PARAGON Technologie GmbH, Systemprogrammierung

Heinrich-von-Stephan-Str. 5c ● 79100 Freiburg, Germany

Tel. +49 (0) 761 59018201 ● Fax +49 (0) 761 59018130

Internet www.paragon-software.com ● Email sales@paragon-software.com

Paragon Exchange Protection

User Guide

Contents

Introducing Exchange Protection 3

What is Exchange Protection? 3

Key Features 3

Full Backup, Incremental Chain, or NCDP? 4

Getting Started with Exchange Protection 5

System Requirements 5

Installation 5

First Start 6

Command Line Parameters 6

Command Line Examples 7

Known Limitations 9

Contacting Paragon Technology GmbH 10

Use Cases with Exchange Protection 11

Automated Protection of a Typical Exchange Server 11

Automated Protection of a Server Hosting Several Mission-Critical Apps 13

Manual Exchange Protection 15

Disaster Recovery of the Host OS and Exchange 15

Restore of Exchange Only 15

Troubleshooter 16

Glossary 16

Introducing Exchange Protection

This chapter will help you get general information on a brand-new product from Paragon – Exchange Protection.

What is Exchange Protection?

Paragon Exchange Protection is a command-line disaster recovery utility for Microsoft Exchange 2007/2010. Employing MS VSS (Volume Shadow Copy Service) API it delivers comprehensive protection and quick point-in-time recovery of active databases with minimal effort. It's ideal for small and medium-business, which needs an affordable, yet reliable solution to provide 24x7 email access to communicate with employees, customers, and partners.

Paragon Exchange Protection is an excellent complement to Drive Backup Server, the company's top-level disaster recovery tool. Using these two products in a bunch opens up the option to have a complete MS Exchange Server protection strategy in place.

Key Features

- **Protection of live MS Exchange**. There's no need to allocate time for backup windows, for Exchange Protection enables to create consistent database backups without any impact on the email server.
- **Log shipping for NCDP (Near Continuous Data Protection)**. Exchange Protection includes a special service that can monitor transaction logs for particular Exchange storage objects to automatically archive them as soon as they are released, this way providing for minimal data loss in case of emergency. Moreover during this type of backup, logs are not truncated, so no impact is made to performance of Exchange Server.
- **Selective backup**. The utility can protect either selected storage groups or all groups at once.
- **Single instant block backup**. Even when creating a full backup, Exchange Protection analyzes and transfers only blocks of databases which have been changed since the last backup, thus providing for the server load optimization and backup storage minimization.
- **Support for incremental backup chains and block-level data de-duplication**. Usage of incremental backups allows additional flexibility by having different time-stamps while block-level delta for full backups contributes to minimization of backup storage requirements.
- **Wide restore options**. Exchange Protection enables to restore separate data stores or storage groups or all groups at once either to the original or some alternative (a different Exchange Server, a new storage group or any physical disk) location.
- **Automated recovery from a broken incremental chain**. When MS Exchange refuses to allow creating an incremental backup, Exchange Protection automatically initiates a full backup. Possible reasons: there's no full backup yet, the full backup is made with a third-party application, a new store is created, VHD file chain is corrupted, there's been detected an unsafe replication switchover, etc.).
- **Data aging monitor**. Automatic elimination of obsolete backups not only saves space, but it also cuts back on the time required to perform backups.
- **Support of MS Exchange replicas and cluster configurations**.

Full Backup, Incremental Chain, or NCDP?

For MS Exchange the answer is not that obvious. In fact only the use of all three in a bunch can guarantee optimal protection for this type of application. Well let's see why:

- A **full backup** includes all files of the selected storage group or all groups at once, so it does not depend on any other backup and can be restored in a single step. Besides during this type of backup, all transaction logs are automatically truncated, which is good for high performance of Exchange. Nevertheless, it doesn't allow various restore points. And it significantly loads the server during the operation, that's why its frequent use is out of question.

