

Vaše téma:

## Vysoká dostupnost

Obsah čísla:

- Virtualizace a zajištění provozu
- Double-Take – rodina nástrojů na ochranu dat a aplikací pomocí asynchronní replikace



V minulé Technické příloze jsme se věnovali ochraně dat a obnově v případě havárie. Obecně jsme se zmínili o tématu vysoké dostupnosti dat a systémů. V dnešní technické příloze na toto téma navážeme a pokusíme se ho rozvést.

Vysoká dostupnost je stav, kdy se spolehlivost a provozuschopnost systémů (služeb, dat, techniky a podobně) blíží ke 100%. Pro zajištění této spolehlivosti nám určitě nebude stačit jeden systém, protože výpadek kterékoliv jeho části bude znamenat snížení kvality poskytovaných služeb nebo neexistenci služby. Výpadek způsobí i údržba takového systému, kdy například dochází k novému startu operačního systému. Shrnuto - jak neplánovaná odstávka, tak plánovaná odstávka způsobí výpadek. Řešení celého problému je zdánlivě triviální - systémy zdvojíme tak, aby se dokázaly navzájem zastoupit. Pokud chceme zabezpečit systém i pro případ živelné katastrofy (požár, povodeň, atd.), je vhodné zdvojený systém rozdělit do různých geografických lokalit. To, jak tuto záležitost zrealizovat a jaké prostředky k tomu potřebujeme, je tématem dnešní Technické přílohy.

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

## Virtualizace a zajištění provozu

Přemýšlíte, jak zajistit nepřetržitý provoz systémů a jak vám v tom virtualizace může pomoci? Pokud ano, jsou právě pro vás určeny následující řádky. Tímto článkem pokračujeme v tématu virtualizace, s jejímiž typy a přínosy pro administraci firemní infrastruktury jsme vás seznámili v minulém roce.

Prvním úkolem v této oblasti je vydefinování pojmu zajištění provozu. V současné době je fungování informačních systémů ve firmách vnímáno stále více jako poskytování služeb jednotlivých systémů uživatelům. V této souvislosti již není tak významné jakou záruku nám dává výrobce hardware nebo dodavatel komunikační linky, ale zajímá nás právě kvalita a dostupnost příslušné služby daného systému. Definujeme a uzavíráme tak nové vztahy smluvně zakotvené v Service Level Agreement (SLA), která obsahuje sadu parametrů služby. Zjednodušeně řečeno, určíme hodnoty, které musejí být splněny, popřípadě sankce v případě neplnění. Je samozřejmé, že u každé jednotlivé služby je možno volit parametry individuálně podle její důležitosti. Úkolem administrátorů je pak naplnit souborem technických a administrativních opatření požadované SLA. Při návrhu systému je nutné si uvědomit, že dostupnost služby ovlivňují nejen odstávky neplánované, ale také plánované. Jak ovlivní výslednou dostupnost služby např. pravidelná údržba systémů.

Údlosti, které řešíme v souvislosti se zajištěním provozu, dělíme do těchto tří typů:

- 1. Plánovaná odstávka** – typicky údržba hardware, operačního systému nebo aplikace
- 2. Neplánovaná odstávka** – servis, porucha hardware nebo softwarové konfigurace apod.

V praxi je možno definovat ještě jeden typ výpadku, který je spíše podskupinou neplánovaného výpadku.

- 3. Neplánovaná odstávka – havárie a obnova po havárii** – nejde jen o výpadek služby, je nutno obnovit celý systém, aplikace nebo data.

**Jaká opatření máme k dispozici pro dosažení vysoké dostupnosti služeb informačních systémů a jak bude vypadat situace, pokud se rozhodneme pro virtualizaci serverů?**

**Jak vidíme z výše uvedeného popisu jednotlivých typů odstávek systémů, první dva se od třetího liší tím, že zde nedochází k poškození dat. Většinou se nám tedy jedná o to, že na konkrétním serveru nemají uživatelé k dispozici odezvu od dané služby.**

Příčiny mohou být velice rozmanité na všech vrstvách od hardware až po aplikaci služby. Pokud má daná služba definovanou vysokou požadovanou dostupnost, je vždy potřeba najít technologii, která dokáže překlenout čas od vzniku incidentu po jeho vyřešení.

**Standardně máme k dispozici následující opatření:**

**1. Redundanci** – znásobení jednotek, které zajišťují danou funkci. Na úrovni hardware je dnes již standardem, že i nekritické systémy využívají zdvojení jednotlivých subsystémů – napájení, řadiče disků, disková pole apod. Nás v tomto případě zajímá tatáž situace o jednu až dvě úrovně výše – redundance serverů (operačního systému), služeb a dat. Mnoho systémů počítá s touto možností již ve svých principech fungování – řadiče Active Directory, DNS servery, mail servery, XenApp farma. Jednotlivé servery vystupují samostatně a vnitřní algoritmy služby zajišťují správnou komunikaci klienta se službou.

