



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

NÁVRH FYZICKÉHO SERVERU A JEHO ZÁLOHOVÁNÍ

DESIGN OF THE PHYSICAL SERVER AND ITS BACKUP

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE

AUTHOR

Jan Pavlát

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. Jiří Kříž, Ph.D.

BRNO 2023

Zadání bakalářské práce

Ústav: Ústav informatiky
Student: **Jan Pavlát**
Vedoucí práce: **Ing. Jiří Kříž, Ph.D.**
Akademický rok: 2022/23
Studijní program: Manažerská informatika

Garant studijního programu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává bakalářskou práci s názvem:

Návrh fyzického serveru a jeho zálohování

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem práce je navrhnout nový fyzický server, který bude náhradou za starý výkonově nevyhovující server, a optimalizovat jeho zálohování s důkladným monitoringem.

Základní literární prameny:

DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

DE GUISE, P. Data Protection. 1. Boca Raton: Taylor & Francis Group, 2017. ISBN 9781482244151. Dostupné z: doi:10.1201/9781315169620

PECINOVSKÝ, J. Archivace a komprimace dat: jak zálohovat data, jak komprimovat soubory WinRAR, WinZip, WinAce, Windows a nástroje komprese dat, jak archivovat data ve Windows. Praha: Grada Publishing a.s., 2003. ISBN 80-24-0659-8.

SOMASUNDARAM, G. a A. SHRIVASTAVA. Information Storage and Management: Storing, Managing, and Protecting Digital Information. Indianapolis: Wiley Publishing, 2009. ISBN 978-0-470-29421-5.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2022/23

V Brně dne 5.2.2023

L. S.

Ing. Jiří Kříž, Ph.D.
garant

doc. Ing. Vojtěch Bartoš, Ph.D.
děkan

Assignment Bachelor's Thesis

Department: Institute of Informatics
Student: **Jan Pavlát**
Supervisor: **Ing. Jiří Kříž, Ph.D.**
Academic year: 2022/23
Study programme: Managerial Informatics

Pursuant to Act no. 111/1998 Coll. concerning universities as amended and to the BUT Study Rules, the degree programme supervisor has assigned to you a Bachelor's Thesis entitled:

Design of the Physical Server and its Backup

Basic sources of information:

DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

DE GUISE, P. Data Protection. 1. Boca Raton: Taylor & Francis Group, 2017. ISBN 9781482244151. Dostupné z: doi:10.1201/9781315169620

PECINOVSKÝ, J. Archivace a komprimace dat: jak zálohovat data, jak komprimovat soubory WinRAR, WinZip, WinAce, Windows a nástroje komprese dat, jak archivovat data ve Windows. Praha: Grada Publishing a.s., 2003. ISBN 80-24-0659-8.

SOMASUNDARAM, G. a A. SHRIVASTAVA. Information Storage and Management: Storing, Managing, and Protecting Digital Information. Indianapolis: Wiley Publishing, 2009. ISBN 978-0-470-29421-5.

Abstrakt

Bakalářská práce se zaměřuje na návrh fyzického serveru a jeho zálohování. Analyzuje současný stav infrastruktury společnosti a identifikuje nedostatky a problémy v oblasti výkonu, dostupnosti a zálohování dat. Obsahuje podrobný návrh fyzického serveru a doporučení pro jeho konfiguraci, které poskytují společnosti solidní základ pro modernizaci infrastruktury a zajištění bezpečného a spolehlivého provozu serverového prostředí.

Abstract

The bachelor thesis focuses on the design of a physical server and its backup. It analyzes the current state of the company's infrastructure and identifies the shortcomings and problems in the areas of performance, availability and data backup. It includes detailed physical server design and configuration recommendations that provide the company with a solid foundation for upgrading its infrastructure and ensuring a secure and reliable server environment.

Klíčová slova

Zálohování, Raid, Server, Data, NAS

Key words

Backup, Raid, Server, Data, NAS

PAVLÁT, Jan. *Návrh fyzického serveru a jeho zálohování* [online]. Brno, 2023 [cit. 2023-05-10]. Dostupné z: <https://www.vut.cz/studenti/zav-prace/detail/152361>.
Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Jiří Kříž.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 13. 5. 2023

Jan Pavlát

autor

Poděkování

Rád bych poděkoval panu Ing. Jiřímu Křížovi, Ph.D., za cenné rady a ochotu při vedení mé bakalářské práce. Dále také Michalu Polákovi za poskytnuté materiály a obětavý přístup při poskytování informací.

OBSAH

ÚVOD	6
CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ.....	7
1 TEORETICKÁ VÝCHODISKA PRÁCE.....	8
1.1 Zálohování.....	8
1.2 Archivace.....	8
1.3 Příčiny ztráty dat	8
1.3.1 Lidský faktor	8
1.3.2 Krádež	9
1.3.3 Chyba softwaru.....	9
1.3.4 Chyba hardwaru	9
1.3.5 Napadení virem	9
1.3.6 Přírodní katastrofa	10
1.4 Typy záloh.....	10
1.4.1 Plná záloha	10
1.4.2 Inkrementální záloha	11
1.4.3 Rozdílová záloha	12
1.4.4 Kombinace typů záloh.....	12
1.5 Pravidlo zálohování 3-2-1	13
1.5.1 Pravidlo 3-2-1-1-0	14
1.6 Obnova dat po havárii	14
1.6.1 Cíl doby obnovy	14
1.6.2 Cíl bodu obnovy	15
1.7 Tvorba plánu obnovy po havárii pro malé firmy a organizace	15
1.8 Zálohovací média	16
1.8.1 CD/DVD.....	17
1.8.2 USB Flash disk.....	17
1.8.3 HDD/SSD	17
1.8.4 NAS.....	17

1.8.5	Cloud	18
1.9	ochrana dat pomocí RAID.....	18
1.9.1	RAID 0	18
1.9.2	RAID 1	19
1.9.3	RAID 5	20
1.9.4	RAID 6	20
1.9.5	RAID 01 a RAID 10.....	21
2	ANALÝZA PROBLÉMU A SOUČASNÉ SITUACE.....	22
2.1	Počítačová síť společnosti.....	22
2.2	Hardwarová výbava společnosti.....	23
2.2.1	Počítač	23
2.2.2	Server.....	24
2.2.3	Router	24
2.2.4	Switch.....	25
2.3	Zálohování.....	26
2.4	Zabezpečení.....	26
3	VLASTNÍ NÁVRHY ŘEŠENÍ.....	27
3.1	Návrh Fyzického serveru.....	27
3.1.1	Požadavky společnosti na server.....	27
3.1.2	DELL PowerEdge R350.....	27
3.1.3	DELL PowerEdge T350.....	28
3.1.4	Vybrané řešení.....	29
3.2	Způsob migrace dat na nový server.....	34
3.2.1	Instalace starého disků do nového serveru	34
3.2.2	Zrcadlení stareho disků na nový.....	34
3.2.3	Vybrané řešení.....	35
3.3	Návrh způsobu zálohování dat mimo lokalitu.....	36
3.3.1	Zálohování do cloudu	36
3.3.2	Zálohování na NAS	36
3.3.3	Zálohování NAS vs. Cloud	38

3.3.4	Vybrané řešení.....	40
3.3.5	Plán obnovy	41
3.3.6	Veeam agent for microsoft windows.....	41
3.3.7	Nastavení plánu zálohy	42
3.4	Zhodnocení návrhu.....	48
ZÁVĚR.....		50
SEZNAM POUŽITÝCH ZDROJŮ		51
SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ.....		55
SEZNAM OBRÁZKŮ.....		57
SEZNAM TABULEK		59

ÚVOD

V dnešní době jsou data pro většinu podniků a organizací klíčovou součástí úspěšného fungování a rozvoje. Ztráta dat může mít pro firmy katastrofální následky. Ztratí se nejen hodnotné informace, ale také zákazníci, příjmy a reputace. Proto je zálohování dat nezbytnou součástí každého bezpečnostního plánu a strategie řízení rizik.

S rozmachem moderních technologií v podobě počítačů a dalších IT zařízení do podnikání se zvýšil i počet hackerských útoků na firmy s cílem získat kontrolu nad cennými daty. Útočníci pak pod výhrůzkou smazání či zveřejnění veškerých dat vyžadují výkupné. S příchodem pandemie COVID-19 a přesunu práce na home office a veškeré komunikace do internetového prostředí se riziko mnohonásobně zvýšilo, protože pro mnoho podniků to bylo poprvé co musely řešit různé sdílení dat mezi zaměstnanci mimo kancelářské prostředí.

Malé a střední podniky ale většinou zanedbávají IT stránku provozu. Většinou se tak děje v kombinaci úspor financí a nedostatečného pochopení důležitosti IT a jeho zabezpečení pro provoz. Běžně je pak možné u těchto podniků, které nemají vlastní IT oddělení nebo někoho, kdo má aspoň minimální přehled v oblasti IT, mít v provozu starý hardware, častokrát s neaktualizovaným softwarem bez zabezpečení v podobě absence hesla či antivirového programu. Takový hardware může být bez dostatečného zálohování časovanou bombou, kdy v případě selhání hardwaru či hackerského útoku může firma přijít kompletně o všechny data. V lepším případě dojde pouze k výpadku a finanční ztrátě kvůli nemožnosti chodu podniku. Je proto důležité, aby malé a střední podniky pochopily, že IT není pouze nákladem, ale investicí do budoucna, která může pomoci podniku růst.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Cílem bakalářské práce je návrh nového fyzického serveru a jeho korektního zálohování podle požadavků společnosti, pro který bude server navrhován

Teoretická část práce má za úkol seznámení s problematikou tématu zálohování a přiblížit technické náležitosti práce s daty a jejich zálohování. Teoretická část poté bude využita k návrhu řešení.

Pro co nejlepší návrh bude provedena analýza současného stavu sítě a informačních technologií společnosti včetně zálohování. Hlavním zaměřením práce pak bude navrhnout nový fyzický server pro zákazníka IT společnosti, pro kterou pracuji, aby odpovídal požadavkům na zajištění co nejkvalitnějšího zálohování s ohledem na co nejrychlejší obnovu dat při havárii v poměru s cenou technického řešení.

1 TEORETICKÁ VÝCHODISKA PRÁCE

1.1 ZÁLOHOVÁNÍ

Zálohování je proces, vytváření kopií produkčních dat, která jsou následně ukládána na jiné datové médium, než je to původní. Záloha slouží jako ochrana dat před krádeží, ztrátou či poškozením dat. V případě že dojde k nějaké ztrátě či poškození dat jsou tyto kopie využity pro obnovu.[2][31]

1.2 ARCHIVACE

Archivace dat se často zaměřuje se zálohou dat. Archivace ale je dlouhodobé uložení nepoužívaných dat mimo produkční prostředí. Tyto data je pak možno v případě potřeby opět využít a zasadit zpět do produkčního prostředí.

Výhodou archivace dat je pak zvýšená kapacita úložiště, jednodušší zálohování, protože se zálohují pouze aktivně využívaná data a záloha tak probíhá rychleji, a zvýšená produktivita díky nižšímu času stráveného údržbou a kontrolou zálohovacího úložiště.[30]

1.3 PŘÍČINY ZTRÁTY DAT

1.3.1 LIDSKÝ FAKTOR

Jedna z nejčastějších příčin ztráty dat je zavinění lidskou chybou. Uživatel během své práce s daty může svou nepozorností nebo nedostatečným proškolením například smazat soubor či celou složku s důležitými daty. Bez přítomné zálohy se pak tato ztracená data těžko obnovují. Dalším lidským zaviněním může být i mechanické poškození z důvodu špatného zacházení se zařízením. Nevhodným zacházením může uživatel poškodit například pevný disk a ztratit tak přístup ke všem datům.[28][29]

1.3.2 KRÁDEŽ

V případě krádeže je myšlena krádež celého zařízení spolu s médiem, na kterém jsou uložena data. V dnešní době jsou to výhradně přenosné zařízení jako jsou mobilní telefony a notebooky. Ale nevylučuje se ani vykradení domu či kanceláře kdy může zmizet i stolní počítač či jiné zařízení obsahující data. Pro okradeného pak mají data mnohem vyšší cenu než samotné zařízení. V případě zařízení obsahující firemní či obchodní data společnosti to pak platí dvojnásobně. Předějit neoprávněnému přístupu k datům se pak dá například pomocí zašifrování disku. Kdy zloděj sice ukládací medium získal ale datum se nedostane.[28][29]

1.3.3 CHYBA SOFTWARE

Ztrátě dat chybou softwaru se dá málokdy z uživatelského hlediska předejít, protože žádný software není dokonalý. Během používání softwaru může dojít k pádu aplikace, kdy se rozpracovaná data špatně uloží a soubor je pak porušený anebo se neuloží vůbec. Stejně tak mohou být data ztracena v případě zálohování, kdy se softwaru nepodaří vytvořit kopii nebo během tvorby kopie nastane chyba a vytvořený soubor je chybný a nelze z něj číst zálohovaná data.[28][29]

1.3.4 CHYBA HARDWARU

Nejčastějším důvodem ztráty dat je chyba hardwaru. Taková chyba může způsobit nenávratnou ztrátu dat. Obvykle se jedná o mechanické pevné disky, které lze poškodit způsoby jako je přehřátí, výpadek el. proudu, lidským zaviněním, chybou firmwaru, poškozením zapisovacího a čtecího zařízení a v neposlední řadě postupným opotřebením mechanických součástí disku během používání.[28][29]

1.3.5 NAPADENÍ VIREM

Počítačový vir může jednoduše napadnout zařízení získat cenné údaje a přístup k datům. Takový virus pak může data na ukládacím médiu ukradnout, zašifrovat a

v nejhorším případě rovnou smazat. Pomocí počítačové sítě má pak vir možnost napadnout celou firemní infrastrukturu a získat tak velké množství dat ze všech zařízení připojených do sítě. Nejčastěji se při napadení virem setkáte s termínem „Ransomware“ kdy útočník pomocí viru získá přístup k datům, ta zašifruje a po napadeném uživateli pak požaduje finanční částku jako výkupné za zašifrovaná data. Pokud napadený odmítne, útočník vyhrožuje sdílením dat na veřejnost nebo kompletním smazáním.[28][29]

