Wikiprint Book

Title: Konfiguracja backapów

Subject: eDokumenty - elektroniczny system obiegu dokumentów, workflow i CRM - AdminGuide/BackupsConfiguration

Version: 7

Date: 11/24/24 13:25:31

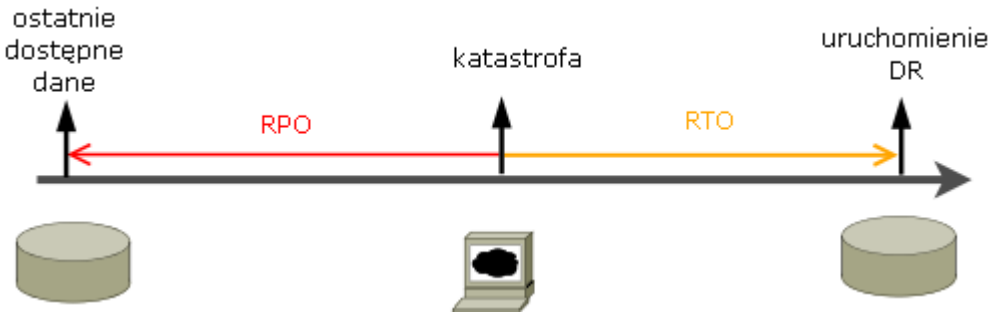
Table of Contents

Konfiguracja backapów

Wprowadzenie do tematyki Disaster recovery

1. Podstawowe aspekty i terminologia

- *Katastrofa/kataklizm* - Czyli zdarzenie niespodziewane o ogromnym negatywnym wpływie na działalność firmy
- BCP - *Business Continuity Plan* - Plan Kontynuacji Biznesu, czyli jakie usługi firmy muszą być świadczone ze względu na wymogi prawne lub finansowe powodujące upadłość firmy.
- RTO - *Recoverty time objective* - określa maksymalny akceptowalny czas od wystąpienia katastrofy, po którym usługa musi zostać uruchomiona.
- RPO - *Recovery Point Objective* - określa możliwe do zaakceptowania straty danych - np. czas od ostatniej kopii



2. Polecana konfiguracja storage'u

- Macież RAID1 software albo hardware - zapewnia szybkie odtworzenie danych w razie awarii jednego z dysków
- LVM - konfiguracja LVM w oparciu o woluminy fizyczne urządzeń RAID zapewnia możliwość łatwego zwiększania powierzchni poszczególnych logicznych partycji np. zwiększanie miejsca na repozytorium plików.
- Inne - Enterprise
  - Network Attached Storage (NAS)
  - Storage Area Network (SAN)

3. Założenia biznesowe - analiza ryzyka i koszt

- Obszary ryzyka - Należy przedyskutować co się stanie jeśli dane po 3 latach pracy zostaną utracone, ile to będzie kosztować firmę
- RTO - należy przedyskutować ile czasu może zająć odtworzenie nie narażając firmy na zbyt duże koszty. Popularne czasy przestoju:
  - 4 godziny
  - 1 dzień roboczy
  - 2 dni robocze
  - 7 dni roboczych

W przypadku awarii komponentu serwera (np. płyty głównej), przy jednoczesnym braku możliwości szybkiej naprawy, należy wziąć pod uwagę możliwość uruchomienia awaryjnego na zapasowej maszynie. Należy określić skąd taka maszyna zostanie dostarczona, kto ma podjąć decyzję o dzierżawie lub zakupie.

4. Zagadnienia związane z tworzeniem i wdrażaniem polityki backupu

- Kategorie danych
- Typy backupów
- Osoby odpowiedzialne
- Rola Zarządu w tworzeniu polityki backupu

5. Ośrodki zapasowe

Należy określić czy jest wymagane aby obliczenia systemu przejęte zostały w razie awarii przez inny ośrodek.

6. Testowanie planu Disaster Recovery - scenariusze katastrofy

Możliwe i najczęstsze przyczyny awarii:

- Awaria komponentu serwera /nie dysku/
- Awaria dysku
- Awaria oprogramowania serwera np. bazy danych po upgradzie, skasowanie konfiguracji Apache lub innej z /etc
- Skasowanie danych z bazy danych
- Skasowanie danych z dysku

7. Wybór polityki backupowej

Należy uzgodnić opisane wyżej tematy i opisać w formie procedury. Przykładowa znajduje się poniżej.

