

23. 백업, 비상사태 관리

SPARCS 11 CLING

백업

백업 [backup]

일반적으로 데이터의 보전이나 사고에 대비해 중요한 데이터들을 미리 다른 장소에 보관하는 작업을 말한다. 즉, 시스템 파괴나 자연적인 재앙, 데이터의 안전 그리고 우발적인 사고에 대비하여 사용자의 파일을 보호하기 위해, 또 시스템의 재설치시 자료의 손쉬운 이동을 확실히 하기 위해 백업을 하게 된다. 또한 가능한 모든 시스템 데이터의 사용가능한 복사본을 보유하는 것이 시스템 관리자의 일이기 때문에 백업을 하게 된다.

출처 **매경닷컴**

Wheel 이 뭘까요??

서버 등의 기계를
관리하는 그룹

백업

서버: 여러 사용자들이 접속하여 공동으로 사용하는 컴퓨터.

SPARCS 서버에 자신의 과제를 업로드하는 사용자가 있었다.
어느날 서버가 고장나서 모든 자료가 날아가버렸다.



백업

아라 서버가 어느날 고장났다.

하드디스크가 고장났다.

아래에 있는 수십만개의 글이 사라졌다.

역사가 사라졌다.

백업

백업은 쉽고, 복잡한 기술을 요하는 것도 아니다.

tar와 gzip을 이용하여 압축하기

- tar [cxvzf] filename
 - c (create): 압축하기
 - x (extract): 압축풀기
 - v (verbose): 작업 진행상황을 화면에 출력
 - z (gzip): gzip으로 압축 또는 해제
 - f (file): 파일로 저장한다
- tar.gz 압축하기
 - tar cvf filename.tar file1...
 - gzip filename.tar
- tar.gz 한번에 압축하기
 - tar cvzf filename.tar file1...
- tar.gz 압축풀기
 - gunzip filename.tar.gz
 - tar xvf filename.tar
- tar.gz 한번에 풀기
 - tar xvzf filename.tar.gz

백업

날카로운 첫세미나의 추억

백업할 파일을 묶어서 원하는 경우 용량 압축을 해서 잘 보관해두면 된다 정말 쉽다.

그런데 무엇을 백업해야 하지?

백업

무엇을 백업할 것인가?

= 어떤 목적의 백업인가?

유저들이 올려둔 파일의 보존: `/home`

유저 정보, 서버에 적용된 환경설정: `/etc`

로그 파일, 각 서비스 데몬이 저장하는 자료 등: `/var`

기타 서버 복구 시 필요하다고 생각되는 자료

백업

이런 자료들을 몽땅 백업하는 것을
full backup이라 한다.

백업

백업과 복원을 할 때는 “어느 날짜에 백업한 것인가”, “어느 날짜의 백업분으로 복원할 것인가”가 중요하다

월요일에 올렸다가 수요일에 실수로 지운 파일을 금요일에 복원하려고 한다. 며칠로 복원?

or

8일에 바꾼 서버 설정 때문에 시스템에 문제가 생겼다. 자료는 백업되어 있다. 8일 이후로 복원하면?

백업

그렇다고 홈 디렉토리를 날마다 백업하기는....

MURISU

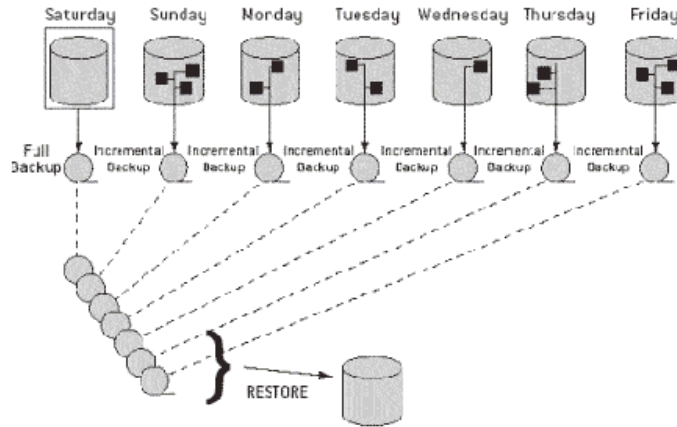
Incremental Backup

:full backup은 드물게(1개월?) 하고,
그날그날 변경된 내용을 다시 백업한다.