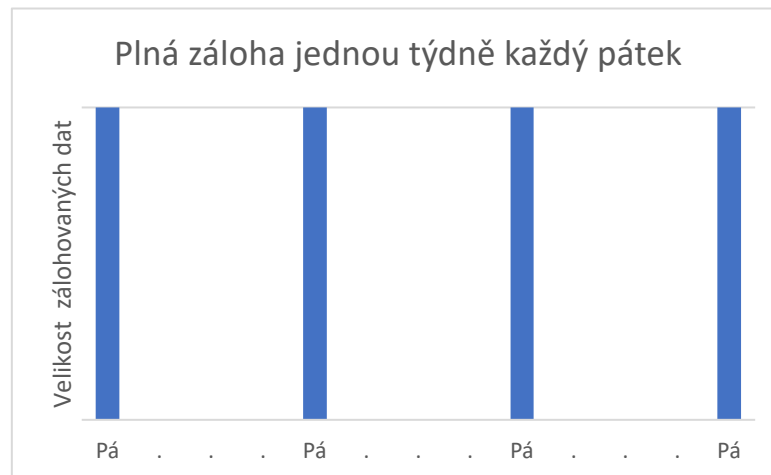
1.3.6 PŘÍRODNÍ KATASTROFA

Méně pravděpodobnou, ale ne vylučitelnou, příčinou ztráty dat je přírodní katastrofa v podobě zemětřesení, požárů, záplav, či obyčejná bouřka, kdy je vlivem těchto přírodních katastrof zařízení poškozeno nebo zničeno.[28][29]

1.4 TYPY ZÁLOH

1.4.1 PLNÁ ZÁLOHA

Plná záloha (Full backup) je proces, při kterém se zálohují kompletně všechna data z vybraného zdroje do místa určeného pro ukládání záloh. Ideálně oddělené úložiště od zdrojového. Jedná se o nejnáročnější zálohy co se týče potřeby volného místa na zálohovacím médiu. Pro obnovu dat z plné zálohy stačí právě jedna plná záloha, zpravidla ta, co proběhla jako poslední. Přičemž jednotlivé zálohy na sebe nejsou závislé. Nejdůležitější podmínkou pro plnou zálohu je široké časové okno, při kterém plná záloha probíhá. Okno musí být dostatečně široké, aby úloha zálohování měla dostatek času a prostoru pro kompletní čtení všech dat. Plné zálohy jsou přípustné spíše pro menší podniky kdy jejich data nemají takovou velikost. Ve středních a velkých podnicích je velikost dat znatelně větší, a proto se pro zrychlení procesu zálohy snaží redukovat množství plných záloh a využívají jiných způsobů záloh nebo častokrát jejich kombinaci.[1][2]



Obrázek 1 Schéma plného zálohování

1.4.2 INKREMENTÁLNÍ ZÁLOHA

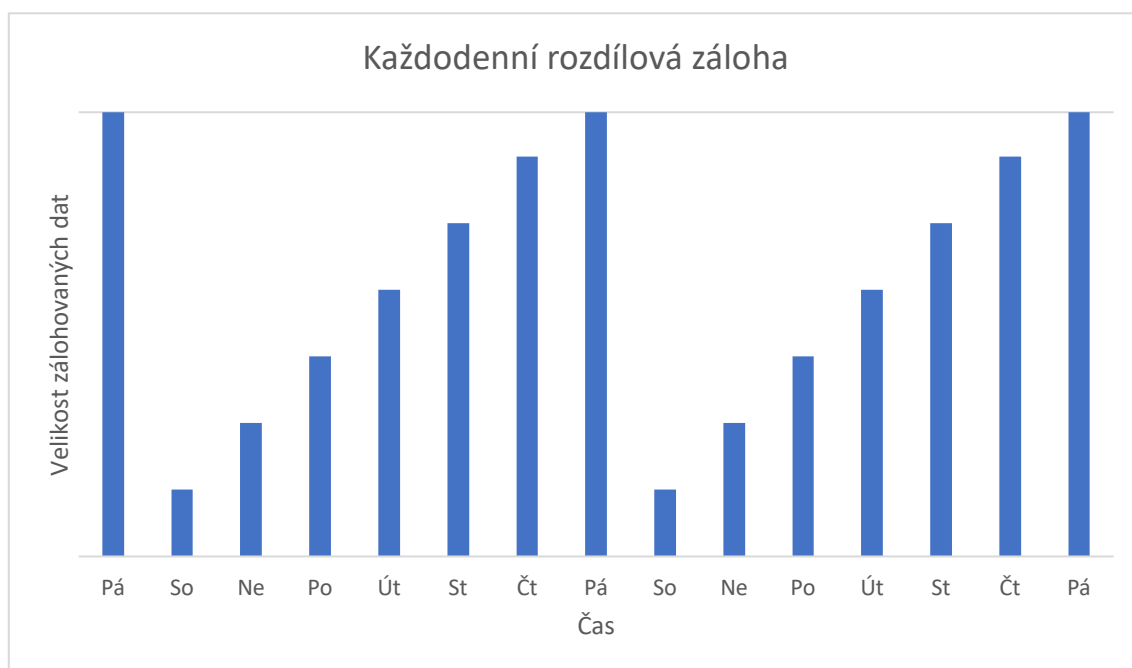
Inkrementální záloha (Incremental backup) nebo také známá jako přírůstková, je záloha, která se zaměřuje pouze na data, která byla změněna od poslední zálohy nehlédě na její typ. Tyto zálohy jsou méně náročné na místo na zálohovacím médiu v závislosti na počtu změněných dat před zahájením zálohování. Díky tomu je dosaženo rychlejšího průběhu úlohy. Na druhou stranu obnova dat z přírůstkové zálohy je mnohem delší. Plná obnova dat z přírůstkové zálohy je možná pouze se všemi přírůstkovými zálohy spolu s počáteční plnou zálohou, která se provádí při prvním spuštění zálohovací úlohy. Pokud je nějaká z těch to záloh poškozená nebo ztracená, nemůže být obnova 100 %. [1][2]



Obrázek 2 Schéma inkrementálního zálohování

1.4.3 ROZDÍLOVÁ ZÁLOHA

Rozdílová záloha (Differential backup) zálohuje změněná či nová data postupně od poslední plné zálohy. Tim pádem každá další záloha od poslední plné zálohy na sebe postupně nabaluje data a tím se zvyšuje i velikost každé další rozdílové zálohy. Pro lepší představu rozdílová záloha uloží veškerá změněná data od poslední plné zálohy. Další rozdílová záloha následující po předchozí uloží všechna změněná či přidaná data od poslední plné zálohy a tak dál dokud se neprovede plná záloha. Od které se pak odvíjí další rozdílová záloha. V dnešní době se od tohoto typu zálohy opouští a není tolik využívána i přes to, že obnova z této zálohy je rychlejší než z přírůstkové. Proces obnovy dat z této zálohy probíhá tak, že se jako první obnoví poslední plná záloha a poté se data přepisují do neaktuálnější podoby pomocí poslední rozdílové zálohy.[1][2][5]



Obrázek 3 Schéma rozdílového zálohování

1.4.4 KOMBINACE TYPŮ ZÁLOH

V dnešní době se místo jednotlivého typu používají zásadně kombinace naplánované na delší časové úseky z důvodu šetření místa na zálohovacím médiu a zkrácení času průběhu záloh. Například měsíční zálohovací plán, kdy na začátku měsíce provedeme plnou zálohu, pak každý den provedeme inkrementální a každý týden

rozdílovou. Dalším příkladem může být plán, kdy plnou zálohu provádíme každý týden a každý den inkrementální. Při návrhu plánu hraje velkou roli velikost zálohovaného zdroje dat, dostupný čas pro spuštění zálohy (zejména večerní až noční hodiny) a velikost úložiště do kterého se budou nahrávat zálohy. [1][2]



Obrázek 4 Schéma kombinovaného zálohování

1.5 PRAVIDLO ZÁLOHOVÁNÍ 3-2-1

Pravidlo zálohování 3-2-1 je strategie, která říká, že při zálohování nemusí vždy jedna kopie stačit. Aby bylo dosaženo pravidla, musí být splněny 3 následující požadavky.[32][33][34]

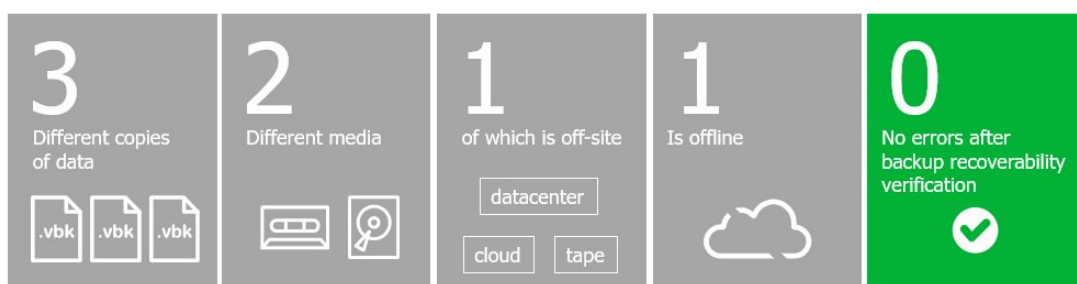
Vytvořit tři kopie dat – Originální data na zařízení a alespoň dvě kopie

Použít alespoň dvě různá ukládací média – Jakékoliv ukládací média. Například cloud a NAS.

Mít jednu kopii jiném místě – Tím to krokem se předejde ztrátě dat způsobeným havárií v lokalitě primárního zařízení.

1.5.1 PRAVIDLO 3-2-1-1-0

Pravidlo 3-2-1-1-0 je modernizovaná verze pravidla 3-2-1, kdy první tři požadavky zůstávají stejné, ale pro ochranu dat je přidána ještě jedna kopie zálohy, která je offline a není připojena k žádnému zařízení s přístupem k internetu. Například externí pevný disk nebo USB. Nula na konci značí nula chyb (zero errors), kdy jsou zálohy monitorovány na denní bázi a pravidelně testovány, zda při obnově dat nedochází k žádným chybám.[32][33][34]



Obrázek 5 Zálohování podle pravidla 3-2-1-1-0 [34]

1.6 OBNOVA DAT PO HAVÁRII

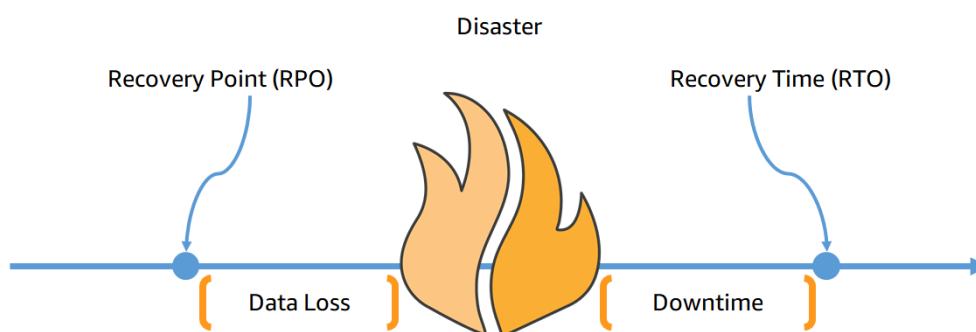
Obnova dat po havárii, známá též jako Disaster Recovery, je souhrn zásad a postupů popisující kroky k rychlému obnovení dat při výskytu incidentu a tím obnovit práci organizaci. Nejdůležitějším článkem obnovy dat a jeho plán je určení jaké aplikace a data jsou pro chod organizace nekritičtější. Klíčovými prvky plánu jsou cíl doby obnovy a cíl bodu obnovy. Například [10]

1.6.1 CÍL DOBY OBNOVY

Cíl doby obnovy (Recovery Time Objective, RTO) vyznačuje maximální dobu potřebnou pro obnovu systémů a dat, aniž by pro organizaci znamenal výraznou škodu zejména finanční. Při plánování doby výpadku se pak nabízí otázka, „*Jak dlouho může být daná služba mimo provoz, aby byly následky výpadku přijatelné?*”. Obvykle pak platí, že čím nižší RTO je požadována, tím nákladnější bude jeho technické řešení.[10][11][13]

1.6.2 CÍL BODU OBNOVY

Cíl bodu obnovy (Recovery Point Objective, RPO) určuje bod z minulosti, ze které lze obnovit data po havárii. Vyjadřuje tedy maximální dobu výpadku i ztráty dat a zároveň je ukazatelem dostupnosti dat. Měl by být kladen důraz na co nejnižší RPO. V závislosti na potřebě organizace se RPO může pohybovat v rámci dnů, hodin či dokonce vteřin. Platí, že čím nižší RPO tím dražší technické řešení je. [10][12][13]



Obrázek 6 Časová osa RPO a RTO [10]

1.7 TVORBA PLÁNU OBNOVY PO HAVÁRII PRO MALÉ FIRMY A ORGANIZACE

Plán obnovy po havárii je sestaven ze čtyř fází. Při těchto fázích je potřeba, aby management firmy úzce spolupracoval s IT, protože obě strany pak mají při tvorbě plánu jistou zodpovědnost. [14][15][16]

První fází tvorby plánu obnovy je inicializace, kdy management podniku požádá IT o vypracování plánu zálohování a plánu obnovení. V praxi, kdy malé podniky nemají vlastní IT a chtějí mít jistotu, tak si tuto službu outsourcují od IT firem, které zastávají většinou pozici IT manažera a většinou inicializace pochází z jejich strany. [14][15][16]

Druhou fází je definice požadavků a strategie. Odpovědností managementu při druhé fázi je přesné definování kritických systémů podniku, které je v případě havárie potřeba obnovit co nejdříve, jelikož by pro podnik mohly znamenat veliké ztráty ať už finanční či reputační. To znamená určit hodnoty RTO a RPO. Výstupem takového

definování je Analýza dopadu na chod podniku, podle které IT oddělení vytvoří návrh zálohovací strategie. [14][15][16]

SLUŽBA	RTO (hod)	RPO (dny)	POZNÁMKA
internet	2 - 48	-	Výpadek do 2 hod. nám nevadí, v rozmezí 2-48 hodin znamená ztrátu zhruba €1k, výpadek delší než 48 hodin je zcela nepřijatelný
pošta	2 - 48	1 - 7	Výpadek max. 48 hodin = ztráta zhruba €1k / den. Ztráta dat větší než 7 dnů je likvidační!
síť. složka „data“	2 - 48	1 - 7	Výpadek max. 48 hodin = ztráta zhruba €1k / den. Ztráta dat = finanční ztráta zhruba €500 / den, delší než 7 dnů je likvidační.
ERP aplikace	2 - 24	1	Výpadek max. 24 hodin = ztráta zhruba €2k / den. Ztráta dat = finanční ztráta zhruba €2k / den, delší než 1 den je likvidační.
účetní aplikace	2 - 24	1	Výpadek max. 48 hodin = ztráta zhruba €1k / den. Ztráta dat = finanční ztráta zhruba €200 / den.

hodnoty RTO a RTP jsou od - do a znamenají malý výpadek - maximální výpadek

Obrázek 7 Analýza dopadu na chod podniku [15]

Třetí fází je návrh a implementace. Zde IT odpovídá za zhodnocení možných rizik, které mohou nastat a následně k nim navrhnout opatření, a zpracovat plán záloh a obnovy. Následuje pak implementování navrženého řešení, které je probráno a odsouhlaseno s managementem firmy. [14][15][16]

Čtvrtou a poslední fází je pak rutinní provoz. Po nasazení řešení už je odpovědností IT pouze kontrola procesu zálohování a funkčnosti plánu obnovy. [14][15][16]

1.8 ZÁLOHOVACÍ MÉDIA

Pro zálohování dat existuje řada médií, na které je možné data ukládat a následně použít pro obnovu či archivovat. Každé z nich má jiné vlastnosti a tím i způsob použití. Výběr vhodného zálohovacího média tak závisí na kritériích jako je například jak často se budou data na zálohovacím mediu měnit, množství dat ukládaných na medium nebo jak často se k uloženým datům bude přistupovat.

