

Vaše téma:

Ochrana dat a jejich obnova v případě výpadku či havárie

Obsah čísla:

- Různé varianty plánu Disaster Recovery
- Zjednodušení plánu Disaster Recovery zavedením virtualizace
- Vysoká dostupnost a Disaster Recovery on-line



Dnešní téma Technické přílohy volně navazuje na třídílný cyklus o tom, jak zálohovat data, následně je obnovovat a zabránit tak jejich ztrátě. Ochrana dat se však dá rozdělit do více oblastí. Data chráníme nejen proti ztrátě, ale také proti jejich zneužití a nedostupnosti. Právě kvalitní řešení v oblasti dostupnosti dat může způsobit, že klasická záloha vůbec nebude využita a uživatel nepocítí, že došlo k havárii na systému. Ochrana dat spočívá také v tom, že data jsou jistým způsobem udržovaná ve stavu, aby záloha vůbec nemusela být použita.

Zajištění vysoké dostupnosti klíčových aplikací a ochrany dat je v dnešních společnostech čím dál důležitějším požadavkem, neboť cena ztráty dat či výpadku různých IT systémů firmy může růst do milionů korun. Dnes vás proto chceme seznámit s tím, jak se systémy dají udržovat v chodu po celou potřebnou dobu provozu, jak mít data neustále přístupná a jak v případě havárie obnovit nejen data, ale i všechny systémy v co nejkratší možné době. Budeme hovořit o tzv. plánu Disaster Recovery, což v překladu znamená „plán obnovy provozu po havárii“, a technických prostředcích pro jeho naplnění.

Věřím, že následující řádky budou pro vás zajímavé a dobře využitelné ve vašich firmách a organizacích.



Petr Nepustil
vedoucí divize Výroba / K-net
petr.nepustil@k-net.cz

Aktuální pojem Dostupnost

Uživatelé chtějí mít své systémy, například hodinky, telefony, auta nebo počítače neustále k dispozici. Dostupnost se vztahuje ke schopnosti uživatelů přistupovat ke svým systémům buď za účelem založení nových aktivit nebo úpravy či kontroly stávajících aktivit, popřípadě pro zjištění výsledků již uskutečněných aktivit. Jestliže uživatelé nemohou přistupovat k systému, říkají, že je systém nedostupný. **Dostupnost v IT** je nejčastěji definována jako zajištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby.

Dostupnost v procentech

Dostupnost je obvykle vyjádřena jako procento času v daném roce, kdy je systém v provozu. Následující tabulka ukazuje vztah mezi požadovaným procentem dostupnosti a odpovídajícím množstvím času, po který může mít systém prostoj (být nedostupný) během roku, měsíce, týdne. Předpokládáme, že se jedná o systém provozovaný v režimu 24x7.

Dostupnost v %	Prostoj za rok	Prostoj za měsíc	Prostoj za týden
90%	36,5 dne	72 hodin	16,8 hodin
95%	18,25 dne	36 hodin	8,4 hodin
98%	7,30 dne	14,4 hodin	3,36 hodin
99%	3,65 dne	7,20 hodin	1,68 hodin
99,5%	1,83 dne	3,60 hodin	50,4 minut
99,8%	17,52 hodin	86,23 minut	20,16 minut
99,9% ("tři devítky")	8,76 hodin	43,2 minut	10,1 minut
99,95%	4,38 hodin	21,56 minut	5,04 minut
99,99% ("čtyři devítky")	52,6 minut	4,32 minut	1,01 minut
99,999% ("pět devítek")	5,26 minut	25,9 sekund	6,05 sekund
99,9999% ("šest devítek")	31,5 sekund	2,59 sekund	0,605 sekund

Přestože je populární uvádět dostupnost systému v % za rok, je přesnější a praktičtější uvádět RTO (Recovery Time Objective – „reálná doba obnovy“) a RPO (Recovery Point Objective – „plánovaný bod obnovy“) – hodnoty, které se vztahují k době obnovení systému a k množství dat, o které můžeme přijít (Oba pojmy budou vysvětleny dále).

Měli bychom si v této souvislosti povšimnout, že pojmy provozuschopnost a dostupnost nejsou synonyma. Systém (server) může být totiž v provozu, ale nemusí být dostupný. To se stane například v případě výpadku počítačové sítě.