**2. Cluster** – jde o situaci, kdy služba jako taková je poskytovaná dvěma nebo více systémy, které pomocí Clusterové služby zpřístupňují službu klientovi pod jednou konfigurací (např. IP adresou, názvem služby). Velmi často se jedná o systém active/passive, kdy je služba poskytovaná z jednoho systému a v případě jeho výpadku je přesunuta na jiný server clusteru. Důvodem k nutnosti využít uspořádání active/passive je často nutnost zajistit jedinečný přístup k datům pro jediný server. Příkladem takového systému je Microsoft Cluster, Symantec Cluster, ale také Symantec Storage Foundation nebo Citrix Access Gateway Enterprise HA.

**3. Load Balancing** – je použitelný tam, kde samotné servery služby pracují samostatně, ale předřazený systém vytěžování (Load Balancing) umožňuje zpřístupnit službu klientovi pod jednou konfigurací (např. IP adresou, názvem služby). Typickým zástupcem služeb je webový server.

**Jak to vypadá ve virtuálním prostředí?**

Uvedené principy jsou platné i ve virtuálním prostředí. Podle použité virtualizační platformy (VMware, XenServer, HyperV apod.) je možné použít např. Microsoft Cluster jak mezi virtuálními servery, tak mezi fyzickým a virtuálním serverem.

Virtuální hardware pro naše operační systémy získáme instalací virtualizační vrstvy (hypervisoru) přímo na fyzický server. Takto připravený server nám umožňuje instalovat a provozovat zároveň několik virtuálních serverů. Hovoříme pak o hostitelském systému, respektive hostiteli.

Virtualizace nabízí další možnosti, které můžeme použít ve strategii vysoké dostupnosti. Virtuální servery nejsou totiž přímo spojeny s fyzickým serverem, na kterém běží. Je možno je přenést z jednoho hardware na jiný nejenom ve vypnutém stavu, ale z hlediska vysoké dostupnosti je důležité, že je možno přesun provést i za běhu virtuálního serveru. Této vlastnosti je možno v manuálním režimu využít při „uvolnění“ hardware pro

údržbu. Systémy hypervisorů s touto akcí přímo počítají, takže pokud administrátor přepne hostitele do režimu údržby, systém automaticky přemigruje virtuální stroje, které na něm běží na jiný hostitelský systém. Technologie migrace je použita i pro balancing (vyrovnávání) výkonu.

Předchozí funkcionalita popisuje výborně situaci, kterou jsme nazvali „plánované odstávky“. V případě neplánovaných odstávek je zde funkcionalita, která je nazvána přímo HA (high availability – vysoká dostupnost). V případě, že dojde k poruše hardware hostitele, virtuální servery, které na něm běžely, jsou spuštěny na jiném hostiteli. To v praxi znamená výpadek služby v délce odpovídající startu operačního systému.

Výše popisované vlastnosti má většina hlavních hypervisorů. Existují některé, které jsou specifické pro jednotlivé výrobce. Jedním z nich je funkce „fault tolerance“, která umožňuje předat funkci virtuálního serveru okamžitě při havárii hardware hostitele na jakýsi „stínový“ virtuální server, který běží na jiném hostiteli, během ms až sekund (podle vytížení VM).

Pokud dojde k poškození dat, potřebujeme provést jejich obnovu. Dostáváme se ke třetímu typu události. Tady se zřejmě výpadku funkcionality služby nevyhneme nejméně po dobu obnovy. Nicméně i zde existují systémy, které dokáží zkrátit dobu potřebnou pro zahájení práce uživatelů. Pro zálohu dat a jejich obnovu je možno použít stejné nástroje pro fyzické i virtuální prostředí.

Pokud jde o virtuální prostředí, tam obnova dat bude probíhat stejně jako ve fyzickém prostředí. Rozdíl bude při obnově kompletních systémů. Virtuální stroj je reprezentován několika soubory, se kterými je možno manipulovat jako s jakýmkoliv jinými soubory, tedy je možno je kopírovat a tedy i zálohovat na disky, popřípadě jiná média. Jednotliví výrobci virtualizačních prostředí kombinují většinou vlastní nástroje pro zálohu/obnovu s podporou řešení třetích stran. Toto je velmi důležité proto, že je možno zahrnout virtuální prostředí do stávajícího zálohovacího systému, které daná společnost používá. Tyto nástroje také většinou dovolují zálohovat nejen celé obrazy serverů, které je možno použít pro obnovu celého serveru, ale také zálohu dat „ zevnitř“ virtuálního stroje.