- An **incremental backup** includes transaction logs that capture the changes since the most recent full or incremental backup. During this type of backup, all transaction logs are automatically truncated as well. It takes little time to create and is correspondingly small. And it allows different time-stamps. Nevertheless, you always need a full backup as a 'parental image' for restore. Moreover, a too long incremental chain can take hours to restore and is really a burden for the backup storage.

- **NCDP** (Near Continuous Data Protection), which is realized through log shipping, includes a special service that can monitor transaction logs for particular Exchange storage objects to automatically archive them as soon as they are released, this way providing for minimal data loss in case of emergency. During this type of backup, logs are not truncated, so no impact is made to performance of Exchange. Nevertheless, you always need a full backup as a 'parental image' for restore and in general the restore operation is the most time-consuming of all three. Moreover, if you don't do full or incremental backups to truncate logs, performance of Exchange will keep degrading.

For more information, please consult the Use Cases with Exchange Protection section.

Getting Started with Exchange Protection

In this chapter you will find all the information necessary to get the product ready to use.

System Requirements

Supported Operating Systems

- Windows Server 2003 x64 (all editions)
- Windows Server 2008 x64, 2008 R2 x64 (all editions)

Supported Exchange Servers

- Exchange Server 2007
- Exchange Server 2010

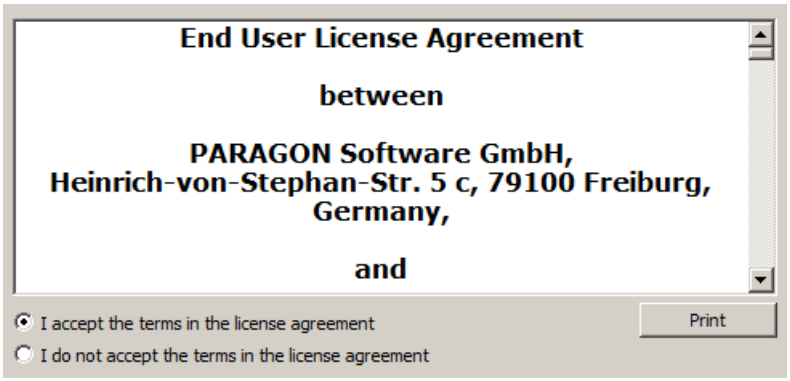
Supported Cluster Configurations

- Back up either an active Exchange database or its replica for LCR configurations
- Back up separate nodes for SCC (Single Copy Cluster) and CCR (Cluster Continuous Replication) configurations

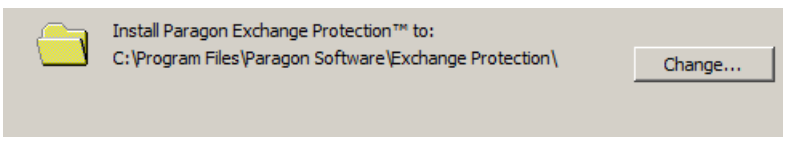
Installation

Before installation, please make sure your platform meets the product requirements. If everything is OK, please do the following to install the utility:

1. Click on the supplied setup file to initiate the installation (**PEP_XX_x64.msi**, where XX indicates localization of the installation package, for instance EN for English, DE for German, ES for Spanish, RU for Russian, etc.).
2. The Welcome page will inform that the application is being installed. Click **Next** to continue.
3. Please Read Paragon License Agreement carefully and then select the appropriate option to accept. Otherwise you won't be able to proceed with the installation. By clicking the **Print** button, the license agreement may also be printed out.



4. On the next page, click **Change** to install the utility to a different location (by default **C:\Program Files\ Paragon Software\Exchange Protection**). Otherwise click **Next** to continue.

