



ZADÁNÍ BAKALÁ SKÉ PRÁCE

Název:	Možnosti firemního zálohování s využitím cloud
Student:	Ond ej Záruba
Vedoucí:	Ing. Pavel Náplava
Studijní program:	Informatika
Studijní obor:	Informa ní systémy a management
Katedra:	Katedra softwarového inženýrství
Platnost zadání:	do konce letního semestru 2015/16

Pokyny pro vypracování

Analyzujte a vyhodno te možnosti využití cloudových technologií pro ú ely zálohování firemních dat. Zam te se primárn na komer ní poskytovatele ve ejných cloud a postupujte následujícím zp sobem:

1. Analyzujte zp soby zálohování a nástroje pro zálohování dat ve firemním prost edí.
2. Analyzujte nabídku poskytovatel cloudového zálohování a prove te srovnání nabídky (ší ka služeb, dostupnost, ceny).
3. Vytvo te obecné modely zálohování dat, které r zným zp sobem kombinují cloudy a on-premise ešení.
4. Vytvo te zobecn ného pr vodce, který pom že vybrat vhodné využití cloud pro ú ely zálohování firemních dat. Pr vodce bude zahrnovat jak technický, tak i ekonomicko-manažerský pohled na problematiku.

Seznam odborné literatury

Dodá vedoucí práce.

L.S.

Ing. Michal Valenta, Ph.D.
vedoucí katedry

prof. Ing. Pavel Tvrdík, CSc.
d kan

V Praze dne 22. ledna 2015

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
KATEDRA SOFTWAREVÉHO INŽENÝRSTVÍ



Bakalářská práce

Možnosti firemního zálohování s využitím cloudů

Ondřej Záruba

Vedoucí práce: Ing. Pavel Náplava

11. května 2015

Poděkování

Rád bych poděkoval vedoucímu mé bakalářské práce Ing. Pavlu Náplavovi za podporu, velkou trpělivost a podnětné nápady. Obrovské poděkování patří také rodině za jejich podporu během mého studia. Neměli to se mnou jednoduché.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů, zejména skutečnost, že České vysoké učení technické v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona.

V Praze dne 11. května 2015

.....

České vysoké učení technické v Praze
Fakulta informačních technologií

© 2015 Ondřej Záruba. Všechna práva vyhrazena.

Tato práce vznikla jako školní dílo na Českém vysokém učení technickém v Praze, Fakultě informačních technologií. Práce je chráněna právními předpisy a mezinárodními úmluvami o právu autorském a právech souvisejících s právem autorským. K jejímu užití, s výjimkou bezúplatných zákonných licencí, je nezbytný souhlas autora.

Odkaz na tuto práci

Záruba, Ondřej. *Možnosti firemního zálohování s využitím cloudů*. Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2015.

Abstrakt

Tato práce se zabývá praktickými i teoretickými otázkami z oblasti zálohování a cloud computingu s ohledem na využití ve firemním prostředí. Cílem práce je vytvoření modelů zálohování a vytvoření „průvodce“, který pomůže zejména netechnický uživatelům provést rozhodnutí, jaký model je pro ně nejvhodnější. Úvodní kapitoly slouží jako teoretický základ pro pochopení dané problematiky. V další části jsou popsány poskytovatelé cloudového zálohování, modely zálohování a samotný průvodce.

Klíčová slova zálohování, cloud computing, poskytovatelé zálohování, modely zálohování, obnova dat, ochrana dat

Abstract

This thesis deals with teoretical and practical issues in the backup and cloud in regards of business backup. The aim is to create backup solutions and create backup "wizard" that helps especially non-technical users to decide which solution is best for them. Introductory chapters serve as a theoretical basis for understanding the issue. The next section describes the providers of cloud-based backup, backup models and wizard itself.

Keywords backup, cloud computing, backup providers, backup solutions, data recovery, data protection

Obsah

Úvod	1
1 Zálohování dat	3
1.1 Definice pojmu zálohování	4
1.2 Základní typy zálohování	4
1.3 Zálohy podle místa uložení	8
1.4 Zálohovací média	9
1.5 Hrozby pro data	13
1.6 Pravidla a osvědčené praktiky zálohování	15
1.7 Nástroje pro on-premise zálohování	18
1.8 Shrnutí	22
2 Cloud computing	23
2.1 Definice cloud computingu	23
2.2 Služby nabízené v cloudu (servisní model)	25
2.3 Modely provozu cloudových služeb	27
2.4 Shrnutí	30
3 Analýza poskytovatelů cloudového zálohování	31
3.1 Robustní řešení	31
3.2 Online zálohování	35
4 Srovnání on-premise a cloudového zálohování	37
4.1 Náklady	37
4.2 Výkon a dostupnost	38
4.3 Shrnutí	38
5 Plán pro obnovu	41
5.1 Tvorba plánu pro obnovu	41
5.2 Ukázka využití na konkrétním příkladě	46

6	Modely zálohování	49
6.1	Použití vlastního existujícího hardware	49
6.2	Zakoupení nového zálohovacího serveru	50
6.3	Hot-swapping	50
6.4	Replikace na vlastní pobočku	51
6.5	Replikace na obecný cloud	51
6.6	Replikace na speciální zálohovací cloud	52
6.7	Replikace z cloudu zpět on-premise	52
6.8	Archivační model	53
6.9	Shrnutí	53
7	Průvodce modely zálohování	55
7.1	Vývoj průvodce	55
7.2	Návod k použití	56
7.3	Rozšíření programu	61
	Závěr	63
	Použité zdroje	65
A	Seznam použitých zkratk	71
B	Srovnání Veeam Availability Suite a Acronis Backup Advanced	73
B.1	Výkon	73
B.2	Použitelnost a funkce	75
B.3	Cloudové zálohování	76
B.4	Cena	76
B.5	Shrnutí	77
C	Ukázka využití průvodce na praktickém příkladě	79
C.1	Současná infrastruktura	79
C.2	Aktuální stav společnosti	79
C.3	Stanovení cílů	80
C.4	Vyhodnocení	83
C.5	Shrnutí	84
D	Obsah příloženého CD	85

Seznam obrázků

1.1	Úplná záloha	5
1.2	Inkrementální záloha	6
1.3	Rozdílová záloha	7
1.4	Zrcadlová záloha	8
1.5	Schéma disk-to-disk-to-tape	16
1.6	Zálohovací software společnosti Ahsay	21
1.7	Zálohování pomocí Vembu BDR	22
3.1	Metoda 3-2-1 pomocí Veeam Availability Suite	33
3.2	Metoda 3-2-1 pomocí Acronis Backup Advanced	34
3.3	Loga produktů Crashplan Pro a Backblaze	36
4.1	Srovnání cen poskytovatelů cloudu za petabajt prostoru	37
7.1	Úvodní obrazovka průvodce	57
7.2	První část průvodce	57
7.3	Doplňující otázky k serverům	58
7.4	Druhá část průvodce	58
7.5	Třetí část průvodce	59
7.6	Doplňující otázky k dostupnosti	60
7.7	Nevyplněný kalkulátor ztrát	60
7.8	Řešení průvodce při defaultních hodnotách	61
B.1	Srovnání rychlostí zálohování a obnovy	74
B.2	Využití prostoru pro zálohu 200 GB dat	74
B.3	Hodnoty RTO testovaných řešení	75
C.1	Současná infrastruktura společnosti Nutrillex	80
C.2	Doplňující otázky k serverům Nutrillexu	80
C.3	Aktuální stav společnosti Nutrillex	81
C.4	Otázky k dostupnosti systému společnosti Nutrillex	81

C.5	Kalkulátor ztrát aplikovaný na výpadek u Nutrillexu	82
C.6	Stanovení cílů společnosti Nutrillex	82
C.7	Výsledné řešení část první	83
C.8	Výsledné řešení část druhá	83
C.9	Výsledné řešení část třetí	84

Seznam tabulek

1.1	Základní srovnání typů záloh	5
1.2	Ceník AhsayOBM	20
B.1	Ceník Acronis Backup Advanced	76
B.2	Ceník Veeam Availability Suite v8	76

Úvod

Zálohování dat je kriticky důležitá součást každého businessu pracujícího s daty. Bohužel je velmi často podceňováno a jeho důležitost si mnoho společností uvědomí, až když je příliš pozdě. Proč tomu tak je? Panuje totiž jakýsi přežitek, že zálohování je časově i finančně nákladný proces s minimální návratností. Katastrofy se navíc týkají pouze „ostatních lidí“. Čtenáře této práce vyvedu z obou těchto omylů.

Cílem bakalářské práce je vytvoření modelů zálohování, které na základě dostupnosti, finančních možností a dalších faktorů budou nejlépe vyhovovat dané společnosti. Na těchto poznacích je pak postaven interaktivní „průvodce“, který po zodpovězení sady otázek navrhne nejvhodnější model. Tento průvodce tak pomůže zejména netechnickým uživatelům vytvořit si představu o možném řešení.

Struktura práce je navržena tak, aby při postupném čtení i laik dokázal pochopit danou problematiku bez dalšího studia. První kapitoly práce slouží především jako teoretický úvod do oblasti zálohování a cloud computingu. Jde zejména o definování základních pojmů, typů zálohování, seznámení se zálohovacími médii a nástroji. V další kapitole je osvětlen pojem cloud computing, jeho vlastnosti, servisní modely a modely nasazení. Na těchto znalostech pak staví třetí kapitola, týkající se poskytovatelů cloudového zálohování. V této kapitole jsem analyzoval nabídku cloudového a online zálohování. Před praktickou částí práce jsem ještě krátce srovnal cloudového a on-premise zálohování.

Poznatky a informace získané v úvodních kapitolách pak dále rozvíjí praktická část o plánech pro obnovu, ve které popisují moderní přístup k ochraně dat. Součástí těchto plánů je také vytvoření optimálního modelu zálohování. Tyto modely pak detailněji charakterizují v navazující kapitole. Finálním produktem celé práce je pak již zmíněný průvodce, který na základě sady otázek vyhodnotí optimální model. Průvodce je naprogramovaný v jazyce Java.

Motivací ke zpracování tématu mi byla zejména atraktivnost a aktuálnost problematiky, neboť jak cloud computing, tak i zálohování jsou kvůli neustále

ÚVOD

rostoucím objemům dat stále více diskutovanými oblastmi. Navíc průvodce tvorbou modelů zálohování se na internetu nenachází.

Zálohování dat

První kapitola práce je zaměřena na teoretický úvod do problematiky zálohování. Cílem kapitoly je definovat pojem zálohování, poukázat na nebezpečí, která hrozí datům a seznámit se s základními typy zálohování a zálohovacími médii. Dále se čtenář seznámí s tzv. *best practises* v oblasti zálohování. Na konci kapitoly nalezne čtenář zmínku o šifrování dat a příklady zálohovacích nástrojů.

Zálohování dat by mělo být jednou z priorit každé společnosti, která při své práci pracuje s důležitými daty. Hardware a software není bezchybný a člověk není neomylný. Lze téměř s jistotou říci, že každého, kdo nezálahuje, potkala a nebo potká ztráta důležitých dat. Přestože si většina společností uvědomuje důležitost zálohování, implementace často pokulhává. Podle společnosti IDC¹, „v roce 2013 vyžadovalo zhruba 40% dat nějakou formu ochrany, méně než 20% dat však tuto ochranu mělo.“[2] Pojďme se nyní podívat na odhady o budoucím vývoji dat od této společnosti, které s největší pravděpodobností ovlivní i trh a trendy zálohování.

„Od roku 2013 do 2022 vzroste celkový objem dat desetinásobně - z 4,4 bilionů² na 44 bilionů. Dojde k více než zdvojnásobení objemu každé dva roky.“[2]

Dle IDC byl dále v roce 2013 podíl užitečných dat 22%, velmi užitečných pak bylo zhruba 5%. Do roku 2020 se očekává nárůst na 37% užitečných respektive 10% velmi užitečných dat.[2]

Na základě těchto předpovědí můžeme předpokládat, že kvalitní a efektivní zálohování bude v budoucnu ještě aktuálnější problematika než dnes, neboť bude zapotřebí chránit tato užitečná data. Otázkou však zůstává, zda začnou

¹„IDC je jedna z nejvýznamnějších světových analytických a poradenských společností. Poskytuje průzkumy a analýzy trhu, předpovídá vývoj a trendy v oblasti informačních a komunikačních technologií (ICT) a pořádá odborné konference.“[1]

²Milión miliónů

společnosti více dbát na ochranu svých dat. Na další důvody, proč by zálohování a ochrana dat neměla být brána na lehkou váhu, se podíváme v sekci 1.5.

1.1 Definice pojmu zálohování

Pravděpodobně každý má představu o tom, co znamená zálohování dat. Často však bývá zálohování zaměňováno s pojmem archivace. Podíváme se nyní na definice těchto pojmů, abychom měli jasno, co který pojem znamená.

Zálohování je proces kopírování dat na jiné médium, aby v případě potřeby mohla být tato data obnovena.[3]

Archivace je přesun málo využívaných dat na jiné médium za účelem dlouhodobého uchování.[4]

Zálohování zpravidla probíhá nad daty, se kterými momentálně pracujeme a potřebujeme je zabezpečit před ztrátou. Dochází k vytvoření kopie.

Archivovaná data mají většinou už finální podobu a přesouváme je obvykle na média s menšími náklady na provoz a delší životností. Nedochozí k vytvoření kopie.

Se zálohováním souvisí také **obnova** dat, to je proces kopírování dat ze zálohovacího média na pevný disk, za účelem obnovení dat do původní podoby.[5]

Hlavním cílem zálohování je rychlé obnovení dat a kvalitní ochrana, neboť každá minuta výpadku stojí peníze. Archivace si pak naopak klade za cíl možnost rychlého vyhledávání mezi daty podle daných parametrů, seznam změn, kdy a kdo tyto změny provedl atd.[6]

Ve firemním prostředí pak zálohování obvykle nabírá širšího formátu a bavíme se potom o tzv. **plánu pro obnovu**³. Přesněji vyjádřeno, jedná se o „předem připravený scénář, který vede k obnově infrastruktury po nastalé havárii – ať již fatální selhání hardware nebo software způsobené lidským faktorem, živelnou katastrofou nebo jiným selháním.“[7]

1.2 Základní typy zálohování

Pokud se zeptáte někoho, kdo nemá se zálohováním zkušenosti, co znamená záloha, pravděpodobně by vám odpověděl, že se jedná o kopii dat z počítače na jiné médium. Ačkoliv jde i takto zálohování nastavit, ve firemním prostředí se většinou používají i pokročilejší metody.

Jako hlavní podklady pro tuto sekci jsem využil stránky [8][9][10]. Pro rychlé shrnutí a porovnání lze nahlédnout do tabulky 1.1.

³Anglicky DRP - Disaster Recovery Plan

Typ zálohy	Zálohovaná data	Rychlost zálohy	Rychlost obnovy	Náročnost na prostor
Úplná	Všechna	Nejpomalejší	Rychlá	Velká
Inkrementální	Pouze nová/změněná	Rychlá	Nejpomalejší	Nejmenší
Rozdílová	Vše od poslední úplné	Střední	Rychlá	Střední
Zrcadlová	Pouze nová/změněná	Nejrychlejší	Nejrychlejší	Největší

Tabulka 1.1: Základní srovnání typů záloh[10]

1.2.1 Úplná (normální) záloha

Úplná záloha je kompletní záloha všech dat. Staví na ní všechny ostatní pokročilejší metody. Bylo by ideální dělat pouze úplné zálohy, neboť bychom měli vždy vše pohromadě v jedné záloze. Velikost úplných záloh a časová náročnost jejich vytvoření to však často neumožňují. Používat jen úplné zálohy se proto hodí, pokud zálohujeme pouze malé objemy dat.

Výhody:

1. Nejrychlejší obnova
2. Vše na jednom místě

Nevýhody:

1. Nejdelší zálohování
2. Zabírá nejvíce místa (pokud máme více úplných záloh viz obrázek 1.1)
3. Bezpečnost (při nelegálním přístupu má hacker či zloděj k dispozici všechna data)



Obrázek 1.1: Úplná záloha[10]

1.2.2 Inkrementální záloha

Inkrementální záloha je mnohem rychlejší než opakované provádění úplných záloh. Začíná provedením úplné zálohy, pak se již provádí zálohy pouze změ-

1. ZÁLOHOVÁNÍ DAT

něných dat od posledního zazálohování viz obrázek 1.2. Názorně, v pondělí provedeme úplnou zálohu, v úterý provedeme inkrementální (zazálohujeme pouze to, co se změnilo od pondělí). Ve středu provedeme další inkrementální, tzn. zazálohujeme změny od úterka atd.

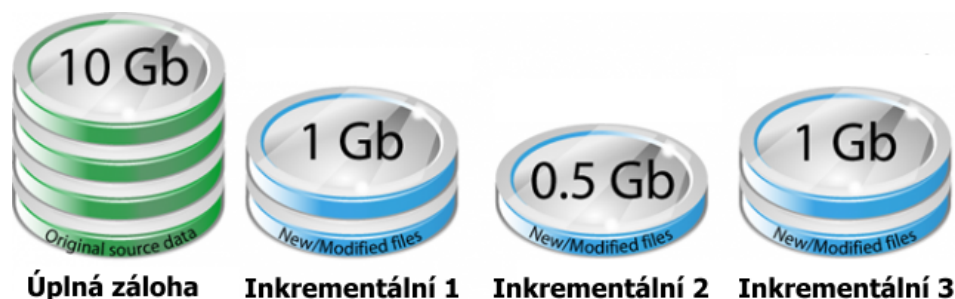
Tento způsob zálohování je velmi rychlý a je nejméně náročný na úložný prostor. Daní za to je složitá obnova. Pokud bychom ve čtvrtek chtěli obnovit, musíme obnovit pondělní úplnou zálohu, poté úterní inkrementální a nakonec středeční inkrementální zálohu (všechny inkrementální zálohy).

Výhody:

1. Rychlé zálohování
2. Nejnižší spotřeba úložného prostoru

Nevýhody:

1. Pomalá obnova



Obrázek 1.2: Inkrementální záloha[10]

1.2.3 Rozdílová záloha

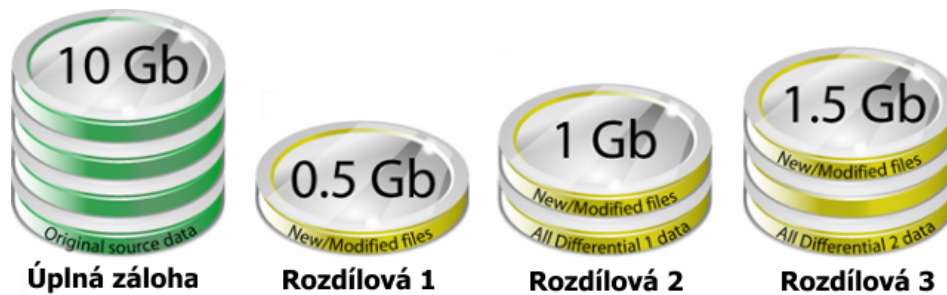
Rozdílová záloha provádí zálohování rozdílu od poslední úplné zálohy, odtud název rozdílová, viz obrázek 1.3. Pokud v pondělí provedeme úplnou a v úterý a ve středu rozdílové zálohy, tak ve čtvrtek potřebujeme k obnovení pouze pondělní úplnou a středeční rozdílovou zálohu. Rozdílová záloha je dobrým řešením, pokud záloh neuchovááme velké množství. V opačném případě mohou rozdílové zálohy snadno zabírat více místa, než nová úplná záloha.

Výhody:

1. Rychlejší obnova než u inkrementální metody
2. Rychlejší zálohování než při úplné záloze
3. Pokud neuchovááme mnoho záloh, není náročné na úložný prostor jako úplné zálohy

Nevýhody:

1. Pomalejší obnova než u plné zálohy
2. Pomalejší záloha než u inkrementální zálohy
3. Náročnější na úložný prostor než inkrementální záloha



Obrázek 1.3: Rozdílová záloha[10]

1.2.4 Zrcadlová záloha

Zrcadlová záloha není záloha v pravém slova smyslu. Je to přímá kopie dat v daném okamžiku, tzv. zrcadlo. Toho je zpravidla docíleno zapojením disků v režimu RAID 1, viz obrázek 1.4 nebo RAID 5. Pokud tedy nějaký soubor smažeme, smaže se i v zrcadle. Chrání proti selhání disků, neochrání však před útoky hackerů, virů apod. Využívá se zejména v případě, kdy potřebuje nepřetržitý přístup k datům.

Výhody:

1. Umožňuje okamžitý přístup k datům v případě selhání jedno z disků
2. Neobsahuje staré a nepotřebné soubory

Nevýhody:

1. Kopírování do dvou disků snižuje výkon
2. Nechrání před viry, chybným smazáním, poškozením dat, ...
3. Kapacita je poloviční, neboť na dvou discích máme stejná data

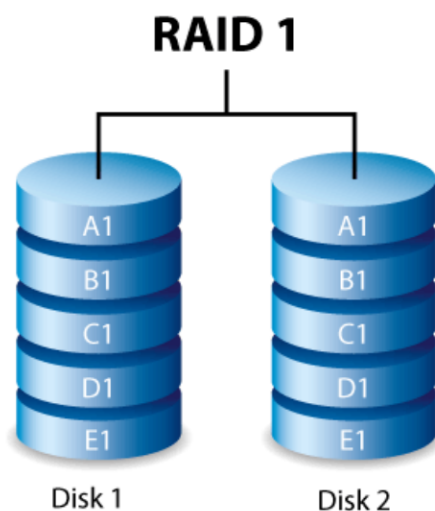
1.2.5 Systémový obraz

Mezi zálohou pomocí systémového obrazu a výše zmíněnými zálohami je dost podstatný rozdíl. Vzhledem k tomu, že je to velmi moderní způsob zálohování počítačů, jak u běžných uživatelů, tak ve firmách, považuji za důležité tuto metodu zmínit.