1.8.1 CD/DVD

Nejlevnější a nejdostupnější médium na ukládání dat. Pro zapisování na tyto média je potřeba mít vypalovací mechaniku. V dnešní době je jejich kapacita pro zálohování velkých dat nedostatečná. Uplatnění najdou v archivaci či v osobním použití (hudba, filmy, fotografie). V případě zacházení či skladování je potřeba s nimi manipulovat šetrně, protože v případě poškrábání média může dojít k poškození či ztrátě dat. [8][9]

1.8.2 USB FLASH DISK

Malé a odolné medium vhodné spíše pro osobní účely či rychlou neobjemnou zálohu. Flash disk svou velikostí, výdrží a kapacitou nahrazuje optická média. Svou kapacitou mohou některé flash disky dosáhnout až 2TB. Jsou snadno skladovatelné a přenositelné. [8][9]

1.8.3 HDD/SSD

Pevné disky jsou vhodné pro zálohování velkého objemu dat. V případě HDD je potřeba opatrného zacházení, kdy může nastat mechanické poškození uvnitř disku. Rychlost zapisování HDD je vysoká ale v případě SSD disku je rychlost zapisování mnohem vyšší. [8][9]

1.8.4 NAS

NAS je síťové úložiště a dostupným řešením zálohování dat pro malé podniky. Jedná se o zařízení připojené do počítačové sítě, do kterého lze, v závislosti na druhu zařízení, zapojit více pevných disků a tím tak dosáhnout většího úložiště. Samotné zařízení pak pomocí vlastního softwaru dokáže spravovat zrcadlení disků či kontrolovat stav a zdraví disků. [8]

1.8.5 CLOUD

Ukládání dat na cloud je moderní a v dnešní době již velice oblíbený způsob. Jeho výhodou je možnost sdílení dat přes internet s kýmkoliv a mít k nim přístup kdekoliv. Data na cloudových serverech jsou uložena na velkém množství serverů po celém světě a zabezpečena proti úniku. [8][9]



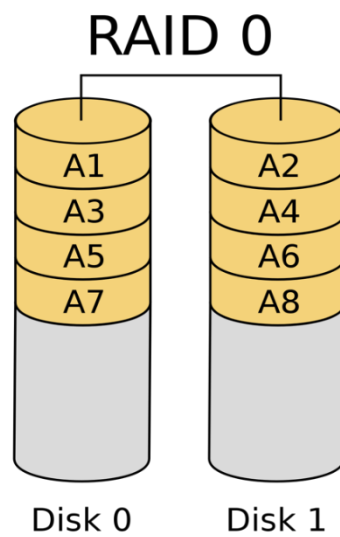
Obrázek 8 Zálohovací média [35][36][37]

1.9 OCHRANA DAT POMOCÍ RAID

RAID (Redundant Array of Inexpensive/Independent Disks) zastupuje označení pro disková pole skládající se ze dvou či více nezávislých disků na které se ukládají data. Z takto zapojených fyzických disků pak příslušný software udělá jednu logickou jednotku. Při selhání některého disku z diskového pole je možné rychle obnovit data díky redundanci. Samotný RAID je ale ochranou před hardwarovým selháním a před ztrátou dat smazáním či hackerským útokem neochrání, a proto je k němu doporučeno mít i standardní zálohování. [2][6]

1.9.1 RAID 0

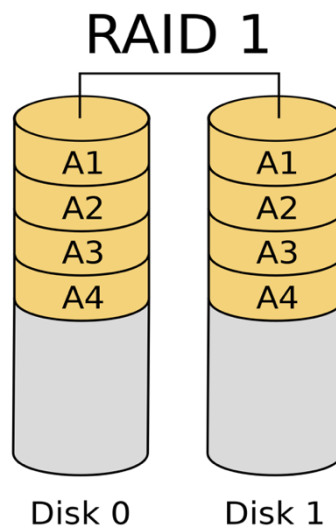
RAID 0 není RAID jako takový, jelikož nevytváří redundantní data. Používá se zejména kvůli vyššímu výkonu, kdy se data ukládají na disky střídavě a díky tomu zápis či čtení probíhá rychleji. Na RAID 0 se nedoporučuje ukládat kritická data. [2][6]



Obrázek 9 RAID 0 [7]

1.9.2 RAID 1

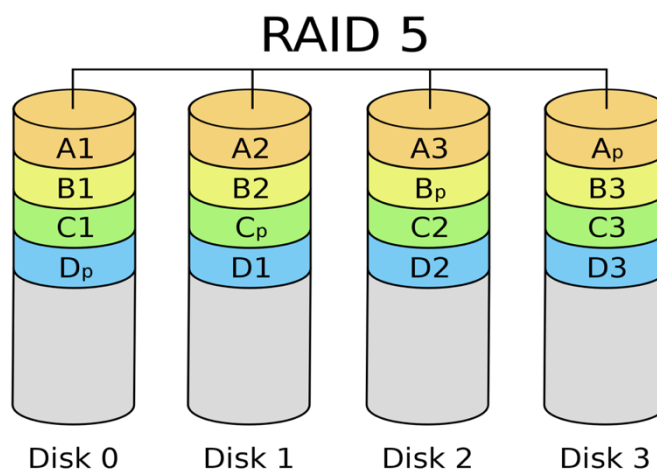
Pro RAID 1 už jsou potřeba disky minimálně 2, protože se data zrcadlí z jednoho disku na druhý a vytvářejí tak redundanci. Tolerance selhání s počtem disků roste. Například při dvou discích může selhat jen jeden a při třech už mohou selhat dva atd... Rychlostí je RAID 1 pomalejší při zápisu dat, protože se data zapisují v závislosti na počtu disků. Čtení je zas naopak rychlejší. [2][6]



Obrázek 10 RAID 1 [7]

1.9.3 RAID 5

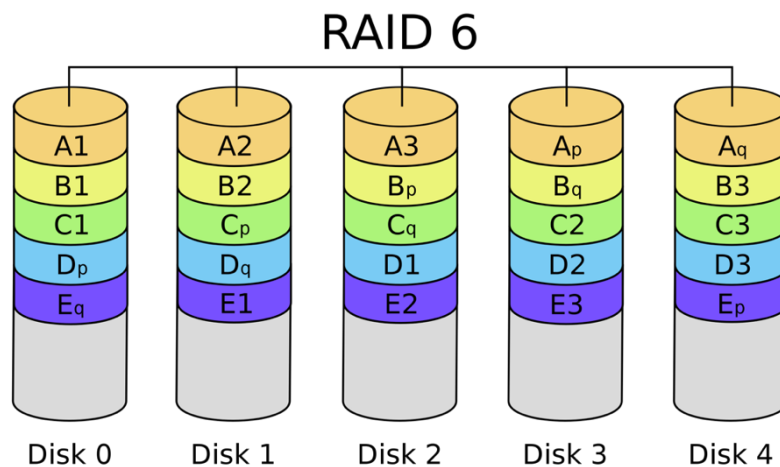
Pro vytvoření RAID 5 je minimální počet potřebných disků 3. RAID 5 ukládá data střídavě na dva a více disků a zároveň k nim vytváří samoopravný kód nebo také známý jako parita, který je rovněž různě ukládán na discích. Samoopravný kód slouží jako pomoc při obnově dat při poškození původních dat. Výhodou RAID 5 je rychlost čtení díky rozdělení dat do bloků mezi jednotlivé disky. Nevýhodou je pak nižší rychlost zápisu kvůli nutnosti výpočtu samoopravného kódu. Dále pak tolerance selhání jen jednoho disku bez ohledu na celkový počet disků v poli. [2][6]



Obrázek 11 RAID 5 [7]

1.9.4 RAID 6

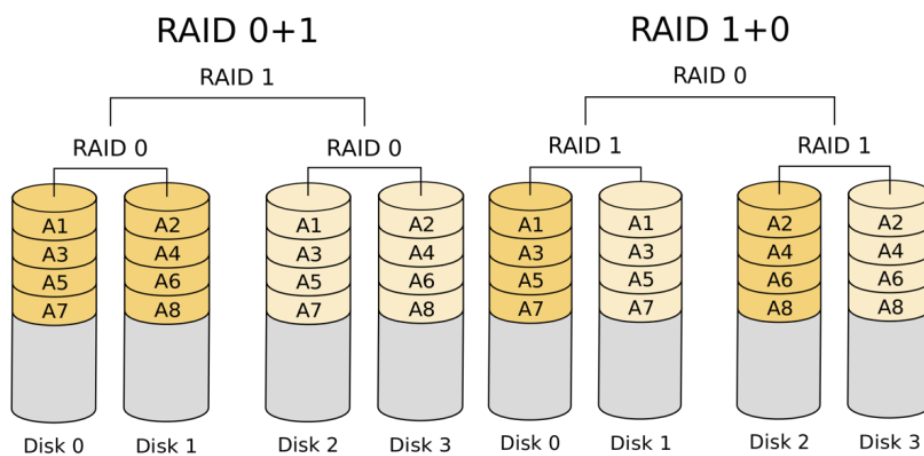
Fungováním je RAID 6 velice podobný jako RAID 5 liší se způsobem vypočítávání samoopravného kódu kdy RAID 6 vypočítává rovnou dva samoopravné kódy. Pro jeho vytvoření je potřeba mít alespoň 4 disky. Právě díky dvou samoopravným kódům toleruje RAID 6 selhání dvou disků. Rychlostí čtení dat je na tom podobně jako RAID 5, avšak při zápisu se na rychlosti podepisuje výpočet samoopravných kódů. Nevýhodou je, že se z velikostí všech disků odečítají dva disky. [2][6]



Obrázek 12 RAID 6 [7]

1.9.5 RAID 01 A RAID 10

RAID 01 (0+1) je zástupce víceúrovňového typu RAID. Jde o kombinaci typu RAID 0 a RAID 1. Pro jeho vytvoření je potřeba minimálně čtyř disků. RAID 01 na první úrovni vytvoří dva totožné páry disků, na který střídavě ukládá data odpovídající RAID 0. Zrcadlení mezi těmito páry disků operuje pomocí RAID 1 na druhé úrovni RAID 10 [2][6]



Obrázek 13 RAID 01 a RAID 10 [7]

2 ANALÝZA PROBLÉMU A SOUČASNÉ SITUACE

Společnost XYZ s.r.o. je poměrně mladý komplexní hráč na poli práva a advokacie, který se zabývá širokým spektrem právních služeb od insolvenčního práva, přes realitní, stavební a pozemkové právo až po zastupování v trestním řízení. Společnost, která je zákazníkem IT firmy pro kterou pracuji, má momentálně více než 25 zaměstnanců, a to i díky nedávnému spojení s další právní společností. Spolu se spojením byly potřeba i větší prostory, a proto se nedávno společnost přestěhovala z centra Brna do moderní kancelářské budovy v městské části Brno Židenice. Právě zmiňované stěhování a rozšiřování kolektivu bylo důvodem a motivací pro modernizaci počítačové sítě.

2.1 POČÍTAČOVÁ SÍT SPOLEČNOSTI

Srdcem počítačové sítě je serverovna, ve které je umístěn server společně s routerem a switchem. K propojení serveru a počítačů mezi sebou a internetem slouží dvojice fyzických prvků od firmy Ubiquity a to konkrétně router UniFi Dream Machine Pro a 48 portový switch USW-48-PoE uložený v nástěnném racku. O bezdrátové připojení se pak starají tři přístupové body UniFi U6-Pro také od firmy Ubiquiti rozmístěné po kanceláři pro zajištění stálého a silného signálu.

Do routeru je přiveden internet pomocí optického kabelu a propojení routeru se switchem je poté realizováno pomocí ethernetových kabelů cat5. Tyto kabely jsou rovněž použity pro propojení switchu s přípojkami umístěnými ve floorboxech v kanceláři.

Do této sítě je i připojen již zmiňovaný server, který plní úlohu doménového serveru a firemního uožiště, ke kterému uživatelé přistupují přes lokální síť jako ke sdíleným diskům. K serveru, konkrétně k sdíleným diskům, se lze připojit i vzdáleně pomocí VPN. Server je zastaralý a již nevyhovuje svým výkonem dnešním standardům. Nevyhovuje ani softwarové vybavení serveru. Server totiž běží na systému Windows Server 2016 essentials, který se dá již považovat za zastaralý. Zároveň s přibývajícimi zaměstnanci se společnost blíží k vyčerpání limitu povolených uživatelů, který je tímto systémem a jeho licencí určen na 25 uživatelů.