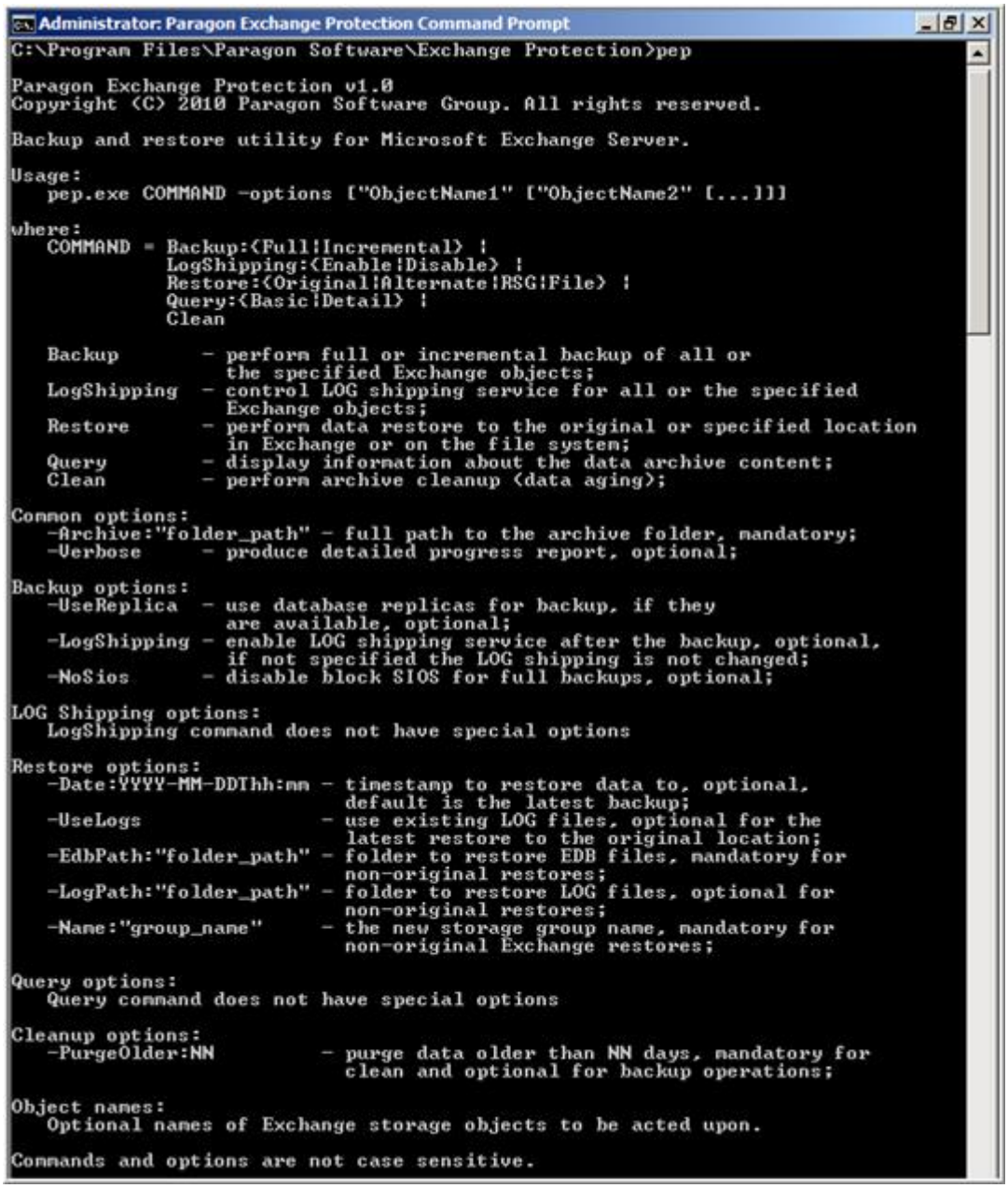


5. On the Ready to Install the Program page click **Install** to start the installation or **Back** to return to any of the previous pages and modify the installation settings.

6. The Final page reports the end of the setup process. Click **Finish** to complete the wizard.

First Start

Launch **Command Prompt**, then type in **pep.exe /?** to view all available options and the usage grammar of the utility.



Command Line Parameters

In the table below you can find available parameters for each operation.

