockage secondaire (FalconStor) du lecteur M 187
Tableau XXVI : Étape 5 – Détail des snapshots du lecteur M 187
Tableau XXVII : Étape 7 - Ressources allouées au stockage secondaire (FalconStor) du lecteur M 188
Tableau XXVIII : Les étapes de l'expérimentation de restauration d'une base de données MS SQL Serveur 189
Tableau XXIX : Séquencement de l'expérimentation 204

Étude des nouveaux outils de protection continue des données (CDP). Mémoire d'Ingénieur C.N.A.M., Nantes 2014.

RÉSUMÉ

La protection continue des données (CDP) est un nouveau concept permettant de journaliser toutes les modifications du système de stockage afin de permettre son repositionnement à un moment antérieur. Cette technologie très attrayante est encore mal connue. Quels sont ses avantages par rapport aux autres technologies existantes ? Quels sont les différents types de protection continue ? Quels sont les véritables enjeux ?

Cette étude a pour but de répondre à ces questions. Dans un premier temps, je dresse l'inventaire des technologies courantes avant de décrire, dans un second temps, ce nouveau concept ainsi que les principaux acteurs dans ce marché. Enfin, j'aborde la mise en œuvre de solutions CDP, afin d'en déterminer leurs réels avantages, ainsi que leurs diverses contraintes.

Tout ce travail permet de mettre en évidence les différents types de protection et les principaux enjeux de cette technologie : plan de continuité d'activité, protection contre la corruption des données, remède contre les fenêtres de sauvegarde trop courtes, etc... Il permet également de mettre l'accent sur l'importance du choix et du paramétrage de la solution, ce qui impacte des critères tels que le temps de rétablissement, la taille de la fenêtre de protection et les besoins en stockage…

Mots clés : CDP, continue, données, FalconStor, PCA, protection, RecoverPoint, sauvegarde

---

SUMMARY

Continuous data protection (CDP) is a new concept to log all changes to the storage system in order to allow repositioning at an earlier time. This very attractive technology is still little known. What are the advantages over other existing technologies? What are the different types of continuous data protection? What is truly at stake?

This study has tried to answer these questions by initially performing a brief inventory of the current technologies. Secondly, we have described this new concept as well as the major market players. Finally, we have worked on the implementation of CDP solutions to determine their real advantages and restrictions.

This research has enabled us to highlight the different types of protection and the main stakes of this technology: business continuity plan, protection against data corruption, addressing the problems of too short backup windows, etc. As well as the importance of the choice and the configuration of the solution, which have an impact on criteria such as recovery time, the size of the protection window and storage needs...

Key words : CDP, continuous, data, FalconStor, PCA, protection, Recoverpoint, backup