V čem se tedy liší od ostatních záloh? Pokud máme například úplnou zálohu dokumentů a fotografií, můžeme při selhání disku tato data opět nakopírovat na nový. Operační systém a programy však musíme nainstalovat znovu. Přijdeme také o různá nastavení systému, registrů apod. To však u obnovy pomocí systémového obrazu neplatí, systém se nám totiž obnoví do stavu, ve kterém byl, když jsme obraz vytvořili, včetně všech programů a nastavení atd. Ostatní zálohy jsou tedy souborové, tato je systémová.

Výhody:

1. Kompletní obnovení systému během několika minut
2. Ideální řešení v případě selhání disku



Obrázek 1.4: Zrcadlová záloha[11]

3. Možnost virtualizovat obraz na cloudu

Nevýhody:

1. Na PC s jiným HW může dojít ke komplikacím při obnově
2. Pokud byl v době tvorby obrazu počítač zavirovaný, je zavirovaný i systémový obraz

1.3 Zálohy podle místa uložení

Zálohy se nedělí pouze podle toho, jak probíhá samotné zálohování. Důležitou roli hraje také místo, kde zálohy uchováváme. Metoda 3-2-1 (viz 1.6.1) dokonce požaduje jednu zálohu na geograficky vzdáleném místě.

V následující sekci rozdělíme zálohy podle geografické polohy a dalších parametrů. Seznámíme se také s výhodami a nevýhodami konkrétních způsobů.

1.3.1 Lokální záloha

Lokální záloha, jak pravděpodobně název napovídá, je uložení zálohy na stejném místě (ve stejné budově), jako se nachází originální data. Ve většině případů je zálohovací médium přímo připojené k počítači nebo jsou obě zařízení ve stejné lokální síti.

Lokální zálohy jsou také často nazývané jako **onsite** nebo **on-premise** zálohy.

Výhody:

1. Chrání před selháním HW, chybným smazáním, ...

2. Rychlé zálohování i obnova (nejsme omezeni rychlostí připojení k internetu)
3. Neplatíme za přenos dat
4. Úplná kontrola nad daty (není třeba důvěřovat třetí straně)

Nevýhody:

1. Nechrání před přírodními katastrofami, krádeží v budově apod.

1.3.2 Offsite záloha

Pokud zálohovací médium přepravíme do jiné lokality, stává se ze zálohy offsite záloha. Je samozřejmě důležité, aby záloha byla dostatečně vzdálená a chránila tak nejen proti požárům, ale také povodním, hurikánům apod.

V minulosti bývala běžná praktika, kdy například administrátor bral každý den s sebou domů zálohu klíčových dat. Při dnešním objemu dat to však není příliš reálné. Navíc získání přístupu k takové záloze může trvat až několik hodin, což také není příliš příznivé pro spoustu businessů.

Z těchto důvodů valná většina společností volí řešení v podobě tzv. **online zálohy**. Jak název napovídá, jedná se o zálohu, která je vždy dostupná prostřednictvím internetu. Dalším benefitem oproti klasické offsite záloze je funkčnost bez lidského zásahu, není zapotřebí nic zapojovat.

Výhody online offsite záloh:

1. Ochrana před přírodními katastrofami, krádeží
2. Data jsou „rozprostřena“ po data centru, proto je riziko ztráty dat kvůli selhání HW minimální
3. Pro přístup není zapotřebí nic zapojovat
4. Dostupnost více než 99 %

Nevýhody:

1. Zpravidla dražší než lokální zálohy
2. Rychlost i dostupnost závislá na připojení k internetu

1.4 Zálohovací média

V této sekci se seznámíme s nejčastěji používanými zálohovacími médii, jejich výhodami a nevýhodami, cenou a kapacitou. Podíváme se také na nejmodernější technologie, které pravděpodobně zamíchají momentálním rozložením na poli datových médií.

1.4.1 Mechanický pevný disk

Velká část dat je v dnešní době uložena na pevných discích. Je to nejlevnější médium s náhodným přístupem. Oproti pásce také nevyžaduje speciální podmínky pro uchování a při běžném provozu mají mechanické pevné disky

životnost mezi 3-7 lety. Navíc cena za GB dat každý rokem klesá a dříve výrazný rozdíl mezi cenou disku a pásky se postupně vytrácí.

Kapacita: až 16 TB (běžně dostupné disky do 3 TB)

Cena za GB: \$0,03[12]

Výhody:

1. Vhodná volba pro zálohování velkého množství dat
2. Nejlevnější řešení s náhodným přístupem k datům
3. Při správném zacházení vcelku spolehlivé

Nevýhody:

1. Náchylné na poškození (pád, otřesy)

1.4.2 Solid State Drive (SSD)

SSD disky vypadají na první pohled podobně jako klasické mechanické pevné disky, nicméně fungují naprosto odlišně. Neobsahují žádné rotující plotny ani pohyblivé části. SSD disky pracují na podobném principu jako všem dobře známé USB flash disky. Moderní disky většinou využívají NAND flash paměť, která uchovává data i po ukončení napájení.

Životnost disků je omezena počtem zápisů. Současné 240 GB SSD disky však zvládnou zapsat více než 1PB dat.[13]

V březnu 2015 byla oznámena nová technologie 3D NAND. „Díky 3D NAND čipům, se podle Briana Shirleyho ze společnosti Micron již brzy můžeme těšit na SSD disky s kapacitou přes 10 TB. U high-endových tabletů nebo lehkých laptopů bychom se mohli dočkat SSD disků s kapacitou přes 3,5 TB.

Nové flashové čipy se velmi liší od standardních NAND flashových čipů, u nichž jsou jednotlivé články k ukládání dat skládány vedle sebe. U 3D NAND technologie jsou články naopak skládány vertikálně na sebe, díky čemuž se snižuje vzdálenost, na kterou s sebou články musejí komunikovat a data se tak přenáší rychleji.“[14]

Klíčové vlastnosti 3D NAND technologie:

- **Velká kapacita:** ve stejném prostoru bude více paměťových buněk.
- **Snížená cena na GB:** „první generace 3D NAND je navrhována tak, aby nabídla vyšší nákladovou efektivitu než dvojrozměrné NAND.
- **Rychlost:** velká pásmová šířka čtení/zápisu, I/O rychlosti a náhodného čtení.
- **Ekologická šetrnost:** nové režimy spánku umožňují provoz v nízko-energetickém modu, kdy se odpojí přísun energie neaktivním NAND či-

pům (i když ostatní zůstanou aktivní). To výrazně sníží spotřebu energie v pohotovostním režimu.

- **Inteligentní technologie:** inovativní funkce zlepšují latentnost a zvyšují trvanlivost oproti předchozím generacím. Rovněž usnadňují systémovou integraci.“[14]

Kapacita: až 4 TB (běžně dostupné disky do 1 TB)

Cena za GB: \$0,47[15]

Výhody:

1. Vysoký výkon - čtení, zápis, přístup k datům
2. Spolehlivější než mechanické disky, není tak náchylné na poškození
3. Nová technologie 3D NAND

Nevýhody:

1. Momentálně stále výrazně dražší než mechanické disky
2. Životnost omezená počtem zápisů do buněk. (riziko pro extrémně vytěžované servery)

Můžeme tedy očekávat, pokud se technologie 3D NAND osvědčí, že SSD disky s touto technologií začnou vytlačovat standardní mechanické pevné disky, jak pro běžné použití, tak pro zálohování.

1.4.3 Magnetická páska

Magnetická páska je zpravidla uložena v kazetách. Oproti mechanickému disku má tu výhodu, že selhání pohonných mechanismů kazety zpravidla nepoškodí samotnou pásku a tu tak lze přemístit do nové kazety. Na druhou stranu, nevýhodou je sekvenční zápis a čtení. To má za následek delší dobu přístupu k datům a pro zálohy, které je potřeba co nejrychleji obnovit, tak páska není jako médium vhodná.

Síla pásky spočívá v obrovské kapacitě, životnosti a nízké ceně. FujiFilm ve spolupráci s IBM loni představil pásky s kapacitou 154 TB. Ty se začnou prodávat v druhé polovině roku 2015.[16] Tím však vývoj pásky nekončí a během následujících let se očekává nárůst až na kapacitu 220 TB/páska.[17] Při vhodných podmínkách má navíc páska životnost i několik desítek let a cena za GB je stále nižší, než u pevných disků. Páska je také mnohem snadněji přepravitelná než mechanické pevné disky, neboť není náchylná na poškození vibracemi, a je tak možné poštou snadno přemístit pásky z místa na místo.

Nevýhodou je již zmíněná přístupová doba, která také omezuje potenciálně vysokou rychlost čtení, jenž má páska vyšší než mechanický disk. Na tuto vysokou rychlost však bývá často problém se dostat a hlavně ji udržet, pokud požadovaná data nejsou uložena sekvenčně za sebou. Kvůli tomu je páska ve většině případů až několika násobně pomalejší při obnově dat než mechanické disky. Další nevýhodou jsou požadavky pro uchování. Pásky je nutné skladovat

v prostředí se stálou teplotou, vlhkostí a co nejmenší prašností, neboť snítka prachu mají negativní dopad na životnost povrchu pásky. Dalším faktorem zkracujícím výdrž pásek je frekvence jejich použití. Velká zátěž, časté roztáčení a opětovné zastavování, opotřebovává pásku a její životnost se výrazně zmenšuje.

Magnetická páska stále má své místo mezi datovými médii. Díky pokračujícímu vývoji navíc nelze očekávat její konec v blízké budoucnosti, přestože do výkonných systému, kde je požadována minimální odezva a maximální výkon, se příliš nehodí. Pro účely archivace či dlouhodobého zálohování je to stále nejvhodnější médium, díky své nízké ceně, vysoké kapacitě, dlouhé životnosti a minimálním nákladům na provoz.[18]

Kapacita: až 154 TB

Cena za GB: méně než \$0,01[19]

Výhody:

1. Vysoká kapacita
2. Životnost za ideálních podmínek
3. Mobilita
4. Maximální rychlost čtení/zápisu
5. Nízká cena za GB a provozní náklady

Nevýhody:

1. Přístupová doba
2. Výrazně se zkracující životnost při dlouhodobé vysoké zátěži
3. Podmínky pro uchování

1.4.4 Optická média

Není to tak dávno, co přišla revoluce v podobě CD a DVD disků, které nahradily diskety jako médium pro přenos a uchování dat. Netrvalo však dlouho a objevila se technologie USB flash disků, která začala optická média rychle vytlačovat a zabránila i Blu-Ray diskům se výrazněji prosadit na poli datových médií.

Mají tedy optická média ještě své využití? Standardní CD a DVD disky již minimální, neboť oproti flash diskům mají několik nevýhod. Data je nutné vypalovat a při tomto procesu nezřídka nastávají chyby a pokud disk není přepisovatelný, je nepoužitelný. Dále také náchylnost na mechanické poškození, zejména poškrábání.

Životnost zapsaného disku je zhruba 5 let, což je srovnatelné s mechanickými pevnými disky, stejně tak jako cena za gigabajt dat.

Existují však speciální technologie, díky kterým optická média mají stále budoucnost, například **M-Disc**. Tyto speciální DVD a Blu-Ray disky jsou odolné proti světlu, vlhkosti, změnám teplot a do určité míry i mechanickému

poškození. Největší předností však je životnost těchto disků, která je odhadována až na 1000 let. To činí M-Disky horkým kandidátem pro dlouhodobé zálohování a archivaci.[20]

Kapacita: až 128 GB

Cena za GB: \$0,03⁴

Výhody:

1. Nízká cena
2. Technologie M-Disc

Nevýhody:

1. Kapacita
2. Životnost
3. Náchylnost na poškození

1.5 Hrozby pro data

Abychom byli schopni zvolit správný zálohovací model, je důležité si mimo jiné uvědomit druhy nebezpečí, které našim datům hrozí. Podíváme se teď na nejčastější hrozby a nastíníme možnosti jejich minimalizace.

1.5.1 Selhání média

Každé datové médium může selhat. Pevné disky jsou jednoznačně nejčastěji selhávající komponenta počítačů s podílem 80,9 %[21] ze všech selhání. Postupný nástup SSD disků se ale jeví jako velmi slibný, neboť podle dosavadních statistik po prodeji několika tisíců disků selhaly při běžném použití pouze jednotky disků. SSD disky však stále nejsou dostatečně zaběhnuté a až čas ukáže, zda jsou opravdu dlouhodobě spolehlivé. Nicméně aktuálně zveřejněná technologie 3D NAND představuje revoluci ve flash pamětech a dá se očekávat, že během následujících let bude postupně vytlačovat již 60 let starou technologii pevných disků.

1.5.2 Viry

Viry se mohou nepozorovaně šířit a potom začít poškozovat data. Velké nebezpečí hrozí zejména u rozsáhlých počítačových sítí, kdy se vir může z jednoho PC nepozorovaně rozšířit do celé sítě a napáchat obrovské škody. Boj proto virům stojí ročně miliardy dolarů. Nejlepší prevencí je kvalitní antivirový program, firewall a vyhýbání se rizikovým webovým stránkám. Ochranou pro data je pak offsite záloha nebo záloha na optická média.

⁴zdroj: Amazon.com

1.5.3 Záměrné poškození

Úmyslně poškodit naše data mohou chtít například hackeři. Odstrašujícím případem může být osud společnosti Code Spaces⁵. Společnost běžela na AWS⁶. Hacker získal přístup k datům a pod pohrůzkou jejich vymazání požadoval zaplacení velké sumy peněz. Společnost toto odmítla a hacker tak vymazal téměř všechna data. Sedm let rostoucí společnost tak byla zlikvidována během několika hodin.[22] Jistou hrozbou představují také naštvaní zaměstnanci, kteří mohou úmyslně smazat důležitá data. Ochranou pro oba případy je opět offsite záloha, ideálně i na hodně geograficky vzdálených místech.

1.5.4 Chyba operačního systému

Zaseknutí, pád systému, každému se již některá z těchto chyb stala. Někdy se operační systém dokonce z některých selhání již nevzpamatuje. Proto je důležité rozpracovanou práci ukládat a pravidelně zálohovat. Pro obnovu celého systému je pak vhodné vytvářet systémové obrazy.

1.5.5 Výpadky proudu a elektrické výboje

Zásah objektu bleskem dokáže zničit veškerou elektroniku během okamžiku. Ochranné zdroje mohou zabránit poškození, nicméně jistá záruka to není. Řešením je záloha offsite.

1.5.6 Krádež a ztráta

Ztracená flashka, zapomenutý externí disk, ukradený notebook. Nic z uvedeného nelze vyloučit, a proto je nutné data chránit. Disky s důležitými daty šifrovat, aby nemohlo dojít k zneužití dat a data mít uložená i na jiném médiu, ideálně opět offsite.

1.5.7 Přírodní katastrofy

Je nutné také počítat s přírodními katastrofami, a proto se doporučuje mít alespoň jednu kopii na geograficky jiném místě. Hurikán Sandy v roce 2012 napáchal škody za 65 miliard dolarů. Více než 300 000 společností bylo hurikánem postiženo a bez elektřiny bylo více než 8,5 milionu lidí.[23] Pro společnosti bez záloh a nouzových řešení může mít takováto katastrofa fatální následky.

1.5.8 Lidská chyba

Lidská chyba je jednou z nejčastějších příčin ztráty dat. Omylem smazaný či poškozený soubor není výjimečnou situací. Ochranou nám je v tomto případě jakákoliv záloha.

⁵Společnost provozující hosting zdrojových kódů

⁶Amazon Web Services

Jak můžeme vidět, hrozeb pro naše existuje velké množství. Myslet si tak, že se nám všechny budou navždy vyhýbat je velmi naivní. Z tohoto důvodu je opravdu nutné alespoň klíčová data pravidelně zálohovat.

1.6 Pravidla a osvědčené praktiky zálohování

Po přečtení minulé kapitoly je jasné, že zálohování je nutností pro zajištění provozuschopnosti společnosti po jakékoliv katastrofě. Nyní se podíváme na doporučenou metodiku při zálohování, konkrétně pravidlo 3-2-1. Dále také na důležitost testování provedených záloh a nakonec si osvětlíme význam šifrování v oblasti zálohování.

1.6.1 Pravidlo 3-2-1

Pravidlo 3-2-1 je velmi nadčasové a je odpovědí na dvě důležité otázky v oblasti zálohování: kolik pořídit záloh a kde je uchovat.

- Mějte alespoň **3 kopie dat** (originál + 2 kopie)
- Uložte je na alespoň **2 různá média**
- **Jednu** z kopií mějte na jiném místě (offsite)

Pokud by byla pravděpodobnost selhání média 1:100, ztráta všech tří kopií najednou by znamenala naplnění pravděpodobnosti 1:1000000, což je velmi nepravděpodobné.

Druhý bod bývá v automatizovaném prostředí pro velké objemy dat často problém, neboť počítače i servery využívají pevné disky. V každém případě se alespoň doporučuje nepoužívat stejné disky zakoupené ve stejnou dobu, neboť na výrobní lince může dojít k chybě a vyrobení několika kusů náchylnějších k závadě a tím pádem se rapidně zvyšuje šance selhání, navíc v podobném časovém horizontu.

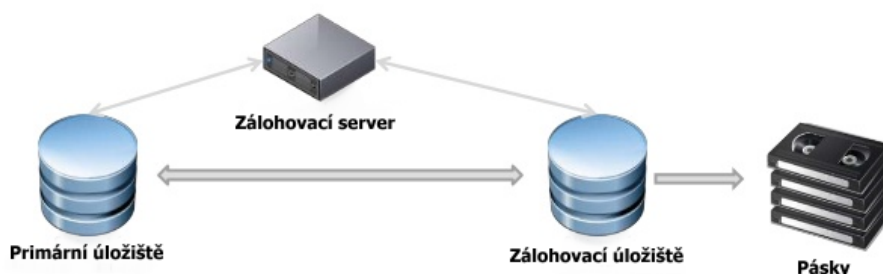
Pokud bychom měli všechna média v jedné místnosti, tak hrozí, že v případě požáru přijdeme o vše, proto je dobré umístit alespoň jednu kopii na vzdálené místo.[24]

Varianty metody 3-2-1:

Disk-to-disk-to-tape(D2D2T)

D2D2T architektura je potomkem dříve hojně využívané D2T (disk-to-tape), tedy zálohování pouze na pásku. Rostoucí nároky na rychlost obnovy a dobu přístupu, společně s klesajícími cenami disků však způsobily, že se tradiční zálohování na pásku dostalo do pozadí.

Páska však nevymizela úplně, pouze do hry vstoupil další disk a vzniklo tak schéma D2D2T. Tedy zálohování z disku na jiný pevný disk a následná replikace na pásku (obrázek 1.5). Tento způsob tak přináší „to nejlepší z obou světů“. Rychlost a flexibilitu disku ve spojení s kapacitou a životností pásky.[25]



Obrázek 1.5: Schéma disk-to-disk-to-tape[26]

Když se však nad schématem zamyslíme, zjistíme, že se v podstatě jedná o D2D (disk-to-disk) + dlouhodobá záloha. Uvedme si příklad, společnost zálohuje data na disk každé dvě hodiny. Každý pátek jsou pak zálohy nahrány na pásku a ta je odeslána pryč jako offsite záloha. Pokud se však něco pokazí při obnově z disků a dojde na obnovení z pásky, nejenže bude minimálně několik hodin trvat doprava, ale také obnovovaná data mohou být až týden stará.

Z těchto ale i dalších důvodů společnosti stále častěji přecházejí na celodiskový model, tzv. D2D2D.

Disk-to-disk-to-disk(D2D2D)

Architektura D2D2D je rozšířením D2D schématu o diskovou offsite zálohu (obrázek 1.6). Ačkoliv je model D2D dnes již běžně rozšířeným, implementace offsite zálohování je (bez ohledu na benefity) stále často podceňována.

Ačkoliv pořízení diskové offsite zálohy stojí peníze, není částka tak vysoká, jak by se na první pohled mohlo zdát. Zásahu na tom má především stále se zdokonalující technologie **deduplikace**. Ta dokáže běžně

zajistit redukci 20:1. Pokud takto zredukovaná data navíc zkomprimujeme, dostáváme se na výrazně nižší požadavky na datový prostor.

Deduplikace a komprese dat navíc posiluje pozici D2D2D ve srovnání s D2D2T, kde jsou data na pásce uložena neefektivně. Navíc architektura D2D2D zbavuje nutnosti starat se o odesílání a uchování pásek. A přestože jsou pásky stále levnějším médiem než disky, měkké náklady na manipulaci, uchování a přepravu (během které se mohou poškodit nebo ztratit) jsou srovnatelné s během efektivního replikačního serveru.[27]

Disk-to-disk-to-cloud(D2D2C)

Schéma D2D2C se je velmi podobné D2D2D s tím rozdílem, že offsite záloha putuje na cloud. To s sebou přináší některé výhody a nevýhody.

Hlavním benefitem je škálovatelnost datového prostoru, dostupnost odkudkoliv prostřednictvím internetu a také správa infrastruktury, která odpadá.

Tyto výhody však nejsou zadarmo a proto nás nesmí překvapit výsledná cena (více viz srovnání on-premise a cloudu v kapitole 4). Dále také svěřujeme data do rukou třetí straně. Je proto nutné předem zjistit, jak konkrétní poskytovatel zabezpečuje data svých zákazníků a vybrat takového poskytovatele, který bude splňovat naše požadavky.

1.6.2 Testování záloh

Není tajemstvím, že velké množství IT administrátorů netestuje zálohy. A důvod? Není čas. Na zálohování je však důležitá pouze jedna část, a tou je obnova. Záloha je k ničemu, pokud nelze obnovit. A testování je jediný způsob, jak mít jistotu, že zálohy fungují.

Jaké jsou další důvody, proč testovat zálohy?