	Archive	NoSios	PurgeOlder	UseReplica	LogShipping	Date	EdbPath	LogPath	UseLogs	Name	Verbose	*storage_name(s)*
Backup:Full	m	o	o	o	o						o	o
Backup:Incremental	m		o	o							o	o
LogShipping:Enable	m			o							o	o
LogShipping:Disable											o	
Restore:Original	m					o			o		o	o (+stores)
Restore:Alternative	m					o	m	o		m	o	m (+stores)
Restore:RSG	m					o	m	o		o	o	m (+stores)
Restore:File	m					o	m	o			o	m (+stores)
Query:{Basic|Detail}	m										o	o (+stores)
Clean	m		m								o	o

m - Mandatory parameter
o - Optional parameter
<empty> - Not applicable
+stores - Not only storage group name(s), but individual stores can be specified in form “Storage Group Name\Data Store Name”

Command Line Examples

To get a better notion on how to use Exchange Protection, please consult the given below examples:

1. **pep.exe Backup:Full -Archive:"D:\ExchArchive" -Verbose -NoSios -UseReplica "First Storage Group"**

This example shows how to do a full backup of the "First Storage Group" to "D:\ExchArchive" with the following optional parameters active:

-Verbose – there will be a detailed report on all actions;

-NoSios – SIOS (Single Instance Object Storage) will be disabled;

-UseReplica – database replicas will be used during the operation (if there are any).

2. **pep.exe Backup:Incremental -Archive:"D:\ExchArchive" -PurgeOlder:14 "First Storage Group"**

   This example shows how to do an incremental backup of the "First Storage Group" to "D:\ExchArchive" with the following optional parameter active:

   -PurgeOlder:14 – all data older than 14 days will be purged during the operation.

3. **pep.exe Backup:Full -Archive:"D:\ExchArchive" -Verbose -NoSios -LogShipping "First Storage Group"**

   This example shows how to do a full backup of the "First Storage Group" to "D:\ExchArchive" with the following optional parameters active:

   -Verbose – there will be a detailed report on all actions;

   -NoSios – SIOS (Single Instance Object Storage) will be disabled;

   -LogShipping – right after finishing the full backup, there will be enabled NCDP (Near Continuous Data Protection) for the specified backup object to provide for minimal data loss in case of emergency.

4. **pep.exe LogShipping:Enable -Archive:"D:\ExchArchive" -Verbose -UseReplica "First Storage Group"**

   This example shows how to enable NCDP for the "First Storage Group" with the following optional parameters active:

   -Verbose – there will be a detailed report on all actions;

   -UseReplica – database replicas will be used during the operation (if there are any).

5. **pep.exe Restore:Original -Archive:"D:\ExchArchive" -Date:2010-02-20 "First Storage Group\Mailbox Store"**

   This example shows how to restore the "First Storage Group\Mailbox Store" from "D:\ExchArchive" to the original location with the following optional parameter active:

   -Date:2010-02-20 – a time-stamp created on 2010/02/20 will be used during the operation.

6. **pep.exe Restore:RSG -Archive: "D:\ExchArchive" -EdbPath:D:\TmpData -Name:"TempGroup" "First Storage Group"**

