

Dostupnost

Proč?

- Hackeři, bezpečnostní slabiny
- Závady systému, disků, ...
- Ztráty napájení
- Požáry
- Bouře
- Zápavy, voda
- Zemětřesení
- Teroristé
- Vandalismus, kriminální živly
- Extrémní teploty, vlhkost, ...
- Ztráty klíčových pracovníků
- Logické chyby, chyby obsluhy

Proto a mnoho dalších důvodů.

Základní přehled nástrojů

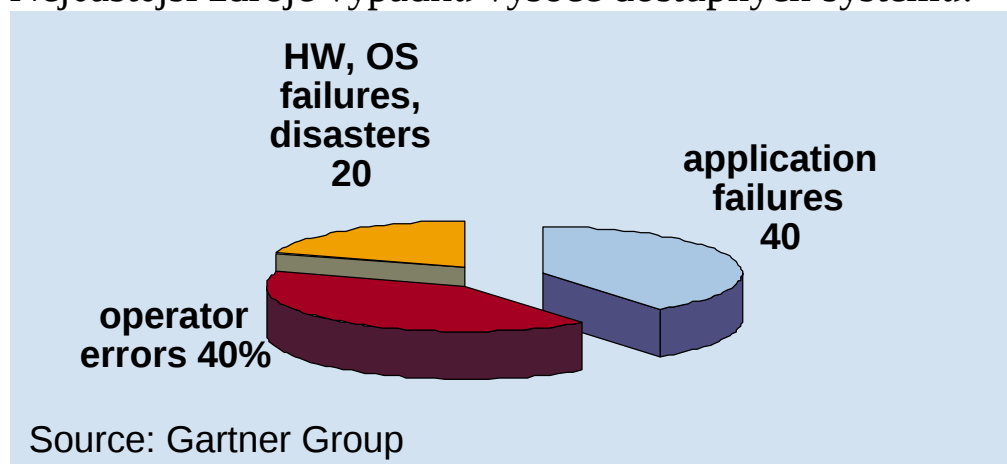
- redundance
- replikace
- zálohování
- archivace

Memento:

lidská chyba je důvodem poloviny všech výpadků vysoce dostupných systémů za posledních 30 let (zdroj: SUN)

Memento 2:

Nejčastější zdroje výpadků vysoce dostupných systémů:



Jinými slovy je potřeba dát si pozor, abychom nebyli technologicky fanatičtí.

Co je to dostupnost:

Materiál slouží výhradně jako pomůcka pro absolvování přednášky *Aplikace bezpečnostních mechanismů* na MFF UK V Praze. Není určen k samostudiu problematiky. Jeho obsah se nemusí shodovat s rozsahem látky přednášené v konkrétním semestru

$$\text{Dostupnost} = \text{uptime} / (\text{uptime} + \text{downtime}) * 100\%$$

Co znamenají devítky v ročním provozu:

Počet devítek	Procentní dostupnost	Neplánovaný výpadek
2	99%	88 hours
3	99.9%	9 hours
4	99.99%	45 minutes
5	99.999%	5 minutes
6	99,9999%	31 sekund

a teď uvažte, že pokud jste závislí na službách více dodavatelů, jejich výpadky, která vás zastaví, budou mít povahu nezávislých náhodných jevů ...

Ne vše je důležité, celý IS lze rozdělit dle důležitosti a potažmo i rychlosti obnovy:

- 1 Mission critical Služby, které musí být dostupná za všech okolností. Např. databázové služby, LDAPy ...
- 2 Must be available Služby, které jsou nezbytné, ale lze vystačit s omezeným výkonem. Např. messaging nemusí být v určitých oborech kritický.
- 3 Can be postponed Služby, které jsou potřeba v daném období. Kalendář, účetní systém, ...
- 4 Optional Služby, které bez kterých lze být libovolně dlouho. Např. přístup k webu je užitečný, ale ne nezbytný.

Organizační zajištění

Vnitřní opatření organizace pro schopnost omezenou dobu fungovat bez podpory IS

Základem vždy SLA smlouva na dodávku náhradního zařízení v definovaném čase, lidských zdrojů, ...