Vysoká dostupnost a doba obnovy (High Availability and Recovery Time)

Vysoká dostupnost je systémový návrh postupu a souvisejících operací, který zajistí požadovaný stupeň provozní stability během určitého období (viz. výše uvedená tabulka).

Pro návrh postupu je právě doba obnovy (recovery time) klíčovým parametrem a následně vypracování a ověřování „Disaster Recovery“ plánu je základním stavebním kamenem pro dodržení smluvních ujednání spojených se službami zajištění vysoké dostupnosti.



Ing. Tomáš Knettig
jednatel / IT konzultant
tomas.knettig@k-net.cz

Různé varianty plánu Disaster Recovery

Pokud uvažujeme o vypracování plánu Disaster Recovery, máme k dispozici několik variant. Podívejme se na nejběžnější způsoby ochrany.

Řešení na bázi off-line zálohy systémů

- ▶ **1. Pokud používáme fyzický server, použijeme vhodnou hardwarovou náhradu tohoto serveru,** aby v případě výpadku bylo zajištěno, že ze zálohy dokážeme tento server či systém obnovit. Musíme mít dostupnou zálohu a dostupný HW, na němž systém obnovíme.
- ▶ **2. Máme k dispozici virtuální systémy.**
 - a) Máme udržovaný fyzický server a virtuální server máme pouze pro případ havárie. Tento virtuální server pravidelně zálohujeme a provádíme pravidelnou obnovu tohoto systému s originálním.
 - b) Použijeme plnou virtualizaci, kdy máme virtuální systém uložený na diskovém poli. V případě havárie serveru dokážeme zprovoznit systém bez zásahu administrátora na jiném serveru v plné kvalitě.

Řešení zálohy off-line variantami znamená, že uživatel pozná výpadek. U variant 1 a 2a může přijít o některá aktuální data, která nemá uložena. Naopak u varianty 2b v některých případech výpadek nezaznamená.

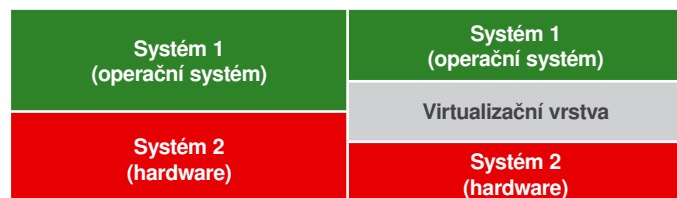
Řešení na základě vysoké dostupnosti systémů

- ▶ **3. Využijeme dvou systémů, které nám běží paralelně on-line.** Při této variantě je plně využíván výkon systémů. Musíme mít k dispozici 2 HW, na kterých běží jeden systém. Všechna data jsou ukládána souběžně na oba systémy, v případě výpadku je pro uživatele vždy funkční jeden systém. Uživatel výpadek vůbec nepozná a nepřijde o žádná data.

Zkušenosti z praxe nejen společnosti K-net zatím hovoří ve prospěch varianty 2, tedy pro spolupráci s virtualizační vrstvou, a u kritických systémů pro řešení dle varianty 3. Varianta 1 znamená nutnost mít zajištěný stejný HW. Klasické zálohování, používané po dlouhá léta, je dnes již pro řadu moderních společností překonané. Požaduje odstávky systémů a samotné obnovení dat trvá neúměrně dlouho. Často také chrání pouze data, ale kromě jejich obnovy nenabízí žádné jednoduché prostředky pro obnovení provozu IT systémů.

ad2) Zjednodušení plánu Disaster Recovery zavedením virtualizace

Pojem virtualizace je ve slovnících vysvětlen jako „něco, co není reálné, ale může zobrazovat charakteristickou kvalitu reality“. A také jako „něco, co je simulováno v počítači nebo připojením na síť“. Tak to uvádí Wikipedie a Wiktionary. Vysvětit tento pojem hned na začátku je žádoucí, neboť pochopení principu virtualizace nám dovoluje efektivně využívat její vlastnosti v IT a pracovat s aplikacemi a daty kontinuálně, bez výpadků či jiných omezení v případě havárie apod. Virtualizaci si také můžeme představit jako oddělovací vrstvu mezi virtualizovaným systémem a zařízením či mezi dvěma systémy tak, aby se na sobě staly nezávislémi.