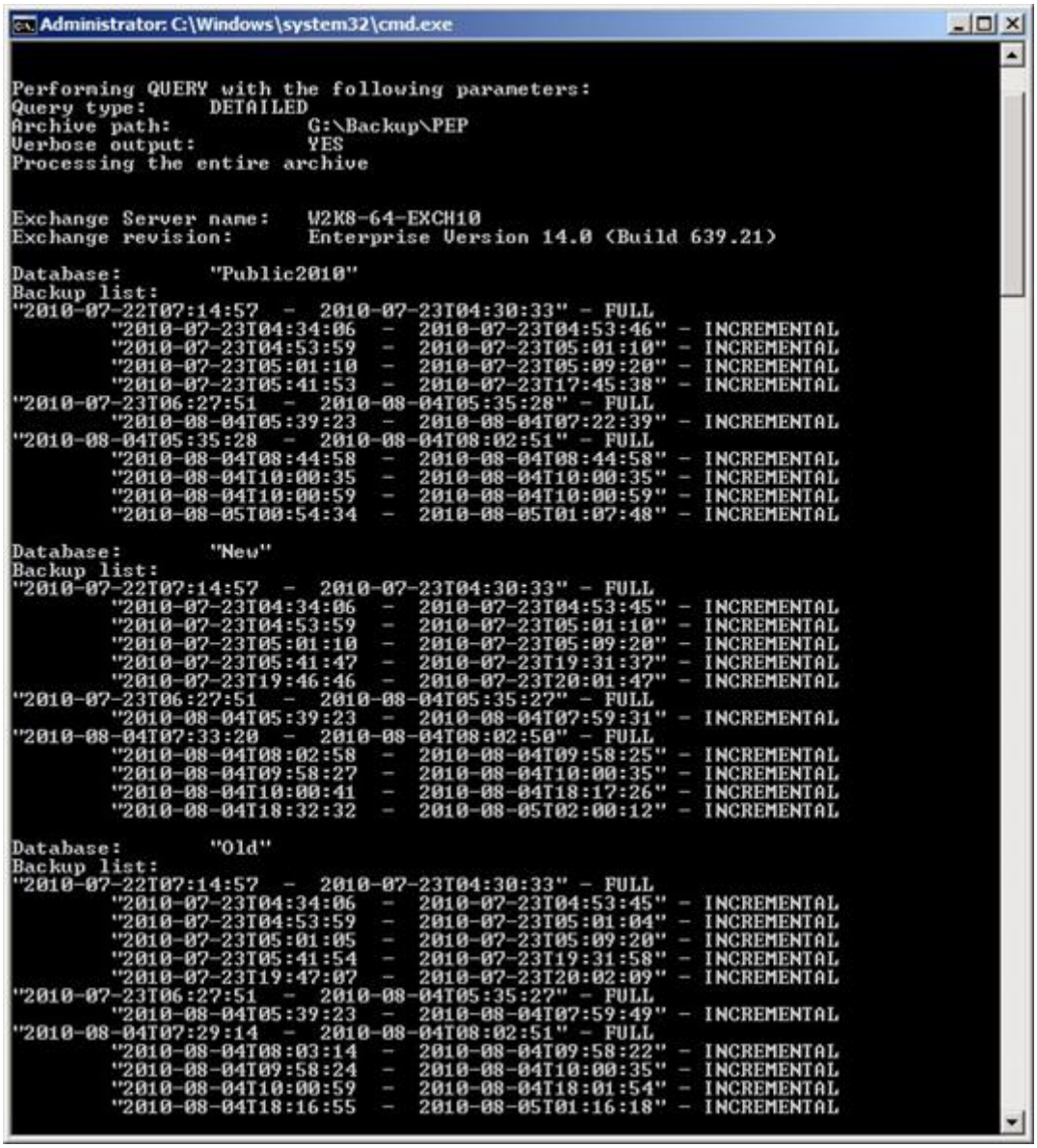
   This example shows how to restore the "First Storage Group" from "D:\ExchArchive" to the RSG (Recovery Storage Group) with the following mandatory parameters active:

   - EdbPath:D:\TmpData – all EDB files will be restored to "D:\TmpData"

   - **Name: "TempGroup"** – the storage group will acquire the name "TempGroup"

7. **pep.exe Query:Detailed -Archive:"D:\Backup\PEP"**

This example shows how to get detailed information on all archive contents stored in "G:\Backup\PEP"



Known Limitations

- The maximum size of a storage group allowed to back up is 2TB (VHD limitation). If more, the utility will return a corresponding error and won't start the backup operation.

- It is not recommended to cancel an already started backup/restore operation. If a backup operation has been abnormally terminated, MS Exchange will return to a pre-backup state, i.e. the backup operation will not be registered and LOG files will not be truncated. If a restore operation has been abnormally terminated, the administrator will have to repeat the restore operation to get Exchange Server back on rails.

