Bezpečnosť IT infraštruktúry

Ochrana dostupnosti údajov

RNDr. Jaroslav Janáček, PhD.
Katedra informatiky

Príčiny narušenia dostupnosti

- technické zlyhania médií
- deštrukcia celých systémov, príp. priestorov
  - požiar, voda, zemetrasenie, ...
  - zrútenie budovy
  - krádež
- úmyselné vymazanie údajov (útočníkom)
- neúmyselné vymazanie údajov (omylom, chybou SW)

Opatrenia na ochranu dostupnosti

- zálohovanie údajov
- RAID (Redundant Array of Independent Disks)
- záložné dátové centrá v inej lokalite
- riadenie prístupu

Zálohovanie

- záložné média
  - pásky, disky, CD/DVD, ...
- ukladanie záloh
  - lokálne vs. vo vzdialenej lokalite
- bezpečnosť záložných médií
  - dôvernosť, integrita, autentickosť

Zálohovanie

- úplné zálohy (full backup)
- inkrementálne zálohy
  - len zmeny od poslednej zálohy vyššej úrovne
  - redukcia objemu dát
  - počet úrovní
    - malý – novšie zálohy sú väčšie
    - veľký – náročnejšia obnova vybraného stavu

Zálohovanie

- príklad 1 (3 úrovne)
  - plná záloha mesačne
  - inkrementálna týždenne oproti poslednej mesačnej
  - inkrementálna denne oproti poslednej týždennej
- príklad 2 (2 úrovne)
  - plná záloha mesačne
  - inkrementálna denne oproti poslednej mesačnej
- príklad 3 (veľa (30) úrovní)
  - plná záloha mesačne
  - inkrementálna denne oproti predošlej dennej

Zálohovanie

- príklad 1 (3 úrovne)
  - obnova z 3 súborov
  - denné súbory obsahujú len zmeny od začiatku týždňa
- príklad 2 (2 úrovne)
  - obnova z 2 súborov
  - denné súbory obsahujú zmeny od začiatku mesiaca
- príklad 3 (veľa úrovní)
  - obnova potenciálne z veľa súborov
  - denné súbory obsahujú len denné zmeny

RAID

- jednotlivé bloky dát sa rozdelia na viacero diskov
- RAID0 – striping
- RAID1 – mirror
- RAID5, RAID6
- kombinované RAIDy – RAID10, RAID0+1, ...

RAID0

- neposkytuje redundanciu
- zvyšuje výkon
- min. počet diskov: 2
- S=n*s, ef=1

disk 0	disk 1	disk 2	disk 3
0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

RAID1

- n diskov zabezpečuje odolnosť voči výpadku n-1 diskov
- min. počet diskov: 2
- S=s, ef=1/n
- umožňuje rýchlejšie čítanie

disk 0	disk 1	disk 2
0	0	0
1	1	1
2	2	2
3	3	3

RAID5

- zabezpečuje odolnosť voči výpadku jedného disku
- min. počet diskov: 3
- S=(n-1)*s, ef=1-1/n
- P=XOR ostatných
- pomalšie zápisy
- pomalé v degradovanej prevádzke

disk 0	disk 1	disk 2	disk 3
0	1	2	P
3	4	P	5
6	P	7	8
P	9	10	11

RAID6

- zabezpečuje odolnosť voči výpadku 2 diskov
- min. počet diskov: 4
- S=(n-2)*s, ef=1-2/n
- P a Q musia byť nezávislé
  - XOR a Reed-Solomon
- pomalšie zápisy
- veľmi pomalé v degradovanej prevádzke

disk 0	disk 1	disk 2	disk 3
0	1	P	Q
2	P	Q	3
P	Q	4	5
Q	6	7	P

RAID0+1

- RAID1 z *m* zariadení typu RAID0 z *k* diskov
- min. počet diskov: 4
- odolné voči výpadku (m-1) RAID0 zariadení (od (m-1) po k(m-1) diskov)
- S=k*s, ef=1/m
- zvyšuje výkon

disk 0	disk 1	disk 2	disk 3
0	1	0	1
2	3	2	3
4	5	4	5
6	7	6	7

pre m=2, k=2
- výpadok 1 disku je OK
- výpadok 2 diskov je OK s pravdepodobnosťou 1/3

Po výmene chybného disku je potrebný zápis na *k* diskov.

RAID10 = RAID1+0

- RAID0 z *k* zariadení typu RAID1 z *m* diskov
- min. počet diskov: 4
- odolné voči výpadku od (m-1) po k(m-1) diskov
- S=k*s, ef=1/m
- zvyšuje výkon

disk 0	disk 1	disk 2	disk 3
0	0	1	1
2	2	3	3
4	4	5	5
6	6	7	7

pre m=2, k=2
- výpadok 1 disku je OK
- výpadok 2 diskov je OK s pravdepodobnosťou 2/3

Po výmene chybného disku je potrebný zápis na 1 disk.

Paradoxy RAIDov

- so stúpajúcou kapacitou diskov je čoraz reálnejšia situácia, že druhý disk v RAID5 zlyhá počas rekonštrukcie poľa po výmene prvého zlyhaného disku
  - RAID6 to čiastočne rieši, avšak v skutočnosti to len trochu odsúva do budúcnosti
  - preto stúpa popularita RAID10 a RAID50 (RAID0 postavený z RAID5 zariadení)

Záložné dátové centrum

- offline replikácia
  - pravidelná synchronizácia údajov z primárneho do záložného centra
- online replikácia
  - online synchronizácia z primárneho do záložného centra (napr. RAID1 cez sieť)

Zhrnutie

	zálohovanie	RAID	záložné datacentrum	riadenie prístupu
techn. zlyhanie	čiastočne	áno (v medziach)	čiastočne – áno	nie
deštrukcia syst.	čiastočne (ak sú zálohy mimo)	nie	áno	nie
neúmyselné vymazanie	čiastočne	nie	nie – čiastočne	čiastočne
úmyselné vymazanie útočníkom	čiastočne	nie	nie – čiastočne	áno