Typy virtualizace

Dnešní IT svět hovoří o třech typech virtualizace:

- ▶ **Serverová virtualizace** je asi nejznámější a nejpoužívanější. Zde je vložena virtualizační vrstva mezi operační systém (např. Microsoft Windows 2003, Linux, aj.) a mezi HW. Operační systém se tak stává nezávislý na HW na kterém běží, což s sebou přináší velkou řadu výhod právě pro DR.
- ▶ **Virtualizace desktopů** je provedením velice podobná serverové virtualizaci. Je vložena virtualizační vrstva mezi desktopový operační systém (Windows XP, Vista, Windows 7 aj.) a mezi HW. Způsobem použití se však od serverové virtualizace značně liší. Její hlavní význam spočívá v centralizaci, energetické úspoře a flexibilitě.
- ▶ **Virtualizace aplikací** je asi nejstarší virtualizací vůbec, i když jako o virtualizaci o ní mluvíme až s příchodem virtualizace desktopů. Technicky jsou na trhu dvě varianty jak virtualizaci aplikací provést:
 - ▶ Terminálová služba či publikování aplikací. Vrstvu mezi desktopovým operačním systémem a aplikací zajišťuje terminálová služba serveru. Aplikace běží na serverovém operačním systému a mezi klientem a serverem jsou přenášeny pouze obrazovky a stisky klávesnice, resp. myši. Podmínkou této virtualizace je, že musí existovat IP konektivita mezi serverem a klientským zařízením.
 - ▶ Streaming aplikací, resp. vytváření spouštěcích balíčků, je metoda, kdy je aplikace zapouzdřena virtualizační vrstvou a stane se nezávislá na desktopovém operačním systému. Aplikace se díky svému zapouzdření nemusí instalovat a může být spuštěna ihned po doručení na klientské zařízení.

Způsob využití virtualizace pro DR

Pro DR se nejčastěji využívá serverové virtualizace. Důvodem je hlavně to, že zajištění bezpečného chodu serverů je pro IT úkolem číslo 1. Případná havárie serverů má na provoz společnosti nejvyšší dopad ve srovnání s havárií desktopů či aplikací. Zásadní vlastností virtualizace pro DR je právě nezávislost operačního systému na HW. Získáváme tak následující zjednodušení:

- ▶ V případě havárie HW můžeme náš server spustit skoro na libovolném zařízení s alespoň trochu srovnatelným výkonem.
- ▶ Dobu zprovoznění systému po výpadku dokážeme zkrátit z několika hodin až dnů na výpadek v řádu minut až sekund.
- ▶ Velice jednoduše a efektivně dokážeme provádět ověřování a testování nastaveného plánu pro DR.
- ▶ Razantně je snížena finanční náročnost na udržení plánu DR ve funkčním stavu. Vytvořit kvalitní plán DR tak může i malá společnost.

Princip virtualizace dat

S moderními systémy je možné a velmi reálné udržovat data v tzv. kopiích, a to buď v kopiích on-line nebo off-line. Přestavte si, že máte konkrétní datový soubor, se kterým pracujete. Tento soubor je kopírován při každé vaší změně do nějakého jiného místa, abyste nepřišli o vaši práci v případě, že zdroj, na kterém je soubor uložen, je nefunkční.

Je-li úložiště dokumentů ve stavu off-line, znamená to, že se jedná o běžnou zálohu, která je prováděna průběžně. V případě havárie se data obnoví ze zálohy, tzn. uživatel je přesměrován na záložní dokument. Tuto skutečnost uživatel obvykle pozná, protože je vhodným způsobem na ni upozorněn a je přerušena jeho práce do doby, než je záložní zařízení připraveno nabízet své služby. Pokud je záložní úložiště dokumentů ve stavu on-line, je schopno ihned poskytovat svoje služby a ztrátu produkčního zařízení nemusí uživatel zaznamenat vůbec. V tomto případě se jedná o zcela totožné systémy z hlediska datového obsahu a všechny změny, které uživatel udělá, jsou ukládány na dvě místa zároveň. Uživatel nepozná, na kterém zařízení pracuje a v případě odstávky jednoho zařízení není jeho pracovní proces nijak ovlivněn.