2.2 HARDWAROVÁ VÝBAVA SPOLEČNOSTI

2.2.1 POČÍTAČ

V současné době společnost disponuje širokým výběrem počítačů s různými parametry, kde většina z nich nesplňuje naše výkonnostní požadavky, které doporučujeme. Právě tyto nevyhovující počítače postupně modernizujeme za nové s následujícími parametry.

Konfigurace:

Název: Dell Optiflex 3000

Procesor: Intel(R) Core(TM) i5-12500 3.00GHz

Operační paměť: 16GB DDR4

Úložiště: SSD M.2 256GB

Operační systém: Windows 10/11 Pro



Obrázek 14 Dell OptiPlex 3000[18]

2.2.2 SERVER

Server je v provedení „Mini tower“. Momentálně server obsluhuje služby DNS, DHCP, Active Directory a VPN. Zároveň funguje i jako firemní úložiště (File server).

Konfigurace:

Název: Dell PowerEdge T30

Procesor: Intel(R) Xeon(R) CPU E3-1225 v5 @ 3.30GHz

Operační paměť: 8GB DDR4

Úložiště: 4TB

Operační systém: Microsoft Windows Server 2016 Essentials



Obrázek 15 Server PowerEdge T30 Mini Tower[20]

2.2.3 ROUTER

UniFi dream machine pro je zařízení, které v sobě sjednocuje router, switch a bezpečnostní bránu. Toto zařízení je vhodné pro provoz v podnikových sítích malých a středně velkých firmem. Router disponuje již zmiňovanými 8 lan porty s přenosovou

rychlostí 1 Gbps, dvěma SFP+ porty pro připojení optického kabelu a jednoho WAN portu.

Hlavními přednostmi zařízení jsou podpora VPN, vysoká přenosová rychlost až 3,5 Gbps a jednoduchá správa pomocí aplikace UniFi Controller.[23]



Obrázek 16 Router UniFi Dream Machine[23]

2.2.4 SWITCH

USW-48-PoE je gigabitový switch s podporou PoE (Power over Ethernet), který je ve společnosti využíván zejména pro napájení přístupových bodů bezdrátového připojení k internetu. Switch je také možné spravovat pomocí aplikace UniFi controller, díky kterému lze PoE porty vzdáleně vypnout a následně zapnout.[24]



Obrázek 17 Switch USW-48-PoE[24]

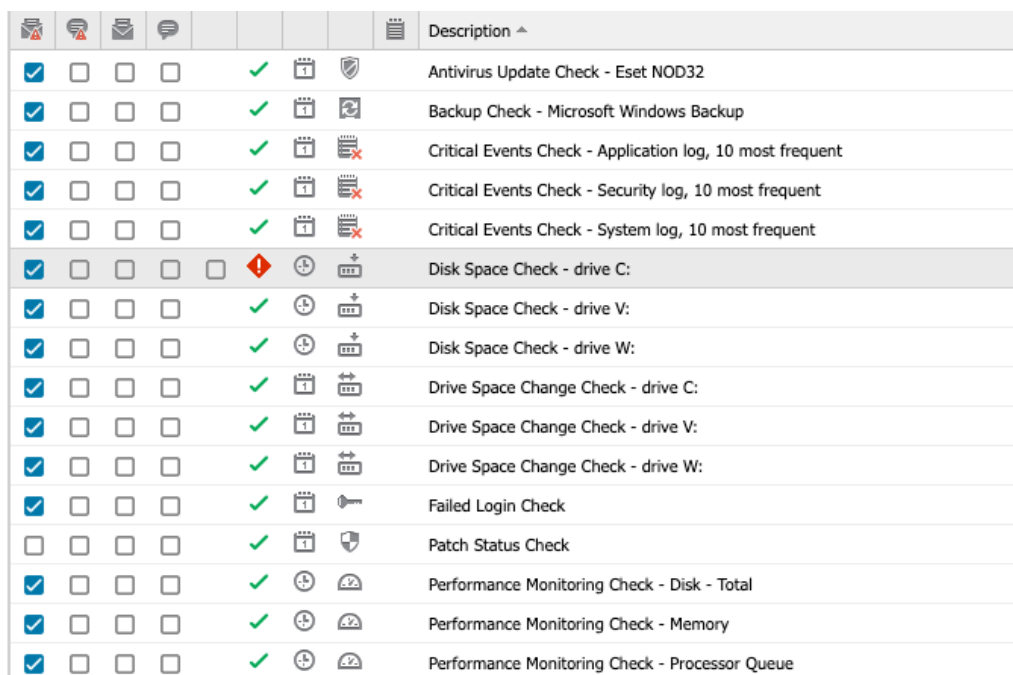
2.3 ZÁLOHOVÁNÍ

Momentální způsob zálohování probíhá pomocí softwaru Microsoft Windows backup na dva externí pevné disky připojené do počítače. Úloha spuštění záloh je nastavena na každý den ve večerních hodinách, aby nenarušovala běžný chod během pracovního dne. Toto řešení je nespolehlivé a nevyhovující, protože zde není žádné zrcadlení disků a v případě kritické havárie hardwaru nemáme žádný jiný disk na kterém bychom zálohovaná data měli.

2.4 ZABEZPEČENÍ

Všechna firemní zařízení včetně serveru jsou chráněna pomocí antiviru ESET Endpoint security napojeného na vzdálenou správu, kde kontrolujeme podezřelé chování nebo aktuálnost verzí.

Dále pak všechna zařízení monitorujeme pomocí softwaru, který do našeho systému sbírá telemetrická data o zařízení a jsme tak schopni předpovědět, zda-li zařízení selhává a s předstihem daný problém řešit. Tento software nám také dovoluje kontrolovat stav aktualizací aplikací nebo operačního systému a vzdáleně je aktualizovat.



						Description ^
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Antivirus Update Check - Eset NOD32
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Backup Check - Microsoft Windows Backup
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Critical Events Check - Application log, 10 most frequent
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Critical Events Check - Security log, 10 most frequent
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Critical Events Check - System log, 10 most frequent
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		Disk Space Check - drive C:
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Disk Space Check - drive V:
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Disk Space Check - drive W:
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Drive Space Change Check - drive C:
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Drive Space Change Check - drive V:
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Drive Space Change Check - drive W:
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Failed Login Check
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Patch Status Check
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Performance Monitoring Check - Disk - Total
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Performance Monitoring Check - Memory
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Performance Monitoring Check - Processor Queue

Obrázek 18 Přehled sledovaných telemetrických dat

3 VLASTNÍ NÁVRHY ŘEŠENÍ

3.1 NÁVRH FYZICKÉHO SERVERU

3.1.1 POŽADAVKY SPOLEČNOSTI NA SERVER

Hlavním požadavkem ze společnosti je zaručení bezproblémové funkčnosti a dostupnosti. Protože se k uložení na serveru bude připojovat velké množství uživatelů, je potřeba zajistit dostatečný výkon, aby nedocházelo k zpomalení serveru. Jelikož s firmou vedeme již dlouhou spolupráci v oblasti IT, tak velice dobře známe jejich požadavky. Server bude obsluhovat službu VPN, DNS, DHCP, Active Directory a bude sloužit jako úložiště pro firemní dokumenty (tzv. File Server). Společnost nevyužívá pro práci žádný speciální software, který by potřeboval výrazně vyšší výkon serveru.

Zařízení, které budeme navrhovat, bude primárně od firmy Dell. Se značkou máme ve firmě dlouholetou zkušenost, co se týče funkčnosti a spolehlivosti, ale také jsme spokojeni s jejich technickou podporou, kdy v případě nouze jsou schopni nefunkční zařízení do 24 hodin vyměnit.

3.1.2 DELL POWEREDGE R350

Jelikož společnost v nových prostorách disponuje nástěnným rackem, kde je uložený router společně se switchem, nabízí se možnost pořídit server v provedení pro uložení do racku. V tomto případě je zvolen konfigurovatelný model **DELL PowerEdge R350** s následujícími technickými údaji.[17]

Technické údaje:

Název: Dell PowerEdge R350

Procesor: Intel® Xeon® řady E-2300 s až 8 jádry na procesor

Sloty pro paměťové moduly: 4 sloty DDR4 DIMM (Max 128 GB)

Úložiště: Až 4× 3,5palcový disk SAS/SATA (pevný disk nebo disk SSD), maximálně 64 TB

Operační systém: Microsoft® Windows Server® s technologií Hyper-V



Obrázek 19 Dell PowerEdge R350[18]

3.1.3 DELL POWEREDGE T350

Jako druhou variantu serveru jsem vybral věžový server, kdy jde o zařízení v klasické počítačové skříni. Důvod pro tento výběr je, že společnost má svůj momentální server v provedení MiniTower. Výhodou věžového serveru je snadná dostupnost pro výměnu komponentů, nebo případě poruchy se server v rychlosti odpojí a je připraven k odvozu do servisu. Pro tento případ jsem si vybral konfigurovatelný model **DELL PowerEdge T350** s následujícími technickými údaji. [17]

Technické údaje:

Název: Dell PowerEdge T350

Procesor: Intel® Xeon® řady E-2300 s až 8 jádry na procesor

Sloty pro paměťové moduly: 4 sloty DDR4 DIMM (Max 128 GB)

Úložiště: Až 4× 3,5palcový disk SAS/SATA (pevný disk nebo disk SSD), maximálně 64 TB

Operační systém: Microsoft® Windows Server® s technologií Hyper-V



Obrázek 20 Dell PowerEdge T350[17]

3.1.4 VYBRANÉ ŘEŠENÍ

Pro finální řešení byl zvolen fyzický server „DELL POWEREDGE T350“ v provedení věžový server, z důvodu kapacitního omezení nástěnného racku, do kterého by se rackový server nevešel. Dalším důvodem je lehčí přístupnost, jelikož je rack umístěn vysoko na stěně a v případě jakýchkoliv potřeb by byla manipulace se serverem v racku obtížná. Co se týče výkonu jsou si oba servery podobné. Server bude umístěn v serverovně, kde je umístěn i nástěnný rack z důvodu zabezpečení zamykatelnými dveřmi, ke kterým má přístup jen správce sítě.

3.1.4.1 HARDWAROVÁ KONFIGURACE

Vybraný server byl vybrán v následující konfiguraci.

Procesor: Intel® Xeon® E-2378G 2.8GHz, 16M Cache, 8C/16T, Turbo (80W), 3200 MT/s

Operační paměť: 4x 16 GB UDIMM

Úložiště: 2x 480 GB SSD

2x 8 TB HDD

Operační systém: Windows Server 2022 Standard,16CORE, FI, No Med,No CAL, MultiLanguage

3.1.4.2 SYSTÉMOVÉ NASTAVENÍ

Před uvedením serveru do ostrého provozu ho bude potřeba nejdříve nastavit. Potřeba je správně nainstalovat a nastavit operační systém, nakonfigurovat Active Directory, GPO politiky, nainstalovat tiskárny, vytvořit uživatele, adresářové sktruktury, přesunout uživatelské profily do nového doménového prostředí, VPN řešení ze starého serveru, vytvořit segmentaci sítě pro oddělení záloh od produkčních dat, nastavení zálohování, nastavení monitoringu.

3.1.4.3 LICENCOVÁNÍ

Momentálně starý server běží na operačním systému Microsoft Windows Server 2016 Essentials s licencí vázanou na server, která je vhodná pro malé firmy do 25 uživatelů a 50 zařízení bez nutnosti pořízení CAL (Client Access Licenses) licence.

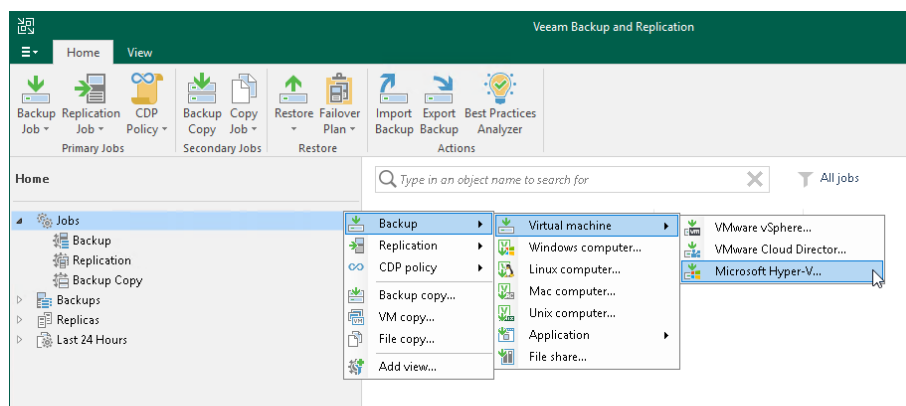
Firma má momentálně přes 25 zaměstnanců, a právě proto je potřeba pořídit na nový server novější a vyšší verzi operačního systému Microsoft Windows Server 2022 Standart licencovanou podle počtu jader procesoru. Zároveň pro tento operační systém je již potřeba pro každého zaměstnance/uživatele přistupujícího k serveru pořídit CAL licenci.

CAL licence lze licencovat na uživatele nebo zařízení a dotyčnému pak umožňuje přístup ke službám a funkcím Windows serveru jako je například Active Directory, tisknutí nebo File Server. V tomto případě budeme CAL licence pořizovat pro jednotlivá zařízení v organizaci.[38][39]

3.1.4.4 ZÁLOHOVÁNÍ

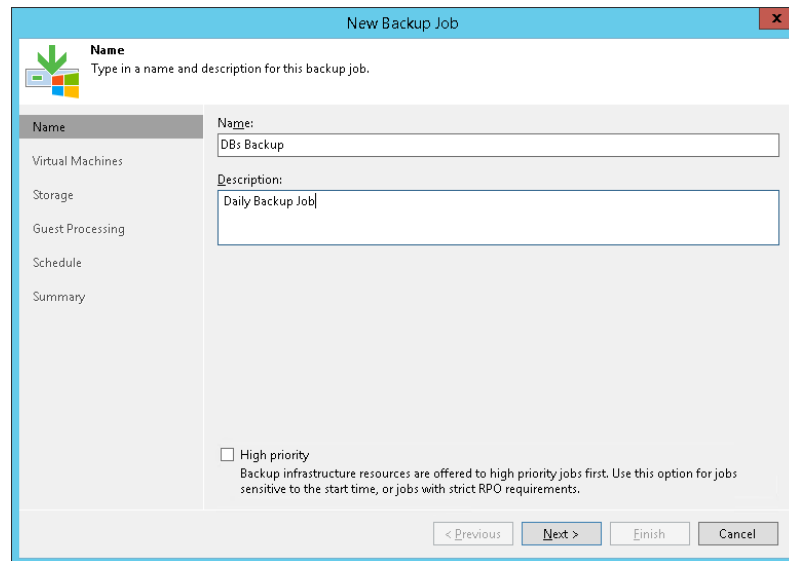
Licence Microsoft Windows Server 2022 Standart umožňuje na fyzickém serveru provozovat 2 virtuální prostřední. Jedno využijeme jako server pro produkční data a druhé využijeme pro zálohovací software Veeam backup and replication, kterým budeme server s produkčními daty zálohovat. Nastavení zálohování vypadá následovně.