- MS Exchange does not allow running multiple backup operations simultaneously if the backup objects are crossed.

- When restoring to the original location, all storage groups and data stores to restore are to remain in AD (Active Directory). Otherwise, the administrator should manually configure AD in advance or use restore to some alternative location (AD will be automatically configured with the default parameters).

- When restoring multiple storage groups to an alternative location, the administrator needs to run the corresponding number of restore commands, each time specifying a new group name and disk location.
- All Exchange Server replication configurations are supported for a standalone Exchange Server. Windows Failover Cluster configurations are only supported when running Exchange Protection on the appropriate cluster node.
- After restore of an Exchange Server in CCR, SCR, SCC, or Site Resilience configurations, the administrator should manually configure these configurations.

Contacting Paragon Technology GmbH

If you have any questions about the company products, please do not hesitate to contact Paragon Technology GmbH.

Service	Contact
Visit Paragon GmbH web site	www.paragon-software.com
Registration & updates web-service	kb.paragon-software.com
Knowledge Base & Technical Support	kb.paragon-software.com
Support	support@paragon-software.com
Pre-sale information	sales@paragon-software.com

Use Cases with Exchange Protection

This chapter lists a number of scenarios that demonstrate how Paragon Exchange Protection can be used as a part of an efficient disaster recovery plan to keep Microsoft Exchange Server protected.

Automated Protection of a Typical Exchange Server

A typical Exchange Server within a modern SMB-scale company is based on Windows Server 2003/2008 that hosts MS Exchange 2007/2010. So when thinking over an efficient disaster recovery strategy for this type of server, first we should point out the main backup objects, i.e. the host operating system and Exchange, for these two objects require different backup policies. While the host operating system tends to change a little and we only need it to keep Exchange running, Exchange databases – is our primary objective, for they contain mission-critical information and we need to make sure none of this information will be lost in case of disaster.

So taking these considerations into account, let's see how Paragon Exchange Protection can help to establish an efficient rock-solid disaster recovery plan for a typical Exchange Server:

Objective: Comprehensive protection of a typical Exchange Server that contains no other critical information, but Exchange databases.

Disaster recovery apps: Paragon Exchange Protection to protect Exchange databases and an appropriate disk-imaging utility to protect Windows Server (Paragon Drive Backup Server in our case).

Backup parameters for Drive Backup Server: A cycle full sector backup of the entire server to a network share every week, providing Exchange is excluded from backup (backup storage space savings), and two latest backups are always at the disposal. It also makes sense to protect the system partition only, so then no exclude options are necessary. **Objective** – get the system back on track as fast as possible even to a different hardware configuration (Adaptive Restore) or a virtual environment (P2V Restore).

Backup parameters for Exchange Protection: Scheduled weekly full backups of all storage groups/selected storage groups for optimal use of the backup storage, combined with daily incremental backups for maintaining enough restore points to recover Exchange from a latent corruption plus log shipping to minimize data loss in case of disaster. The data aging parameter for backups is 30 days to use them if necessary for granular recovery. It is selected whether to back up the main database or its replica. **Objective** - keep the latest time-stamps of Exchange databases.

Backup cycle: 14 days.

		System Volume/Entire PC Backup (Smart Exclude DLL Usage)	Exchange Backup	
Week 1	Sunday	Full Backup 1	Full Backup	
	Monday		<< NCDP >>	Incremental
	Tuesday			Incremental
	Wednesday			Incremental
	Thursday			Incremental
	Friday			Incremental
	Saturday			
Week 2	Sunday	Full Backup 2	Full Backup	
	Monday		<< NCDP >>	Incremental
	Tuesday			Incremental
	Wednesday			Incremental
	Thursday			Incremental
	Friday			Incremental
	Saturday			
Week 3	Sunday	Full Backup 1	Full Backup	
	Monday		<< NCDP >>	Incremental
	Tuesday			Incremental
	Wednesday			Incremental
	Thursday			Incremental
	Friday			Incremental
	Saturday			
Week 4	Sunday	Full Backup 2	Full Backup	
	Monday		<< NCDP >>	Incremental
	Tuesday			Incremental
	Wednesday			Incremental
	Thursday			Incremental
	Friday			Incremental
	Saturday			