V případě nutosti lze mít vybraný záložní HW na místě

Outsourcing služeb – zajištěná doba reakce, dostupnost kompetentních pracovníků

Monitoring

- Základem je dohled nad systémem, který zajistí pokud možno proaktivní odhalování závad, nebo alespoň
- provozní manuál

- protokoly o činnosti
- automatická analýza logů
- alerting

Doplňkem musí být dostatečné provozní rezervy

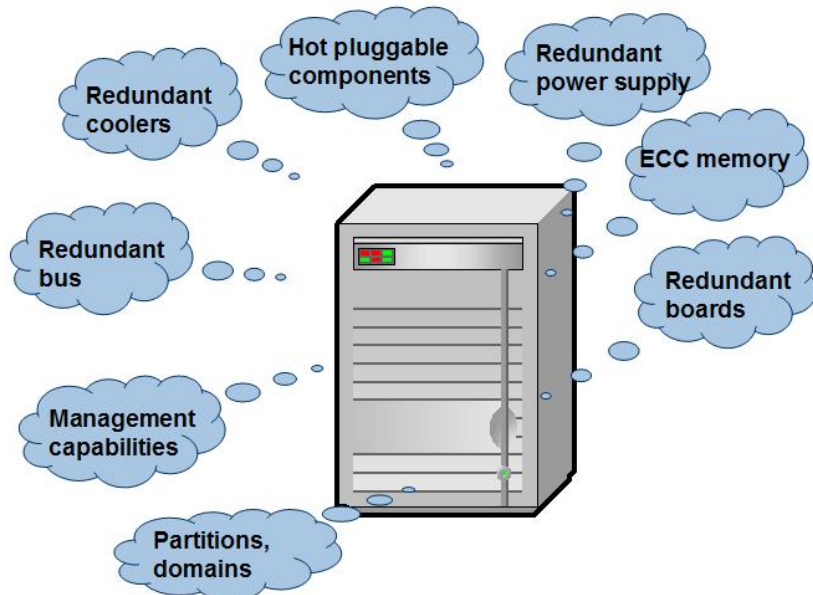
Pasivní bezpečnost systému

“Dostupné” prostředí

zajištění co nejideálnějšího prostředí pro provoz systému

teplo, vlhkost, vibrace, prašnost, kvalita napájení, odolnost vůči povodním, ohni, ... všechny tyto vlivy mohou dramaticky (násobně) zvýšit poruchovost zařízení

Funkčnost vlastního HW



Datová persistence

Níže uvedené mechanismy se doplňují, spíše než nahrazují

Zálohování

technologie flash copy, instant flash, shadow copy apod.

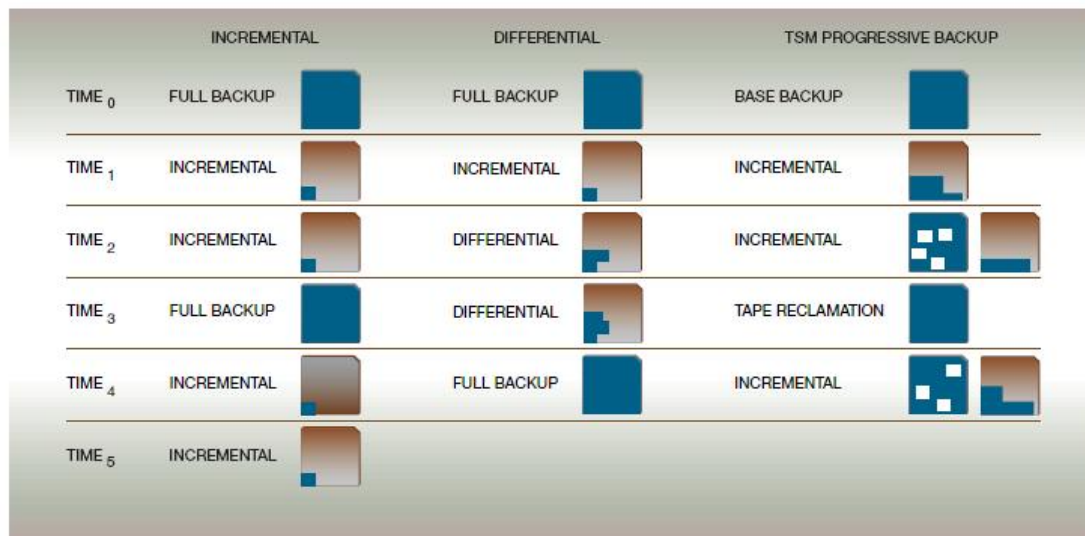
nezbytností management zajišťující plánování záloh, podporu restore, evidenci záloh

- off-line konzistentní zálohy
- on-line zálohy
- on-site zálohy

- off-site zálohy (archivy)

Příklady zálohovacích strategií:

- Inkrementální zálohy
- Diferenční zálohy
- Komplexní systém řízení záloh (zde Tivoli Storage Manager)



Disková pole typu RAID

- Level 0 Striping – data jsou rozložena po částech na všech discích, neposkytuje ochranu proti HW závadě.
- Level 1 Mirroring – veškerá data replikována na separátních discích.
- Level 2 Ochrana pomocí Hammingova kódu – na dalších discích se ukládá redundance umožňující opravu 1-bitových chyb a detekci 2-bitových. Prokládání po bitech či blocích.
- Level 3 Datové bloky jsou rozkládány na disky pole, na vyhrazený disk se zapisují paritní bity.
- Level 5 Datové bloky rozloženy podobně jako při stripingu, ale paritní bloky jsou distribuovány přes všechny disky.

Pole obvykle obsahuje tzv. hot-spare disky, které nejsou aktuálně používány, ale využijí se jako operativní záloha v případě poruchy některého z disků, na která se ukládají data.

Důležité další vlastnosti pole – **flash copy, instant copy, remote replication**

Zachování funkčnosti aplikace

Co se dá dosáhnout

- extrémně rychlý návrat
- omezení rozsahu výpadku
- transparentnost výpadku

typy clusterů

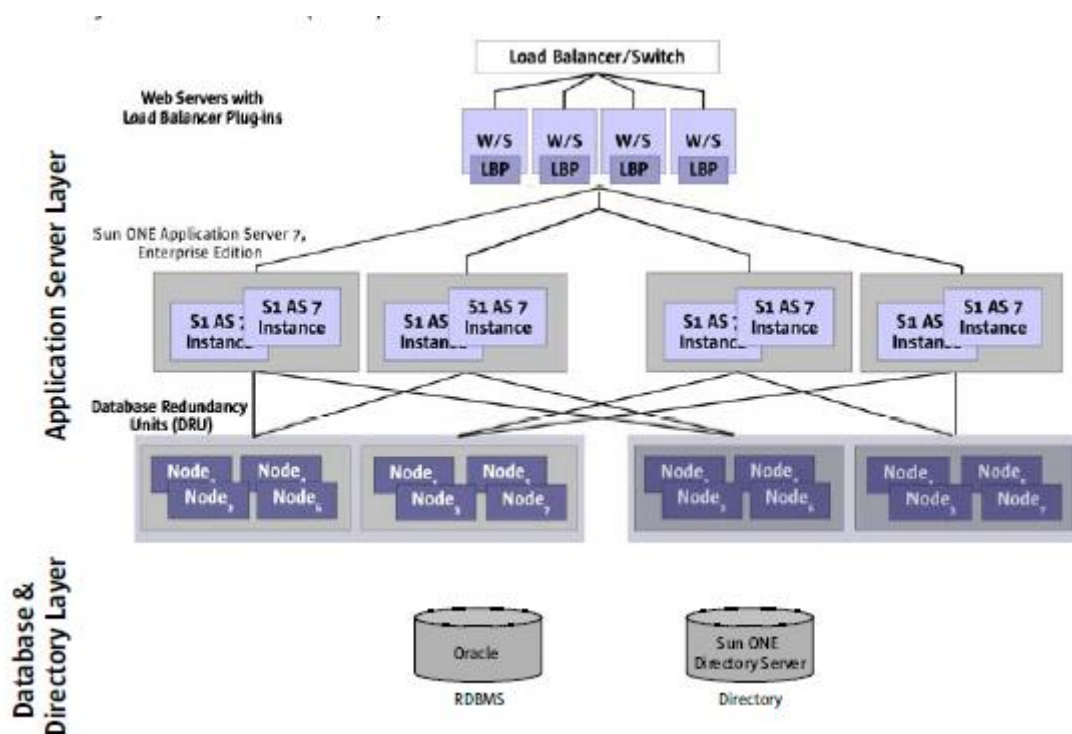
- hot – standby
- active - active

Základní strategie

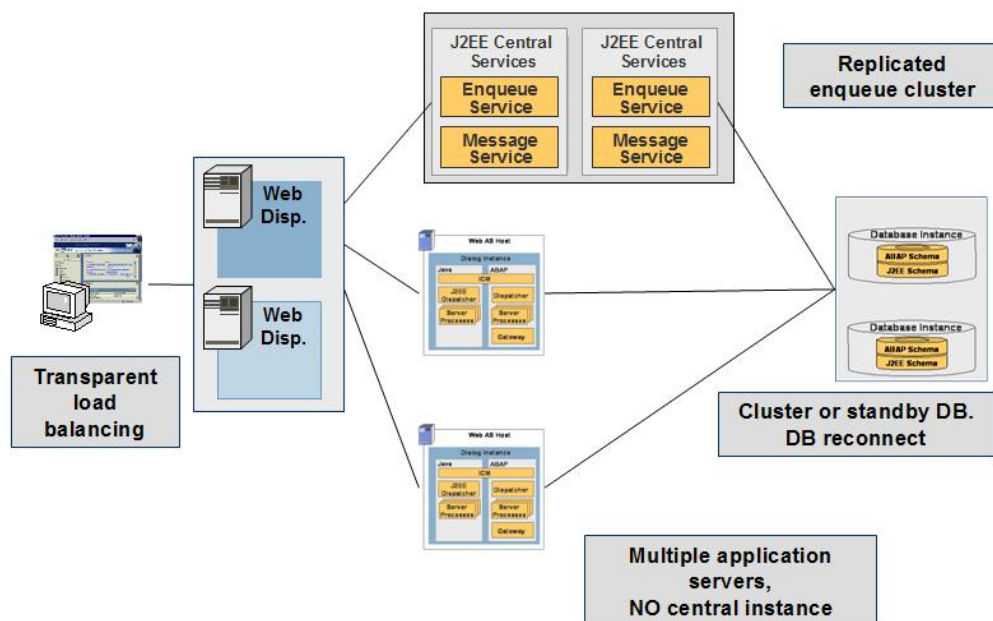
- Fault tolerance