Základem je vytvořit si nový zálohovací plán v na domovské stránce aplikace, kdy si z levé lišty rozklikneme nabídku „Jobs“, vybereme „Backup“ a následně vybereme Virtual machines a v našem případě vybereme Microsoft Hyper-V.



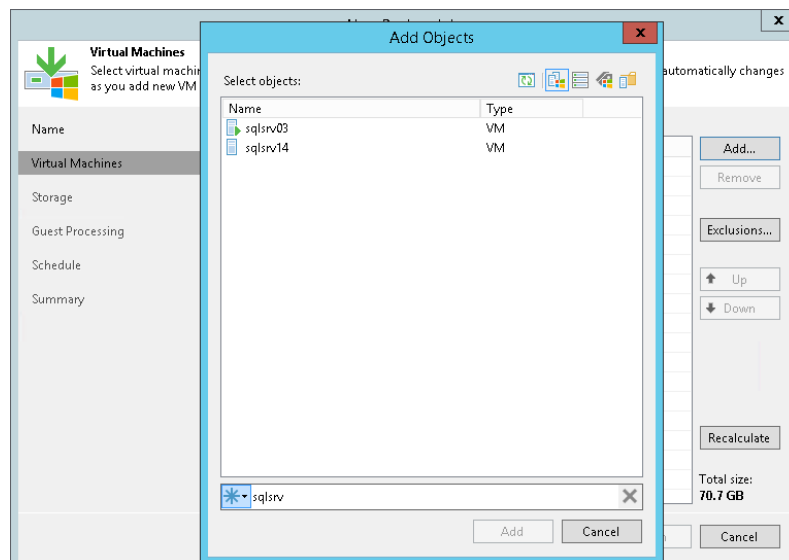
Obrázek 21 Vytvoření nového plánu[42]

Dále nás pak průvodce nastavení vyzve k pojmenování a popisu zálohovacího plánu



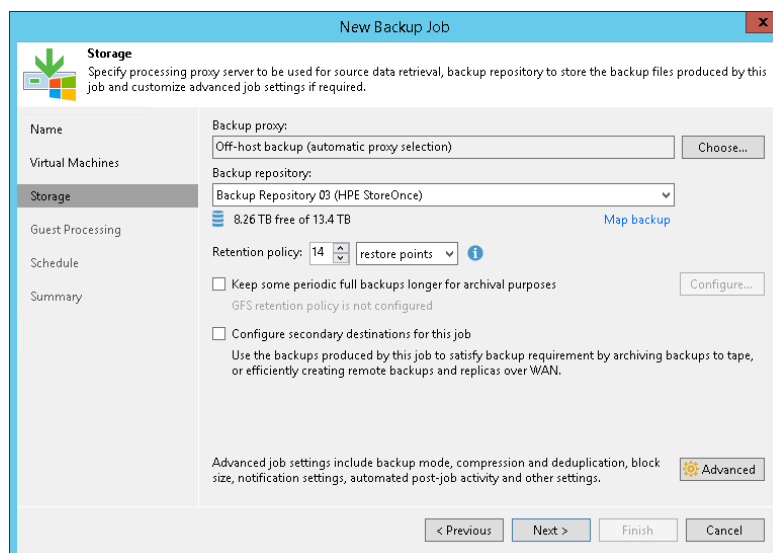
Obrázek 22 Pojmenování zálohovacího plánu[42]

Třetí krok nám umožňuje vybrat, které virtuální prostředí chceme zvolit. V našem případě vybereme ten server, na kterém jsou produkční data. V tomto kroku lze nastavit i pořadí zálohování, ale vzhledem k zálohování pouze jednoho virtuálního prostředí nemusíme pořadí nastavovat.

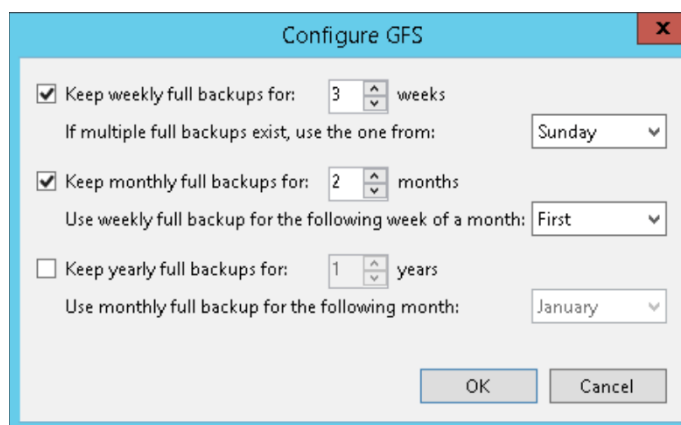


Obrázek 23 Výběr virtuálního prostředí[42]

Následně nás průvodce nastavením vyzve k vybrání úložiště, na které budeme chtít ukládat zálohy.



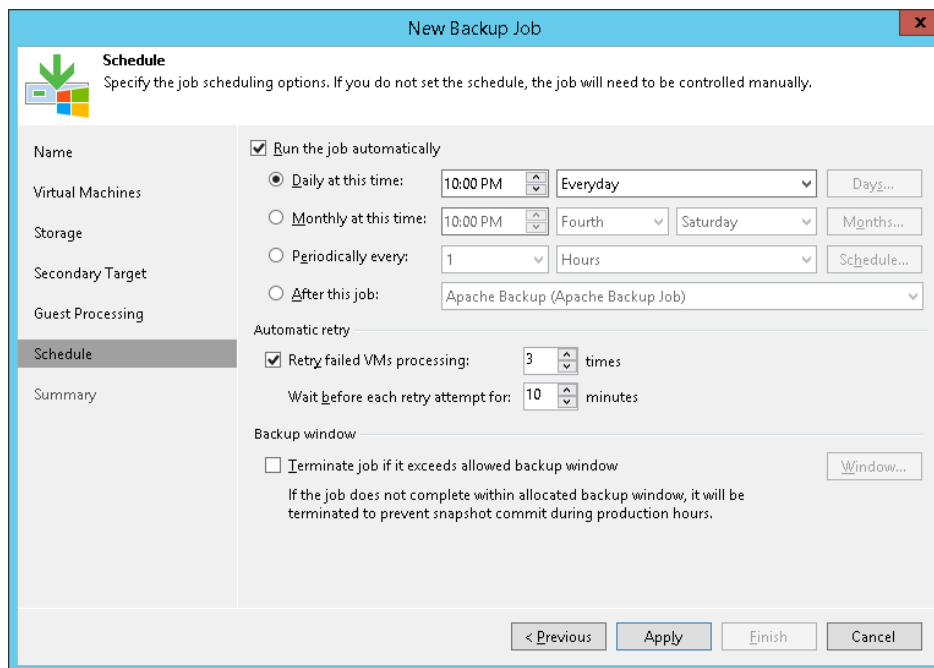
Obrázek 24 Výběr úložiště pro zálohování[42]



Obrázek 25 Nastavení rotace plných záloh[42]

Během výběru úložiště můžeme nastavit i délku doby po jakou se na úložišti uchovávají jednotlivé opakovatelné plné zálohy.

Posledním krokem před uložením a spuštěním plánu je nastavení času spuštění. V našem případě budeme provádět zálohu každý den ve večerních hodinách, kdy již na serveru nikdo nebude pracovat a budeme moc využít výkon serveru pro zálohování.



Obrázek 24 Nastavení časového plánu spouštění[42]

Pak už jen zálohovací plán uložíme a spustíme první plnou zálohu serveru.

3.2 ZPŮSOB MIGRACE DAT NA NOVÝ SERVER

3.2.1 INSTALACE STARÉHO DISKŮ DO NOVÉHO SERVERU

Jako první řešení připadá v úvahu do nového serveru připojit disk ze starého serveru. Řešení by to bylo velice jednoduché v případě provedení věžového serveru, ale je třeba brát v potaz stáří disku, které by mohlo do budoucna vyvolat problém v podobě poruchy disku a možné ztráty dat. Tomu lze předejít důkladným monitoringem a sledováním zdraví hardwaru.

3.2.2 ZRCADLENÍ STAREHO DISKŮ NA NOVÝ

Druhým řešením je zrcadlení starého disku na nový. Oproti prvnímu řešení je toto dražší a časově náročnější varianta, protože je potřeba pořízení nových disků a poté pomocí speciálních softwarů kopírování všech dat ze starého disku na nový.

3.2.3 VYBRANÉ ŘEŠENÍ

Po důkladné analýze zdraví a spolehlivosti instalovaných disků bylo rozhodnuto o pořízení nových disků do nového serveru. Konkrétně dvou osmi terabajtových serverových pevných disků od společnosti DELL vhodných pro vybraný server.

Staré disky již nevyhovují požadovaným nárokům nového serveru. Dále pak při spuštění zálohování jsou disky maximálně vytíženy, což v dlouhodobém měřítku může znamenat hardwarové selhání vzhledem k věku instalovaných disků.

Veškerá data na starých discích by se pak pomocí programu po lokální síti kopírovala bez příslušných práv na nové disky v novém serveru.

3.3 NÁVRH ZPŮSOBU ZÁLOHOVÁNÍ DAT MIMO LOKALITU

3.3.1 ZÁLOHOVÁNÍ DO CLOUDU

První možnou variantou zálohování datového úložiště je zálohování do cloudu. Výhodou zálohování do cloudu je především lokalita. Uložená data se posílají přes internet do datových center a v případě nějakého incidentu ve firmě v podobě krádeže, havárie nebo hackerského útoku máte data kompletně izolovaná a jsou přístupná odkudkoliv. Rovněž dnešní poskytovatelé cloudových služeb jsou certifikováni na nejvyšší úrovni bezpečnosti a prací s daty zákazníků. Nevýhodou je potřeba pro úlohu zálohování velmi rychlý a stabilní internet pro přenos velkého množství dat.

Další nevýhodou je provozní náklad v podobě měsíčního pronájmu cloudových služeb. Poskytovatelé služeb si za každý GB účtují peníze a při uložení čítající terabajty se to na ceně služby značně projeví.

3.3.2 ZÁLOHOVÁNÍ NA NAS

Dalším řešením je zálohování na chytré datové úložiště připojené do místní sítě firmy. Z pohledu spolehlivosti a bezpečí dat je toto řešení vyhovující hlavně pro menší a středně velké firmy kdy NAS umístíme do jiné místnosti, než je server a tím snížíme riziko ztráty dat při havárii. Do NAS je možné zapojit více disků a zajistit zrcadlení úložiště a tím předejít hardwarovému selhání. Z finančního hlediska se jedná spíše o investici, kdy jednorázově pořídíme hardware, který pak následně bez dalších poplatků využíváme.

3.3.2.1 SYNOLOGY DS220J

Jako první na výběr se nabízí NAS SYNOLOGY DS220J jako zástupce cenově dostupnějšího zařízení, které má dvě volné pozice pro pevné disky. Výkon tohoto zařízení není zas tak úplně vyhovující[40]

Technické údaje:

Maximální kapacita: 32 000 GB

Operační paměť: 512 MB

Procesor Realtek RTD1296 1,4 GHz

Spotřeba: 12,46 W při plném zatížení, 5,06 W při hibernaci

Cena: 4 049,- bez dph

3.3.2.2 SYNOLOGY DS220+

SYNOLOGY DS220+ je výkonnější nástupce DS220J. Jeho operační systém nabízí více možností a obsahuje dva 1GbE porty pro rychlejší nahrávání dat.[22]

Technické údaje:

Maximální kapacita: 32 000 GB

Operační paměť: 2 GB

Procesor Intel Celeron J4025 2 GHz

Spotřeba: 14,69 W při plném zatížení, 4,41 W při hibernaci

Cena: 7 143,- bez dph

3.3.2.3 QNAP TS-231P3-2G

QNAP TS-231P3-2G je konkurenční zařízení pro DS220+. Jedná se rovněž o dvou diskové úložiště s lehce nižším výkonem ale vyšší spotřebou. Cenově toto zařízení je dražší.[41]

Technické údaje:

Maximální kapacita: 32 000 GB

Operační paměť: 2 GB

Procesor Alpine AL314 1,7 GHz

Spotřeba: 15,6 W při plném zatížení, 8,46 W při hibernaci

Cena: 7 437,- bez dph

3.3.3 ZÁLOHOVÁNÍ NAS VS. CLOUD

Při rozhodování mezi zvolenými variantami NAS nebo Cloud je potřeba se zamyslet nad typem ukládaných a zálohovaných dat a jejich využitím. Dalším bodem při rozhodování je zabezpečení.

V dnešní době se cloudové služby spíše využívají jako místo pro ukládání, sdílení a synchronizaci dat a jsou zaměřeny na používání více uživateli než jako jednotné úložiště pro zálohy. A podle toho je pak nastavena nabídka služeb, kdy poskytovatelé těchto služeb počítají s více uživateli a případnou synchronizací s počítači uživatelů úložiště.

Soubory používané v organizaci jsou výhradně dokumentových typů jako je například .docx programu Microsoft Word, .xlsl pro Microsoft excel, .pdf pro Adobe Acrobat Reader a nebo multimédia v podobě fotek či videí potřebných k soudním řízením. Zálohování na cloud by pak mělo smysl z hlediska velikosti nahrávaných souborů kdy v případě inkrementální zálohy by se na cloud nahrávalo malé množství změněných či nahraných souborů a tím by záloha netrvala zbytečně dlouho.

Jak už je výše uvedeno, jedná se o advokátní kancelář, která pracuje s dokumenty jako jsou například smlouvy, trestní oznámení a podobné obsahující citlivé či důvěrné informace. Z toho to důvodu je velice riskantní zálohovat tyto soubory na cloudová úložiště.