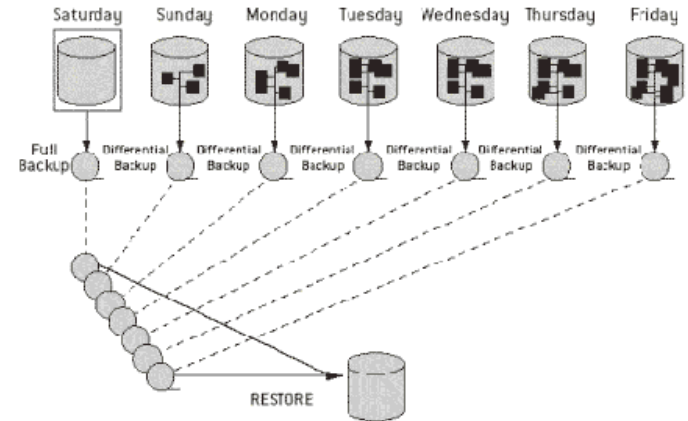
Differential Backup

:full backup 이후로 변경된 내용을 모두 변경한다.

FULL + INCREMENTAL



FULL + DIFFERENTIAL



백업

이것으로 우리는 백업에 대한 기본적인 지식을 갖추게 되었다.

생각해보면 예전에 **cron**이나 **shell script**라는 것도 배웠었다

왠지 이제 백업을 자동화할 수 있을 것 같은 기분이 든다.

마나의 기운이 느껴집니다

백업

아주아주 간단한 백업 스크립트 예제

```
backupHome=/backup/home_dir_backup_$(date +%Y%m%d).tar
```

```
backupPass=/backup/passwd_backup_$(date +%Y%m%d).tar
```

```
backupGroup=/backup/group_backup_$(date +%Y%m%d).tar
```

```
dirfiles='find \home -mtime -1 type f'
```

```
for dir in $dirfiles ; do
```

```
    tar -rvf $backupHome $dir;
```

```
tar cvfz $backupPass /etc/passwd
```

```
tar cvfz $backupGroup /etc/group
```

이 스크립트를 **cron.daily**에 추가하면 끝

다른 프로그램을 이용해도 좋다

백업

그런데 서버 본체가 날아가면 어떡하죠?

.....



백업

학식이 안하면 버거킹을 먹으면 되고
로컬 백업이 걱정되면 백업 서버를 만들면 된다.

로컬에서는 용량 부족으로 오래된 백업 파일을 삭제하더라도 백업 서버에 유지할 수 있으니까 일석이조!

백업

rsync – 원격 파일 복사 프로그램

자료전송을 최소화하면서 로컬과 다른 장소 사이에 파일을 동기화
(소스와 대상을 비교하여 다른 파일만을 전송)

+

복사의 대상을 정하는 다양한 옵션

=

백업과 미러링에 널리 쓰인다

백업

로컬 모드:

cp와 유사한 용법

```
$ rsync -av /tmp/photos/ ~
```

백업

원격 셸 모드:

SSH를 사용하며 **scp**와 유사한 용법

```
$ rsync -av *.c foo:src/
```

```
$ rsync -avz foo:src/bar /data/tmp
```

```
$ rsync -avz foo:src/bar/ /data/tmp
```

```
$ rsync -avz foo:src/bar/ /data/tmp/bar
```

로컬과 원격 모두 **rsync**가 설치되어 있어야 한다

백업

데몬 사용 모드:

TCP 873번 포트를 이용해서 원격 **rsync** 데몬에 직접 연결
(원격 시스템에서 **rsync** 데몬이 실행중이어야 한다)

Single colon : 대신에 **double colon ::** 사용

혹은 **rsync:// URL** 사용

rsync -av host::src /dest

백업

rsync를 이용한 백업 스크립트 예제

```
#!/bin/sh
# This script based on work by Michael Jakl (jakl.michael AT gmail DOTCOM) and used
# with express permission.
HOST=mymachine.example.com
SOURCE=$HOME
PATHTOBACKUP=home-backup

date='date +%Y-%m-%dT%H:%M:%S'

rsync -az --link-dest=$PATHTOBACKUP/current $SOURCE $HOST:PATHTOBACKUP/back-$date

ssh $HOST "rm $PATHTOBACKUP/current && ln -s back-$date $PATHTOBACKUP/current"
```

소프트웨어 / 하드웨어 / 인적 문제

비상사태 관리

소프트웨어적 문제

내부

파일시스템 에러

장치 설정의 오류

부팅 에러

기타 프로그램 에러

커널 패닉

메모리 오버플로

.....