**Ing. Tomáš Kiedroň**  
IT konzultant  
tomas.kiedron@k-net.cz

**Double-Take – rodina nástrojů na ochranu dat a aplikací pomocí asynchronní replikace**

V dnešním článku se podrobněji podíváme na zajištění online vysoké dostupnosti a geografické ochrany – Disaster Recovery – pomocí nástrojů Double-Take. Produkty Double-Take představují spolehlivé replikační a zálohovací systémy zajišťující obnovu dat i aplikací – tj. kompletní funkcionality serverů i v případě kompletního výpadku datacentra nebo dokonce jeho zničení. Díky ucelenému portfoliu jsou nástroje rodiny Double-Take vhodné do jakékoliv infrastruktury. Zároveň je možné nabízet ochranu dat zákazníkům i formou služby pomocí programu SPLA (Service Provider License Agreement) a tím je ušetřit jednorázových velkých investic – zákazník platí provozní měsíční poplatek a veškeré zajištění vysoké dostupnosti mu smluvně garantuje poskytovatel.

**Jak fungují nástroje Double-Take?**

I když Double-Take dnes nabízí celou řadu specifických nástrojů pro různá prostředí i nasazení, obecný princip jejich fungování používá většinou stejnou základní techniku pro ochranu dat. Jejím nejvýznamnějším stavebním kamenem je patentovaná technologie STAR (Sequential Transfer Asynchronous Replication). Na serverech jsou sledována data všech kritických služeb (případně celých systémů) a změny v nich jsou na úrovni bytů

neustále přenášeny přes síť na záložní servery, které se mohou nacházet v naprosto odlišné - sekundární lokalitě. Rovnocenná kopie všech dat se tak nachází na bezpečném odděleném místě a slouží jako záloha. Navíc jsou v případě výpadku primárních systémů v řádu sekund nastartovány služby na záložních serverech, které použijí aktuální kopii dat a převezmou identitu primárních systémů. Klienti využívající výše zmíněných služeb tak nezaznamenají žádný výpadek, nejsou nuceni přerušovat práci, ani přestavovat své aplikace na alternativní systémy.



Základní schéma replikace dat nástroji Double-Take

Různé nástroje Double-Take používají různě modifikovaného základního principu replikace v kombinaci s dalšími nástroji a službami. Existují čtyři základní skupiny softwaru Double-Take, z nichž se pro účely tohoto článku zaměříme zejména na dvě. Jedná se o skupiny produktů Double-Take Availability a Double-Take Backup. Další skupinou je pak Double-Take Move, nástroje určené pro živé migrace systémů (operační systém, aplikace a data) mezi různými fyzickými i virtuálními platformami, a Double-Take Flex, řešení pro centrální ukládání, zálohování a správu datových úložišť serverů a klientských stanic připojených k systémům pomocí iSCSI protokolu.

Základní rozdíl mezi dvěma skupinami nástrojů Double-Take určenými primárně pro řešení vysoké dostupnosti a Disaster Recovery přináší následující tabulka:

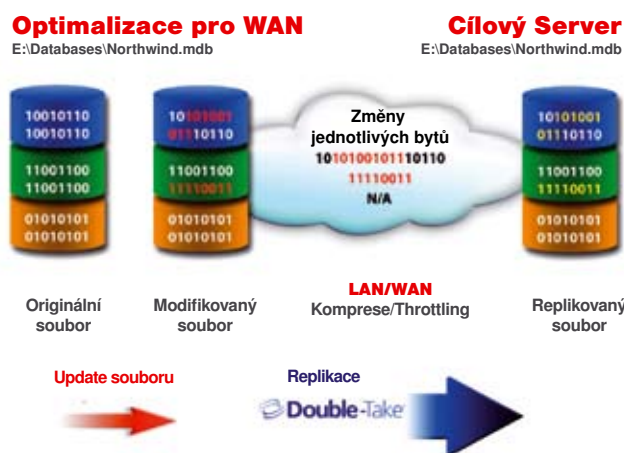
Nástroje	RTO	RPO	HA	DR
Double-Take Availability (fyzické i virtuální systémy)	5 min	~0	ano	ano
Double-Take Backup (fyzické i virtuální systémy)	1-2 hod	~0		ano

Rozdíly mezi nástroji Double-Take Availability a Double-Take Backup

Hlavním rozdílem je fakt, že nástroje skupiny Availability přináší online řešení s časem výpadku (RTO) v řádech sekund, maximálně minut, zatímco nástroje skupiny Backup v řádech desítek minut či hodin. Hlavním důvodem, zjednodušeně řečeno, je skutečnost, že nástroje Availability replikují data mezi dvěma běžícími systémy, zatímco nástroje Backup vytvářejí neustále online image (obraz celého systému) a v případě výpadku je z tohoto obrazu zapotřebí daný server obnovit. Náklady na nástroje Availability jsou pak vyšší (výkon, kapacita, licence OS i aplikací) a na nástroje Backup nižší (ušetříte zejména na výkonu a licencích). Běžnou praxí pak je, že u zákazníků jsou kritické servery, kde musí být výpadek eliminován na minimum, chráněny produkty Availability a méně kritické servery, kde je možné tolerovat např. hodinový výpadek, chráněny nástroji Backup.

