Disaster Recovery Plan

Procedures

Fira Barcelona

Document control

Project	Disaster Recovery
Organisation	Fira de Barcelona
Title	Disaster Recovery
Version	3.4
Date issued	13/3/2007
Author(s)	Xavi Verde

CONTENTS

1 Introduction

The purpose of this document is to summarise the configuration of the different levels for the various Disaster Recoveries that may be required.

Disaster Recovery encompasses the processes, policies or procedures to be performed to prepare a recovery plan or a critical infrastructure assessment when faced with a human or natural disaster.

Disaster Recovery forms part of business continuity, integrating the planning required to preserve all those aspects of a business that can be disrupted.

1.1 Levels

In our case, we divide Disaster Recovery into 3 levels.

- Backups: Backups with Brighstor (Windows and VmWare) and Data Protector (Linux) with the goal of being able to restore files and even servers.
- 1st degree “Setups”: Those disasters that do not corrupt either the operating system or the server’s hardware.
- 2nd degree “Operating systems and setups”: Disasters that involve damage to the operating system, which in turn affects the server’s setups.
- 3rd degree “Hardware”: Disasters that damage both the hardware and the operating system.
- 4th degree “Backup DB catalogue”: This level requires holding the backup copy outside of the location where the servers are kept in order to enable recovery.

1.2 Definition of criticalities

This is the critical or recovery sequence ordered by priority

- Disk array
  XP10000
- Oracle
  Abraham/Homer/Marge
- LDAP and folders
  Neptuno / Plutón /Afrodita / Hefesto
- VmWare servers
  Asterix / Obelix
- ESX
  Isidrix//Tragicomix//Catamito//Moe//Duff
  //Milhouse
- DNS
  Odin / Tatum
- SAP
  R3→ Dafne (Pandora//Diana)

  BW/XI→Nereo

  CRM→Euridice

  SMP→Filemón
- Mailing
  Gorgonas
- Weblogic
  Nike2

  Cerbero2
- JBOSS
  Smithers

  Mcclure
- Balanceador
  Baldur
- Apache
  Atena

  Artemis

  Hestia
- Tomcat
  Hod

  Hermes
- Meta4
  Japeto
- Backups
  Apolo
- Pentaho
  Skuld
- WebDav
  Hati
- Footprints
  Anfitrion

  Electrion
- McAfee Appliance
  Helios

  Selene

  Eos
- FTp Premsa
  Eolo
- Notes
  Thor

  Atlas

  Posets

  Teide

  Marbore →Veleta

  Matagalls→Elektra
- Biométricos and SMS
  Argos
- SQL and SUS
  Fenix
- RightFax
  Venus

  Hathor and Vulcano
- Gespa
  Eris and Discordia

- TPV
  Autonea
- NAGIOS
  Nagios

Skinner

Marte

Io

Cadi

- Others
  Gigantes

1.3 Operating procedures

In the event of an emergency or Disaster Recovery at any level, the following personnel must be notified.

- Moises Ramos (Team leader for the client)
- Ana Santamaria (Team leader for Oesia)

In addition, the following document must be completed and placed in the department's crash reports folder and must also be sent by e-mail to the above-stated personnel.

Informe Caída
Sistema SLA AA-MM-[

In the safe, there is also a sealed envelope with an encrypted CD with the servers' passwords. These passwords are only known by the above-stated personnel.

Should recovery be wished, both must be notified so that they may authorise use of these passwords.

2 Disaster Recovery

2.1 Backups

Backups are made of all of Fira de Barcelona's servers using Brighstor, Virtual Center Backup, and Data Protector.

The backup policy in the case of Brighstor is the following:

Time windows

- VMWare
  - Daily jobs
    - Mondays to Saturdays, 9.00 p.m. to 11.00 p.m. approx.
  - Weekly jobs
    - Sundays, 9.00 p.m. to 11.00 p.m. approx.
- Windows
  - Daily jobs
    - Mondays to Sundays, 11.45 p.m. to 2.30 a.m. approx.
  - Weekly jobs
    - Saturdays, 3.00 a.m. to 5.00 a.m. approx.
  - Monthly jobs
    - The last Sunday of each month.