- **Otestování hodnoty RTO** - stanovení papírové hodnoty RTO je jedna věc, druhá je však skutečnost. Pokud chceme ověřit, jak dlouho obnova trvá, musíme testovat.
- **Seznámení se s procesem obnovy** - obnova dat trvá určitou dobu, nicméně i lidský faktor zde hraje roli. Čím více jsme obeznámeni s procesem obnovy, tím rychleji ve vypjatých situacích budeme schopni vše správně spustit.

Jaké jsou způsoby testování?

- **Automatická verifikace** - spousta zálohovacích nástrojů dokáže kontrolovat integritu provedených záloh. Neposkytne však takový pocit jistoty, jako „ručně“ provedené testy.

- **Obnova souborů a složek** - připojení zálohovacího obrazu a obnovení několika souborů a složek nám dá jistotu, že data jsou dostupná a čitelná.
- **Virtualizace** - systémové obrazy je možné virtualizovat a otestovat, zda systém nabootuje a funguje.
- **Bare Metal Recovery** - pokud máme možnost, můžeme zkusit obrazy obnovit na „holém železe“, tedy na počítači bez nainstalovaného operačního systému. Získáme tím také představu, jak dlouho se daný obraz obnovuje.
- **Simulace katastrofy** - vyzkoušení si situace, kdy například zkratoval hlavní server. Umožňuje mimo jiné také otestovat, zda pověřené osoby vědí, co v takové situaci dělat.

Jak často testovat? Odpověď na tuto otázku je snadná - tak často, jak to jen jde. Testování však trvá a čas jsou peníze. Reálně je tedy vhodné důsledně testovat každý čtvrt rok, minimálně však jednou ročně.[28]

1.6.3 Šifrování disků

Existují dvě základní metody šifrování. První je zašifrování jednotlivých souborů/složek. Takto zašifrovaná data lze zobrazit pouze při znalosti hesla. Šifrovat tímto způsobem lze například i pomocí známého komprimačního programu WinRar.

Druhým, robustnějším řešením je šifrování disku. Není tak zapotřebí šifrovat jednotlivé soubory, neboť nejen ty, ale i celý operační systém a veškerá data jsou šifrována průběžně. Díky tomu jsou data chráněna proti krádeži, neboť bez znalosti hesla nelze získat z disku žádná data. Po zadání hesla jsou pak data automaticky dešifrována a systém se chováním neliší od nezašifrovaného, pouze je čtení a zápis pomalejší. Šifrování disků u pracovních počítačů a notebooků by mělo být samozřejmostí. Stejně tak je vhodné šifrovat disky se zálohovanými daty, neboť v případě krádeže/ztráty máme jistotu, že data jsou ochráněna. Příkladem softwaru umožňujícím šifrování disku je například open-source program TrueCrypt.[29]

1.7 Nástroje pro on-premise zálohování

Softwaru specializujícího se pouze na on-premise zálohování již není mnoho. Nebudeme se proto omezovat touto podmínkou a zaměříme se na software, který sice umožňuje i zálohování na cloud, nicméně to není jeho podstatou, ale pouze volitelnou vlastností.

1.7.1 Windows Server Backup

Zabudované zálohovací nástroje Windows byly dlouho dobu považovány za „odpad“, což umožnilo rozkvět trhu se zálohovacím software. S příchodem Windows Serveru 2008 se však Microsoft rozhodl napravit svoji reputaci a představil první „použitelnou“ zálohovací utilitu.

Tato verze Windows Server Backup s sebou přinesla:

- Větší flexibilitu při volbě zálohovaných dat - možnost zálohovat jednotlivé složky či soubory. Dříve bylo možné zálohovat pouze celé diskové jednotky. Lze také zúžit výběr na základě cesty nebo typu souboru.
- Automatická správa úplných a inkrementálních záloh - Windows Server Backup automaticky vytváří inkrementální zálohy, které se chovají jako úplné zálohy. Při obnově tak není nutné postupně spouštět jednotlivé inkrementální zálohy. Dále také v pravidelných intervalech odmazává staré zálohy, aby se uvolnil prostor pro nové.
- Rozšířené možnosti pro zálohovací prostor - možnost vytvářet plánované zálohy do vzdálené sdílené složky (remote shared folder) nebo jednotky (remote shared volume). Dále přibyla možnost zálohovat na virtuální disky.
- Vylepšení systému vytváření systémových záloh a obnov - uživatelské rozhraní Windows Server Backup nyní nabízí možnost vytvářet body obnovení pro případ obnovy systému. Tyto lze vytvořit jak zvlášť, tak společně se zálohou dalších dat.[30]

Aktuálně nejnovější verze Windows Server Backup 2012 dále představila možnost zálohovat a obnovovat virtuální zařízení odděleně od zálohy fyzického serveru. Dříve byly zálohovány jako součást zálohy celé jednotky.[31]

Windows Server Backup není špatným nástrojem, pokud požadujeme základní zálohování a obnovu. V případě, že jsou našimi požadavky i výkon, efektivita a spolehlivost, je zapotřebí se poohlédnout jinde.

Proces zálohování si odřezává až příliš velký díl z výkonu systému a zálohování je tak vhodné provádět spíše až v nočních hodinách. Dále si nemalé množství uživatelů stěžuje na nespolehlivost zálohování virtuálních zařízení. Ačkoliv vše správně nastavili, po pár dnech fungování systém přestal zálohovat.

1.7.2 AhsayOBM

Ahsay Systems Corporation (dříve Leb Shama) byla založena v roce 1999 s ambicí vytvořit prvotřídní zálohovací řešení, které bude atraktivní svou cenou, nenáročnou údržbou a uplatněním napříč společnostmi bez ohledu na velikost a zaměření.[32]

1. ZÁLOHOVÁNÍ DAT

Společnost Ahsay nabízí zajímavé produkty, které zaujmou zejména cenou a možností nadefinovat „robustnost“ řešení a zvolit tak pouze součásti, které zákazníci využijí a nemusí tak platit velké peníze, pokud mají menší požadavky. Provázanost konkrétních produktů viz obrázek 1.6.

Vlastnosti AhsayOBM:

- Průběžné zálohování - kritická data zvolená k zálohování jsou při změně automaticky opět zazalohována.
- Využití potenciálu procesorů - AhsayOBM vytváří pro každé jádro procesoru dvě vlákna. Díky tomu většina operací proběhne rychleji než u jedno-vláknových aplikací.
- Volitelná síla šifrování - možnost volby šifry, délky klíče a módu šifrování. Data lze následně dešifrovat pouze při znalosti klíče.
- Tvorba zálohovacích sad - AhsayOBM podporuje tvorbu zálohovacích sad. Pokud se rozhodneme zálohovat soubory a Microsoft SQL databázi, lze pro obě zálohy nakonfigurovat odlišná nastavení.
- Široká podpora databází, virtuálních zařízení a aplikací - například VMware Server/Station, Microsoft Hyper-V, MS Exchange databáze, MS SQL Server, Oracle a MySQL databáze a další

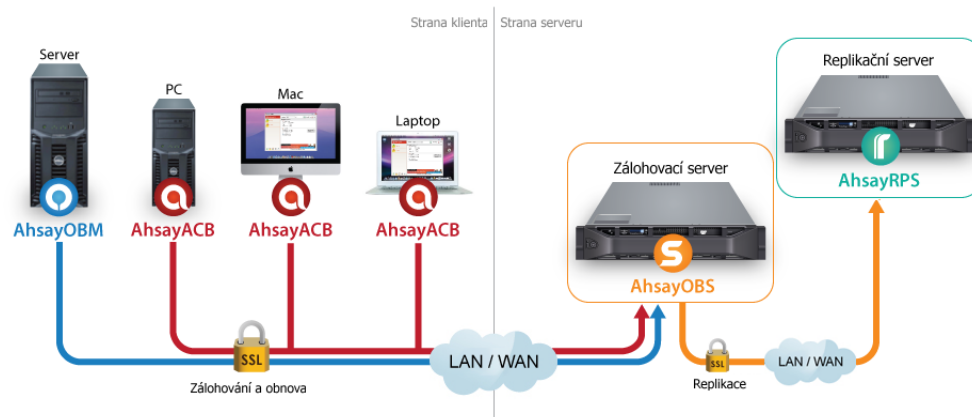
Jak jsem již zmínil, cenění produktu AhsayOBM je atraktivní (viz tabulka 1.2). Koupě jedné licence vyjde nevýhodně, od 10 licencí jsou však ceny velmi příznivé. Zákazníci, kteří mají zájem pouze o malé množství licencí navíc nemusí kupovat za nevýhodnou sazbu a mohou využít některého z prodejců Ahsay a licence pořídit za lepší peníze.

Základní řešení neobsahuje možnost zálohovat virtuální stroje. Toto rozšíření lze zakoupit v rozmezí \$45 - \$30 v závislosti na počtu zakoupených licencí. Platí se zvláště za VMware a Hyper-V.[33]

Počet zakoupených licencí	Cena/Licence
1 - 4	\$525
5 - 9	\$200
10 - 19	\$75
20 - 49	\$70
50 - 99	\$65
100 - 199	\$60
200 a více	Další sleva na vyžádání

Tabulka 1.2: Ceník AhsayOBM[33]

1.7. Nástroje pro on-premise zálohování



Obrázek 1.6: Zálohovací software společnosti Ahsay[34]

1.7.3 Vembu BDR

Vembu Technologies od roku 2004 dodaly zálohovací řešení do více než 25 000 společností a spolupracují s více než 4000 správci a dodavateli zálohovacích řešení. Software Vembu je vyvíjen zejména pro malé a střední společnosti, které potřebují chránit jejich fyzické i virtuální prostřední.[35]

Stejně jako Ahsay software i Vembu nabízí neobvyklé cenění svých licencí. Řešení je pak obzvláště zajímavé pro společnosti, které nedisponují velkým vstupním kapitálem, neboť licence funguje na principu měsíčního předplatného a částka nepřesahuje \$20 za server (případně 2 procesory).

Způsob zálohování u Vembu je dvojitý - jednodušší a levnější variantou je klasické zálohování souborů a složek. Druhou, o něco dražší a komplexnější, je zálohování pomocí systémových obrazů. To umožňuje kompletně obnovit servery a počítače v případě potřeby (více o systémových obrazech zde - 1.2.5).[36]

Vlastnosti Vembu BDR:

- Obnova spadlého či poškozeného systému - díky vytváření systémových obrazů je možné v případě nenabíhajícího či jinak nefunkčního systému, kompletně obnovit celý systém bez nutnosti přeinstalace. Vembu BDR navíc garantuje obnovení a maximální stáří zálohy 15 min.
- Virtuální prostředí - kvůli Vembu Backup Serveru není nutné zakupovat nový server, pokud disponujete dostatečně výkonným, neboť lze Backup Server virtualizovat.
- Záruka konzistence - i během probíhající zálohy jsou sledovány změny v databázích. Pokud během zálohování nastane výpadek, jsou obnovena i data vytvořená během zálohy.

1. ZÁLOHOVÁNÍ DAT

- Částečná obnova - pokud chceme obnovit nějaký záznam z databáze, není zapotřebí přehrát celou databázi. Je možné obnovit pouze vybrané tabulky či řádky.
- Extrémně rychlá obnova virtuálních zařízení - Technologie VM Power Replication™ udržuje vždy dvě kopie zálohované virtuální mašiny, obnova tak může proběhnout až dvakrát rychleji.[36]

Vembu nabízí zálohování serverů pomocí systémových obrazů a standardní zálohování souborů a složek za \$20, respektive \$7 měsíčně. Předplatné se platí rok dopředu. K oběma řešením možné přikoupit cloudový prostor za \$0,1/GB/měsíc.[37] Jednoduchý náčrt hierarchie systému zde 1.7.



Obrázek 1.7: Zálohování pomocí Vembu BDR[38]

1.8 Shrnutí

Hlavním cílem této kapitoly bylo ukázat, jak komplexní problematika zálohování je. Uvědomili jsme si, že zálohovat se dá mnoha způsoby, na mnoho médií, s využitím různých architektur a nástrojů. Rozhodnutí, kterou cestou se vydat, záleží na mnoha faktorech, jak se dozvíme v praktické části práce.

Zálohování se však celkově postupně odvrací od pásky a implementují se spíše architektury D2D2D a D2D2C, neboť tato schémata fungují automaticky, jsou rychlejší a dostupnější. Stejnou cestou se proto v práci vydáme i my.

Cloud computing

Cloud computing se pomalu ale jistě stává nedílnou součástí moderního IT světa a lze očekávat, že tomu tak bude i nadále. Přestože se tento koncept rozšířil teprve během několika posledních let, jeho principy jsou známé již poměrně dlouho. Nicméně až nyní pokročily technologie natolik (zejména běžně dostupné vysokorychlostní připojení k internetu), aby mohl cloud prorazit. V cloudu tak nyní máme služby, aplikace, data, celé počítače a servery, skutečně vše, na co si vzpomeneme. Výjimkou není ani zálohování dat a cloud je tak horkým kandidátem na uchování offsite záloh. Abychom byli schopni se rozhodnout, zda cloudu využít, je důležité si uvědomit výhody a nedostatky, které využití cloudu obnáší.

Cílem kapitoly je definovat pojem cloud, popsat jeho jednotlivé vlastnosti, které jsou pro něj charakteristické a seznámit se s jeho servisními modely a modely provozu.

2.1 Definice cloud computingu

Nalézt přesnou definici pojmu cloud computing dle mého názoru není možné, neboť jich existuje hned několik. Podle serveru cloud.cz je „Cloud computing nový způsob využívání zdrojů (zejména hardware, software) v IT, vycházející z možnosti jejich sdílení mezi aplikacemi a odstranění přímé vazby aplikační logiky na fyzické komponenty (virtualizace).“[39]

Přední analytická a poradenská společnost v oblasti IT Gartner definuje cloud computing jako „styl správy výpočetní techniky, který je škálovatelný, elastický a je zprostředkován jako služba prostřednictvím Internetu.“[40]

Podle Národního institutu standardu a technologie (NIST) je definice cloud computingu takováto: „Cloud computing je model umožňující všudypřítomnou, vyhovující, a na požádání přístupnou sdílenou zásobu konfigurovatelných počítačových zdrojů (např. síť, servery, úložný prostor, aplikace a služby), které mohou být velmi rychle poskytnuty s minimální režií nebo interakcí s po-

skytovatelem služby.“[41] Dále pak specifikuje pět základních vlastností, které musí cloudová služba splňovat:

- **Samospráva na vyžádání** (*on-demand self service*): Výpočetní výkon, datové úložiště a další zdroje musí být poskytovány s co nejmenší možnou reží při konfiguraci a s co největší mírou automatizace. Přes online kontrolní panel by měl uživatel být schopen regulovat či navyšovat (téměř neomezeně) tyto zdroje bez nutnosti kontaktovat svého poskytovatele. Tímto se dostáváme do kontrastu oproti klasickému on-premise modelu, kdy je navýšení zdrojů obvykle nutné konzultovat s administrátorem a vedením společnosti.
- **Široké možnosti přístupu** (*broad network access*): Přístup ke cloudové službě je nezávislý na druhu a povaze komunikačního zařízení. Ke cloudu by tak mělo být možné se připojit nejen z klasických počítačů a notebooků, ale také smartphonů, tabletů a dalších zařízení.
- **Sdílení výpočetních zdrojů** (*resource pooling*): Cloudové služby mohou obsluhovat i miliony uživatelů najednou, přičemž spotřebitel nepotřebuje znát umístění zdroje ani způsob realizace služby. Díky sdílení zdrojů není potřeba každému klientovi vyhrazovat vlastní hardware. Zdroje jsou uživatelům přidělovány dynamicky za účelem efektivního využívání dostupných infrastrukturních zdrojů a snížení provozních nákladů.
- **Vysoká elasticita** (*rapid elasticity*): Jak již bylo naznačeno v prvním bodě, cloudová služba by měla být schopná během okamžiku podle potřeby zvýšit nebo snížit množství poskytovaných zdrojů. Zákazník tak má dojem, že zdroje jsou v podstatě neomezené.
- **Měřitelnost služby** (*measured service*): Jednou z předností cloudu je, že zákazník platí pouze za zdroje, které využil nebo si předplatil. K tomu je zapotřebí měřit a monitorovat využití zdrojů. Zákazník tak platí například pouze za využitý prostor nebo procesorový čas. Poskytovatelům měření dále umožňuje efektivní využití zdrojů, prediktivní analýzu apod.[42]

Zjednodušeně řečeno, pod pojmem cloud computing se skrývá koncept, který umožňuje vzdálený přístup k aplikacím, datům, nebo třeba službám, jež jsou umístěny mimo konkrétní počítač. Jak jsem se již zmínil, jedná se o relativně starý koncept. Pokud se na chvíli zamyslíme, jak vlastně funguje obyčejný email, dospějeme k závěru, že se ve své podstatě jedná o cloudovou službu. Příchozí emaily se nám ukládají na serveru (v cloudu), přistupujeme k nim přes webové rozhraní (vzdálený přístup) a jen pokud si nainstalujeme nějakého emailového klienta, můžeme si emaily stáhnout k sobě do počítače.

S rozvojem virtualizace výpočetního výkonu se mohly naše servery stát nezávislé na hardwaru. Virtuální servery dnes mohou být vytvořeny během několika minut přes jednoduché webové rozhraní a právě to je jednou z příčin rozvoje využití cloudu v takovém měřítku, jak se to děje právě nyní.

Společnosti využily možnosti škálovatelnosti virtuálních strojů a začaly nabízet nevyužitý výpočetní výkon svých serverů jako službu. Nakonfigurování serveru přes jednoduché webové rozhraní zvládne i středně pokročilý uživatel. Podle mého názoru však hlavní roli v masivním rozšíření cloudu hraje především rozvoj infrastruktury, rychlost a stabilita internetové konektivity. V době, kdy jsme přes vytáčené připojení stahovali emaily několik minut, nebylo možné uvažovat o přenesení výpočetního výkonu na vzdálené servery. Výpočetní operace by sice proběhly za zlomek času, ale vypočtená data by přes síť putovala neúměrně dlouhou dobu. Dnes, kdy jediný optický kabel zvládne přenosové rychlosti až 1 Pbit/s[43], je již situace podstatně jiná.

Rozvoj cloud computingu tak umožnil vznik velkých cloudových gigantů, kterými v současnosti jsou Microsoft (Microsoft Azure), Amazon (Amazon Web Services), Google (Google Cloud), HP (HP Cloud System), IBM (IBM Smart Cloud) a Rackspace.

2.2 Služby nabízené v cloudu (servisní model)

V současnosti rozeznáváme tři základní druhy služeb napříč poskytovateli cloudu. Jejich rozdělení umožňuje snadnější orientaci mezi různorodou nabídkou a pomáhá zákazníkům vybrat si nejvhodnějšího poskytovatele podle konkrétních požadavků a kritérií výběru. Patří mezi ně:

- Software as a Service - SaaS (Software jako služba)
- Platform as a Service - PaaS (Platforma jako služba)
- Infrastructure as a Service - IaaS (Infrastruktura jako služba)

S vývojem cloudových služeb se samozřejmě začínají objevovat i nové podkategorie. Se zálohování pak úzce souvisí:

- Backup as a Service - BaaS (Zálohování jako služba)
- (Disaster) Recovery as a Service - (D)RaaS (Obnova (po katastrofě) jako služba)

2.2.1 Software jako služba

Je koncept poskytování softwaru ve formě cloudové služby. Software se nachází na vzdálených serverech a je spravován poskytovatelem. Odběratel služby k aplikacím přistupuje prostřednictvím svého webového prohlížeče. Pokud se

rozhodneme využít SaaS, přinese nám to mnoho benefitů. Mezi hlavní výhody patří především úspora financí i zdrojů.

V případě nákupu samostatné aplikace je také nutné zajistit instalaci napříč všemi zařízeními ve firmě, což s sebou mnohdy přináší problémy s kompatibilitou či nedostatečným výkonem a s tím spojené náklady na nákup nového hardwaru a softwaru. Tento problém při využití cloudu odpadá. Mezi další výhody SaaS patří také snadná konfigurovatelnost, dostupnost a minimální nutnost údržby.

SaaS má však i své slabé stránky. Jednou z nich je problematické přenesení aplikace k jinému poskytovateli. Reálně totiž hrozí, že poskytovatel ukončí své služby a my tak přijdeme o zavedenou fungující aplikaci, v horším případě i o svá data (pokud pravidelně nezálohujeme). Je proto nutné obezřetně vybírat poskytovatele a věnovat pozornost SLA⁷ smlouvám.

Systémy vhodné pro koncept SaaS:

- „Customer relationship management (CRM)
- Enterprise resource planning (ERP)
- Human resource management (HRM)
- Content management (CM)“[44] ...

2.2.2 Platforma jako služba

Poskytuje všechny prostředky nutné k vytváření aplikací a služeb výlučně z internetu, aniž by bylo potřeba stahovat, nebo instalovat software. Využití platformy jako služby může být výhodné v případě, že firma potřebuje krátkodobě aplikaci s vysokými nároky na platformu.

Není už tak vhodné pro aplikace, které jsou dlouhodobě pro firmu kritické. Aplikace postavené na PaaS jsou totiž závislé na unikátním řešení daného poskytovatele a v případě nutnosti migrace může být tento proces zdlouhavý a nákladný.

2.2.3 Infrastruktura jako služba

Dává zákazníkovi možnost pronájmu virtuálních serverů a úložišť, která jsou fyzicky v datacentrech poskytovatele. U tohoto řešení se nejvíce projevují výhody cloud computingu.

Pro IaaS jsou typické tyto vlastnosti:

- Škálovatelnost
- Spuštění a konfigurace pronajaté infrastruktury v jednotkách minutách

⁷Service-level agreement - označuje smlouvu sjednanou mezi poskytovatelem služby a jejím konzumentem.

- Nezávislost na hardwaru
- Geografická vzdálenost
- Snadná migrace mezi jednotlivými poskytovateli
- Dynamické účtování služeb na základě spotřeby

2.2.4 Zálohování jako služba

BaaS zajišťuje zálohování a obnovu z cloudu. Poskyvatelé se starají o provoz potřebných zařízení a aplikací v jejich datacentru. U zákazníka je pak zpravidla nainstalována zálohovací jednotka, která zajišťuje provádění záloh. O nic dalšího se zákazník nemusí starat.