Automated Protection of a Server Hosting Several Mission-Critical Apps

A multi-purpose server that hosts not only Exchange, but other mission- critical applications or data (file server, SQL, etc.) requires a different backup approach. In this case, an efficient disaster recovery strategy should include regular protection of all mission-critical data and the host operating system, taking into account the relevance of each backup object.

So let's see how Paragon Exchange Protection can help to establish an efficient rock-solid disaster recovery plan for this type of server:

Objective: Comprehensive protection of a multi-purpose server that hosts not only Exchange databases, but other mission-critical data.

Disaster recovery apps: Paragon Exchange Protection to protect Exchange databases and an appropriate disk-imaging and file backup utility to protect Windows Server and other critical data (Paragon Drive Backup Server in our case).

Backup parameters for Drive Backup Server: A daily cycle differential sector backup of the entire server to a network share, providing Exchange is excluded from backup (backup storage space savings), and 7-12 latest backups are always at the disposal. If the operating system is placed on a separate partition, it makes sense to protect the system partition weekly, then no exclude options are necessary, while partitions that contain critical data – daily, thus optimizing the usage of the backup storage. **Objective** – get the system back on track as fast as possible even to a different hardware configuration (Adaptive Restore) or a virtual environment (P2V Restore), while keeping the latest time-stamps of the critical information.

Backup parameters for Exchange Protection: Scheduled weekly full backups of all storage groups/selected storage groups for optimal use of the backup storage, combined with daily incremental backups for maintaining enough restore points to recover Exchange from a latent corruption plus log shipping to minimize data loss in case of disaster. The data aging parameter for backups is 30 days to use them if necessary for granular recovery. It is selected whether to back up the main database or its replica. **Objective** - keep the latest time-stamps of Exchange databases.

Backup cycle: 14 days.

		System Volume/Entire PC Backup (Smart Exclude DLL Usage)	Exchange Backup	
Week 1	Sunday	Full Backup 1	Full Backup	
	Monday	Differential 1 to Backup 1	>>> NCDP <<<	Incremental
	Tuesday	Differential 2 to Backup 1		Incremental
	Wednesday	Differential 3 to Backup 1		Incremental
	Thursday	Differential 4 to Backup 1		Incremental
	Friday	Differential 5 to Backup 1		Incremental
	Saturday			
Week 2	Sunday	Full Backup 2	Full Backup	
	Monday	Differential 1 to Backup 2	>>> NCDP <<<	Incremental
	Tuesday	Differential 2 to Backup 2		Incremental
	Wednesday	Differential 3 to Backup 2		Incremental
	Thursday	Differential 4 to Backup 2		Incremental
	Friday	Differential 5 to Backup 2		Incremental
	Saturday			
Week 3	Sunday	Full Backup 1	Full Backup	
	Monday	Differential 1 to Backup 1	>>> NCDP <<<	Incremental
	Tuesday	Differential 2 to Backup 1		Incremental
	Wednesday	Differential 3 to Backup 1		Incremental
	Thursday	Differential 4 to Backup 1		Incremental
	Friday	Differential 5 to Backup 1		Incremental
	Saturday			
Week 4	Sunday	Full Backup 2	Full Backup	
	Monday	Differential 1 to Backup 2	>>> NCDP <<<	Incremental
	Tuesday	Differential 2 to Backup 2		Incremental
	Wednesday	Differential 3 to Backup 2		Incremental
	Thursday	Differential 4 to Backup 2		Incremental
	Friday	Differential 5 to Backup 2		Incremental
	Saturday			

Manual Exchange Protection

It's an additional scenario to the considered above use cases that makes sense to accomplish before introducing major changes to Exchange or its reconfiguration. So the general cyclic backup routine is kept intact, while the administrator manually launches Paragon Exchange Protection with certain parameters.