Polityka zarządzania kopiami zapasowymi

Data przyjęcia: 20 października 2008 r.

Administrator kopii - Osoba odpowiedzialna za tworzenie kopii J.N - Administrator Systemów IT

Decydent - Osoba odpowiedzialna za podjęcie decyzji o przywróceniu działania usługi na zapasowym serwerze: B.K - Prezes Zarządu

Dane objęte backupem

Kategoria danych	Procedura	Cykl
1. Baza danych	P2. DB INNY DYSK W MASZYNIE	cykl codzienny
2. Baza danych	P3. DB+FILES ZEWNĘTRZNY NOŚNIK	cykl tygodniowy
3. Pliki danych	P4. FILES - INNY DYSK W MASZYNIE	cykl codzienny
4. Pliki danych	P3. DB+FILES - ZEWNĘTRZNY NOŚNIK	cykl tygodniowy
5. OS	P5. OS - ZEWNĘTRZNY NOŚNIK	cykl miesięczny

Procedury tworzenia kopii zapasowych

P1. RAID

Automatyczna replikacja danych na dodatkowy dysk fizyczny. Dla prawidłowego wykonywania nie wymaga podejmowania żadnych czynności przez *Administratora kopii*. Nie spełnia w zasadzie wymogów backupu. Zapewnia jedynie szybkie odtworzenie danych w wypadku awarii jednego z dysków macierzy.

P2. DB INNY DYSK W MASZYNIE

W maszynie zamontowany jest dodatkowy dysk, na który zapisuje się zrzut bazy danych. Wykonuje to polecenie cron backupdb umieszczone w katalogu /etc/cron.daily. W katalogu /mnt/backup/db na którym podmontowany jest osobny dysk 500GB, w katalogach numerowanych według dnia tygodnia przetrzymywane są kopie bazy danych edokumentów, z ostatniego tygodnia.

P3. DB+FILES ZEWNĘTRZNY NOŚNIK

Nośnik zewnętrzny w postaci dysku USB umieszczany jest w ognioodpornym sejfie. Wykonuje to Pan M.W w poniedziałek o godz. 8.00. Dane na nośniku zapewniane są poprzez skrypt usb_backup umieszczony w /etc/cron.weekly. Backup obejmuje system, repozytorium oraz bazę danych edokumentów. Co tydzień dysk jest wymieniany, tak że zawsze jeden dysk znajduje się w sejfie, a jeden jest podłączony pod serwer. Na opakowaniu dysku lub dołączonym do niego protokole należy zapisywać daty w których zostały umieszczone w napędzie/sejfie.

P4. FILES INNY DYSK W MASZYNIE

Wykonywany automatycznie przez skrypt umieszczony w /etc/cron.daily *backup_system*. Zapisuje wszystkie pliki danych z katalogów repos, files i repository.

P5. OS - ZEWNĘTRZNY NOŚNIK

Wykonywany raz w tygodniu przez skrypt */etc/cron.monthly/usb_backup_os* zapisuje wszystkie pliki systemu na dysku zewnętrznym.

Data i podpis adminstratora

Data i podpis osoby decyzyjej

Procedura odtworzenia systemu

Zależna od przyjętej procedury backapów, miejsc przechowywania kopii i stosowanego sprzętu. Należy wykonywać testowo co przynajmniej rok, w celu weryfikacji.

- Montaż nowej maszyny
- Instalacja systemu operacyjnego (może być z kopii ghostem)
- Podmontowanie nośnika z kopią zapasową.
- Przywrócenie konfiguracji systemu
- Instalacja systemu eDokumenty
- Odtworzenie wersji aplikacji eDokumenty
- Odtworzenie bazy danych
- Przywrócenie repozytorium

Przykłady skryptów

Skrypty znajdują się w katalogu instalacyjnym ed-wheezy-installer. Skrypty mogą być modyfikowane np. automatyczne powiadomienie o niezamontowaniu zasobu:

```
#!/bin/bash
DST="/mnt/backup/files"

if [ -f /mnt/backup/no_disk ]
then
       cat /etc/backup/no_file.mail |msmtp --logfile=/var/spool/uucp/msmtp.log --file=/var/spool/uucp/.msmtprc admin@firma
else

       if [ -d $DST ]
       then
               sleep 1
       else
               mkdir $DST
       fi


rsync -a /home/edokumenty/files/ /mnt/backup/files/

fi
```