Poskyvatel se zákazníkem konzultuje jeho požadavky a společně vytvoří SLA smlouvu. Poskyvatel, někdy nazývaný jako MSP,⁸ se poté stará o chod zálohování. Tím se BaaS velmi liší například od online zálohování (více sekce 3.2), kde zákazník získává výhradně zálohovací prostor na cloudu.

BaaS je vhodné řešení pokud:

1. Dramaticky narůstají naše data a virtualizujeme serverové prostředí
2. Máme nedostatek místa nebo pracovních síly
3. Preferujeme nižší vstupní náklady na úkor provozních
4. Máme problém naplnit požadavky v současné SLA smlouvě
5. IT pracovníci tráví neúměrně velké množství času správou zálohování

BaaS se nehodí pokud:

1. Již máme dobře vyřešené zálohování
2. Jsme omezeni vyhláškami, které znemožňují provoz v cloudu
3. Nemáme dostatečné připojení k internetu[45]

2.2.5 Obnova po katastrofě jako služba

BaaS a DRaaS jsou na první pohled vypadají velmi podobné služby. A je tomu opravdu tak, obě služby fungují na podobných principech. V čem se tedy liší?

Prvním rozdílem je rychlost obnovy a četnost provádění záloh. DRaaS jako robustnější řešení nabízí rychlejší obnovu a četnější zálohování. Liší se také zálohovaná data. BaaS se zaměřuje především na zálohu jednotlivých disků, souborů a složek. Zatímco DRaaS zálohuje celé aplikace a systémy. DRaaS je tak zjednodušeně řečeno nadstavbou BaaS.

2.3 Modely provozu cloudových služeb

Model nasazení určuje, jakým způsobem jsou koncovým uživatelům služby cloud computingu poskytovány.

⁸Managed service provider - správce služby

Poté, co si zákazník vybere druh služby, stojí před dalším rozhodnutím. Využívat plně zdroje poskytovatele, nebo využít své vlastní infrastruktury pro provoz cloudu? Pokud ani jedna z těchto variant není vhodná, existuje ještě „střední cesta“. Spojit své zdroje a zdroje poskytovatele a vytvořit tak „hybridní řešení“.

2.3.1 Veřejný cloud

Pokud firma zvolí řešení veřejného cloudu, znamená to, že IT služby jsou poskytovány pomocí internetu externí organizací (třetí stranou). Zdroje cloudu jsou sdíleny více organizacemi. Jinými slovy se na jednom fyzickém serveru může nacházet více virtuálních serverů. Z pohledu poskytovatele je virtualizace zcela zásadní prvek, neboť umožňuje plné využití fyzického serveru.

Z pohledu zákazníka však takové sdílení může představovat potenciální bezpečnostní rizika. Data různých společností se totiž fyzicky často nacházejí hned vedle sebe. Bezpečnost virtualizace je natolik komplexní problematika, že by si vyžádala samostatnou bakalářskou práci. Pro naše potřeby bude stačit fakt, že z pohledu technologie virtualizace je pravděpodobnost pomíchání dat jednotlivých společností minimální. Mnohem větší bezpečnostní riziko často představují sami uživatelé, kteří mnohdy nedodržují stanovené postupy a nechávají tak útočníkovi doslova otevřená vrátka. Pokud bychom si měli shrnout výhody veřejného cloudu, byly by to:

- Nulové vstupní náklady na pořízení libovolně škálovatelného výpočetního výkonu
- Údržba, správa, renovace a konfigurace hardwaru výhradně na straně poskytovatele.

Hlavní nevýhodou je již zmiňované bezpečnostní riziko. Některé dokumenty navíc podléhají speciální legislativě, z níž vyplývá zákaz jejich uložení ve veřejném cloudu. Jsou to například data, na něž se vztahuje zákon HIPAA⁹. Jedná se totiž o citlivé zdravotní záznamy a informace. Poskytovatelé však po splnění stanovených podmínek mohou obdržet certifikaci a i tyto záznamy následně uchovávat.

Mezi další problematiku veřejného cloud computingu patří geopolitická hlediska. Na data se totiž vztahují zákony země, ve které jsou fyzicky uložena. Pokud tedy nahrajete například do úložiště Google Docs 3 nějaký dokument a ten bude následně fyzicky uložen například v USA, vztahují se na něj zákony USA. Nelze také vyloučit vloupání do cloudového datacentra a odcizení našich dat.

⁹Health Insurance Portability and Accounting Act

2.3.2 Privátní cloud

U privátního cloudu zůstávají zachovány všechny již zmíněné výhody, jako je škálovatelnost, přístup z různých zařízení a podobně. Hlavní rozdíl je tedy v tom, že IT služby jsou poskytovány pomocí intranetu v rámci jedné organizace, chráněné firewallem.

Zdroje cloudu jsou plně využívány pouze touto jednou organizací. Z toho vyplývá, že firma má plnou kontrolu nad svými daty, včetně jejich umístění a zabezpečení. Nevýhoda spočívá v nutnosti nadále vlastními silami provozovat datacentrum a tedy investovat jak do samotného hardwarového vybavení, tak zajištění údržby. Řešením tohoto problému může být přenechání správy třetí straně (MSP). Máme na výběr několik možností provozu privátního cloudu:

1. Provoz privátního cloudu je plně v režii naší firmy
2. Externí firma provozuje privátní cloud nad naším datacentrem
3. Pronájem privátního cloudu od externí firmy,
4. Externí firma pro nás na zakázku vybuduje vlastní datacentrum včetně jeho správy

Pro provoz na privátním cloudu se potom nejvíce hodí tyto služby:

- Analytické aplikace
- Datové sklady
- ERP systémy
- Transakční databáze ...

2.3.3 Hybridní cloud

Hybridní cloud, jak už název napovídá, představuje jakýsi hybrid mezi veřejným a privátním cloudem. Jedním z případů užití tohoto řešení může být navýšení výkonu privátního cloudu. V době běžného provozu je aplikace plně obsluhována privátním cloudem. V době špičky se potom od poskytovatele veřejného cloudu pronajímá dodatečný výpočetní výkon, zajišťující plynulý provoz aplikace. Často pak bývá použit v případě, že pracujeme s velice citlivými daty. Řešením je potom hybridní cloud, kdy citlivá data máme pod svou výhradní kontrolou v privátním cloudu a funkčnost a výpočetní výkon zajišťujeme pomocí veřejného cloudu.

Obecně však neexistuje žádný univerzální model, který by popisoval, která část aplikace má být ve veřejném a která část v privátním cloudu. Každé řešení hybridního cloudu je tedy v podstatě unikátní a „ušité na míru“ dané organizaci.

2.4 Shrnutí

Klíčovou myšlenkou této kapitoly bylo nastínit výhody cloud computingu, které jsou hlavním motivem pro využití cloud computingu za účelem zálohování. Zároveň je důležité systém navrhnout tak, aby počítal se všemi možnými nevýhodami, které jsou nedílnou součástí každého řešení využívající cloud a případnou kombinaci s on-premise řešením. Pokud se v práci budeme dále bavit o cloudu, bude se jednat zejména o cloud veřejný, neboť nabídka služeb je největší a výhody cloudu jsou zde nejvýraznější.

Analýza poskytovatelů cloudového zálohování

Poskytovatelů cloudového zálohování je obrovské množství. Rozsáhlá analýza by sama za sebe vydala na samostatnou bakalářskou práci. Vybral jsem proto zástupce, které jsem shledal nejzajímavějšími a seznámíme se tak nejen s produkty společností se zvučnými jmény, ale i menšími řešeními pro méně náročné.

3.1 Robustní řešení

Pokud požadujeme kompletní zálohování, kvůli maximalizaci dostupnosti, nestačí pouze zálohovat data. Zajímají nás musí také údaje jako je rychlost obnovy, stáří nejnovější zálohy, spolehlivost provedených záloh a tak dále.

S tak vysokými požadavky si online zálohovací služby nejsou schopné poradit a je zapotřebí se poohlédnout po více robustních řešeních.

V rámci analýzy jsem se zaměřil, jak daní poskytovatelé splňují níže uvedené požadavky. Z nich jsem poté vybral tři dle mého názoru nejzajímavější představitelé.

1. **Rychlost obnovy** - co nejnižší RTO¹⁰, protože systém mimo provoz znamená obrovské ztráty a v případě veřejně dostupných systémů i poškození jména apod.
2. **Průběžnost záloh** - co nejnižší RPO¹¹, aby výpadek systému neznamenal velkou ztrátu dat.
3. **Spolehlivost záloh** - automatické testování záloh, úspěšnost obnovení

¹⁰Recovery Time Objectives - doba, za kterou je nutné obnovit systém po výpadku, aby nedošlo k nepřijatelným škodám.[46]

¹¹Recovery Point Objective - popisuje stáří dat, která musíme obnovit v důsledku výpadku.[46] Bývá definováno i jako množství dat, které jsme ochotni ztratit.

3. ANALÝZA POSKYTOVATELŮ CLOUDOVÉHO ZÁLOHOVÁNÍ

4. **Efektivita zálohování** - deduplikace, komprese, rychlost zálohování, vytěžování systému
5. **Správa produktu** - plánování, monitoring, výstrahy, přehled nad daty
6. **Bezpečnost** - šifrování, ochrana cloudových datacenter
7. **Další služby** - možnosti virtualizace záloh, zálohování metodou 3-2-1
8. **Cena** - cena produktu

3.1.1 Veeam Availability Suite

Mladá švýcarská společnost založená v roce 2006 má nyní více než 135 000 zákazníků a její produkt Veeam Availability Suite se stal konkurencí produktům největších softwarových společností zaměřených na zálohy a obnovu po katastrofách.[47]

Veeam Availability Suite je komplexní produkt, zaměřený zejména na společnosti, které potřebují fungovat 24/7/365. Klade si za cíl odstranit tzv. „Availability Gap“¹², který výrazně snižuje kvalitu informačního systému, zejména, pokud po výpadku následuje dlouhá obnova a ztráta dat. [48]

Veeam Backup & Replication (produkt, který je součástí Availability Suite) umožňuje obnovu veškerých dat(RTO) a softwaru do 15 minut včetně:

- Obnovy všech virtuálních zařízení v několika minutách
- Bezproblémové obnovy jednotlivých souborů a složek
- Kompletní obnovy Microsoft SQL Database Server databáze, Microsoft Active Directory objektů atd.

Backup & Replication dále nabízí průběžné bezpečné zálohy mimo síť a zajišťuje také maximální stáří poslední zálohy (RPO) 15 minut. Toho je docíleno pomocí:

- Automatické kontroly obnovitelnosti každé zálohy
- Automatické testování bodů obnovy všech virtuálních zařízení
- Zrychlení přenosu zálohovaných dat po síti až 50x zásluhou WAN-akcelerace, která využívá efektivní cachování, variabilní datovou délku a optimalizaci TCP/IP protokolu.
- Deduplikace na straně zdroje i cíle - optimální rychlost přenosu a využití datového prostoru
- Zálohování s minimálním dopadem na vytížení systému
- 24x7 monitoring a výstražná hlášení
- Plně konfigurovatelný reporting
- Optimalizace zdrojů a automatické plánování kapacity
- Celý proces zálohování i zálohovací úložiště chráně AES-256 šifrováním
- Možnost nastavit automatické zálohování metodou 3-2-1 viz obrázek 3.1[49]

¹²Mezera(nedostatek) v dostupnosti

Cena: \$1700/licence/processor
\$17400 za 5 TB cloudu/rok[50]



Obrázek 3.1: Metoda 3-2-1 pomocí Veeam Availability Suite[49]

3.1.2 Acronis Backup Advanced Suite

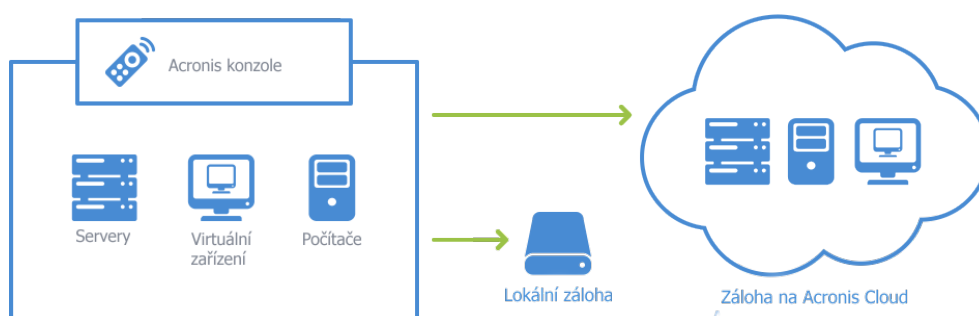
Acronis je švýcarská společnost se zaměřením na ochranu dat. Specializuje se na řešení v oblasti zálohování, obnovu po katastrofách a zabezpečené sdílení a přístup k datům. Společnost vznikla v roce 2003 a momentálně jejich služeb využívá více než 5 000 000 jednotlivců a 300 000 firem.

Acronis Backup Advance si klade za cíl chránit data celé společnosti - od fyzických zařízení, přes virtuální, po cloud. To vše pomocí jediného produktu. Backup Advance je speciálně vyvinut pro velké společnosti a zajišťuje kvalitní ochranu všech dat bez ohledu na velikost a složitost prostředí.

- Acronis Backup Advance provádí především inkrementální a rozdílové zálohy pro snížení vytížení
- Konkrétní hodnoty RTO a RPO Acronis neuvádí, více viz srovnání Acronis a Veeam v příloze B.
- Vytváří bleskové obrazy disků - možnost kompletní obnovy OS
- Deduplikace na straně zdroje i cíle - optimální rychlost přenosu a využití datového prostoru
- Wake On Lan - automatické probuzení uspaných strojů pro zálohování
- Zálohování s minimálním dopadem na vytížení systému + možnost regulace
- Centralizovaná, vzdálená správa zálohování a obnovy
- Obsahuje kontrolní panel pro celkový přehled o stavu zálohování
- Optimalizace zdrojů a automatické plánování kapacity
- Celý proces zálohování i zálohovací úložiště chráněné AES-256 šifrováním
- Možnost nastavit automatické zálohování metodou 3-2-1 s využitím cloudu přímo od Acronis, viz obrázek 3.2

Cena: \$2199/licence/server
\$1599 za 1 TB cloudu/rok[50]

3. ANALÝZA POSKYTOVATELŮ CLOUDOVÉHO ZÁLOHOVÁNÍ



Obrázek 3.2: Metoda 3-2-1 pomocí Acronis Backup Advanced[51]

3.1.3 StorageCraft Recover-Ability

StorageCraft je mezinárodní společnost zabývající se vývojem software, založená v roce 2003. Co odlišuje tuto společnost ostatních, je důraz na budování vztahů se správci, kteří jsou najímáni různými společnostmi jako zodpovědné osoby za zálohování (MSP). Ti pak pro zajištění bezproblémového zálohování a obnovu využívají jejich produkty. [52]

Zálohování pomocí balíku Recover-Ability je založeno na principu průběžného vytváření systémových obrazů (více viz 1.2.5). Pokud tedy dojde k selhání disku, je možné na novém disku obnovit systém do stejného stavu, jako byl před selháním. Výhodou tohoto přístupu je také možnost virtualizace těchto obrazů na serveru či cloudu. Díky tomu je například v případě selhání disku možné pokračovat v práci, bez nutnosti čekat na objednávku nového. Dalšími vlastnostmi produktu jsou:

- Možnost volby mezi úplnou, inkrementální nebo rozdílovou zálohou
- Zálohování fyzických i virtuálních zařízení, serverů, počítačů, laptopů
- Monitorování a správa zálohování přes centrální konzoli
- Kontrola volného prostoru a integrity záloh
- Možnost omezit/zvýšit přenosové rychlosti záloh v závislosti na vytížení systému
- Již zmíněná virtualizace zálohovaných obrazů
- Plánování on-premise i offsite testování záloh
- Obnova systémových obrazů na stejný či nový HW, případně do virtuálního prostředí.[53]
- Zajímavé cenění cloudového prostoru. Zákazník platí za každý GB, který využil konkrétní měsíc. Neplatí se tak předem pronajatý prostor, ale zpětně každý měsíc pouze využité GB.[54]

Cena: \$1095/licence/server[55]
\$0,52 - \$0,85 za 1 GB cloudu/měsíc[56]

3.2 Online zálohování

Abychom mohli zálohovat na cloudu, není nutné za každou cenu kupovat drahá robustní řešení s širokou nabídkou služeb. Spoustě lidí i společností stačí mít zálohovaná pouze některá klíčová data. Samozřejmě i takováto řešení jsou dostupná a nyní se blíže podíváme na dva, dle mého názoru nejprovedenější zástupce.

3.2.1 Backblaze for Business

Backblaze nabízí pouze jeden formát: neomezená data za \$50/počítač/rok. Jediným omezujícím faktorem je tu pouze minimální počet počítačů, který je roven pěti.

Způsob zálohování

Zálohování funguje na principu inkrementálního průběžného zálohování. Po úvodní záloze vybraných souborů a složek software sleduje, zda byly soubory změněny, či přibyly nové, a ty okamžitě automaticky zálohuje.[57]

Verzování

Po upravení zazálohovaného souboru se vytvoří nová verze. Backblaze umožňuje přístup ke všem verzím za posledních 30 dní.[58]

Výkon

Systém automaticky komprimuje a šifruje data, které následně posílá do Backblaze datacentra optimální rychlostí, aby uživatel nepocítil zpomalení. Rychlost lze také manuálně omezit.

Zabezpečení

Před přenosem jsou data zašifrována pomocí AES 128-bit klíče a následně přes SSL spojení přesunuta do datacentra, kde zůstávají zašifrována. Na žádost je možné nechat zašifrovat data primárním klíčem, kterým disponuje pouze zákazník. Nicméně na sebe bere riziko, neboť v případě ztráty klíče data nikdo nerozšifruje, ani samotný Backblaze.

Další služby

Existují dva typy správy: individuální a IT. Při individuálním si uživatelé spravují zálohování sami a mají k němu přístup pouze oni a administrátor. IT přístup pak znamená, že celá společnost má jeden velký zálohovací prostor a data z něj lze získat po odeslání žádosti IT týmu.

Dále je možné lokalizovat poslední známou lokalitu zařízení. Tato funkce se může velmi hodit například v případě ztráty či krádeže notebooku.[59]

3. ANALÝZA POSKYTOVATELŮ CLOUDOVÉHO ZÁLOHOVÁNÍ

3.2.2 Crashplan PRO

Při nákupu Crashplan PRO také nemáme moc na výběr, existuje totiž pouze jedna varianta: \$9,99/měsíc/počítač.

Způsob zálohování

Každou minutu probíhá kontrola, zda data, která uživatel zálohuje, byla nějak změněna, pokud ano, dojde k vytvoření nové verze zálohy.

Verzování

Narozdíl od Backblaze, Crashplan nelimituje stáří verzí na 30 dní. Dostupné tak jsou všechny verze od prvního do posledního zazálohování.

Výkon

Data jsou před zazálohováním deduplikována, čímž se výrazně snižuje vytížení internetu a optimalizuje využití datového prostoru. Přenosovou rychlost lze regulovat.[60]

Zabezpečení

Před přenosem jsou data zašifrována AES 128-bit klíčem. Na cloudu jsou pak šifrována 448-bit Blowfish klíčem. Stejně jako Backblaze, nabízí zašifrování privátním klíčem na zákazníkovo riziko.[61]

Další služby

Možnost volby, na kterém cloudu budou data uložena.

Největším rozdílem mezi oběma řešeními je cena a uchování verzí. Pokud chceme uchovávat všechny verze záloh a jsme ochotni si připlatit, Crashplan je tu pro nás. Jestliže se však spokojíme s aktuálnějsími zálohami, Backblaze nás odmění neuvěřitelně nízkou cenou a jednoduchým uživatelským rozhraním. Na obrázku 3.3 pak můžeme vidět loga obou řešení.



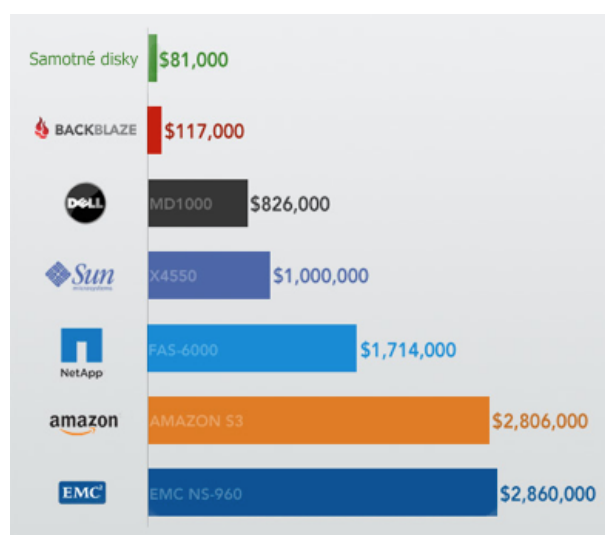
Obrázek 3.3: Loga produktů Crashplan Pro a Backblaze

Srovnání on-premise a cloudového zálohování

Dříve než se začneme zabývat tím, jak probíhá tvorba zálohovacích řešení, bylo by vhodné si nejprve ukázat a shrnout, jaké výhody a nevýhody s sebou přináší obě varianty.

4.1 Náklady

Jedním z hlavních marketingových lákadel poskytovatelů cloudů je úspora financí. Pokud se však podíváme na obrázek 4.1, situace tomu příliš nenasvědčuje.