Backup parameters for Exchange Protection: Depending on the amount of changes to introduce, a one-time full or incremental backup of all storage groups/selected storage groups, selecting whether to automatically back up the main database or its replica. **Objective** - keep the latest time-stamp of Exchange databases before a major change.

Disaster Recovery of the Host OS and Exchange

Let's consider the most devastating scenario that could ever happen – a complete crash of a server that hosts MS Exchange. The business is facing a major downtime or even at the verge of bankruptcy, if no adequate disaster recovery plan has been established, just one if those we discussed earlier.

So let's see how fast and easily an Exchange Server can be back on rails after a complete disaster when Paragon Drive Backup Server and Paragon Exchange Protection are used together as disaster recovery facilities:

Objective: Recovery of an Exchange Server after a major disaster involving hardware failure and data loss. Actually the disaster recovery operation includes two steps, i.e. restore of the entire server or only the system partition from a sector backup with Drive Backup Server, and then restore of Exchange databases from the latest available backup with Exchange Protection.

Restore parameters for Drive Backup Server: Depending on the faced problem, there are several options to choose from (bare-metal recovery from the Linux/DOS or WinPE 3.0 bootable environments with the option to restore to dissimilar hardware or restore directly to a virtual environment of any major virtualization software vendor).

Restore parameters for Exchange Protection: Restore from the latest backup to the original location.

Restore of Exchange Only

If only Exchange databases are corrupted, depending on the faced problem, Exchange Protection includes several options how to recover exactly what you need with minimal effort:

- Restore all storage groups, selected groups or data stores
- Restore from the latest backup or any available time-stamp
- Restore to the original or some alternative (a different Exchange Server, a new storage group or any physical disk) location

Troubleshooter

If you've faced a problem while using our product, please send an operation log file (you can find it in "C:\Windows\Logs\Paragon\Exchange Protection") to support@paragon-software.com, describing your actions just before the glitch in every single detail. Please note logs are deleted according to the data aging parameter. We'll do our best to help you out as soon as possible.

Glossary

SCC - Single Copy Cluster

This is a minimum two node cluster that relies on Microsoft Failover Clustering Services. This requires shared disk like a SAN and has a single copy of the data.

LCR - Local Continuous Replication

This is a single Exchange Server 2007 solution to provide data redundancy. You can run all of the server roles on this however there are some caveats for public folders. To be effective this solution requires two external drive arrays and two array controllers to provide true redundancy.

CCR - Cluster Continuous Replication

This is a two node cluster that relies on Microsoft Failover Clustering Services on Exchange Server 2007. This does not require shared disk however would require a "witness" node. Other than the mailbox role, no other roles can be installed on the cluster. There active node of the cluster replicates all changes to a passive copy of the database. A minimum of three Exchange servers would be required (2 mailbox nodes and a non-redundant Client Access and Hub Transport).

SCR - Standby Continuous Replication (SP1)

This allows replication of databases to other Exchange Server 2007 located anywhere on the Intranet. This replication can be done to and from any type of mailbox node (other than a mailbox server that uses LCR).

SIOS - Single Instance Object Storage

It's a method of redundancy elimination, when, before running a full backup, it is analyzed if any identical data block already exists on the backup storage to process and store one copy of any block only, thus minimizing the backup storage requirements.

High Availability and Site Resilience

It's a new replication technology implemented in Exchange Server 2010 (see http://technet.microsoft.com/en-us/library/dd335211.aspx).

VSS - Volume Shadow Copy Service

It's a technology that provides the copy/backup infrastructure for the Microsoft Windows XP/Vista/7/Server 2003/2008 operating systems. It offers a reliable mechanism to create consistent point-in-time copies of data known as shadow copies. Developed by Microsoft in close cooperation with the leading copy/backup solution vendors on the market, it is based on a snapshot technology concept.