Virtualizace serverů a operačních systémů

Virtualizace serverů je oproti virtualizaci dat složitější, a to především proto, že v případě zálohovaných dat nezáleží na tom, o jaký hardware či software se jedná, ale většinou data dokážeme obnovit na jakémkoliv systému. U operačních systémů, které jsou závislé na hardwaru, musíme na obnovu použít stejný

hardware (proto se společně vyplatí investovat do nákupu stejných serverů, které lze v případě výpadku zaměnit).

Tuto nepříjemnost v operačním systému odstranila právě virtualizace, která je v současné době velmi využívána. Virtuální systém (software) představuje vrstvu mezi operačním systémem a hardwarem a díky této vrstvě se operační systém stává nezávislým na hardwarem. Pokud tedy zálohujeme operační systém, který je na virtuálním systému, je velmi jednoduché v případě havárie tento systém na jakémkoliv virtuálním serveru ve velmi krátké době obnovit. Další výbornou vlastností virtualizační vrstvy je to, že na jednom hardwarem je možné spustit více operačních systémů. V případě havárie operačního systému je tedy velmi jednoduché převést všechny systémy, které na tomto serveru běžely, na jiný hardware, na kterém běží virtualizační vrstva, a po dočasné době v tomto nouzovém režimu provozovat na jednom hardwarem daleko více serverů. Díky virtualizační vrstvě dokážeme velmi efektivně zajistit obnovu provozu systémů po havárii – tedy službu dnes známou pod anglickým názvem „Disaster Recovery“. V případě plánovaných investic do Disaster Recovery operačních systémů je tedy velice zajímavé a účelné uvažovat o virtualizaci, protože díky jejím vlastnostem provedete svůj Disaster Recovery plán efektivně a za zajímavou cenu.

Virtualizační nástroje

Virtualizační nástroje nabízejí všichni přední světoví hráči, a to je především VMware, Citrix a Microsoft.

Producenti software	Produkt	Oblast virtualizace	Vlastnosti
VMware	ESX Server (vSphere)	virtualizace serverů	průkopník technologie dobré vlastnosti pro administraci operačních systémů
	VMware VIEW	virtualizace desktopů	využívá znalostí serverové virtualizace
	ThinApp	virtualizace aplikací	vytváření balíčků na klienta
Citrix	XenServer free Citrix Essentials pro XenServer a Hyper V	virtualizace serverů	kvalitní a velice výkonný 64-bitový hypervisor
	Citrix XenDesktop	virtualizace desktopů	vynikající zobrazovací protokol HDX
	Citrix XenApp (Presentation Server, Fundamentals)	virtualizace aplikací	průkopník technologie umí varianty publikace i streamingu aplikací
Microsoft	Hyper V	virtualizace serverů	nový, technicky vyspělý nástroj
	Terminal Services	virtualizace aplikací	využívá hlavně terminálové služby



Ing. Petr Nepustil
vedoucí divize Výroba / IT konzultant
Petr.Nepustil@k-net.cz

ad3) Vysoká dostupnost a Disaster Recovery on-line

Pohled do historie a základní pojmy

Kontinuální zachování funkčnosti IT systémů včetně ochrany dat jsou technologie, které se používají již přes čtyřicet let. Nicméně do nedávné doby byly tyto technologie vyhrazeny pouze pro speciální a často úzce specializované systémy, které se staraly např. o řízení letového provozu a podobné velmi kritické oblasti nasazení počítačů. Naštěstí však doba pokročila a dnes jsou podobné technologie dostupné již všem zákazníkům. Jaké všechny přístupy lze použít?

Jasnou špičkou mezi systémy nabízejícími kontinuální dostupnost jsou tzv. systémy FTS (z anglického Fault Tolerant Systems). Tyto úzce specializované servery se vyznačují spolehlivostí blížící se 100% a jsou postaveny na kompletně redundantním hardwarem, kdy je zdvojnásobena opravdu každá komponenta. V případě poruchy části hardwarem tak okamžitě přebírá její funkci část záložní. Systémy FTS se proto vyznačují hodně specifickou a nákladnou architekturou a běží na nich pouze specializovaný, na míru psaný software s úzkými možnostmi nasazení.