Obrázek 4.1: Srovnání cen poskytovatelů cloudů za petabajt prostoru

Jak je tedy možné, že se cloud prezentuje jako levnější alternativa? Před zodpovězením této otázky je nutné si říci, o jakém servisním modelu se bavíme. Office 365 jako SaaS opravdu je levnější variantou oproti pořízení a provozování Exchange serveru. SaaS je totiž dělaný na míru požadavkům a v případě Office 365 není zapotřebí extrémně vysoký upload pro každého zákazníka, ani velký diskový prostor.

Cloud jako Amazon S3 však „slouží mnoha pánům“ a musí tak nabídnout excelentní výkon, spolehlivost a dostupnost. Společně s faktem, že Amazon také musí hardware nakoupit, udržovat, obnovovat, platit elektřinu a prostory způsobí, že cena za datový prostor dramaticky narůstá. To samé platí i pro specializované cloudy, jako je například Acronis Cloud, určený pro obnovu po katastrofě (\$799 za 500 GB/ročně). Jedním z hlavních důvodů v tomto případě je zajištění rychlého downloadu i uploadu pro všechny předplatitele.

Vše tedy záleží na konkrétních požadavcích. Pokud budeme zálohovat pouze 500 GB dat, vychází levněji využít Acronis Cloudu, než pořizovat a provozovat zálohovací server. Pokud se však začneme bavit o terabajtech dat, situace se rychle obrací.

Je tedy nutné si uvědomit, jaké máme požadavky a to, že pokud požadujeme špičkové služby, nemůžeme očekávat nízké ceny. V případě, že si však vystačíme s nižší funkcionalitou a výkonem, můžeme zálohováním na cloud ušetřit, neboť pokud k nákladům na nákup hardware připočteme správu, licence a elektřinu, online zálohování mnoha poskytovatelů vychází levněji.

4.2 Výkon a dostupnost

Výsledek srovnání výkonu a dostupnosti asi nikoho nepřekvapí. Vzhledem k tomu, že u cloudu do hry vstupuje internet, který může omezovat jak svojí dostupností, tak rychlostí, je jasným vítězem on-premise zálohování. Pokud totiž využijeme levných cloudových řešení, může obnova trvat až 1000x déle než lokální obnova.

Z tohoto důvodu je téměř nutné, abychom předtím než odešleme větší množství dat na cloud, data deduplikovali a zkomprimovali. Při obnově se pak projeví kvalita poskytovatele a rychlost uploadu, kterou je schopen poskytnout.

4.3 Shrnutí

Pokud bychom museli vyhlásit vítěze, bylo by jím on-premise zálohování. Cena zálohovacích cloudů, které jsou schopné výkonem konkurovat, je totiž výrazně vyšší. Vydat se cestou pouze cloudového zálohování tak dává smysl pouze v případě, kdy nám podmínky neumožňují zároveň zálohovat i on-premise (nedostatek prostoru), nebo pokud zálohujeme pouze malé množství dat.

Naštěstí toto srovnání nebylo o korunování vítěze. Cílem bylo poskytnout různé pohledy na ceny obou řešení a zdůraznit, že naše konkrétní požadavky hrají obrovskou roli.

Stejně tak je nutné vyzdvihnout skutečnost, že v ideálním případě jsou cloud i on-premise spojenci. Lokální záloha nám umožní rychlou a dostupnou zálohu, zatímco cloud kryje záda v případě, kdyby se cokoliv pokazilo.

Plán pro obnovu

V této kapitole si představíme, jakým způsobem se v dnešní době chrání data ve společnostech, aby byla zajištěna bezpečnost za jakékoliv situace. Na úvod se seznámíme s tím, co obnáší tvorba plánu pro obnovu (disaster recovery plan), neboť modely zálohování, kterými se budeme zabývat v další kapitole, jsou součástí těchto robustních řešení. Na konci kapitoly se potom nachází konkrétní případ využití na reálném zákazníkovi.

5.1 Tvorba plánu pro obnovu

V této části se podíváme na obecný postup při tvorbě plánů pro obnovu. Zjistíme tak, jak moc se komplexní ochrana dat před katastrofami (cokoliv, co naruší provoz firmy) liší od pouhého zálohování a podíváme se i na další výhody spojené se zavedením DRP¹³, které zvyšují návratnost investice (ROI). Inspirací a zdrojem informací pro tuto kapitolu mi byl ebook [62].

Vývoj v informačních technologiích jde stále kupředu a narůstá nejen výkon a efektivita, ale také množství rizik, neboť informační systémy jsou stále komplexnější a každá součást s sebou přináší nejen výhody, ale též určité nevýhody. Zákazníci navíc stále častěji požadují nepřetržitě fungující systémy bez výpadků, dlouhých načítání a chyb. Delší výpadky nebo výraznější ztráta dat jsou nemyslitelné.

Z tohoto důvodu nestačí pouze nějaký způsobem zálohovat data a tím si odškrtnout pomyslnou kolonku ochrana dat. Jedna věc je mít vytvořený plán zálohování. Druhá je mít jistotu, že záloha je obnovitelná a vědět, co vše je třeba obnovit podle velikosti havárie, a zajistit tak opětovný plný provoz systému.

K tomu je zapotřebí důkladná analýza prostředí celé společnosti, veškeré techniky, vazeb, povinnosti zaměstnanců atd. V této práci se nebudeme zabývat kompletní tvorbou plánu, neboť takto vzniklá dokumentace má několik

¹³Disaster Recovery Plan - plán pro obnovu po katastrofě.

desítek stran. Podíváme se však na některé otázky, které je potřeba si při tvorbě takového plánu položit a nahlédneme na různá řešení.

Jak již bylo naznačeno, zavedení ochrany před katastrofami předchází důkladná analýza a následné optimalizování současného stavu systému, infrastruktury apod., neboť nelze zavést kvalitní ochranu v prostředí, kde je spousta chyb, nejasností a zastaralý hardware. Tento fakt je mimo ochrany před pohromou dalším z důvodů, proč je investice do DRP výhodná.

Stává se opravdu velmi zřídka, že by měly společnosti kvalitně zpracovanou dokumentaci o svém businessu. Proto se nyní podíváme, co vše je zapotřebí zanalyzovat a zdokumentovat, pokud chceme zavést DRP.

Doplnil bych, že společnosti zpravidla nedisponují dostatečně kvalifikovaným personálem pro tuto práci. Proto se obracejí na externí firmy, které vše potřebné zařídí a následně po zavedení i spravují, jsou to takzvané MSP (Managed service provider). Ochrana před katastrofami, kterou provádí externí firma za měsíční poplatek pak říkáme DRaaS (Disaster Recovery as a Service - viz 2.2.5).

5.1.1 Analýza prostředí

Informace o společnosti

Dobrý zvykem na začátek dokumentace je uvést základní informace o společnosti. Například jméno, adresa, tel. kontakt, kontakt na vedení, stručný popis náplně práce společnosti atd.

Infrastruktura

Přehled o počtu serverů, počítačů, notebooků, tiskáren, externích disků atd. Po této hrubé analýze pak detailní informace o každém kusu HW - typ, sériové a modelové číslo, stáří, výrobce, informace o záruce, nastavení zálohování (pokud existuje), IP adresa aj. Není zapotřebí vše dělat manuálně, lze využít například nějakého RMM¹⁴ řešení.

Přístupová práva

Aby bylo možné zavést/zlepšit DR řešení, je zapotřebí mít přístup ke klíčovým systémům jako je emailový klient, cloud (pokud společnost využívá), routery, firewally, VPN a další. Samozřejmostí je tyto informace pečlivě chránit.

Kontakty na poskytovatele

V případě nouze může být zapotřebí kontaktovat například dodavatele elektřiny, internetu, telefonu apod. Je dobré mít tyto informace na jednom místě a vědět tak, kde je v případě potřeby hledat.

¹⁴Remote Monitoring and Management - kolekce nástrojů, které mimo jiné dokáží se zařízení získat spoustu informací a nastavení.

Vytvoření přehledu

Po posbírání výše uvedených bodů je vhodné vytvořit názorný přehled, mapu. V ní uvést veškeré závislosti, nastavení routerů, switchů atd. U počítačů uvést IP adresy, přístupová práva a veškeré klíčové informace. V případě potřeby tak zjistíme vše, co potřebujeme, pohledem oka.

Virtualizaci lze provést například pomocí programu Visio. K dokonalosti pak můžeme doplnit ještě o fotografie konkrétních zařízení.

Vyhodnocení aktuálního stavu

Po analýze je načase vyhodnotit současnou situaci a položit si důležité otázky, na základě kterých můžeme následně navrhnout optimální model zálohování. Příklady takovýchto otázek jsou:

- „Která zařízení by mohla být modernizována nebo se blíží hranici svojí životnosti a tím pádem je vysoké riziko jejich selhání?
- Která zařízení jsou nejkritičtější? Je možné se obejít bez souborového serveru či Exchange serveru?
- Které z klíčových zařízení snese výpadek? Jak dlouhý výpadek? Hodinu? Den?
- Kolik stojí hodina kompletně nefungující společnosti?
- Kolik stojí hodina nefunkčního klíčového zařízení?
- Jaké jsou závislosti? Které zařízení potřebuje ke svému chodu jiné? (zejména u klíčových zařízení)
- Jsou nějaké nedostatky v síti? Je vše nastaveno efektivně?
- Jsou nějaké možnosti využít cloudových řešení a ušetřit náklady? Jak je to s virtualizací? Jak tyto věci ovlivní zálohu a DRP?
- Kdo má na starosti IT problémy? Lze se na tuto osobu spolehnout, že v případě potřeby provede správné úkony?“ [62]

Často se stává, že společnost nezná odpověď na tyto otázky a je na osobě zodpovědné za zavedení DRP, aby je pomohla najít a navrhla i případné další optimalizace a doporučení.

5.1.2 Stanovení cílů a očekávání

Jakmile se klient seznámí s vytvořenou dokumentací, je načase zjistit jeho cíle a požadavky. Opět zde platí, že nemusí vždy vědět, co přesně chce, jaké jsou možnosti apod., a je proto dobré vždy navést správným směrem. Vzájemnému pochopení může napomoci i vhodná formulace otázek. Srozumitelné jsou například „scénářové“ otázky.

- Co byste dělali, kdybyste zítra ráno zjistili, že váš hlavní server neběží?

- Jak dlouho jste schopní fungovat bez něj?
- Jak produktivní mohou být vaši zaměstnanci?
- Co kdyby nefungovaly všechny vaše servery?

Pomocí těchto a dalších otázek zjistíme, co klient potřebuje/požaduje a na základě toho může být navrženo optimální řešení.

Nyní je doufám jasnější význam úvodní analýzy a dokumentace, neboť dokud detailně nerozumíme fungování a požadavkům klienta, nemůžeme rozhodnout, jak robustní řešení zvolit. DRP je navíc potřeba nasadit na dobře fungující prostředí a to se neobejde bez důkladné analýzy a případných optimalizací. Zadavatel navíc získává velmi cennou dokumentaci svojí společnosti a provedená analýza mu může pomoci v jeho dalším růstu.

5.1.3 Návrh řešení

V této části práce se zaměříme na tvorbu řešení. Blíže se podíváme nad čím vším je nutné se při návrhu komplexní ochrany dat zamyslet.

Nastavení zálohování

Jakmile se seznámíme s zařízeními, která má klient k dispozici, je zapotřebí učinit rozhodnutí, co se bude zálohovat a kam se záloha uloží. Má klient k dispozici NAS¹⁵ zařízení? Nebo využívá RAID pole? Bude se sám starat o zálohování, či je někdo bude spravovat vzdáleně? Budou data zálohována on-premise, na cloudu, či obojí? Pokud bude využito cloudu, jak dostupná budou tato data? Je možná virtualizovat záložní diskové obrazy na cloudu? Tyto a další otázky je důležité si položit a nalézt odpovědi vzhledem k finančním možnostem klienta a dostupnosti cloudových a dalších služeb.

Vzhledem k metodě 3-2-1 je vhodné využít jak on-premise zálohování, tak cloudu, neboť pokud společnost pracuje s větším množstvím dat, není reálné, aby si každý den bral někdo domů diskové pole s druhou zálohou. Na konkrétnější příklady a návrhy zálohování se podíváme v kapitole 6. Ať už ale zvolíme jakýkoliv model, opět vše zaznamenáme do vytvořené dokumentace, aby obsahovala aktuální informace.

Zařízení

V případě havárie je důležité mít k dispozici alespoň několik kusů záložních zařízení, neboť i dostupná záloha je k ničemu, pokud dojde k výboji a zničení několika počítačů a zaměstnanci nebudou mít na čem pracovat. Platí to i například pro routery, switche. Tato zařízení jsou dost poruchová a je rozhodně levnější rychle vyměnit zlobící router, než mít

¹⁵Network Attached Storage – datové úložiště na síti

na několik hodin oddělení bez internetu. Proto je vhodné mít alespoň pár záložních:

- Switchů a routerů
- Počítačů
- Pracovních stanic (notebooků)
- Mobilů
- Tiskáren
- Kabelů aj.

Cílem je redukovat závislost na funkčnosti jednotlivých zařízení a mít jistotu, že v případě potřeby jsou k dispozici náhradní a je tak možné bez velkých prostojů pokračovat v práci.

Pracovní stanoviště

Co bude klient dělat v případě požáru, povodně, kdy nebude možné chodit do standardního pracoviště? Málokterá společnost si může dovořit vlastnit externí pracovní plochu pro případ vážné havárie. Nicméně pro velké společnosti je toto opravdu věc ke zvážení, pokud je tolerance na delší výpadky minimální. Menší společnosti pak mohou sestavit plán, které hotely nabízí dostatečné připojení k internetu, či zda některá z partnerských společností by byla ochotná poskytnout krátkodobý azyl. Od věci nejsou ani velké obývací pokoje či suterény některého ze zaměstnanců. Důležité je mít za každé situace jistotu, že se business úplně nezastaví.

Elektrina

Elektrická energie vypadává z různých důvodů a nikdo se bez ní dlouhou dobu neobejde. Závislost na elektřině je opět u každé společnosti různá, některé mohou poslat své zaměstnance domů a nechat je pracovat z domova, jiné potřebují pracovníky na pracovišti. Zejména ty by pak měly zvážit nákup záložního generátoru pro případ delšího výpadku, zvláště pak, pokud se nacházejí v oblasti, kde častěji než jinde dochází k neplánovaným výpadkům.

Služby pro veřejnost

Přehlížet bychom neměli ani služby, které nás na první pohled nenapadnou, jako například call centra u větších společností. A zde je na místě vytvořit nějakou formu redundance. Externí centrum se může hodit nejen v případě, kdy padne telefonní linka, ale také během přírodních katastrof či přetížení. Opět navíc pracujeme na splnění požadavku o odstranění co nejvíce závislostí.

Přístup k internetu

Využití cloudu místo vlastního provozu Exchange serveru s sebou přináší úspory, nicméně roste závislost na připojení k internetu. Pokud navíc klient provozuje významnou část či dokonce celý business v cloudu, stává se dostupnost internetu kriticky důležitou. Abychom odstranili nebo alespoň minimalizovali takto velkou závislost, je nutné mít i minimálně druhého poskytovatele připojení.

Většina firewallů jde nastavit, aby při výpadku jednoho připojení došlo k aktivování záložního. Navíc lze druhého spojení využít při kopírování větších záloh na cloud.

Zaměstnanci

Stejně jako je vhodné mít několik kusů náhradního hardware, tak je důležité mít vycvičených více zaměstnanců, kteří budou schopni v případě havárie vykonat klíčové kroky k nápravě. Snadno se může stát, že IT administrátor nebude k dispozici a v rámci minimalizace závislosti je nutné, aby alespoň jeden další zaměstnanec měl přístupová práva a věděl, jak se zachovat.

Testování

Než se pustíme do testování, je zapotřebí aktualizovat dokumentaci, aby nyní reflektovala nově vytvořené řešení. Ideálně také pověřit několik zaměstnanců, aby do ní zaznamenávali veškeré změny, které v budoucnu nastanou.

Testování často bývá problém, neboť stojí peníze a mnoho společností raději doufá, že vše bude fungovat podle plánu. Pokud ale chceme mít jistotu, musíme testovat.

Vybereme čas, například po pracovní době či o víkendu a námi vytvořené řešení otestujeme. Zaznamenáme vše, co šlo dobře, co špatně, co by se dalo vylepšit. Případné změny pak opět zaevidujeme v dokumentaci.

Po přečtení této sekce je myslím každému jasná obrovská přidaná hodnota, kterou s sebou přináší DRP řešení. Klient získává nejen ochranu před všemi druhy katastrof, ale také velmi cennou dokumentaci vlastní společnosti a zároveň optimalizaci stávajícího businessu.

5.2 Ukázka využití na konkrétním příkladě

Abychom si uvedli alespoň krátký příklad, podíváme se, jak by se dala vyřešit momentálně problematická ochrana dat v malé zubní ordinaci. Na tomto případě si ukážeme několik důležitých věcí, na které je třeba si dát pozor.

5.2.1 Současný stav

V ordinaci běží počítač, který obsahuje:

- Záznamy o pacientech
- Aplikaci pro správu zubní ordinace (např. Dentrix¹⁶)
- Rentgenové snímky

Pan zubař na konci pracovní doby zazálohuje data na dva externí disky, jeden si odnese s sebou domů. Využívá tak model hot-swapping (více zde 6.3). Je však tento model v tomto případě dostačující? Není, pokud totiž dojde v odpoledních hodinách k selhání disku, ztratí veškeré záznamy provedené za daný pracovní den, navíc data obsahující tyto záznamy, musí být podle HIPPA šifrována (což nejsou). V opačném případě hrozí milionové pokuty.[63]

5.2.2 Řešení

Jak nejlépe tuto situaci vyřešit? Potřebujeme zajistit, aby data byla opravdu pečlivě chráněna a nedošlo k žádným ztrátám dat.

Zdokonalit současné on-premise zálohování jde například použitím StorageCraft ShadowProtect (součást StorageCraft Recover-Ability balíku - viz 3.1.3), a zajistit tak kompletní ochranu systému včetně všech dat a záznamů.

Vyřešit problematické offsite zálohování však není tak jednoduché. Každodenní nošení zálohy sice není až takový problém, nicméně data bylo nutné začít šifrovat, což by se negativně projevilo době zálohování. Je tedy možnost zálohovat na cloud, ačkoliv připojení k internetu je v ordinaci pouze 3Mbps download a upload pouze 512 Kbps?

Řešením je kontaktovat poskytovatele cloudu a odeslat mu disk se systémovým obrazem do cloudového datacentra. Tím se zbavíme nutnosti odesílat 100 GB počátečních dat po pomalém připojení. Poté lze již posílat pouze malé inkrementální zálohy. Lze dokonce nastavit, aby přes den byla data odesílána pomaleji, a přes noc pak byla linka využita naplno. Získáme tak mnohem aktuálnější offsite zálohu, a navíc se zbavíme starostí spojených s hot-swappingem.

Na závěr bych tedy dodal, že ochranu kritických dat nesmíme podceňovat, zejména pokud se jedná o citlivá data, která podléhají například HIPPA. V takovém případě za nedbalost hrozí i obrovské pokuty. Důležité je také se nezaleknout nepříznivých podmínek, jako je například pomalé připojení a snažit i tak najít co neideálnější řešení, kterou dané prostředí nabízí.

¹⁶více informací na <http://www.dentrix.com/>

Modely zálohování

V této sekci se budeme detailněji zabývat různými modely zálohování. Tyto modely vychází z toho, co má klient k dispozici, jakými finančními prostředky disponuje, a dalších faktorů. Každý model si popíšeme a podíváme se na jeho výhody a nevýhody. Bohatým zdrojem informací a nápadů mi byl ebook od společnosti StorageCraft[64].

6.1 Použití vlastního existujícího hardware

Často se stává, že společnosti mají již nakoupená různá zařízení, servery. Nebo se při optimalizaci pro DRP dojde k závěru, že je zapotřebí hlavní server modernizovat kvůli nedostatečnému výkonu. Pokud takový server, není příliš zastaralý, je možno ho využít jako BDR jednotku¹⁷.

Je však nutné počítat s tím, že životnost takového zařízení bude kratší, než pokud by se nově zakoupilo. Proto by měla společnost vzít na vědomí, že bude zapotřebí obnovit tento HW dříve.

Architektura: D2D

Výhody:

1. Využití nepoužívaného hardware
2. Levnější než nákup nového serveru či BDR zařízení
3. Lze nastavit, aby probíhala replikace i mimo pracoviště (offsite)

Nevýhody:

1. Méně spolehlivé než nový hardware
2. Bez offsite replikace nedodržíme metodu 3-2-1

¹⁷BDR jednotka je speciálně upravený server pro účely DRP. Obsahuje veškeré konfigurace zálohování, včetně replikace offsite. Zpravidla má i vlastní diskové pole pro on-premise zálohování.[65]

6.2 Zakoupení nového zálohovacího serveru

Pokud společnost žádným použitelným HW nedisponuje, je možností nákup nových zařízení. Zde však můžeme často narazit, neboť mnoho společností nemá či není ochotno dát relativně velkou sumu peněz na nové „železo“ nebo mají tak malé prostory, že není kde umístit takový HW. Pro druhou skupinu je pak pravděpodobně řešením zálohování na dva různé cloudy a disponování minimálně dvěma internetovými připojeními. První skupina může využít služeb MSP, kteří zpravidla BDR jednotky mají možnost půjčit.

Obrovskou výhodou, kterou s sebou přináší disponování BDR jednotkou je rychlost a dostupnost. Internetové připojení stále není takové úrovně, aby se vyrovnala rychlostem kopírování disků, vše máme navíc na dosah ruky. Kvalitní BDR jednotky nabízí i možnost virtualizace, takže v případě havárie a čekání na obnovu je možné záložní diskové obrazy spustit a pokračovat v práci.