Tape sets

- Daily Windows
  - 7 Tapes each in 2 sets
    - Nomenclature: WUSR***01//14***
- Weekly Windows
  - 1 set of 4 tapes
    - Nomenclature: WSEM***01//04***
- Monthly Windows
  - 1 set of 12 tapes
    - Nomenclature: WMEN***01//12***
- Daily VMWare
  - 1 set of 6 tapes
    - Nomenclature: VMW***01//06***R
- Weekly VMWare
  - 1 set of 4 tapes
    - Nomenclature: VMSEM***01//04***

Changing tapes

- The following tapes are taken to Fira de Barcelona's other venue on a **WEEKLY** basis:
  - Set of 7 daily Windows tapes
  - Weekly Windows tape
  - Weekly VMWare tape
- The following tapes are taken to Fira de Barcelona's other venue on a **MONTHLY** basis:
  - Monthly tape of the current month.
- Verifications after inserting the new tapes
  - That the tape corresponding to the appropriate day of the week is in the pool
    - Monday 1
    - Tuesday 2
    - Wednesday 3
    - Thursday 4
    - …..
  - That the tape corresponding to the appropriate week is in the pool
    - Week 1 →WSEM01
    - Week 2 →WSEM02
    - Week 3 → WSEM03
    - …
  - That the tape corresponding to the appropriate month is in the pool
    - January 1
    - February 2
    - March 3
    - April 4
    - May 5
    - ….

The backup policy for Data Protector is as follows:

Time windows

Backup	Target	Time start	Time end (approx.)
WL_PRD	Hercules1	4.00	5.00
WL_INT	Iris Scsi 3	2.45	3.20
WL_DES	Iris Scsi 3	5.00	6.16
SAP_PRD	Pandora 3	1.00	4.50
SAP_DEV_INT	Hercules1	1.00	4.15
MISC_PRD	Iris Scsi 2	1.00	2.28
MISC_DI	Iris Scsi 3	5.15	7.02

Tape Sets

Changing tapes

- **WEEKLY:**
  The tape corresponding to the Sunday to Monday backup is removed and taken to the safe at Fira de Barcelona's other venue

2.1.1 Recovery

The procedure for full recovery of systems is described in Appendix I.

2.2 1st degree “Setups”

Tasks scheduled at different frequencies (depending on their criticality) are carried out, consisting of extracting the setup file from those applications or services that allow this and which are considered critical to a specific server, which saves each of the setups exported in a shared folder, for their next backup.

In addition, these files are recorded once a month on a DVD and placed in a sealed envelope in the safes at M1 (Barcelona-Montjuïch venue) and M2 (Barcelona-Gran Via venue).

These files will help us when the administrator, after receiving approval by the CAB (Change Approval Board), makes a change to the software or the system that crashes it and which can be restored by importing the previous setup.

This type of backup is also useful for the higher levels of Disaster Recovery; after recovering an operating system, or a hardware plus the operating system, we may wish to see whether the date of the setup backup is later than that to which the operating system has been restored.

The services for which this type of backup by setup export is available are listed below:

- McAfee Appliance: Helios / Selene
- McAfee Antivirus: Ned
- Disc array : XP10000
- Gespa and RightFax applications: Eris, Discordia, Venus, Hathor and Vulcano
- Apaches, Weblogic, and Jboss: Atena, Artemis, Hestia, Nike2, Cerbero2, Smithers and Mcclure
- Printers: Cadi
- Group policies: Neptuno and Pluton
- DNS: Odin, Tatum, Neptuno and Pluton
- Dhcp: Urano
- Mail and Blackberry: Gorgonas, Nelson, Canigo, Aneto, Elektra, Veleta
- VmWare (Virtual Infrastructure Center): Asterix and Obelix
- Backups: Obelix and Apophis jobs and setups
- Nagios: Ralph

This level also includes what we call “System State”. These are the system states at a particular date and time, enabling a backup of a server’s setup and all the programs installed on it to be recovered at any time.

In order to differentiate this section from that of operating systems, it is important to note that with System State, it is not the operating system that is recovered. Rather, the OS must be installed correctly to enable the “setups” on that server and all its applications to be reimported.

The services for which this type of System State is available are listed below:

- LDAP: Neptuno and Pluton
- DNS: Odin, Tatum, Neptuno and Pluton
- DHCP: Urano
- Gespa: Eris and Discordia
- RightFax: Venus, Hathor and Vulcano
- Antivirus: Ned
- File Server: Afrodita and Hefesto
- Blackberry: Elektra and Veleta
- VmWare (Virtual center Infrastructure): Asterix and Obelix

2.2.1 Recovery

There are two ways of recovering the setups of any software, which are explained below:

- Connect to Jeff, and access the shared folder where all the servers, using a script, place their setup exports. Within this path, there is a folder containing the server's name and its setup files.