외부

해킹

악성코드, 바이러스

접속자 폭주 등

하드웨어(물리)적 문제

내부

랜선 고장

케이블 절단

전원장치 고장

파워 이상

냉각 이상

특정 부품의 파손

.....

외부

물 같은 걸 끼었나?

먼지

...

인적 문제

내부

관리자의 실수

음모와 계략

잘못된 입력, 오타

외부

도둑

해커

악성 유저

북한

인적 문제의 해결



소프트웨어 내부 문제

깨진 파일시스템: 가장 흔한 문제

fsck 명령어로 파일시스템을 점검 및 복구

해당 파일시스템을 언마운트시킨 상태에서 수행하는 것이 좋다

(5번 세미나 참조)

/etc/fstab에서 장치명을 잘못 지정하는 경우도 흔하다

Linux secure로 부팅한 후 수정하여 재부팅한다.

소프트웨어 내부 문제

부팅이 안될 때:

CD/DVD나 USB로 부팅

(미리 설정해 놓는 것이 좋다)

그 후 **GRUB** 등 부팅 관련 파일을 복구한다

Kernel Panic:

운영체제가 안전하게 복구할 수 없는 치명적인 오류를 만난 경우.

장치 드라이버 문제가 가장 흔한 원인

메모리 문제, 오작동의 누적 등

소프트웨어 내부 문제



보안, 해킹

복구하기:

대부분 명령어를 못쓰게 하거나, 중요 파일을 삭제하고 에러가 나도록 변조

로그가 삭제되거나 변조되고 비밀번호 에러가 뜨기도 한다

미리 백업해 놓은 시스템 코어로 대체한 후 작업

강경책:

해킹 감지 즉시 싱글유저모드 부팅,

랜선 등 네트워크 강제 차단 등

보안, 해킹

예방하기:

안쓰는 포트는 닫아놓기, 의심가는 프로세스는 죽이기

모의 해킹 등으로 보안 점검

주기적인 프로그램 업데이트

root로 로그인하고 자리 비우지 않기!!!

숨기지 않은 파일에 중요한 정보 적어놓지 않기

물리적인 보안도 중요합니다. 서버실을 지켜주세요

하드웨어 문제

단순 접촉불량 및 랜선 고장:
바꿔끼워보고 접촉부위 점검

먼지는 주기적으로 털어주자

시끄러운 비프음은 대체로 냉각 혹은 파워 문제
냉각은 소중해. 무슨 소리냐고 하겠지만, 이걸 중요하다.

그래도 안되면.... A/S 맡기는 거다.....

갖가지 에러들 많기도 하다

원인을 알 수 없는 에러도 있고

뭘 어떻게 손댈 수 없는 경우도 있고 정말 답이 없다

하지만 백업이 출동하면 어떨까?

백! 업!

의심가는 건 싹 다 밀어버리고 백업한 걸로 대체하면 된다
고생은 좀 하겠지만....

최악의 상황에서도 적은 피해로 복구가 가능하며
로그 등이 변조당해도 이전 데이터에서 추적할 수 있다
누적된 오작동으로 인한 버그 등도 해결 가능.

한번의 백업이
하룻밤 삽질,
10번의 복구작업,
100번의 후회와 해고를 막습니다

- by sillo -

REFERENCE

[http://www.utm.edu/organizations/tsa/Books/\(OReilly\)%20Running%20Linux,%204th%20Edition.pdf](http://www.utm.edu/organizations/tsa/Books/(OReilly)%20Running%20Linux,%204th%20Edition.pdf)

<http://www.wikipedia.org/>

http://www.phpschool.com/gnuboard4/bbs/board.php?bo_table=tipntech&wr_id=48099

<http://rsync.samba.org/>

http://www.ibm.com/developerworks/kr/library/auspunix_rsync/index.html

선배님들의 세미나

제가 백업본 하나 만들었습니다...ㅠㅠ