Při napadení hackery poskytovatele cloudových služeb hrozí, že se citlivé informace dostanou do nesprávných rukou a mohou být sdíleny s kýmkoliv po celém internetu. I když je toto riziko málo pravděpodobné skrze úroveň zabezpečení poskytovatelů není vylučitelné. Stejně tak tomu může být v případě přístupnosti odkudkoliv přes internet. Zaměstnanec se může v rámci přípravy na soudní jednání připojit na nezabezpečenou wifi a útočník může napadnout jeho zařízení a opět získat přístup na cloudové úložiště.

V případě zálohování na NAS lze toto riziko ztráty dat útočníkům ztížit. Tím, že NAS úložiště umístěno v kanceláři, lze nastavit přístup pouze jen z lokální sítě a vytvoří se uživatelský účet na NAS jenom pro zálohování který bude mít nastavený přístup jenom do složky se zálohami a dostatečně dlouhé a složité heslo a dvou fázové ověření. Zaměstnanci pak k datům uloženým na serveru mimo lokální síť budou přistupovat přes zabezpečenou VPN. Dále pak server i zaměstnance zaopatřit kvalitním antivirem a důkladným monitoringem sledovat dění na síti i na serveru. A v neposlední řadě nastavení firemní IT politiky týkající se síly hesel. Data se pak při zálohování neodesílají na internet, ale pohybují se pouze v lokální síti.

Pro porovnání mezi NAS a cloudovými službami jsem vybral jako zástupce NAS zařízení od firmy SYNOLOGY, a to konkrétně model DS220+, který je jako zálohovací medium pro malé a střední organizace vhodnou volbou. Pro zástupce cloudových služeb jsem zvolil trojici poskytovatelů Microsoft a jeho OneDrive, Dropbox a Google Drive, kteří patří mezi špičku cloudových úložišť.

Společnost si od úložiště slibuje vysokou kapacitu s přesahem do budoucnosti, kdy postupem času budou data přibývat. Dále pak požaduje vysokou úroveň zabezpečení. A jako poslední si přála mít zálohy uspořádané na jednom místě

V porovnání pak lze vidět pořizovací cenu jednotlivých možností, velikost, úložiště a dostupnost a požadavky společnosti na úložiště.

Tabulka 1 Porovnání NAS vs Cloud

	NAS	Cloudové úložiště		
Zařízení/služba	Synology DS220+	OneDrive	DropBox	Google Drive
Cena	7189,- + Disky	8,40€/uživatel/měsíc	18€/uživatel/měsíc	18€/uživatel/měsíc
Max.úložiště	Dle potřeby	5 TB	Dle potřeby	5 TB
Dostupnost	Lokální síť	Kdekoliv z internetu		
Kontrola nad zařízením/službou	Kompletní	Pouze nad daty uložených na serverech poskytovatele		

Úroveň zabezpečení	Vysoká	Vysoká (Zaručeno poskytovatelem)		
Požadovaná kapacita úložiště	Vyhovuje	Nevyhovuje	Vyhovuje	Nevyhovuje
Organizace dat	Jednotné úložiště	Osobní úložiště pro uživatele		

Pokud budeme pak brát v potaz životnost disků do NAS v délce 3-5 let pak se nám sice z hlediska ceny vyplatí pořídit jakoukoliv cloudovou službu zejména pak OneDrive který je ze tří uvedených nejlevnější.[22][25][26][27]

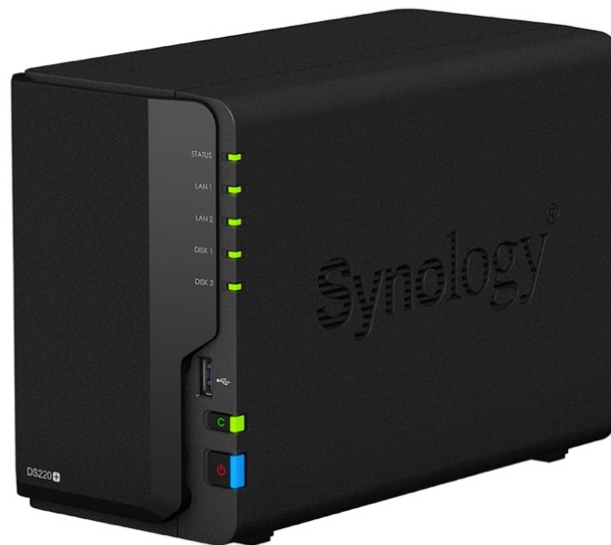
Požadovanou kapacitou vyhovuje pouze NAS a online úložiště dropbox které ve své nabídce umožňuje mít libovolně veliké úložiště.

Co se týče organizace dat je pro naše použití vhodnější NAS, protože v případě ukládání či synchronizování dat na online úložiště může dojít během hackerského útoku k zašifrování či přepsání dat vícekrát než dovoluje historie online úložiště a tím pádem bychom neměli žádné data k obnově. Mezitím zálohováním na NAS pomocí programů je možné vytvářet kopie záloh a mít tak uložený daný stav v daném časovém období a tím zvýšit šanci na obnovu dat po havárii.

Z hlediska bezpečnosti a citlivosti dokumentů je vhodnější data na internet vůbec nenahrávat a ukládat je na fyzický sever v kanceláři, jelikož nad nimi máme kompletní kontrolu, a ze serveru je pak následně zálohovat na jiné zařízení.

3.3.4 VYBRANÉ ŘEŠENÍ

Pro způsob zálohování mimo lokalitu bylo rozhodnuto vybrat variantu pořízení chytrého datového úložiště NAS připojeného do místní sítě. Konkrétní řešení bylo vybráno z důvodů využití serveru, kdy se server nevyužívá pouze jako file server, a proto je zbytečné, aby si firma platila výpočetní výkon na cloudu. Zároveň zálohy obsahují data, které obsahují citlivé informace, a proto je nežádoucí jejich posílání a ukládání na internet. Pro tento případ navrhuji pořídit „SYNOLOGY DS220+“, se kterým máme ve společnosti dobré zkušenosti.



Obrázek 25 NAS Synology DS220+

3.3.5 PLÁN OBNOVY

Abychom zajistili co nejrychleji a nejkvalitněji obnovu po havárii volíme RPO 1 den, kdy při výkonu serveru a NAS vychází tato volba neekonomičtěji a data nejsou nijak kritická pro chod firmy, aby je bylo potřeba zálohovat například každou hodinu. V návaznosti na to jsme stanovili RPO na 12-24 hodin kdy v případě výpadku je možné že většina zaměstnanců je mimo kancelář na soudních jednáních či na konzultacích s klienty Pro co nejrychlejší obnovu proto volíme strategii každodenního inkrementálního zálohování s plnou zálohou jednou týdně, aby v případě havárie obnova netrvala příliš dlouho.

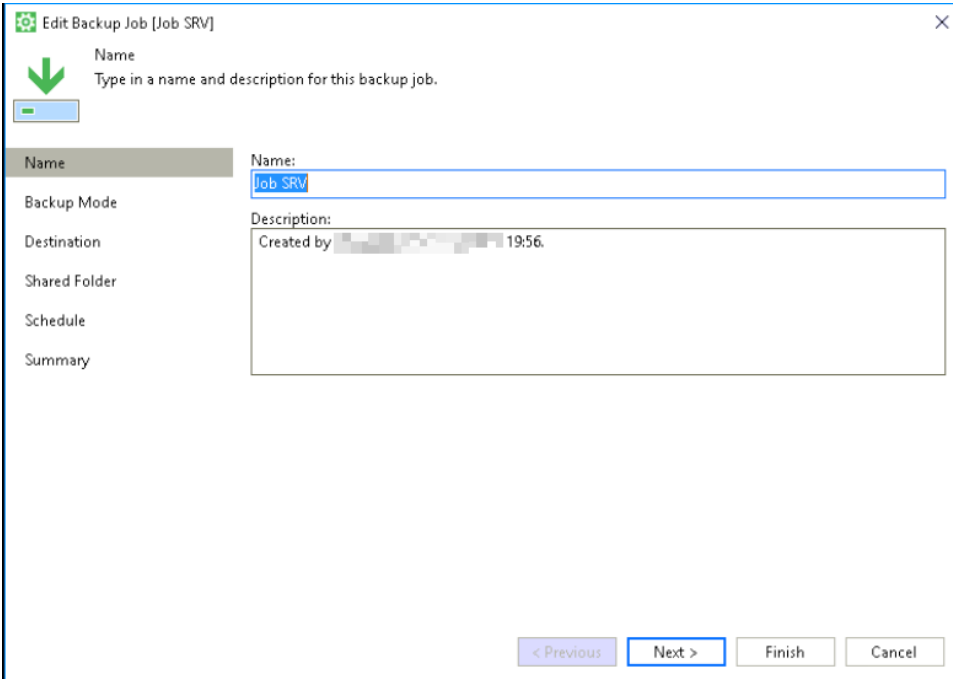
3.3.6 VEEAM AGENT FOR MICROSOFT WINDOWS

Pro úkony zálohování jsem zvolil program Veeam Agent for Microsoft Windows. Veeam Agent je bezplatný a umožňuje vytvářet zálohy v podobě bitových kopií a jejich následné obnovení. Počítač je tak možné zálohovat na externí disk nebo na NAS.

Tento agent funguje na stejné technologii jako jeho sesterský software Veeam Backup & Replication který je komerční a využívá se převážně pro virtuální prostředí jako je například VMware.

3.3.7 NASTAVENÍ PLÁNU ZÁLOHY

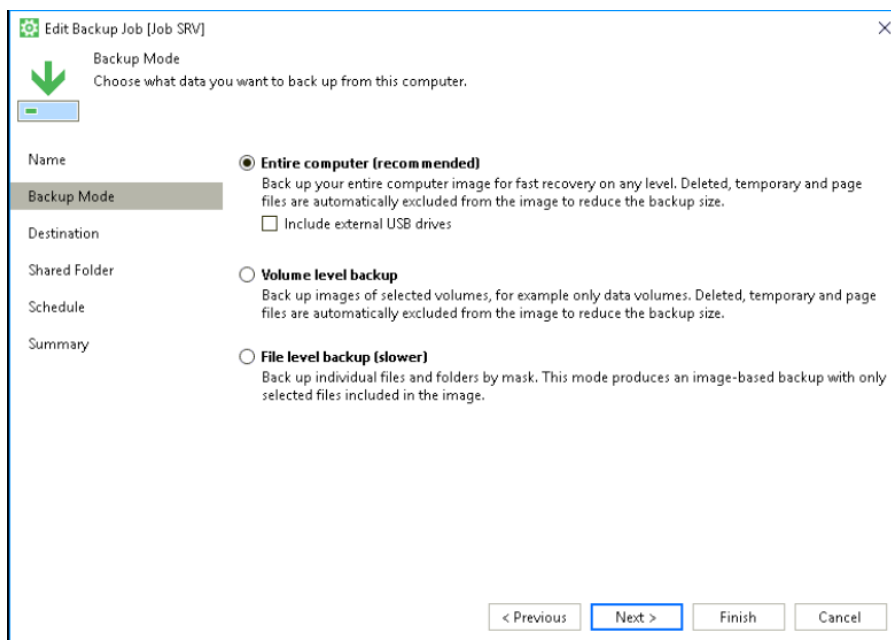
Při nastavování plánu zálohy nás program jako první vyzve k pojmenování úlohy a případnému popisu



The screenshot shows a dialog box titled "Edit Backup Job [Job SRV]". On the left, there is a vertical list of tabs: "Name", "Backup Mode", "Destination", "Shared Folder", "Schedule", and "Summary". The "Name" tab is currently selected. Above the tabs, there is a green downward arrow icon and the text "Name" and "Type in a name and description for this backup job." Below this, there is a small blue button with a minus sign. The "Name" field contains the text "Job SRV". The "Description" field contains the text "Created by [redacted] 19:56". At the bottom right of the dialog, there are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

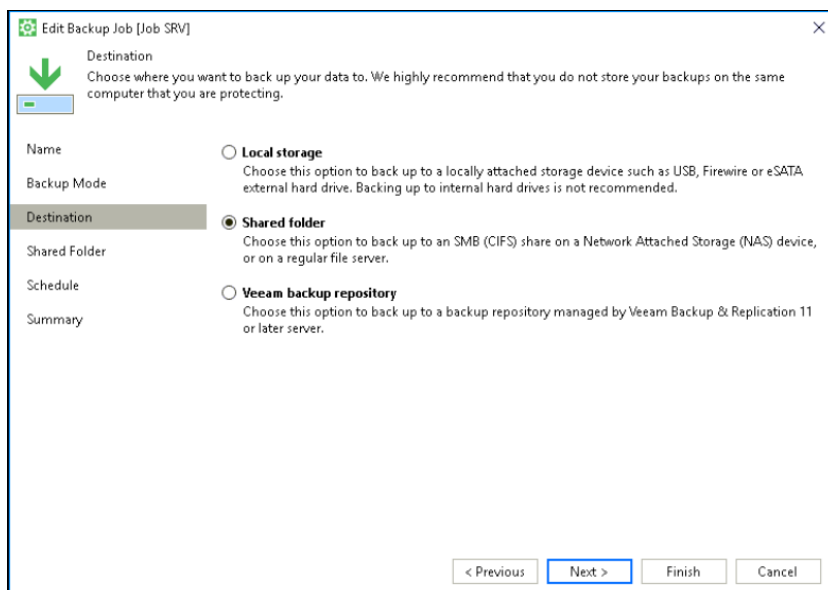
Obrázek 26 Pojmenování zálohovacího plánu

V dalším kroku se nás program zeptá, jaký druh zálohování chceme zvolit. V našem případě volíme „Entire computer“ kdy se nám za zálohuje kompletně celý počítač včetně systému a všech jeho disků. „Volume level backup“ nám umožňuje vybrat jednotlivé disky které si přejeme za zálohovat a „File level Backup“ umožňuje výběr přímo vybrané složky nebo souboru.