Architektura: D2D

Výhody:

1. Jednoduché nastavení a správa
2. Robustní DRP řešení (virtualizace, dostupnost, replikace offsite)
3. Technická podpora (od MSP)

Nevýhody:

1. Velké počáteční náklady
2. Bez offsite replikace nedodržíme metodu 3-2-1

6.3 Hot-swapping

Ačkoliv název zní dost složitě, je vlastní metoda velmi jednoduchá. Trik spočívá v tom, že si po práci odneseme další zálohu s sebou domů. Je to nejlevnější řešení offsite zálohy, nicméně v praxi použitelné pouze pro společnosti, jejichž zálohy se vejdou na rozumný počet pevných disků.

Velmi vhodné je takové disky zašifrovat, pro případ ztráty nebo krádeže. Pokud záloha obsahuje data zákazníků, je to dokonce nutné. Toto řešení je navíc komplikované, neboť záloha není okamžitě dostupná a v případě potřeby je pro ná nutné dojet. Navíc přicházíme o data ze dne havárie.

Architektura: D2D2D

Výhody:

1. Jednoduchá forma offsite zálohy
2. Nejlevnější řešení

Nevýhody:

1. Složitá obnova

2. Omezené možnosti zálohování
3. Nutnost denního přenášení záloh

6.4 Replikace na vlastní pobočku

Toto řešení může být velmi výhodné pro větší společnosti, které mají více poboček či různé partnery. Mohou si vzájemně prokázat laskavost a uchovávat offsite zálohy jeden druhému. Toto řešení je jedno z těch dražších, neboť bude pravděpodobně zapotřebí přikoupit další disková pole či zálohovací jednotky. Nicméně se tím odbourává závislost na poskytovateli cloudu a data má společnost plně pod kontrolou.

Architektura: D2D2D

Výhody:

1. Jednoduché a efektivní řešení
2. Snadné nastavení a provoz
3. Není zapotřebí využití cloudu

Nevýhody:

1. Vyšší cena
2. Obnova není okamžitá

6.5 Replikace na obecný cloud

Obecným cloudem mám na mysli jeho servisní model IaaS. Tedy pouze jako vzdálené infrastruktury, bez speciálního přizpůsobení pro zálohování.

Jak jsme si již uvedli v kapitole o cloudech, je takovýchto poskytovatelů široké spektrum. Je však třeba mít na paměti, že jsme závislí nejen na rychlosti našeho připojení, ale také na uploadu poskytovatele a obnova tak bude pravděpodobně trvat déle, než u cloudů specializovaných na zálohování. Tato volba proto není nejvhodnější, pokud usilujeme o co nejnižší RTO a RPO.

Architektura: D2D2C

Výhody:

1. Geograficky různorodá offsite záloha
2. Obvykle vcelku levné řešení

Nevýhody:

1. Zpravidla nemožné splnit agresivní RTO a RPO
2. Menší kontrola nad daty
3. Závislost na třetí straně v případě katastrofy

6.6 Replikace na speciální zálohovací cloud

Velkou výhodou „zálohovacích cloudů“ je připravenost splnit i velmi přísné hodnoty RTO a RPO a jsou proto (zejména pokud požadujeme co nejrychlejší obnovy) skvělou volbou.

Kopírování na tyto cloudy je velmi snadné a drtivá většina je připravená během několika okamžiků virtualizovat naše diskové obrazy. Pokud klient disponuje rychlým připojením k internetu a finance nejsou velmi omezující faktor, je toto řešení většinou nejideálnější. V dnešní době není lepší ochrany než rychle dostupná on-premise záloha zkombinovaná s kvalitním zálohovacím cloudem, který nabízí excelentní parametry a špičkovou podporu.

Architektura: D2D2C

Výhody:

1. Rychlá offsite obnova
2. Geograficky různorodá záloha
3. Mnoho možností zálohování a excelentní podpora

Nevýhody:

1. Vysoká cena
2. Nemáme 100% kontrolu nad daty

6.7 Replikace z cloudu zpět on-premise

I takováto situace může nastat a dokonce je stále běžnější. Jak zajistit ochranu dat u společností, kterým jejich business běží v cloudu? Odpovědí je záloha zpět on-premise.

Mohli bychom data pouze replikovat k jinému poskytovateli cloudu, nicméně to nám stále nezajistí bezpečný počet tří kopií, a navíc není nad to mít kritickou část svého businessu „u sebe“. Nezáleží tedy, zda budeme v cloudu či on-premise, princip je stále stejný, pouze se změní směry, kterými proudí zálohy. Data tedy z provozního cloudu zazálohujeme na zálohovací cloud, odsud potom zreplikujeme zpět on-premise.

Pro 100 % virtuální společnosti bez poboček je pak řešením využití dvou nezávislých poskytovatelů cloudového zálohování, více v předchozím řešení.

Architektura: C2C2D

Výhody:

1. Máme pojištěný business on-premise
2. Nejsme odkázáni pouze na třetí strany

Nevýhody:

1. Vysoké náklady na pořízení

2. Nutnost spravovat on-premise jednotku

6.8 Archivační model

Asi si kladete otázku, co k čertu dělá archivace u modelů zálohování, když jsme si navíc v teoretické části zdůraznili rozdíly mezi oběma pojmy. Možná vás to překvapí, ale i archivace má své místo v business zálohování.

Podívejme se na příklad. Zaměstnanec chce editovat databázi, která byla delší dobu nepoužívaná. Vyskočí však hláška, že databáze je poškozená a nelze otevřít. Zkopíruje databázi z nejnovější zálohy, avšak stále chybová hláška. Obnoví tedy soubor z nejstarší, 14 dní staré zálohy, ale stále chyba. Databáze je ztracena.

Můžeme si tedy všimnout, že ani model 3-2-1 není neprůstřelný, pokud zároveň neuchováváme i staré zálohy. K čemu nám jsou tři kopie souboru, pokud jsou všechny poškozené.

Řešením je zachovávat například měsíční úplné zálohy. K tomu však není vhodné využívat výkonných zálohovacích cloudů, neboť k takovýmto zálohám bude přistupovat pouze zřídka a toto řešení je pro takový účel příliš drahé. Mnohem vhodnější je využít nízko-nákladové cloudy určené pro archivaci (například Amazon Glacier). Máme tak možnost využít i staré databáze a dokumenty, které již aktivně nevyužíváme, nebo se nepozorovaně ztratí či poškodí.

Výhody:

1. Levná, dlouhodobá pojistka dat
2. Výhodnější, než uchovávat vše na zálohovacím cloudu

Nevýhody:

1. Pomalá obnova
2. Samotná archivace nám nezajistí dostatečnou ochranu

6.9 Shrnutí

Návrh modelu zálohování závisí na spoustě faktorů. Jedním z hlavních jsou finanční možnosti společnosti, požadovaná dostupnost, současný stav infrastruktury, zda je systém provozován on-premise či v cloudu atd. Nelze tedy paušálně prohlásit, který model je nejlepší.

Optimální model je takový, který splní požadavky a současně je ekonomicky nejvýhodnějším. V ideálním případě také splňuje metodu 3-2-1 doplněnou o archivaci starých záloh na archivační cloud. V takovém případě máme jistotu, že jsou naše data chráněna za každé situace.

Na základě těchto modelů jsem vytvořil průvodce, který umožňuje odhadnout optimální zálohovací model, viz následující kapitola.

Průvodce modely zálohování

Učinit rozhodnutí, kterou cestou se při zálohování vydat není vůbec jednoduché. Jak již víme z předchozích kapitol, zajistit komplexní ochranu businessu není práce na jedno odpoledne a je zapotřebí důkladně zanalyzovat současný stav a minimalizovat co největší počet závislostí.

Pokud se však omezíme pouze na model zálohování, lze na základě „zjednodušené“ analýzy odhadnout, který z modelů je pravděpodobně nejvhodnější. Se stoprocentní jistotou to samozřejmě říct nelze, nicméně pokud se nějaké menší firma o pár zaměstnancích nachází v odlehlé lokalitě, kde není ani přístup k internetu, je jasné, že nebude zálohovat na cloud. Stejně tak velká společnost s obrovským množstvím dat nepoužije model hot-swapping, neboť by to znamenalo pravidelně přesouvat celá disková pole, což je mírně řečeno nepraktické.

Díky znalostem a zkušenostem získaných během vypracovávání práce jsem tak byl schopen naprogramovat v jazyce Java průvodce, který na základě odpovědí sady otázek vyhodnotí nejvhodnější model.

Samotný průvodce vyžaduje po uživateli pouze minimální technické znalosti a předpokládá zejména znalost prostředí společnosti, pro kterou je model navrhován.

7.1 Vývoj průvodce

Jako implementační jazyk jsem zvolil Javu, neboť na rozdíl od „programování“ v MS Excel, či jiném editoru, který umožňuje vytváření „formulářových“ programů, Java nabízí široké množství funkcí a zejména možnost přizpůsobit program specifickým potřebám. Pro vývoj aplikace jsem využil vývojového prostředí Netbeans IDE, které velmi usnadňuje programování.

Při implementaci průvodce jsem se po designové stránce zaměřil na „čistý“ a jednoduchý vzhled, kde každá část programu má svůj účel a vše je jasné a přehledné. K návrhu jsem využil designové prostředí, které je součástí Netbe-

ans a je v podstatě WYSIWYG¹⁸ alternativou ke klasickému programování vzhledu. Této možnosti jsem využil zejména proto, že s programováním designu v Javě nemám velké zkušenosti.

Jak jsem již naznačil, průvodce se skládá ze série otázek, které se týkají současného stavu sledované společnosti a očekávání od navrhovaného řešení. Na otázky se odpovídá formou volby z nabídky odpovědí.

Povinné otázky mají předvyplněné hodnoty a nezměnění této odpovědi znamená souhlas s touto přednastavenou odpovědí. Pokud uživatel nezná odpověď na tuto otázku, musí se pokus alespoň odhadnout.

Nepovinné otázky nemají nastavenou počáteční hodnotu a není nutné na ně odpovídat. Po „rozbalení“ odpovědi je možné nechat políčko prázdné nebo i odpověď vrátit zpět na nevyplněnou. Nicméně se tím uživatel připraví o další zhodnocení a doporučení, která by jinak měl dostupná v závěrečném vyhodnocení.

Program je také navrhnout tak, aby byl snadno rozšiřitelný a upravitelný. Není velkým problémem přidat novou otázku, či zaktualizovat výběr odpovědí. Stejně tak zdokonalení odpovědí, či algoritmu pro vyhodnocení, je snadné.

Jednou z dalších vlastností průvodce je i „samostatnost“, není nutné za každou cenu znát obsah práce, aby byl uživatel schopen pochopit, k čemu program slouží a co se od něj očekává.

7.2 Návod k použití

Přestože je průvodce velmi intuitivní, stručně si nyní projdeme jednotlivými kroky a vysvětlíme konkrétní části. Průvodce je JAR soubor a ke spuštění je tak nutné mít v počítači nainstalovanou Javu, konkrétně JRE¹⁹. JRE lze stáhnout z oficiálních stránek²⁰. Vyplněný průvodce na základě konkrétního příkladu je k nalezení v příloze C.

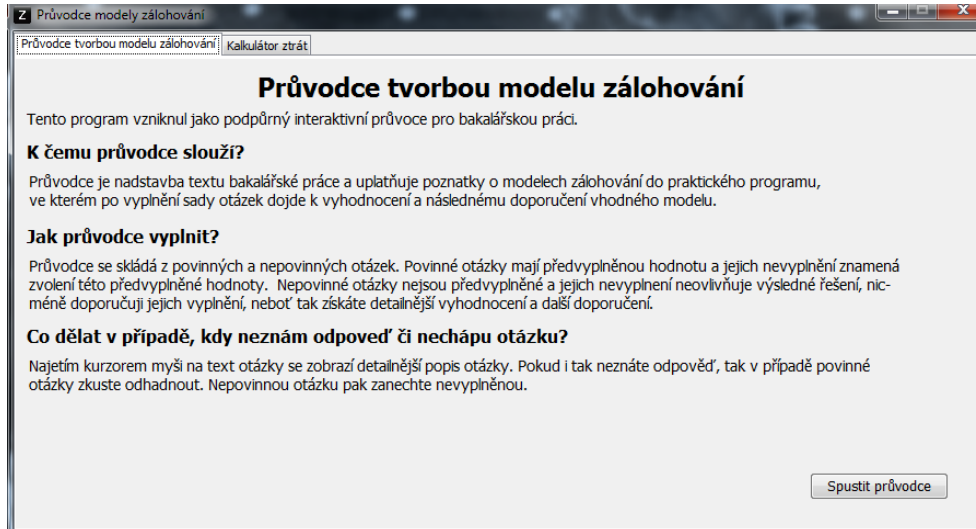
Úvodní strana průvodce (viz 7.1) obsahuje popis aplikace. Tato část je zejména uživateli, kteří neznají celou práci a nevědí, co přesně od programu čekat. Po kliknutí na tlačítko *Spustit průvodce* se zobrazí první část.

V první části je uživatel dotazován na současnou infrastrukturu ve společnosti (obrázek 7.2). Zde pravděpodobně není moc nad čím přemýšlet, jedná se o opravdu základní otázky týkající se počtu serverů, počítačů a rychlosti připojení k internetu. Pokud uživatel odpoví, že společnosti disponuje servery (jedním a více), objeví se ještě tlačítko s nápisem *Upřesnit odpověď*, kde je dotázán na doplňující otázky. Ty se ptají, zda některý z těchto serverů je určený pro zálohování, případně funguje jako Exchange či emailový server. Pokud ano, objeví se ještě dotaz na stáří nejnovějšího z těchto serverů, viz obrázek 7.3.

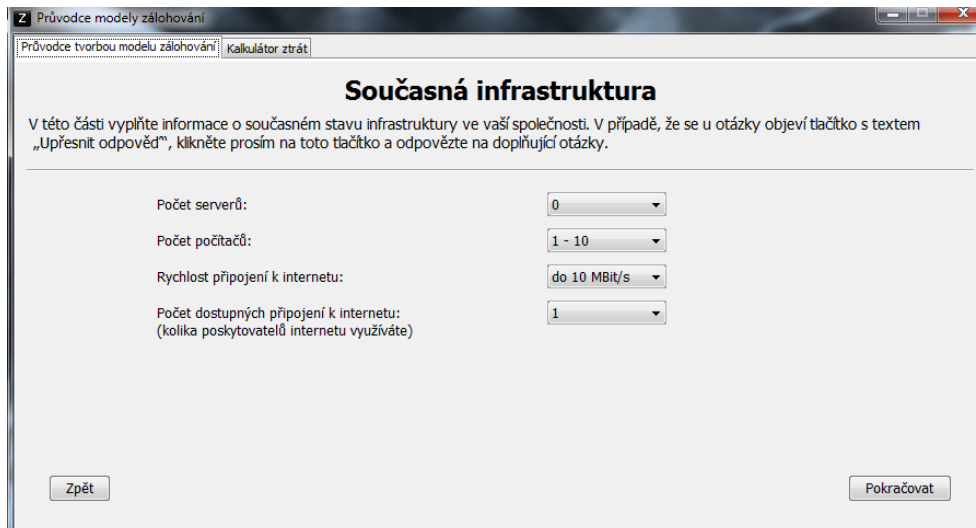
¹⁸What You See Is What You Get - co vidíš, to dostaneš

¹⁹Java Runtime Environment

²⁰<http://www.java.com/en/download/>

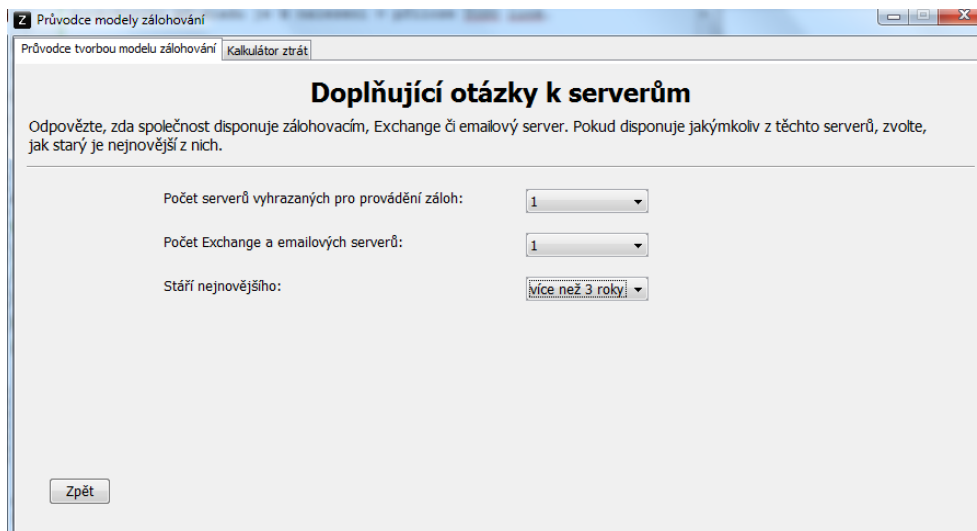


Obrázek 7.1: Úvodní obrazovka průvodce



Obrázek 7.2: První část průvodce

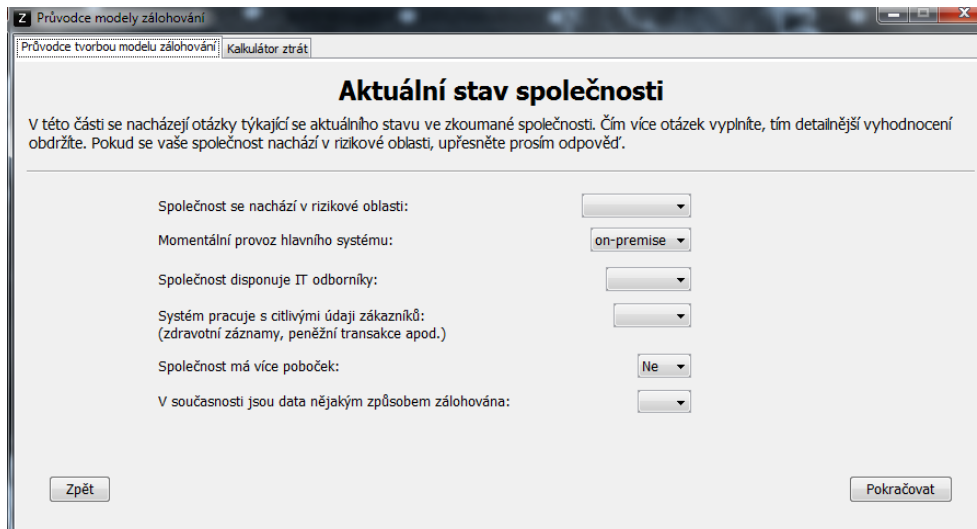
7. PRŮVODCE MODELY ZÁLOHOVÁNÍ



The screenshot shows a window titled 'Průvodce modely zálohování' with a sub-tab 'Průvodce tvorbou modelu zálohování' and a 'Kalkulátor ztrát' button. The main heading is 'Doplňující otázky k serverům'. Below the heading is a paragraph: 'Odpovězte, zda společnost disponuje zálohovacím, Exchange či emailový server. Pokud disponuje jakýmkoliv z těchto serverů, zvolte, jak starý je nejnovější z nich.' There are three dropdown menus: 'Počet serverů vyhrazených pro provádění záloh:' with value '1', 'Počet Exchange a emailových serverů:' with value '1', and 'Stáří nejnovějšího:' with value 'více než 3 roky'. A 'Zpět' button is at the bottom left.

Obrázek 7.3: Doplňující otázky k serverům

Druhá část se týká aktuálního stavu společnosti (obrázek 7.4). Otázky jsou z větší části nepovinné a na jejich zodpovězení není závislý návrh výsledného řešení. Například společnost, které nezaměstnávají žádné IT odborníky, je doporučeno přenechat správu zálohování třetí straně (MSP). Na druhou stranu, zda společnost má i další pobočky, je klíčová informace, neboť replikace dat napříč pobočkami je zajímavá alternativa ke cloudu jako offsite záloze.



The screenshot shows a window titled 'Průvodce modely zálohování' with a sub-tab 'Průvodce tvorbou modelu zálohování' and a 'Kalkulátor ztrát' button. The main heading is 'Aktuální stav společnosti'. Below the heading is a paragraph: 'V této části se nacházejí otázky týkající se aktuálního stavu ve zkoumané společnosti. Čím více otázek vyplníte, tím detailnější vyhodnocení obdržíte. Pokud se vaše společnost nachází v rizikové oblasti, upřesněte prosím odpověď.' There are six dropdown menus: 'Společnost se nachází v rizikové oblasti:', 'Momentální provoz hlavního systému:' with value 'on-premise', 'Společnost disponuje IT odborníky:', 'Systém pracuje s citlivými údaji zákazníků: (zdravotní záznamy, peněžní transakce apod.)', 'Společnost má více poboček:' with value 'Ne', and 'V současnosti jsou data nějakým způsobem zálohována:'. There are 'Zpět' and 'Pokračovat' buttons at the bottom.

Obrázek 7.4: Druhá část průvodce

Poslední část se zabývá cíli a očekáváními od navrhovaného řešení (obrá-

zek 7.5). První otázka je povinná a týká se požadované dostupnosti systému. Kliknutí na tlačítko *Upřesnit odpověď* přesune do upřesňující karty (obrázek 7.6). Zde uživatel musí vyplnit přibližnou požadovanou dostupnost a může specifikovat hodnoty RTO a RPO.

V třetí části jsou pak dále otázky týkající se cloudů - preference škálovatelnosti a upřednostnění nižších vstupních nákladů na úkor provozních. Finanční stránku pak završuje otázka - Finanční možnosti. Zde je doporučeno, zejména pokud se chystáte zvolit odpověď *Co nejnižší cena*, využít Kalkulátoru ztrát, do kterého se lze, bez ztráty vyplněných odpovědí, přepnout kliknutím na stejnojmennou kartu v levém rohu.