Po těchto proprietárních systémech jsou další kategorií serverů nabízejících vyšší dostupnost systémy DPS (Distributed Processing Systems), které dělíme podle použité architektury na systémy MPP (Massively Parallel Processing) a SMP (Symmetric Multi-Processing). Pod systémy MPP řadíme například servery IBM System z. Systémy MPP jsou extrémně škálovatelné (z pohledu výkonu), ale zároveň nákladné a obtížné na programování. Výkon a redundance provozu pak velmi úzce závisí na správně napsané aplikaci, která musí být napsána tím nejlépe možným „distribuovaným“ a redundantním způsobem.

Servery v „naší“ serverovně

Systémy SMP jsou dnes nejběžněji nasazovanými typy serverů. Nabízejí poměrně slušný výkon vhodný pro většinu běžných komerčních využití, jednoduchý design a přijatelnou cenu. Zároveň jsou to však servery nejméně spolehlivé. Jejich hardware ani softwarová architektura sama o sobě žádná řešení redundance pro data ani provoz nenabízí. Abychom dosáhli vyšší úrovně spolehlivosti, je zapotřebí použít specifická softwarová řešení, případně jejich kombinaci s dalším nákladným hardwarem. V další části článku se budeme věnovat podrobněji klasifikaci systémů, které nabízejí zvýšenou spolehlivost a on-line zálohování provozu právě pro tyto SMP systémy. Pro možnost srovnání je důležité definovat čtyři základní pojmy.

Vysoká dostupnost anebo také HA (High Availability) je technologie, která si bere za úkol zpřístupnit lépe IT systémy uživatelům a snížit dobu případného výpadku na minimum. Klíčem je zajištění kvalitnějšího a spolehlivějšího přístupu uživatelů k službám a aplikacím. Tato technologie počítá pro případ selhání s takzvaným procesem „Fail-over“, po jehož doběhnutí mají klienti k dispozici stejné služby, aplikace i data, jako před selháním, a to ve stejné kvalitě. Fail-over přitom musí být transparentním procesem, který pro klienty neznamená žádné požadavky na „součinnost“.

Disaster Recovery anebo DR je technologie, která zvyšuje dostupnost IT systémů na geografické úrovni. Jinými slovy chrání dostupnost dat, služeb a aplikací proti selhání celé „primární lokality“, ať už se jedná o selhání serverů, storage systémů, výpadek napájení, fyzické zničení zařízení či např. přírodní katastrofu. Klíčem je udržování geografické kopie všech klíčových dat a zajištění mechanismu řízeného „přepnutí“, tj. Fail-over procesu na úrovni geografických lokalit. Často se také hovoří o tzv. vzdálené vysoké dostupnosti anebo vysoké dostupnosti přes síť WAN (HA over WAN).

Vaše téma:

Ochrana dat a jejich obnova v případě výpadku či havárie

Recovery Time Objective (RTO) je množství času potřebné pro obnovení dat a provozu. Může být, v závislosti na použité technologii, vyjádřeno v sekundách, hodinách či dnech.

Recovery Point Objective (RPO) je množství dat, o které můžeme přijít, tj. do jakého bodu (stavu) v minulosti obnovíme data. Opět, v závislosti na použité technologii, se může jednat buď o nulovou ztrátu anebo desítky, stovky či dokonce tisíce kilobajtů.

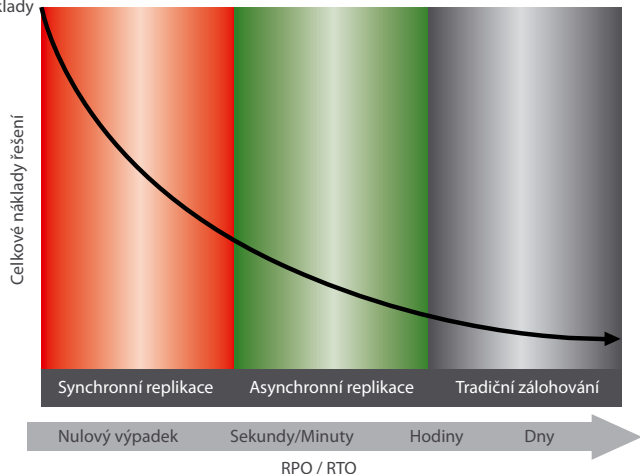
Jak můžeme zajistit vysokou spolehlivost u SMP systémů?