- Load ballancing
- Virtualizace

Dnes módním slovem je *GRID (CLOUD) computing*, což by se ale dalo zahrnout pod pojem load ballancing. V podstatě se jedná o pool zdrojů, které si v případě přetížení mohou dočasně doalokovat jednotlivé produktivní systémy.

Příklad SunONE Application Server



Ještě jeden příklad (SAP application server):



Clustering

principiálně se vyskytují dva typy clusterů:

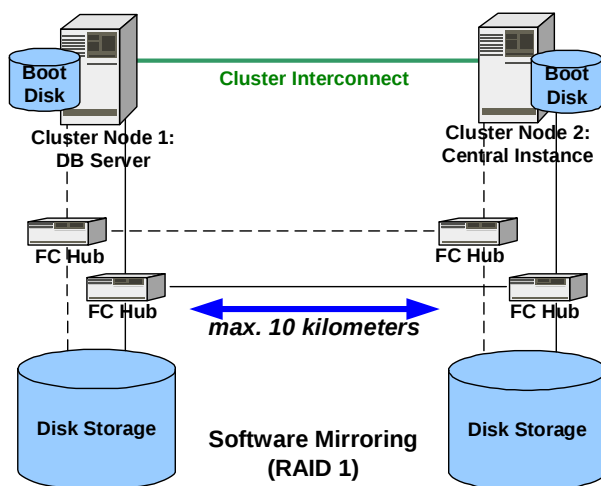
active-passive cluster: zde záložní node převzme funkcionality v případě havárie primárního uzlu, do té doby pouze vytváří repliku dat, případně je zcela neaktivní

active-active cluster: za normálních okolností je zátěž systému rozložena na obě poloviny clusteru, v případě havárie zbylý uzel přebírá aktivitu

Cluster se synchronní replikací

Při malé vzdálenosti primárního a záložního serveru a možnosti zřídit vysokorychlostní (fibre channel) spojení obou systémů ideálním řešením pro udržování redundantní kopie dat (na úrovni databáze) softwarový RAID

Aplikační servery jsou nainstalovány jako fail-over cluster

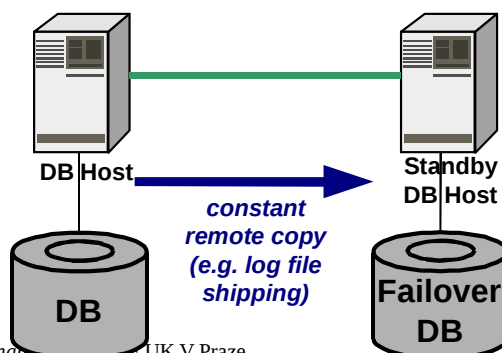


Cluster s asynchronní replikací

Asynchronní replikace s sebou nese riziko ztráty určité části nejaktuálnějších informací v okamžiku poruchy primárního systému.