Obrázek 27 Výběr způsobu zálohování

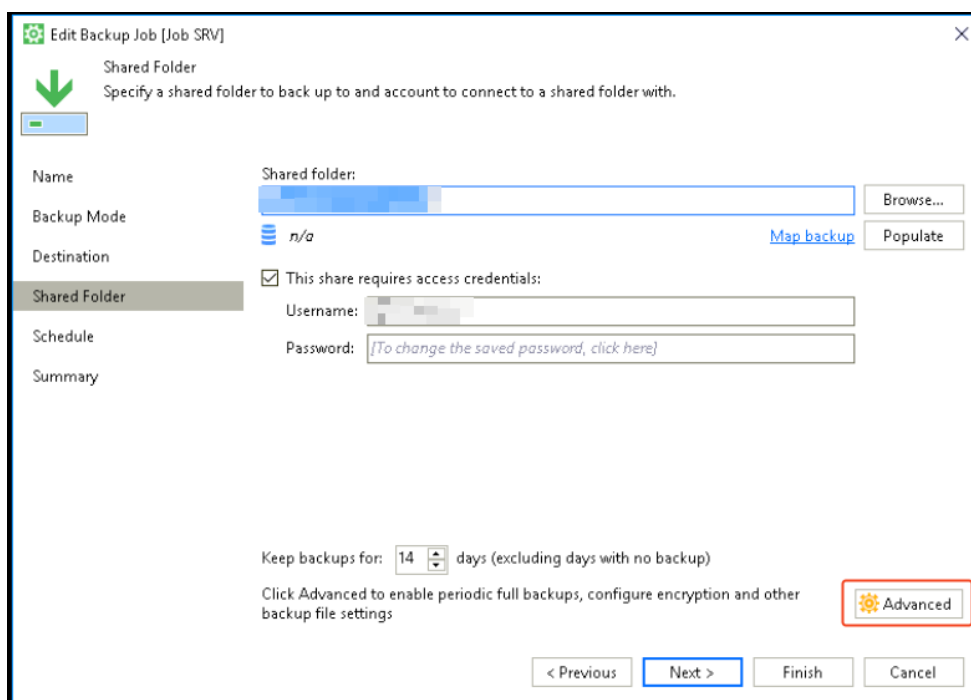
Po vybrání druhu zálohy vybereme destinaci zálohy. Na výběr máme ze tří možností „místní úložiště“, „sdílená složka“ a virtuální úložiště Veem Backup.



Obrázek 28 Cíl uložení zálohy

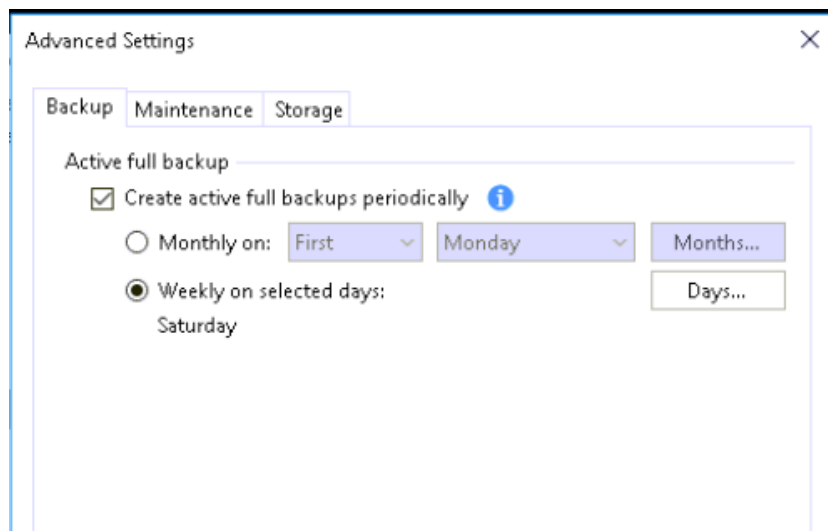
Čtvrtý krok už nás vybízí k nastavení cesty ke sdílené složce. V našem případě je to sdílená složka na úložišti NAS. Pro zvýšení zabezpečení jsem v systému NAS vytvořil speciální složku pro zálohování a k ní i uživatele s dlouhým složitým heslem. Do složky pro zálohy má přístup právě jen výše zmíněný uživatel, který zároveň nemůže do žádných jiných složek a nemá ani admin práva.

Zároveň v tomto kroku nastavujeme počet rotací záloh. Rotaci záloh jsem nastavil na 14 dní. Program počítá rotaci záloh pouze na dny, kdy záloha proběhne. To znamená že, když budeme mít nastavenou zálohu jednou týdně, tak budeme mít rotaci čtrnáctidenních záloh. Jako poslední v tomto kroku klikneme na tlačítko „Advanced“ označené v červeném obdélníku.



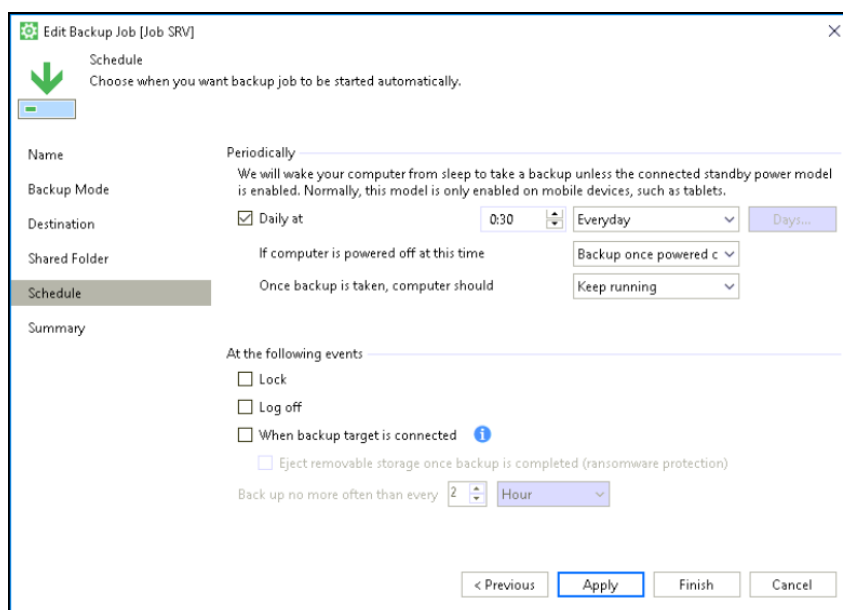
Obrázek 29 Nastavení cíle ukládání

Po rozkliknutí pokročilého nastavení si můžeme nastavit pravidelnou kompletní zálohu počítače. V mém případě jsem vybral týdenní „full backup“ každou sobotu.



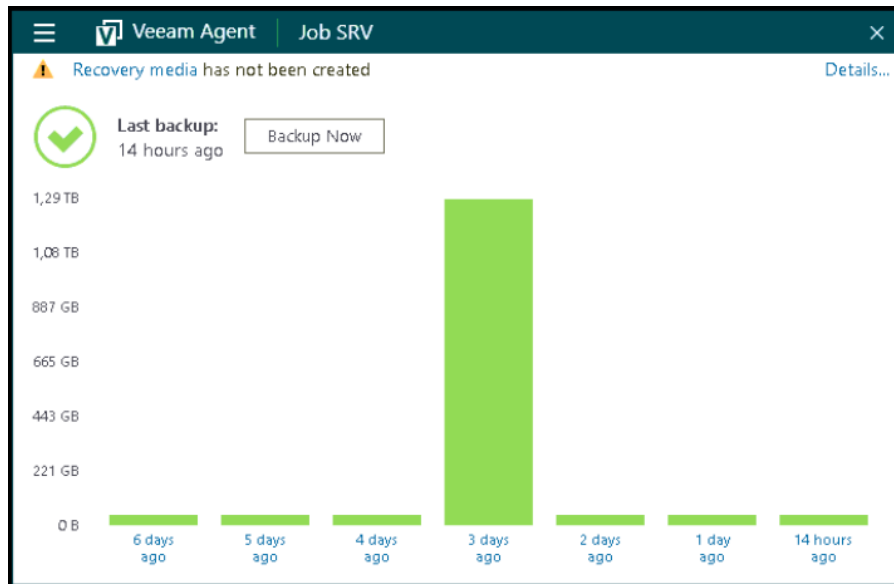
Obrázek 30 Nastavení podrobností zálohování

Posledním krokem v nastavování plánu zálohy je časový plán. Spuštění zálohy je naplánováno na každý den v půl jedné ráno. Důvodem pro volbu noční hodiny je nízká vytíženost serveru kdy, už se v kanceláři nikdo nenachází a nepracuje s dokumenty uloženými na serveru.



Obrázek 31 Nastavení časového plánu zálohy

Po uložení plánu už můžeme v hlavní nabídce agenta sledovat průběh a historii záloh. Pro usnadnění práce s monitorováním průběhu záloh umí agent zasílat notifikace na e-mail, kde vás informuje o výsledku zálohy, zdali byla úspěšná nebo neúspěšná.



Obrázek 32 Historie proběhlých záloh

Na obrázku níže je možné vidět, jak vypadá emailová notifikace o provedení úlohy. V tomto případě se jedná o úspěšný průběh zálohy. E-mail obsahuje veškeré informace o průběhu zálohy jako je čas zahájení a její doba, velikost dat pro zálohu, celková velikost zálohy a její komprese.

Subject: [Success] SRV - Job SRV - Friday, 03 February 2023 01:09:31

Agent Backup job: Job SRV **Success**
 Veeam Agent for Microsoft Windows

Friday, 03 February 2023 00:30:00

Success	1	Start time	00:30:00	Total size	1,8 TB	Backup size	3,3 GB
Warning	0	End time	01:09:31	Data read	14,6 GB	Dedupe	1,0x
Error	0	Duration	0:39:30	Transferred	3,3 GB	Compression	1,8x

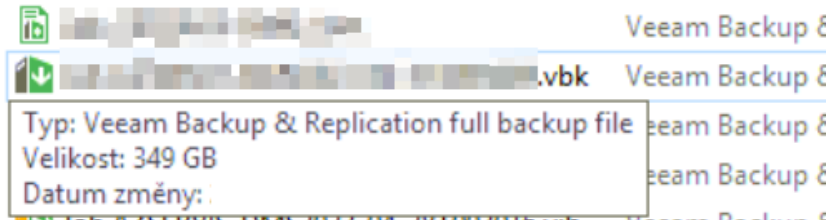
Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
SRV	Success	00:30:03	01:09:31	1,8 TB	14,6 GB	3,3 GB	0:39:27	

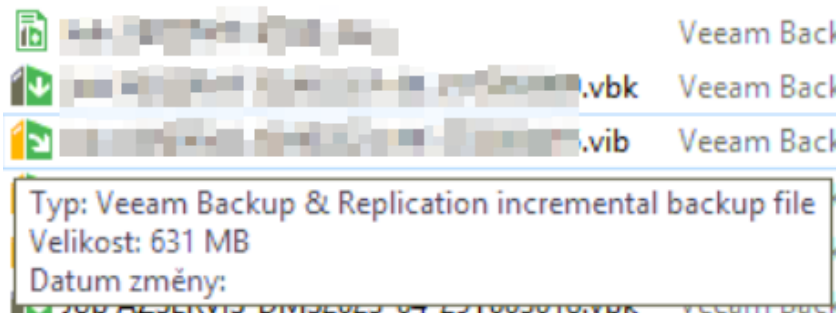
Veeam Agent for Microsoft Windows 5.0.3.4708

Obrázek 33 Emailová notifikace o průběhu zálohy

Samotná aplikace pak vytvoří soubory, které pomocí přípon souboru rozliší o jaký typ záloh se jedná. Soubory s příponou .vbk jsou plné zálohy a soubory s příponou .vib jsou zálohy inkrementální. Níže je pak možné vidět, jak tyto soubory v cílovém uložišti vypadají.



Obrázek 35 Soubor plné zálohy



Obrázek 34 Soubor inkrementální zálohy

3.4 ZHODNOCENÍ NÁVRHU

Zhodnocení výsledného vybraného řešení návrhu v sestavě fyzického serveru, licencí a síťového datového úložiště včetně disků vychází cenově následovně.

DELL PowerEdge T350: 190 231,-

Microsoft Windows Server Standard 2022: 23 766,-

3x Windows Server 2022/ Device CALs (Standard) pro 10 uživatelů: 21 000,-

Synology DS220+: 7 189,-

2x Disk pro NAS WD Red Plus 8TB: 7453,-

Celkem: 249 639,- bez DPH bez práce

Ceny se mohou lišit v návaznosti na momentální cenovou nabídku dodavatele hardwaru.

V porovnání s fyzickým serverem by cloudové řešení ve stejné konfiguraci bez systémového nastavení společnost vyšlo na 61 375,- bez DPH měsíčně.

To při průměrné životnosti serveru 8 let je skoro dvojnásobek pořizovací ceny fyzického serveru a to konkrétně 491 000,- bez DPH a bez požadovaných systémových vlastností jako je například DHCP, VPN nebo tiskový server.

Cenu cloudového řešení byly vypočítané pomocí interních informací IT společnosti.

Časová náročnost celého projektu je pak znázorněna v následující tabulce

Tabulka 2 Časová náročnost projektu

Počet	Název	Jednotkový počet hodin	celkový počet hodin
2	Instalace Windows server	4	8
1	Instalace a konfigurace virtualizační platformy	8	8
1	Konfigurace AD, GPO politik, instalace tiskáren	16	16
30	Vytvoření uživatelů	0,25	7,5
1	Vytvoření adresářové struktury	4	4
30	Migrace uživatelských profilů do nového doménového prostředí	1,5	45
1	Vytvoření segmentace sítě pro oddělení záloh od produkčních dat	4	4
1	Migrace VPN řešení ze současného serveru a konfigurace uživatelům	16	16
1	Nastavení zálohování, nastavení monitoringu nad Veeam standard	8	8
	Práce/Cena Celkem bez DPH		116,50

Nejnáročnější operací celého projektu je migrace uživatelských profilů do nového prostředí. S Tím je spojeno i přejmenování jednotlivých stanic a připojení do doménového prostředí. Přejmenováním získáme přesnější přehled o jednotlivých stanicích připojených do doménového prostředí.

Další časově nejnáročnější aktivitou je nastavování AD a politik. Nastavením politik si připravíme, pomocí skupin, prostředí pro lepší přehled o tom, který ze zaměstnanců má jaké přístupy a práva na serveru, a rovněž urychlíme proces přidávání nebo odebrání práv novým či stávajícím zaměstnancům.