Existuje minimálně pět základních možností:

- ▶ standardní zálohování s dlouhým časem RTO a vysokou ztrátou dat (vysoké RPO),
- ▶ skriptované nástroje na pravidelné kopírování souborů (např. Robocopy), které se vyznačují nízkým výkonem a nemožností pracovat s otevřenými soubory, čas RTO je lepší než v případě zálohování, RPO je na stejné, nízké úrovni,
- ▶ specifická řešení (např. Microsoft Cluster), která nabízí dobré hodnoty RTO i RPO, ale mají podstatná omezení: specifický hardware, pouze „cluster aware“ aplikace a jediná kopie dat (nebezpečí ztráty/selhání úložiště dat),
- ▶ asynchronní replikace dat, která nabízí stejně dobré hodnoty charakteristik RTO i RPO jako MS Cluster, ale zároveň nabízí dvě kopie dat, které mohou být od sebe geograficky odděleny,
- ▶ synchronní replikace dat (např. hardwarový mirroring dat storage serverů), která nabízí nejlepší hodnoty RTO i RPO, avšak jedná se zároveň o velmi nákladné řešení, a to jak vzhledem k nákladům na pořízení, tak i na samotný provoz.

Jednotlivé přístupy vzhledem k charakteristikám RTO i RPO ilustruje následující obrázek:

náklady



Porovnejme nyní dva nejrozšířenější přístupy, a to Microsoft Cluster server a nástroje na asynchronní replikace, jako jsou například softwarová řešení Steeleye Lifekeeper anebo Double-Take. Základní srovnání přináší tato tabulka:

Asynchronní replikace (Lifekeeper, Double-Take)	Sdílené datové úložiště (Microsoft Cluster)
HA, DR či kombinované řešení	Nativně pouze HA ochrana (bez dalších produktů)
Vicenásobné kopie dat	Jediná kopie dat
Standardní verze OS i aplikací	Enterprise verze anebo „cluster aware“ aplikace
Hardwarová nezávislost	Specifický/certifikovaný hardware
Bez omezení vzdálenosti	Omezení maximální vzdálenosti uzlů clusteru
Sít'ová infrastruktura s libovolnou kvalitou	Vysoce propustné linky s nízkou latencí
Jakékoliv aplikace	Specifické certifikované aplikace
Lze ihned využít ve stávající infrastruktuře	Je nutná migrace serverů, dat i aplikací do prostředí Microsoft Clusteru



Ing. Milan Flutka

obchodní ředitel / Kancelářské stroje
obchodní partner K-net
milan.flutka@kancelarskestroje.cz

Rejstřík

„Fail-over“

V počítačích failover (překonání chyby) je schopnost přepnout automaticky na jiný - záložní systém v případě chyby nebo anomálního ukončení aktivního systému.

Recovery time

Doba obnovy (recovery time) je úzce spojena s dostupností. Jedná se

o celkový čas potřebný pro plánovanou odstávku nebo čas potřebný pro úplné obnovení po neplánované odstávce.

Doba obnovy může být i nekonečně dlouhá za předpokladu, že systémový návrh nepočítá s některými chybami. Například se může jednat o požár, kdy dojde ke zničení datového centra a jeho systému a neexistuje záložní datové centrum pro případ havárie.

Technická příloha časopisu LOGIN 3/2009, ročník 4.

Vydala společnost K-net
Uzávěrka čísla: 10. 12. 2009
Připravili: Věra Staňková, Petr Nepustil,
Milan Flutka, Tomáš Knettig
Neprodejné

K-net Technical International Group
Okružní 9a, 638 00 Brno
Tel. + 420 548 220 150
GSM + 420 724 799 101
E-mail: info@k-net.cz, www.k-net.cz

Solidea Net Partner s.r.o.
člen skupiny K-net
Sazečská 560/8, 108 25 Praha 10 – Malešice
Tel. + 420 267 990 521
E-mail: net@solidea.cz, www.solidea.cz