Obrázek 7.5: Třetí část průvodce

Kalkulátor (obrázek 7.7) umožňuje odhadnout ztráty, způsobené výpadkem systému nebo jinou komplikací, která znemožní určité části zaměstnanců pracovat. Stejně jako u průvodce, i zde je možné při neúplném pochopení otázky možné najet kurzorem myši na text a objeví se přeformulovaná, či detailněji vysvětlená otázka. Na rozdíl od průvodce jsou však všechna pole povinná, a nelze tak žádné vynechat, v opačném případě se po kliknutí na tlačítko *Vypočítat* objeví chybová hláška. Stejně tak v případě, kdy do pole uživatel zadá nečíselné, či jinak nesmyslné odpovědi. Po vyplnění a odkliknutí, se v posledním řádku objeví výsledná hodnota. S tou pak lze dále nakládat a uvědomit si, že pokud takové výpadky společnost trápí častěji do roka, vyplatí se investovat do kvalitnějšího řešení, neboť se tato investice vrátí ve zvýšení dostupnosti.

Po ujasnění, kolik financí chce společnost do řešení investovat, už pak pouze stačí kliknout na tlačítko *Vyhodnotit průvodce* a prohlédnout si vyhodnocené řešení. V našem případě, kdy jsme vše nechali nevyplněné či na předvypl-

7. PRŮVODCE MODELY ZÁLOHOVÁNÍ

Doplňující otázky k dostupnosti systému

Vyberte prosím, jakou očekáváte od systému dostupnost. Berte na vědomí, že čím vyšší, tím robustnější model je zapotřebí. Nicméně menší dostupnost znamená častější downtime. S naceněním downtime vám může pomoci Kalkulátor ztrát.

Požadovaná dostupnost systému: alespoň 95%

Požadované RTO:

Požadované RPO:

Obrázek 7.6: Doplňující otázky k dostupnosti

Kalkulátor ztrát

Kalkulátor ztrát složí k odhadu ztrát, způsobených výpadkem systému či jinými komplikacemi. Umožňuje tak přesněji odhadnout, kolik investovat do zálohování a obecně do ochrany před katastrofami, neboť máme srovnání se ztrátami, kterým budeme čelit, pokud tuto ochranu zanedbáme.

Po vyplnění příslušných polí a stisknutí tlačítka „Vypočítat“ dojde k zobrazení výsledku. V případě nejasností, co které pole znamená, je možné najet na text myši a zobrazit podrobnější popis.

Počet zaměstnanců: Hrubý roční příjem společnosti: CZK

Průměrná hodinová sazba zaměstnanců: CZK Otevřeno dní v roce:

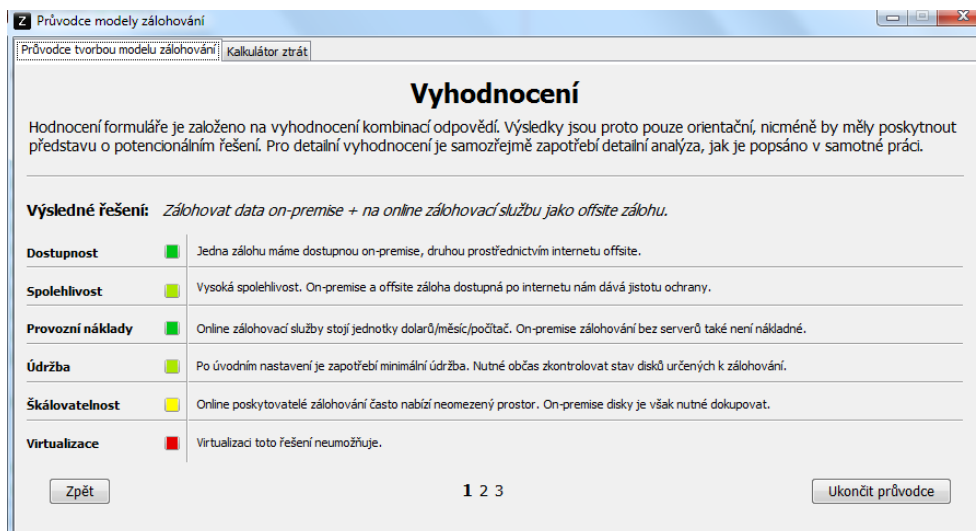
Průměrná ztráta produktivity: Otevřeno hodin denně:

Trvání výpadku (v hodinách): Měna: CZK

Celková cena výpadku:

Obrázek 7.7: Nevyplněný kalkulačtor ztrát

něných hodnotách, pak vyjde řešení *Zálohovat data on-premise + na online zálohovací službu jako offsite zálohu*. (obrázek 7.8).



Obrázek 7.8: Řešení průvodce při defaultních hodnotách

Proč vyšlo zrovna toto řešení? Zejména kvůli nulovému počtu serverů, nízkému počtu počítačů a žádosti o co nejlevnější řešení. Ačkoliv internetové připojení není moc rychlé, tudíž úvodní zálohování bude celkem dlouho trvat. Další zálohy už však budou většinou menší objemy dat, takže pomalejší připojení už nebude takový problém.

Toto vyhodnocení odpovídá například freelancerovi²¹ z menšího města. Nemá žádný server, pouze svůj počítač a chce mít jistotu, že jsou jeho data chráněna, a nepříjde tak o svou práci v případě selhání disku nebo pádu operačního systému. Online zálohovací služba mu bude průběžně zálohovat data, zároveň má data k dispozici i na zvláštním pevném disku pro rychlé obnovení.

7.3 Rozšíření programu

Webové aplikace jsou čím dál více populárnější. Má to své důvody, jsou dostupné odkudkoli prostřednictvím internetu a není nutné nic stahovat ani instalovat. Zde je potenciál růstu průvodce - transformace na webovou aplikaci.

I po designové stránce by mohl program vypadat atraktivněji, zvolil jsem pouze jednoduchý funkční design, neboť vytvářet graficky atraktivní řešení nebylo cílem práce.

Otázky a algoritmus řešení také nabízí prostor k vylepšení, a potenciální vyšší verze programu by mohla nabízet bohatší sadu otázek, a ještě přesnější výpočet řešení.

²¹programátor na volné noze

7. PRŮVODCE MODELÝ ZÁLOHOVÁNÍ

Cílem této kapitoly bylo představit průvodce, popsat jeho funkcionalitu, silné a slabé stránky a v neposlední řadě také poskytnout referenci pro případ nejasností při vyplňování. Na tuto kapitolu volně navazuje příloha C, ve které je průvodce vyplněn na základě údajů konkrétní společnosti.

Závěr

Problematika firemního zálohování je velice široké a obsáhlé téma. Pokud do hry navíc vstoupí cloud computing, virtualizace, a další moderní technologie, je velmi snadné se mezi spoustou informací a nabídkami různých poskytovatelů ztratit.

Hlavním účelem práce je pomoci zorientovat se v této oblasti a umožnit i méně technicky znalým čtenářům pochopit význam zálohování. Aby mohl být tento cíl naplněn, byly čtenáři od základů vysvětleny jednotlivé pojmy, principy a nástroje. Na těchto poznatkách pak bylo dále stavěno v navazující kapitole o poskytovatelích cloudového zálohování a při tvorbě modelů zálohování.

Cílem práce bylo vytvoření těchto modelů, které budou různým způsobem kombinovat on-premise a cloudové zálohování. Každý model je charakteristický svými silnými a slabými stránkami, vstupními a provozními náklady, náročností na údržbu atd. Výběr vhodného modelu pak usnadňuje druhý z cílů této práce, interaktivní průvodce. Podle sady otázek se mi podařilo vytvořit algoritmus, který uživateli doporučí vhodný model.

Vzhledem k rozsáhlosti problematiky by některé části práce mohly být v budoucnu rozšířeny. Zejména trh s poskytovateli cloudového zálohování se dramaticky rozrůstá, a rozsáhlejší a detailnější analýza by umožnila lépe se mezi nimi zorientovat a vybrat nejvhodnějšího poskytovatele na základě specifických požadavků. Prostorem pro zlepšení disponuje také průvodce modely zálohování. Na atraktivnosti by mu přidal například líbivější design, či implementace ve formě webové aplikace.

Zpracování práci mi umožnilo důkladně se seznámit s problematikou zálohování a cloud computingu. Navíc jsou to oblasti, které stále nabývají na popularitě a proto věřím, že získané znalosti v budoucnu dále uplatním.

Použité zdroje

- [1] O IDC. [online], [cit. 2015-02-25]. Dostupné z: <http://idc-czech.cz/cze/o-idc/predstaveni-spolecnosti>
- [2] Executive Summary: Data Growth, Business Opportunities, and the IT Imperatives. [online], [cit. 2015-02-25]. Dostupné z: <http://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm>
- [3] Rouse, M.: Backup. [online], [cit. 2015-02-24]. Dostupné z: <http://searchstorage.techtarget.com/definition/backup>
- [4] Rouse, M.: Data archiving. [online], [cit. 2015-02-24]. Dostupné z: <http://searchdatabackup.techtarget.com/definition/data-archiving>
- [5] Rouse, M.: Restore. [online], [cit. 2015-02-24]. Dostupné z: <http://searchdatabackup.techtarget.com/definition/restore>
- [6] Weisman, R.: What's the Real Difference Between Data Archives and Backup Data? [online], March 2015, [cit. 2015-03-20]. Dostupné z: <http://www.storagecraft.com/blog/difference-data-archives-bdr-data/>
- [7] Co je Disaster Recovery? [online], [cit. 2015-03-01]. Dostupné z: <http://www.disaster-recovery.cz/disaster-recovery>
- [8] Understanding Backup Methods 2. [online], [cit. 2015-02-25]. Dostupné z: <http://www.genie9.com/Support/KB/KnowledgeArticle.aspx?KBID=105>
- [9] Backup Types. [online], [cit. 2015-02-26]. Dostupné z: <http://www.dpbestflow.org/backup/backup-types>
- [10] Backup types. [online], [cit. 2015-02-26]. Dostupné z: <http://www.backup4all.com/kb/backup-types-115.html>

- [11] RAID Modes. [online], [cit. 2015-03-03]. Dostupné z: <http://www.seagate.com/gb/en/manuals/network-storage/business-storage-nas-os/raid-modes/>
- [12] Average Cost of Hard Drive Storage. [online], [cit. 2015-03-17]. Dostupné z: <http://www.statisticbrain.com/average-cost-of-hard-drive-storage/>
- [13] The SSD Endurance Experiment: Casualties on the way to a petabyte. [online], June 2014, [cit. 2015-04-12]. Dostupné z: <http://techreport.com/review/26523/the-ssd-endurance-experiment-casualties-on-the-way-to-a-petabyte>
- [14] Kapacita flash přeloží dramaticky vzroste - na trh má nově 3D NAND Typy - díky spolupráci Intelu a Micronu. [online], [cit. 2015-04-09]. Dostupné z: http://computerworld.cz/hardware/kapacita-flash-ulozist-dramaticky-vzroste-na-trh-miri-nove-3d-nand-cipy-51901?utm_source=rss&utm_medium=web&utm_campaign=rss
- [15] SSD price per GB drops. [online], [cit. 2015-04-12]. Dostupné z: <http://www.myce.com/news/ssd-price-per-gb-drops-below-0-50-how-low-can-they-go-70703/>
- [16] FujiFilm achieves 154TB data storage record on Tape. [online], May 2014, [cit. 2015-04-15]. Dostupné z: <https://storageservers.wordpress.com/2014/05/20/fujifilm-achieves-154tb-data-storage-record-on-tape/>
- [17] FujiFilm achieves 154TB data storage record on Tape. [online], April 2015, [cit. 2015-04-17]. Dostupné z: <https://storageservers.wordpress.com/2015/04/11/ibm-and-fujifilm-to-fit-220tb-data-on-single-tape-cartridge/>
- [18] Tape backup vs disk backup. [online], January 2010, [cit. 2015-04-19]. Dostupné z: <http://www.computerweekly.com/podcast/Tape-backup-vs-disk-backup>
- [19] New Life for Magnetic Tape. [online], January 2010, [cit. 2015-04-19]. Dostupné z: <http://www.technologyreview.com/news/417218/new-life-for-magnetic-tape/>
- [20] M-Disc. [online], [cit. 2015-04-20]. Dostupné z: <http://www.czmdisc.cz/>
- [21] Which Hardware Fails the Most and Why. [online], [cit. 2015-03-21]. Dostupné z: <http://www.storagecraft.com/blog/hardware-failure/>

-
- [22] The Cautionary Tale of Code Spaces. [online], [cit. 2015-03-22]. Dostupné z: <http://mspmentor.net/infocenter-cloud-based-file-sharing/062714/cautionary-tale-code-spaces>
- [23] One year after Sandy, 9 devastating facts. [online], [cit. 2015-03-23]. Dostupné z: <http://www.usatoday.com/story/news/nation/2013/10/29/sandy-anniversary-facts-devastation/3305985/>
- [24] Levkina, M.: How to follow the 3-2-1 backup rule with Veeam Backup & Replication. [online], January 2014, [cit. 2015-03-15]. Dostupné z: <http://www.veeam.com/blog/how-to-follow-the-3-2-1-backup-rule-with-veeam-backup-replication.html/>
- [25] D2D2T Strategy. [online], [cit. 2015-05-07]. Dostupné z: <http://blog.open-e.com/d2d2t-a-disk-to-disk-to-tape-backup-strategy/>
- [26] Disk-to-disk-to-tape. [online], [cit. 2015-05-07]. Dostupné z: <http://www.slideshare.net/VeeamSoftware/core-technologies-used-for-vm-backup-by-eric-siebert-backup-academy>
- [27] Wendt, J. M.: D2D2D is Practical, Possible. [online], December 2010, [cit. 2015-05-07]. Dostupné z: <http://www.d cig.com/2010/12/d2d2d-is-practical-possible.html>
- [28] Morgan, C.: Donâ€™t Let a Disaster Be Your First Backup Test. [online], [cit. 2015-05-09]. Dostupné z: <http://www.storagecraft.com/blog/download/recover-ability-guides/Dont-let-your-disaster-be-your-first-backup-test-final.pdf>
- [29] Full-disk encryption (FDE). [online], [cit. 2015-04-22]. Dostupné z: <http://whatis.techtarget.com/definition/full-disk-encryption-FDE>
- [30] Windows Server Backup Overview. [online], [cit. 2015-05-08]. Dostupné z: <https://technet.microsoft.com/en-us/library/cc772523.aspx>
- [31] Windows Server Backup Feature Overview. [online], [cit. 2015-05-08]. Dostupné z: <https://technet.microsoft.com/en-us/library/jj614621.aspx>
- [32] AhsayOBM Corporate profile. [online], [cit. 2015-04-20]. Dostupné z: http://www.ahsay.com/jsp/en/home/index.jsp?pageContentKey=ahsay_about-us_corporate-profile
- [33] AhsayOBM pricing. [online], [cit. 2015-04-20]. Dostupné z: http://www.ahsay.com/jsp/en/home/index.jsp?pageContentKey=ahsay_products_ahsayobm_pricing

- [34] Ahsay Overview. [online], [cit. 2015-04-20]. Dostupné z: http://www.ahsay.com/jsp/en/home/index.jsp?pageContentKey=ahsay_products_overview
- [35] Vembu BRD Features. [online], [cit. 2015-04-20]. Dostupné z: <https://www.vembu.com/about-us/>
- [36] Vembu BRD Features. [online], [cit. 2015-04-20]. Dostupné z: <https://www.vembu.com/features/bdr/>
- [37] Vembu Buy. [online], [cit. 2015-04-21]. Dostupné z: <https://www.vembu.com/buy/>
- [38] Vembu Buy. [online], [cit. 2015-04-21]. Dostupné z: <https://www.vembu.com/try/>
- [39] Co je cloud computing? [online], [cit. 2015-03-19]. Dostupné z: <http://cloud.cz>
- [40] Cloud Computing. [online], [cit. 2015-03-19]. Dostupné z: <http://www.gartner.com/it-glossary/cloud-computing>
- [41] The NIST Definition of Cloud Computing. [online], [cit. 2015-03-19]. Dostupné z: <http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf>
- [42] Janssen, C.: Measured Service. [online], [cit. 2015-03-14]. Dostupné z: <http://www.techopedia.com/definition/14469/measured-service-cloud-computing>
- [43] NEC and Corning achieve petabit optical transmission. [online], [cit. 2015-04-22]. Dostupné z: <http://optics.org/news/4/1/29>
- [44] Kumar, N.: Advantages and Disadvantages of SaaS. [online], December 2012, [cit. 2015-04-23]. Dostupné z: <http://theprofessionalspoint.blogspot.cz/2012/12/advantages-and-disadvantages-of-saas.html>
- [45] Taylor, C.: Backup as a Service: To BaaS or Not to BaaS. [online], November 2014, [cit. 2015-04-24]. Dostupné z: <http://www.datamation.com/cloud-computing/backup-as-a-service-to-baas-or-not-to-baas-1.html>
- [46] Understanding RPO and RTO. [online], [cit. 2015-03-13]. Dostupné z: <http://www.druva.com/blog/understanding-rpo-and-rto/>
- [47] Veeam Customer Success Stories. [online], [cit. 2015-04-02]. Dostupné z: <http://www.veeam.com/success-stories.html>

-
- [48] Veeam Availability Suite v8. [online], [cit. 2015-04-02]. Dostupné z: <http://www.veeam.com/data-center-availability-suite.html>
- [49] Veeam Availability Suite Features. [online], [cit. 2015-04-02]. Dostupné z: <http://www.veeam.com/availability-suite-features.html>
- [50] Nance, B.: Acronis Backup Advanced vs. Veeam Availability Suite. [online], [cit. 2015-05-09]. Dostupné z: <http://www.networktestinglabs.com/ABA-vs-Veeam.html>
- [51] Acronis Backup Advanced suite. [online], [cit. 2015-03-29]. Dostupné z: <http://www.acronis.com/en-us/business/backup-advanced/>
- [52] About StorageCraft Technology Corporation. [online], [cit. 2015-04-20]. Dostupné z: <https://www.storagecraft.com/about>
- [53] StorageCraft Recover-Ability. [online], [cit. 2015-04-23]. Dostupné z: <https://www.storagecraft.com/sites/default/files/pdf/StorageCraft-Recover-Ability-Overview-DRA1114EN.pdf>
- [54] StorageCraft Recover-Ability. [online], [cit. 2015-04-23]. Dostupné z: <https://www.storagecraft.com/documents/StorageCraft-Cloud-Services-Frequently-Asked-Questions.pdf>
- [55] Backup and Disaster Recovery Software Catalog. [online], [cit. 2015-04-24]. Dostupné z: <https://buy.storagecraft.com/default.aspx>
- [56] New ShadowProtect IT Edition Pricing and StorageCraft Cloud Offering. [online], March 2014, [cit. 2015-04-24]. Dostupné z: <http://blog.sofsol.co.nz/2014/03/25/storagecraft-update-new-it-edition-pricing-and-storagecraft-cloud-offering/>
- [57] 8 Business Online Backup Services Reviewed. [online], [cit. 2015-04-27]. Dostupné z: <http://pcsupport.about.com/od/backup/tp/business-online-backup.htm>
- [58] Backblaze Review. [online], [cit. 2015-04-27]. Dostupné z: <http://pcsupport.about.com/od/backup/fl/backblaze-review.htm/>
- [59] Backblaze. [online], [cit. 2015-04-27]. Dostupné z: <https://www.backblaze.com/business.html>
- [60] Crashplan. [online], [cit. 2015-04-28]. Dostupné z: <https://www.code42.com/products/crashplan/>
- [61] Crashplan Review. [online], [cit. 2015-04-28]. Dostupné z: <http://pcsupport.about.com/od/backup/fr/crashplan-plus-review.htm>

- [62] Guy Baroan, C. M.: Making Disaster Recovery Easy. [online], [cit. 2015-04-03]. Dostupné z: <http://www.storagecraft.com/blog/download/recover-ability-guides/making-disaster-recovery-easy.pdf>
- [63] Weisman, R.: 3 Backup Basics Every MSP Should Deliver. [online], February 2014, [cit. 2015-05-09]. Dostupné z: <http://www.storagecraft.com/blog/3-backup-basics-every-msp-deliver/>
- [64] Morgan, C.: Selling Disaster Recovery as a Service. [online], [cit. 2015-04-10]. Dostupné z: <http://www.storagecraft.com/blog/download/recover-ability-guides/selling-disaster-recovery-as-a-service-final.pdf>
- [65] What is a Backup Disaster Recovery Device (BDR)? [online], July 2012, [cit. 2015-03-29]. Dostupné z: <http://blog.techquility.net/what-is-a-backup-disaster-recovery-device-bdr/>

Seznam použitých zkratk

BDR	Backup disaster recovery
DR	Disaster recovery
DRP	Disaster recovery plan
HIPAA	Health Insurance Portability and Accountability Act
HW	Hardware
IT	Informační technologie
JAR	Java archive
JRE	Java Runtime Environment
LAN	Local Area Network
MSP	Managed service provider
NAS	Network-Attached Storage
RMM	Remote monitoring and management
ROI	Return on investment
RPO	Recovery point objectives
RTO	Recovery time objectives
SLA	Service-level agreement
SW	Software
WAN	Wide Area Network
WYSIWYG	What You See Is What You Get

Srovnání Veeam Availability Suite a Acronis Backup Advanced

V této příloze se detailněji podíváme na dva významné hráče na poli zálohovacích řešení. Pro toto srovnání využijí data zjištěná při testování těchto dvou programů společností Network Testing Labs[50].