## Nástroje Double-Take Availability

Nástroje Double-Take Availability umí chránit libovolné fyzické i virtuální servery či jejich kombinace s různými verzemi operačních systémů Microsoft Windows – včetně podpory pro geografické Microsoft Clusters - a linux. Z pohledu ochrany těchto operačních systémů a na nich běžících aplikací i dat (tj. musí být použita licence pro patřičný operační systém) jsou podporovány libovolně fyzické a virtualizované platformy (VMware, Hyper-V, Citrix XEN atd.). Zároveň existují dvě specifické verze pro virtualizační řešení VMware ESX a Microsoft Hyper-V, které se instalují na hostitelské systémy (hypervisor) a umí chránit virtuální stroje na úrovni obrazu jejich virtuálních disků, tj. zcela bez ohledu na uvnitř běžící operační systém, aplikace i data. Typy licencí Double-Take Availability se v tomto případě liší podle verze operačního systému či hypervisoru. Princip fungování je postavený na běžících zdrojových a cílových serverech a online replikaci dat. V případě výpadku primárního systému dochází k okamžitému startu jeho záložní kopie (ať už služeb na fyzickém serveru či celého obrazu na virtualizovaném řešení) a aplikace i data jsou tak během sekund opět dostupná klientům pod původní identitou. Neboť dochází k přenosu pouze změněných bytů, jsou redukovány požadavky na výkon, kapacitu i přenosové pásmo. Princip replikace přináší následující obrázek:



Replikace dat nástroji Double-Take Availability

## Nástroje Double-Take Backup

Nástroje Double-Take Backup také replikují neustále online veškerá změněná data. Na rozdíl od produktů z rodiny Availability je však neukládají na běžící cílový server, ale do obrazu konkrétního chráněného serveru, který spravuje tzv. „repository“ systém. Ten může online ukládat desítky produkčních serverů a zajišťovat tak, aby byla vždy k dispozici jejich aktuální online záloha. Kromě změněných dat jsou ukládány i systémové stavy (snapshots)



Replikace dat a principy obnovy nástroje Double-Take Backup

Produkty Double-Take Backup tak minimalizují náklady spojené se zálohováním a obnovou systému pomocí dokonalé zálohy a ochrany produkčních serverů a šetří čas i práci při obnově jejich funkcionality. Umožní zároveň ušetřit náklady na zálohovací software (zálohovací klient pro ukládání dat na pásky stačí na jediném – repository systému) a pomocí speciální funkcionality „Cargo“ umí řešit hierarchickou archivaci dat (přesouvání velkých a dlouho nepoužívaných souborů do archivu na záložní straně).

- Dvě kopie produkčních dat – ochrana proti zničení diskového úložiště
- Splnění legislativních požadavků (např. Sarbanes-Oxley Act, Basel II apod.)
- Garance vysoké úrovně SLA (Service Level Agreement)
- Možnost centrálního zálohování dat z jediného místa
- Podpora pro systémy Windows, linux, VMware, Hyper-V a další

Více informací naleznete na: <http://www.doubletake.cz/>

## Hlavní výhody nástrojů Double-Take

- Jednoduchá integrace vysoké dostupnosti aplikací i dat v libovolném prostředí
- Podpora pro Disaster Recovery díky podpoře ochrany dat ve více lokalitách
- Možnost jistit větší počet serverů jediným záložním systémem (N:1)



**Ing. Milan Flutka**

obchodní ředitel / Kancelářské stroje  
obchodní partner K-net  
[milan.flutka@kancelarskestroje.cz](mailto:milan.flutka@kancelarskestroje.cz)

### Rejstřík

**Recovery Time Objective (RTO)** je množství času potřebné pro obnovu 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.

**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).

### Technická příloha časopisu LOGIN 1/2010, ročník 5.

Vydala společnost K-net  
Uzávěrka čísla: 31. 3. 2010  
Připravili: Věra Staňková, Petr Nepustil,  
Milan Flutka, Tomáš Knettig, Tomáš Kiedroň  
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](mailto:info@k-net.cz), [www.k-net.cz](http://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](mailto:net@solidea.cz), [www.solidea.cz](http://www.solidea.cz)