  This must be copied to the server's path and imported, if necessary. In most cases, it is necessary to reboot.

- Another option would be to restore the setup file located on the server path from the backup tape containing Jeff for the date and time we want to recover.

-

2.3 2nd degree “Operating Systems”

At this level, the backups are made on the operating system as such, i.e., a “snapshot” is periodically made of the system for a specific date and time with the goal of recovering both the operating system and the setups if everything except the hardware should fail.

This would enable the service to be restored within a reasonable time after system crash.

In the case of Vmware, we use Brighstor together with VCB, creating a daily job from which we extract one tape a week, from which we could recover any VMWare server.

For Linux, we use Acronis Backup & Recovery Server which enables us to create an image of the server, without having to turn it off, and even cipher the image so that it can only be cloned by an administrator. In this case, the frequency is one month, since it is more time-consuming to obtain this backup.

In the case of Windows, ASR jobs are created using the ntbackup program, which enables the server to be restored, at any given time and after installing the OS, the status it had when the ASR backup was made.

This backup is valid for about 60 days, i.e., once this period has expired the ASR Backup is repeated to prevent any possibility of having an expired backup when it is wished to recover it.

How does this work? It uses a Diskette, Pen Drive, or HDD with setup information and a backup set. When starting the Recovery process, this diskette – together with the System Partition Backup and the Cd-Rom for installing Windows Server 2003 – is crucial for recovery.

For this recovery process, the diskette and ASR media containing the Backup files are required, so that the operating system can be restored to the same status it had at the time the ASR Backup was performed, enabling the system to be booted.

2.3.1 Recovery

There are two ways of recovering the operating system images for any server, which are explained below:

- Connect to Jeff, and access the shared folder where the system images of all the Windows and Linux servers are kept. Within this path, there is a folder with the server’s name which contains its files.

  The server must then be booted either by means of a network device or a backup CD of the image.

  Exceptionally, with this type of recovery for Windows, it would be necessary to install a base system of the Windows to be recovered, which would then be placed on top of the copied image.

  In addition, in the case of Windows, it will be necessary to have the Pen Drive with information about the backup located in the Safe, under the name “ASR Windows Backup”.

- Another option would be to restore from backup tape containing Jeff corresponding to the date and time we wish to recover.

  This solution is the only one which would cover all three platforms, i.e., Windows, Linux, and VmWare.

  Once the image has been restored, for Linux and Windows, it will still be necessary to follow the steps described in the previous point. However, for Vmware, it will be sufficient to restore the image in its original location, using Virtual Center Backup.

2.4 3rd Degree “Hardware”

For cases affecting the hardware, we have “Care Packs” contracted with suppliers, with a response time between 4 and 48 hours, depending on the criticality contracted.

Once the hardware has been recovered, if the HDD has not been affected, no further operations will be required. If the HDD has been affected, it will be necessary to refer to the information given in point 2.3.

An example can be found in Appendix II.

2.4.1 Recovery

To recover a server at hardware level, it will be necessary to call the technical assistance numbers provided by the supplier in the maintenance contract. So that the process can be done as quickly as possible, it would be advisable to keep a record of the server’s series number together with the maintenance contract number.

From then onwards, depending on the service affected (which is associated with a particular maintenance level), we would have a shorter or longer response time.

2.5 4th Degree: Backup DB Catalogue

This level is for when the disaster includes the loss of the server containing the backups. This would mean that when trying to recover servers using a backup tape, it would not be possible because the backup servers' DB does not exist.

This basically consists of making a backup of the DB containing the backup software, so that we would be able to first restore this DB on another machine with the same software, and from then on recover the other machines affected.

This backup is done monthly and stored in the safe located in the venue that does not have the CPD.

2.5.1 Recovery

In order to recover this service, it would be necessary to install a server with the same backup software and import this catalogue into the new program. Thus, if we wish to start recovery of servers affected by the same crash, it would recognise the tapes and sessions.

3 Sample recovery test

A procedure that should be performed annually is to review this document and simulate random service recovery tests in order to confirm that everything works properly.

A document with recovery tests for a critical service is attached.

Pruebas recuperacion ORacle