Replikace na úrovni DB

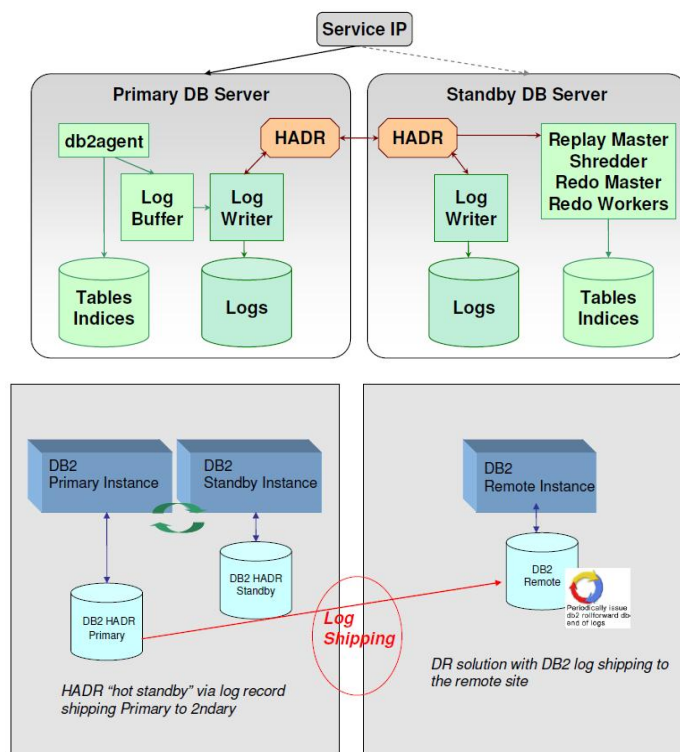
Databázové servery podporují, kromě primárního záznamu logů, v různé formě



synchronní, či asynchronní zápis logů do sekundární kopie, která může být topologicky dostatečně vzdálená.

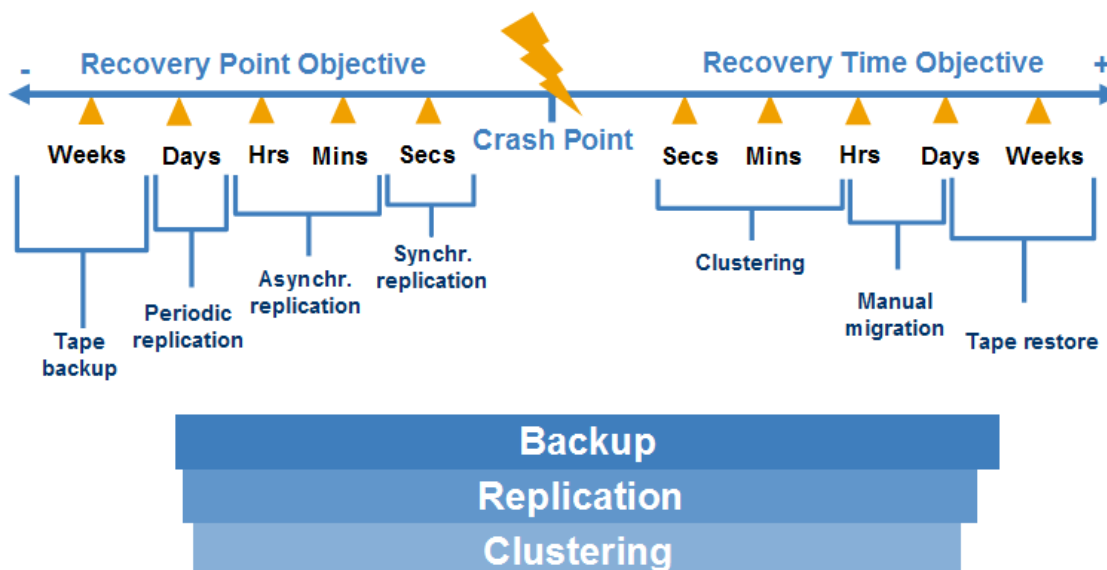
Příklad:

- Oracle Standby Database - asynchronní replikace pomocí logů,
- Oracle Symmetric replication -asynchronní a synchronní replikace na základě příkazů



- DB2 (HADR)
- DB2 Log Shipping

Plánování dostupnosti



třetím rozměrem zálohování jsou náklady na pořízení zálohy:

- doba odstávky potřebná pro pořízení zálohy
- omezení provozu v době tvorby zálohy (snížení výkonu, nemožnost některých operací, ...)
- cena zálohovacího mechanismu
- zvýšení složitosti systému