B.1 Výkon

K porovnání výkonu byly vybrány čtyři hodnoty:

- Rychlost zálohování a obnovy
- Disk-to-disk využití prostoru
- Vytížení sítě
- Hodnota RTO

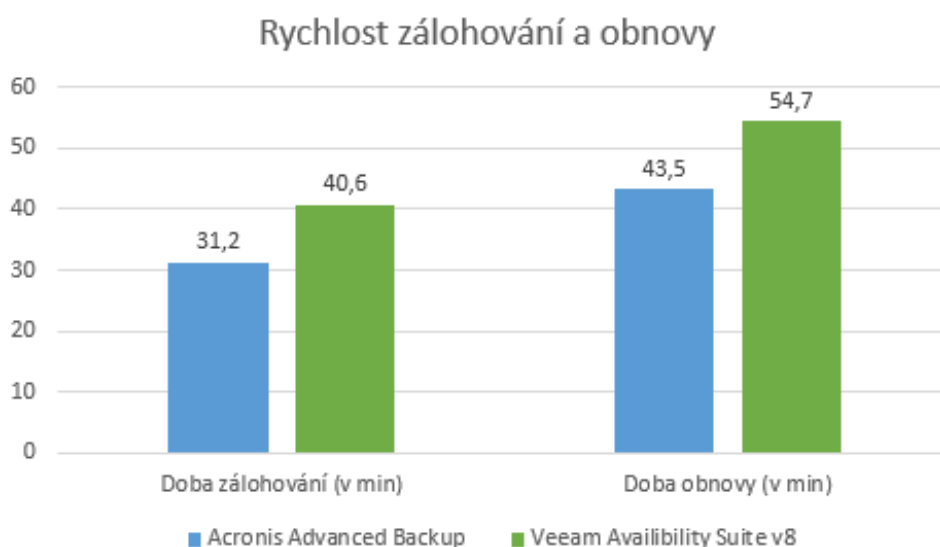
V další části testu byla dále porovnána:

- Použitelnost a funkce
- Cloudové zálohování
- Cena

B.1.1 Rychlost zálohování a obnovy

Pro tento test byl měřena čas, který programy potřebovaly pro zálohu a obnovu 140 GB dat z různých serverů - souborový server, emailový server, web server a databázový server. Hodnoty byly následně zprůměrovány, výsledky zobrazuje obrázek B.1. V obou případech si vedl lépe Acronis.

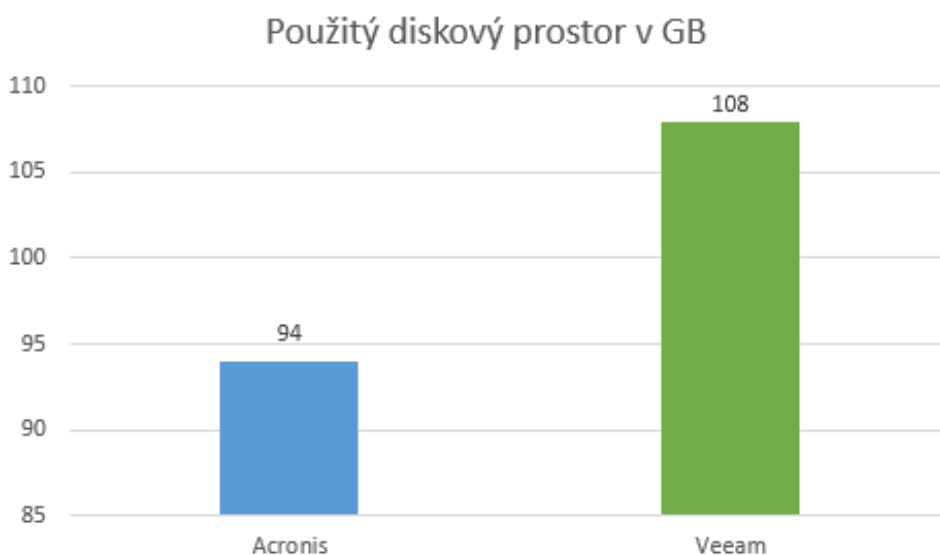
B. SROVNÁNÍ VEEAM AVAILABILITY SUITE A ACRONIS BACKUP ADVANCED



Obrázek B.1: Srovnání rychlostí zálohování a obnovy

B.1.2 Disk-to-disk využití prostoru

V tomto testu byla data ze serveru kopírována na záložní disk. Oba programy dostaly za úkol zazálohovat 200 GB dat. Testována byla efektivita deduplikace a komprese dat. Výsledky jsou vykresleny na obrázku B.2 (méně je lépe).



Obrázek B.2: Využití prostoru pro zálohu 200 GB dat

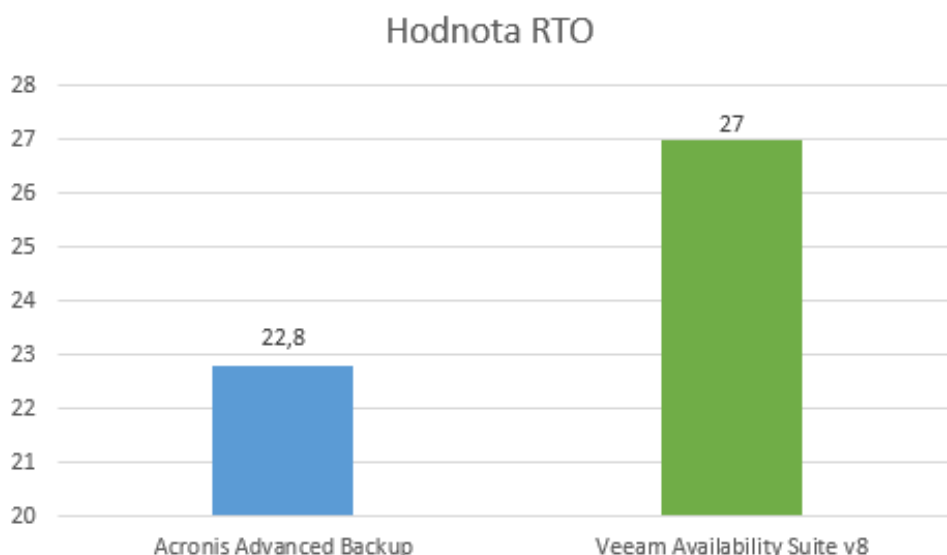
B.1.3 Vytížení sítě

Třetí test porovnává, jak velký díl z připojení k internetu si pro sebe softwary uzmuly při zálohování a obnově v předchozím testu. Spojení probíhalo na 1 Gbit/s ethernetové lince.

I v tomto testu si vedle lépe Acronis, využil 13 % propustnosti sítě, zatímco Veeam si alokoval 16 %.

B.1.4 Hodnota RTO

V posledním výkonnostním testu bylo nasimulováno zničení čtyř malých serverů obsahujících 65 GB dat. Byla měřena doba, za jakou se programům podařilo obnovit provoz těchto serverů. Výsledky popisuje obrázek B.3. Stejně jako v předchozích testech je vítězem Acronis, servery se mu podařilo obnovit o více než 4 minuty rychleji.



Obrázek B.3: Hodnoty RTO testovaných řešení

B.2 Použitelnost a funkce

Největším rozdílem ve funkcionalitě jsou prostředí, ve kterých jsou programy schopné pracovat. Acronis Advanced Backup dokáže pracovat jak ve fyzické, virtuálním a hybridním prostředí, Veeam Availability Suite umí pracovat pouze v prostředí virtuálním.

Zatímco Acronis Advanced Backup podporuje širokou škálu virtuálních zařízení - Citrix XenServer, Oracle VM, Linux KVM and Red Hat Enterprise

B. SROVNÁNÍ VEEAM AVAILABILITY SUITE A ACRONIS BACKUP ADVANCED

Virtualization a samozřejmě VMware produkty a Hyper-V. Je navíc možné mezi těmito variantami kombinovat. Veeam Availability Suite podporuje pouze VMware a Hyper-V. Navíc je možné používat pouze jednu nebo druhou variantu.

Uživatelské prostředí je přehlednější a snadněji ovladatelné také u Acronis Availability Suite.

B.3 Cloudové zálohování

Veeam přerušil provoz vlastního cloudu a místo toho nabízí *Cloud Connect*. Tedy zálohování na cloud partnerů Veeam, kterými jsou méně známí poskytovatelé - Cirrity, iland Internet Solutions, Newcloud Networks, OffsiteDataSync a Phoenix NAP.

Acronis na druhou stranu provozuje vlastní cloud. Funkcionalita je přímo zabudovaná do Advanced Backup a Acronis Cloud se tak chová jako každá jiná disková jednotka.

B.4 Cena

Acronis licence se platí na každý server. Veeam oproti tomu licencuje každou patičku procesoru serveru zvlášť. Servery obvykle mají dvě, čtyři, šest nebo osm patiček. Licencování se proto výrazně prodraží, zejména u serverů s velkým počtem patiček.

Pokud by měl servery dvě patičky, vychází licence pro Acronis a Veeam Enterprise \$7995, respektive \$13600.

Ještě výraznější rozdíl je pak mezi cenami cloudů. Za 5TB Acronis Cloudu zaplatíme za rok \$7995. Pro Veeam si však musíme připravit celých \$32400. Pro více informací nahlédněte do tabulek B.1 a B.2.

Platforma	MSRP
Univerzální licence (všechny platformy)	\$2199
Acronis Cloud	\$1599 ročně za 1TB

Tabulka B.1: Ceník Acronis Backup Advanced

Edice	MSRP
Standard	\$1,100 za každou CPU patičku
Enterprise	\$1,700 za každou CPU patičku
Enterprise Plus	\$2,400 za každou CPU patičku
Cloud Connect – 5 TB	\$17,400 ročně

Tabulka B.2: Ceník Veeam Availability Suite v8

B.5 Shrnutí

Acronis Backup Advanced se stál jasným vítězem ve všech testech. Nabízí vyšší výkon, více funkcí a nižší cenu než Veeam Availability Suite. Funguje navíc jak ve fyzické tak virtuálním prostředí.

Ukázka využití průvodce na praktickém příkladě

V této kapitole vyplníme průvodce podle fiktivní společnosti, která si chce udělat představu o vhodném zálohovacím modelu. Jedná se o společnost zabývající se výrobou a distribucí sportovní a náhradní výživy. Pro naše účely pojmenujeme společnost Nutrillex. Společnost má své sídlo v Brně, kde jsou doplňky vyráběny a zároveň zde je hlavní distribuční a marketingové centrum. Další pobočky se nacházejí v Praze, Plzni a Ostravě. Zde jsou pouze prodávány hotové výrobky.

C.1 Současná infrastruktura

V Brněnském sídle se dále nachází 3 servery. Na jednom běží webová aplikace, přes kterou zákazníci objednávají po internetu zboží. Druhý server pohání firemní software, který slouží k evidenci objednávek, sledování jejich stavu, vyřizování případných reklamací a skladovou evidenci. Třetí je pět let starý emailový server (viz obrázek C.2).

Připojení k internetu se pohybuje v průměru kolem 30 Mbit/s download a upload asi 20 Mbit/s. Společnost pak dále disponuje 40 pracovními počítači. Vyplněná první část průvodce na obrázku C.1.

C.2 Aktuální stav společnosti

Nyní se zaměříme na další část průvodce. V té je stručně analyzován současný stav společnosti. Nutrillex se nachází v České republice a tu lze z pohledu přírodních katastrof považovat za bezpečnou. Oba firemní systémy běží na serverech v Brně, tedy on-premise. O jejich běh, správu webových stránek a celkový chod infrastruktury se starají čtyři IT pracovníci.

C. UKÁZKA VYUŽITÍ PRŮVODCE NA PRAKTICKÉM PŘÍKLADĚ

Počet serverů:	3
Počet počítačů:	10 - 100
Rychlost připojení k internetu:	10 - 100 Mbi...
Počet dostupných připojení k internetu: (kolika poskytovatelů internetu využíváte)	1

Obrázek C.1: Současná infrastruktura společnosti Nutrillex

Počet serverů vyhrazených pro provádění záloh:	0
Počet Exchange a emailových serverů:	1
Stáří nejnovějšího:	více než 3 roky

Obrázek C.2: Doplnující otázky k serverům Nutrillexu

Systém nepracuje s extrémně citlivými údaji zákazníků (jako jsou zdravotní záznamy, či bankovní výpisy), které by vyžadovaly speciální certifikace a pravidla pro uchování. Co se poboček týče, již jsme zmínili, že společnost má další tři pobočky.

Zálohování v tuto chvíli probíhá pouze ve formě kopírování databází na externí pevný disk na konci pracovní doby. Po naplnění kapacity se vždy odmazává nejstarší databáze.

Vyplněná druhá část viz obrázek C.3.

C.3 Stanovení cílů

Poslední část se zabývá specifikací cílů a očekávání uživatele od navrhovaného modelu. Pro zodpovězení první otázky je nutné kliknout na tlačítko s textem *Upřesnit odpověď*. Kliknutí nás přesune do nového panelu, ve kterém se nachází povinná otázka na požadovanou dostupnost systému a nepovinné otázky na specifikaci hodnot RTO a RPO.

Vedení společnosti si uvědomuje, že běžící systémy (jak webové stránky, tak interní systém) jsou klíčové pro běh společnosti a požaduje dostupnost alespoň 99,5 %. Z odpovědí v nabídce splňuje tuto podmínku odpověď *více než 99,9 %*. Hodnoty RTO a RPO ideálně samozřejmě co nejnižší. RPO by

Společnost se nachází v rizikové oblasti:	Ne
Momentální provoz hlavního systému:	on-premise
Společnost disponuje IT odborníky:	Ano
Systém pracuje s citlivými údaji zákazníků: (zdravotní záznamy, peněžní transakce apod.)	Ne
Společnost má více poboček:	Ano
V současnosti jsou data nějakým způsobem zálohována:	Ano
Klíčové zálohy jsou archivovány na archivační cloud:	Ne

Obrázek C.3: Aktuální stav společnosti Nutrillex

u databáze měly být nulové, neboť si společnost nemůže dovolit ztratit provedené objednávky. Systém by pak měl po výpadku naběhnout do půl hodiny. Vyplněná část průvodce týkající se dostupnosti tedy vypadá následovně - viz obrázek.

Požadovaná dostupnost systému:	více než 99,9 %
Požadované RTO:	15 - 60 min
Požadované RPO:	do 15 min

Obrázek C.4: Otázky k dostupnosti systému společnosti Nutrillex

Po návratu zpět na předchozí panel můžeme pokračovat ve vyplňování. Nutrillex před třemi lety spustil provoz interního systému a proběhla rekonstrukce webových stránek. Od té doby se již větší změny nekonaly a ani se nepředpokládají v blízké budoucnosti. Škálovatelnost tedy není pro společnost zvlášť podstatná, nicméně ne úplně nepodstatná, proto necháme odpověď prázdnou. Šifrování dat je nutné kvůli ochraně dat zákazníků a celkové odolnosti proti neoprávněnému přístupu. Co se týče vstupních a provozních nákladů, společnost disponuje slušným kapitálem a zajímají ji spíše dlouhodobé náklady, zde je tedy odpovíme *Ne*. Minimální údržba je určitě plusem, neboť IT pracovníci již teď mají plné ruce práce, vyplníme *Ano*. Před zodpovězení poslední otázky nejprve odhadneme cenu výpadku pomocí kalkulátoru.

Společnost Nutrillex v současné době zaměstnává 110 zaměstnanců. Je

C. UKÁZKA VYUŽITÍ PRŮVODCE NA PRAKTICKÉM PŘÍKLADĚ

jich hodinová sazba je v průměru 180 Kč. Tržby společnosti za minulý rok činily přibližně 260 000 000 Kč. Pracovní doba je od pondělí do pátku (což je přibližně 251 dní za rok - po kliknutí na tlačítko *Upřesnit* a vyplnění příslušných dní dojde k výpočtu) od 7 do 16 hodin. Loni v březnu došlo k výpadku elektřiny v celém brněnském areálu na 2h. Záložní zdroje, kterými společnost disponuje zajistily pouze bezpečné vypnutí všech zařízení. Více než 80 % zaměstnanců tak nemohlo efektivně pracovat. Výsledný výpočet můžete vidět na obrázku C.5

Počet zaměstnanců:	<input type="text" value="110"/>	Hrubý roční příjem společnosti:	<input type="text" value="260 000 000"/>	CZK	
Průměrná hodinová sazba zaměstnanců:	<input type="text" value="180"/>	CZK	Otevřeno dní v roce:	<input type="text" value="251"/>	<input type="button" value="Upřesnit"/>
Průměrná ztráta produktivity: (procento prac. síly postižené výpadkem)	<input type="text" value="80"/>	Otevřeno hodin denně:	<input type="text" value="9"/>		
Trvání výpadku (v hodinách):	<input type="text" value="2"/>	Měna:	<input type="text" value="CZK"/>	<input type="button" value="Vypočítat"/>	

Celková cena výpadku: 261870 CZK

Obrázek C.5: Kalkulátor ztrát aplikovaný na výpadek u Nutrillexu

Na základě tohoto zjištění se společnost rozhodla, že nechce za každou cenu šetřit a má zájem o efektivní řešení za rozumnou cenu. Poslední odpovědí je tedy *Optimální poměr cena/výkon*. Obrázek C.6 zobrazuje vyplněnou třetí část průvodce.

Dostupnost systému:	<input type="button" value="Upřesnit odpověď"/>
Pružnost výkonosti a kapacity paměti diskového prostoru pro zálohování:	<input type="text" value=""/>
Šifrování dat:	<input type="text" value="Ano"/>
Nižší vstupní náklady na úkor vyšších provozních:	<input type="text" value="Ne"/>
Minimální údržba:	<input type="text" value="Ano"/>
Finanční možnosti:	<input type="text" value="Optimální poměr cena/výkon"/>

Obrázek C.6: Stanovení cílů společnosti Nutrillex

C.4 Vyhodnocení

Výsledným řešením je *Zakoupení nového HW a zálohování na zálohovací cloud* (viz obrázek C.7). Je to jeden z nejkvalitnějších modelů se slabinou pouze v nákladech, neboť je zapotřebí pořídit zálohovací jednotku a platit cloud. Nutrillex tak bude muset zainvestovat část svých zisků, nicméně tato investice se jim vrátí, zejména pokud vytvoří kompletní plán pro obnovu (více kapitola 5), který by s jistotou obsahoval zakoupení rezervního generátoru, aby se minimalizovalo riziko dalšího výpadku kvůli přerušení dodávky elektrické energie.

Výsledné řešení: <i>Zakoupit nový HW pro on-premise zálohování + zálohovat na cloud určený pro zálohování jako offsite zálohu</i>	
Dostupnost	■ Jednu zálohu máme dostupnou on-premise, druhou prostřednictvím internetu offsite.
Spolehlivost	■ Maximální spolehlivost. Okamžitě dostupná on-premise záloha + zálohovací cloud s perfektními parametry a službami.
Provozní náklady	■ Energie na provoz serverů, správa a údržba HW. Placení vysokých poplatků za specializovaný cloud.
Údržba	■ Nutná u on-premise záloh. Minimální u cloudové.
Škálovatelnost	■ Maximální škálovatelnost cloudou. U on-premise nutný nákup HW.
Virtualizace	■ Možné virtualizovat jak on-premise, tak na cloudu.

Obrázek C.7: Výsledné řešení část první

Na obrázku C.8 pak můžeme vidět, že je doporučeno zajistit ještě druhé připojení k internetu. To nejen pojistí zálohování na cloud, ale také odstraní závislost na jednom poskytovateli. Když navíc využijeme kalkulátor tak zjistíme, že i velmi krátký výpadek znamená ztráty vyšší než několik let vysokorychlostního připojení k internetu.

Optimalizace	Vyhodnocení není k dispozici.
Stav hardware	Díky zakoupení nového HW pravděpodobně nebude v nejbližších letech zapotřebí provádět upgrade.
Připojení k internetu	Rychlost připojení k internetu by bylo optimální navýšit za účelem zrychlení offsite zálohování. Zároveň také zajistit druhého poskytovatele.
Lokalita	Žádné doporučení.
Citlivé údaje zák.	Žádné doporučení.
Správa zálohování	Zvažte přenechání správy zálohování třetí straně (MSP).

Obrázek C.8: Výsledné řešení část druhá

V poslední části výsledků (obrázek C.9) se pak mimo jiné dozvíme, že pro zajištění téměř 100 % dostupnosti je nutností zrcadlení databází, neboť je tím systém chráněn před selháním disku. Což se však projeví na ceně, neboť je nutné zakoupit hardwarový RAID řadič, další disky a možná i obnovit HW serveru, pokud nebude mít dostatečný výkon.

C. UKÁZKA VYUŽITÍ PRŮVODCE NA PRAKTICKÉM PŘÍKLADĚ

Archivace	Je vhodné archivovat úplné zálohy pro případ potřeby v pravidelných intervalech. Ideálním řešením je využít archivačních cloudů.
Výkon řešení	Téměř 100% dostupnosti jde docílit mimo jiné pouze s využitím zrcadlení, což se negativně projeví na ceně.
Podpora	Díky uložení offsite zálohy u třetí strany, můžete očekávat podporu z jejich strany, pokud jí budete potřebovat
Šifrování	Při výběru cloudového poskytovatele sledujte, zda jsou disky s uloženými daty a veškeré přenosy šifrovány.
Vstupní náklady	Díky využití cloudů nemusíte kupovat další HW i pro offsite zálohu. Tím snížíte vstupní náklady.
Shrnutí	Zálohovací cloudy jsou perfektním řešením a nabízí skvělou ochranu a široké služby za flexibilní ceny.

Obrázek C.9: Výsledné řešení část třetí

C.5 Shrnutí

Jak jsme si mohli všimnout, byl průvodce schopný vcelku přesně odhadnout zálohovací model pro danou společnost. Zprostředkoval tak jakýsi nástřel řešení, na němž lze pak dále stavět při tvorbě plánu pro obnovu. Znalost přibližného řešení navíc snižuje šanci naletět na některé nabídky, které by pouze chtěly z uživatele vylákat větší peníze, přestože by nabídka neodpovídala požadavkům.

Obsah přiloženého CD

ctiMe.txt.....	stručný popis obsahu CD
zadani.pdf	zadání bakalářské práce
exe	adresář se spustitelnou formou implementace
src	
├─ impl.....	zdrojové kódy implementace
latex.....	adresář zdrojů práce ve formátu L ^A T _E X
├─ img.....	adresář obsahující obrázky použité v práci
text	text práce
├─ bakalarka.pdf	text práce ve formátu PDF