ZÁVĚR

Cílem bakalářské práce byl návrh nového fyzického serveru a jeho zálohování s důkladným monitorováním pro společnost jejíž momentální server nesplňuje výkonové požadavky a licenční podmínky z důvodu velkého počtu zaměstnanců.

Teoretická část práce měla za úkol přiblížit a seznámit se s problematikou zálohování. Pro tu to část bylo čerpáno z příslušné literatury a internetových zdrojů. Teoretická část byla pak využita i pro vlastní návrhy řešení.

Po teoretické části následovala část, ve které jsme provedli analýzu současného stavu. Tato analýza se zaměřovala na hardwarové vybavení společnosti a odhalila nedostatky a oblasti, které lze vylepšit. Zejména výkon serveru a jeho zálohování.

Poslední část se již věnuje vlastnímu návrhu. Návrhy vznikly právě za pomoci analýzy současného stavu a byl vybrán vhodný server věžového typu, který vyhovuje dle požadavků jak výkonově, tak i licenčně. Dále pak byl pro server a data na něm uložená navrhnout zálohovací plán, který se skládá ze zálohy do virtuálního prostředí na serveru a zálohy mimo lokaci do NAS zařízení. Součástí je i nastavení plánu v zálohovacím softwaru.

SEZNAM POUŽITÝCH ZDROJŮ

- [1] DE GUISE, Preston. *Data Protection*. 1. Boca Raton: Taylor & Francis Group, 2017. ISBN 9781482244151. Dostupné z: doi:10.1201/9781315169620
- [2] SOMASUNDARAM, G. a A. SHRIVASTAVA. *Information Storage and Management: Storing, Managing, and Protecting Digital Information*. Indianapolis: Wiley Publishing, 2009. ISBN 978-0-470-29421-5.
- [3] . DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1.
- [4] PECINOVSKÝ, Josef. *Archivace a komprimace dat: jak zálohovat data, jak komprimovat soubory WinRAR, WinZip, WinAce, Windows a nástroje komprese dat, jak archivovat data ve Windows*. Praha: Grada Publishing a.s., 2003. ISBN 80-24-0659-8.
- [5] HAJDUCH, Ondřej. 59.1 Organizace a zálohování dat (Studijní text). *Digitalní učební materiály* [online]. c2013-2023 [cit. 2023-03-15]. Dostupné z: https://dum.hajduch.net/VY_32_INOVACE_1ICT9roc_59_B
- [6] MŮČKA, Jan. RAID disková pole: jaké jsou základní typy a v čem se liší?. *MasterDC* [online]. Česká republika, c2023. Dostupné z: <https://www.master.cz/blog/raid-diskova-pole-jake-jsou-zakladni-typy-a-v-cem-se-lisi/>
- [7] RAID. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné z: <https://cs.wikipedia.org/wiki/RAID#/>
- [8] Zálohování dat: věnujte mu pár desítek minut a budete mít klid na X let dopředu. *Digitální pevnost* [online]. Česká republika, c2018. Dostupné z: <https://www.digitalnipevnost.cz/zpravodaj/detail/zalohovani-dat>
- [9] Zálohování. *Jak na internet* [online]. Česká republika, c2023. Dostupné z: <https://www.jaknainternet.cz/page/1180/zalohovani/>
- [10] Disaster recovery – jak obnovit své IT a nezbláznit se. *MasterDC* [online]. Česká Republika, c2023. Dostupné z: <https://www.master.cz/blog/disaster-recovery-plan-obnovy-it-infrastruktury/>
- [11] RTO. *MasterDC* [online]. Česká Republika, c2023. Dostupné z: <https://www.master.cz/help/slovník/rto/>

- [12] RPO. *MasterDC* [online]. Česká Republika, c2023. Dostupné z: <https://www.master.cz/help/slovník/rpo/>
- [13], Acronis. What is the difference between RPO and RTO?. *Acronis* [online]. c2003–2023, December 20, 2022. Dostupné z: <https://www.acronis.com/en-us/blog/posts/rto-rpo/>
- [14] FRANČLOVÁ, Ing. Martina. Plán obnovy po havárii (Disaster Recovery plan) a jak ho vytvořit. *Datasys* [online]. c2023, 28. 11. 2022. Dostupné z: <https://www.datasys.cz/plan-obnovy-po-havarii-disaster-recovery-plan-a-jak-ho-vytvorit/>
- [15] LÁTAL, Jaroslav. Zálohovací strategie a plán obnovy v malých firmách a organizacích. *LinkedIn* [online]. c2023, 23. prosince 2016]. Dostupné z: <https://www.linkedin.com/pulse/zálohovací-strategie-plán-obnovy-v-malých-firmách-jaroslav-látal/>
- [16] Disaster Recovery: 5 Key Features and Building Your DR Plan. *Cloudian* [online]. c2023. Dostupné z: <https://cloudian.com/guides/disaster-recovery/disaster-recovery-5-key-features-and-building-your-dr-plan/>
- [17] Věžový server PowerEdge T350. *Dell* [online]. c2023. Dostupné z: <https://www.dell.com/cz/domacnosti/p/poweredge-t350/pd>
- [18] Rackový server PowerEdge R350. *Dell* [online]. c2023. Dostupné z: <https://www.dell.com/cz/domacnosti/p/poweredge-r350/pd>
- [19] Stolní počítač OptiPlex 3000 v provedení Tower a Small Form Factor. *Dell* [online]. c2023. Dostupné z: <https://www.dell.com/cz/domacnosti/p/optiplex-3000-sff/pd>
- [20] Server PowerEdge T30 Mini Towe. *Dell* [online]. c2023. Dostupné z: <https://www.dell.com/cz/domacnosti/p/poweredge-t30/pd>
- [21] Veeam Agent for Microsoft Windows FREE. *Veeam* [online]. c2023. Dostupné z: <https://www.veeam.com/cz/windows-endpoint-server-backup-free.html>
- [22] DiskStation® DS220+. *Synology* [online]. c2023. Dostupné z: <https://www.synology.com/cs-cz/products/DS220+>
- [23] Dream Machine Pro. Ubiquiti store [online]. c2023. Dostupné z: <https://eu.store.ui.com/collections/unifi-network-unifi-os-consoles/products/udm-pro>

- [24] Switch 48 PoE. *Ubiquiti store* [online]. c2023. Dostupné z: <https://eu.store.ui.com/collections/unifi-network-routing-switching/products/usw-48-poe>
- [25] Secure cloud storage—and so much more. *Dropbox* [online]. c2023. Dostupné z: <https://www.dropbox.com/plans>
- [26] Porovnání cen a plánů cloudového úložiště. *Microsoft 365* [online]. c2023. Dostupné z: <https://www.microsoft.com/cs-cz/microsoft-365/onedrive/compare-onedrive-plans?activetab=tab:primaryr2>
- [27] Choose your Google Workspace pricing plan. *Google* [online]. c2023. Dostupné z: <https://workspace.google.com/intl/en/pricing.html>
- [28] Data loss. *CFI* [online]. c2015-2023. Dostupné z: <https://corporatefinanceinstitute.com/resources/data-science/data-loss/>
- [29] 8 Most Common Reasons for DATA Loss. *Salvation Data* [online]. c2023, 2022-03-23. Dostupné z: <https://www.salvationdata.com/knowledge/8-most-common-reasons-for-data-loss/>
- [30] Data Archiving. *Druva* [online]. c2023. Dostupné z: <https://www.druva.com/glossary/what-is-data-archiving-definition-and-related-faqs>
- [31] What is Backup? (Data Backup) Comprehensive Guide. *Acronis* [online]. c2023. Dostupné z: <https://www.acronis.com/en-eu/blog/posts/data-backup/>
- [32] Acronis Cyber Protection Week: What is the 3-2-1 backup strategy?. *Acronis* [online]. c2023. Dostupné z: <https://www.acronis.com/en-eu/blog/posts/backup-rule/>
- [33] VANOVER, Rick. What is the 3-2-1 backup rule?. *Veeam* [online]. c2023, 21 October 2021. Dostupné z: <https://www.veeam.com/blog/321-backup-rule.html>
- [34] LOSSCHAERT, Nico. 3-2-1-1-0 Golden Backup Rule. *Veeam* [online]. c2023, 18 February 2021. Dostupné z: <https://community.veeam.com/blogs-and-podcasts-57/3-2-1-1-0-golden-backup-rule-569>
- [35] CD-RW. In: *Verbatim* [online]. c2023. Dostupné z: <https://www.verbatim-europe.cz/cz/prod/cd-rw-12x-43480/>
- [36] SanDisk Ultra Flair 128GB černá. In: *Alza* [online]. c1994 - 2023. Dostupné z: <https://www.alza.cz/sandisk-ultra->

[flair?dq=4016976&kampan=adwacc_prislusenstvi-pro-it-tv_pla_all_obecnacss_bryle_c_9062850__DU049y3f_456135983250_~109587574067~&gclid=CjwKCAjw0N6hBhAUEiwAXab-TeQVT7xEkPF5NMnyx4nm2okB9B4Eqlu5KiOty2c874QcdsOXykyvQRoCBGUQAvD_BwE](https://www.pocitarna.cz/pevne-disky/500gb-hdd-3-5--sata-sata-6gb-s/)

- [37] 500GB HDD / 3,5" / SATA / SATA 6GB/S. In: *Počítarna* [online]. c2023. Dostupné z: <https://www.pocitarna.cz/pevne-disky/500gb-hdd-3-5--sata-sata-6gb-s/>
- [38] Přehled cen a licencování pro Windows Server 2022. *Microsoft* [online]. c2023. Dostupné z: <https://www.microsoft.com/cs-cz/windows-server/pricing#layout-container-uida3b9>
- [39] Client Access Licenses and Management Licenses. *Microsoft* [online]. c2023. Dostupné z: <https://www.microsoft.com/en-us/licensing/product-licensing/client-access-license>
- [40] DiskStation® DS220j. *Synology* [online]. c2023. Dostupné z: <https://www.synology.com/cs-cz/products/DS220j#specs>
- [41] TS-231P3-2G. *QNAP* [online]. c2023. Dostupné z: <https://www.qnap.com/cs-cz/product/ts-231p3/specs/hardware>
- [42] Veeam Backup & Replication 12 User Guide for Microsoft Hyper-V. *Veeam* [online]. c2023. Dostupné z: <https://helpcenter.veeam.com/docs/backup/hyperv/backup.html?ver=120>

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

- AD – aktivní složka (Active Directory)
- CAL – licence pro přístup klienta (Client Access License)
- CD – kompaktní disk (Compact Disc)
- DHCP – dynamický protokol konfigurace hostitele (Dynamic Host Configuration Protocol)
- DNS – systém doménových jmen (Domain Name System)
- DPH – daň z přidané hodnoty
- DVD – digitální univerzální disk (Digital Versatile Disc)
- ERP – plánování prostředků podniku (Enterprise Resource Planning)
- GB – gigabajt (Gigabyte)
- GbE – gigabitová ethernetová síť (Gigabit Ethernet)
- Gbps – gigabity za sekundu (Gigabits per second)
- GPO – objekt skupinové politiky (Group Policy Object)
- GHz – gigahertz (Gigahertz)
- HDD – pevný disk (Hard Disk Drive)
- IT – informační technologie (Information Technology)
- NAS – síťové úložiště (Network-Attached Storage)
- PoE – napájení přes ethernet (Power over Ethernet)
- RAID – redundantní pole nezávislých disků (Redundant Array of Independent Disks)
- RPO – obnova cílového bodu (Recovery Point Objective)
- RTO – doba obnovy (Recovery Time Objective)
- SFP+ - malý přídatný modul (Small Form-factor Pluggable Plus)
- SSD – pevný disk bez pohyblivých částí (Solid State Drive)

TB – terabajt (Terabyte)

USB – univerzální sériová sběrnice (Universal Serial Bus)

VPN – virtuální privátní síť (Virtual Private Network)

W – watt (Watt)

WAN – rozsáhlá síť (Wide Area Network)

SEZNAM OBRÁZKŮ

Obrázek 1 Schéma plného zálohování	11
Obrázek 2 Schéma inkrementálního zálohování	11
Obrázek 3 Schéma rozdílového zálohování	12
Obrázek 4 Schéma kombinovaného zálohování	13
Obrázek 5 Zálohování podle pravidla 3-2-1-1-0 [34]	14
Obrázek 6 Časová osa RPO a RTO [10]	15
Obrázek 7 Analýza dopadu na chod podniku [15]	16
Obrázek 8 Zálohovací média [35][36][37]	18
Obrázek 9 RAID 0 [7]	19
Obrázek 10 RAID 1 [7]	19
Obrázek 11 RAID 5 [7]	20
Obrázek 12 RAID 6 [7]	21
Obrázek 13 RAID 01 a RAID 10 [7]	21
Obrázek 14 Dell OptiPlex 3000[18]	23
Obrázek 15 Server PowerEdge T30 Mini Tower[20]	24
Obrázek 16 Router UniFi Dream Machine[23]	25
Obrázek 17 Switch USW-48-PoE[24]	25
Obrázek 18 Přehled sledovaných telemetrických dat	26
Obrázek 19 Dell PowerEdge R350[18]	28
Obrázek 20 Dell PowerEdge T350[17]	29
Obrázek 21 Vytvoření nového plánu[42]	31
Obrázek 22 Pojmenování zálohovacího plánu[42]	32
Obrázek 23 Výběr virtuálního prostředí[42]	32
Obrázek 24 Výběr úložiště pro zálohování[42]	33
Obrázek 25 Nastavení rotace plných záloh[42]	33
Obrázek 26 Nastavení časového plánu spouštění[42]	34
Obrázek 27 NAS Synology DS220+	41
Obrázek 28 Pojmenování zálohovacího plánu	42
Obrázek 29 Výběr způsobu zálohování	43
Obrázek 30 Cíl uložení zálohy	43

Obrázek 31 Nastavení cíle ukládání	44
Obrázek 32 Nastavení podrobností zálohování	45
Obrázek 33 Nastavení časového plánu zálohy	45
Obrázek 34 Historie proběhlých záloh	46
Obrázek 35 Emailová notifikace o průběhu zálohy	46
Obrázek 36 Soubor inkrementální zálohy	47
Obrázek 37 Soubor plné zálohy	47

SEZNAM TABULEK

Tabulka 1 Porovnání NAS vs Cloud	39
Tabulka 2 Časová náročnost projektu	49