Implementace systému zálohování virtualizované IT infrastruktury fakultní nemocnice

Bc. Jaromír Berka

Diplomová práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jaromír Berka**
Osobní číslo:	**A14497**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Implementace systému zálohovaní virtualizované IT infrastruktury fakultní nemocnice**
Téma anglicky:	**The Implementation of a Systems' Backup of the Virtualized IT Infrastructure of a Faculty Hospital**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na předmětnou tématiku.**
2. **Proveďte analýzu stávajícího stavu zálohování virtualizovaného prostředí.**
3. **Popište přehled vhodných zálohovacích řešení na trhu pro potřeby zálohování virtualizovaného prostředí.**
4. **Navrhněte postup obnovy chodu IT služeb organizace. K tomu zpracujte scénáře obnovy adresářových služeb Active direktory, souborových služeb, instance virtualizovaného operačního systému.**
5. **Navrhněte způsob implementace systému zálohování.**
6. **Navrhněte formuláře plánu obnovy u adresářových služeb, souborových služeb, instance virtualizovného operačního systému.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **BRUCKNER, Tomáš. Tvorba informačních systémů: principy, metodiky, architektury. 1. vyd. Praha: Grada, 2012, 357 s. Management v informační společnosti. ISBN 978-80-247-4153-6.**
2. **LUKÁČ, Ľubomír. IT management. Brno: Computer Press, 2011, 208 s. ISBN 978-80-251-3378-1.**
3. **RUEST, Danielle a Nelson RUEST.Virtualizace: podrobný průvodce. Vyd. 1. Brno: Computer Press, 2010, 408 s. ISBN 978-80-251-2676-9.**
4. **Availability for the modern data center [online]. [cit. 2015-09-30]. Dostupné z: http://www.veeam.com/cz/vm-backup-recovery-replication-software.html.**
5. **Veeam Backup & Replication | User Guide for Microsoft Hyper-V | REVISION [online]. [cit. 2016-01-10]. Dostupné z: https://www.veeam.com/backup-replication-resources.html.**

Vedoucí diplomové práce: **doc. Ing. Jiří Gajdošík, CSc.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **5. února 2016**

Termín odevzdání diplomové práce: **16. května 2016**

Ve Zlíně dne 5. února 2016

doc. Mgr. Milan Adámek, Ph.D.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 13. 05. 2016

.....
podpis diplomanta

ABSTRAKT

Práce reflektuje problematiku zálohování a obnovení virtualizované ICT infrastruktury v prostředí Fakultní nemocnice Olomouc. Provází problematikou zabezpečení ICT služeb / aplikací z pohledu dostupnosti. Dotýká se problematiky disaster recovery a obnovení ICT služeb / aplikací po havárii. Rozvádí běžné metody zálohování, včetně doporučení k uchovávání zálohovaných dat. Rozvíjí pojem zálohování do složitého a důležitého procesu. Nabízí důležité rady, které je vhodné využít i během zálohování v domácím prostředí.

Významnou část práce tvoří komplexní implementace profesionálního zálohovacího řešení Veeam Backup & Replication v prostředí Fakultní nemocnice Olomouc. Součástí práce je realizace testovacího plánu obnovy pro instanci virtuálního počítače, adresářových a souborových služeb.

Klíčová slova: Veeam, Zálohování, Obnovení, Hyper-V, Replikace, Virtualizace, Vysoká dostupnost.

ABSTRACT

The project reflects on the issue of backup and restoration of virtualized ICT infrustructure in the environment of the University Hospital in Olomouc. It walks through the problems of ICT service protection / aplications in the perspective of availability. It also touches on the issue of disaster recovery and restoration of ICT services / aplications after breakdown. It deals with the usual backup methods including recommendation of how to store backed up data. It develops the term backup into a complex and important process. It offers important pieces of advice which are convenient to be used during backup in domestic environment.

An important part of the project comprises a complex implementation of professional backup solution Veeam Backup & Replication in the environment of the University Hospital in Olomouc. A part of the project is the realization of the trial plan of restoration for the instance of virtual computer, directory and filing services.

Keywords: Veeam, Backup, Restore, Hyper-V, Replication, Virtualization, High availability.

PODĚKOVÁNÍ

Děkuji doc. Ing. Jiřímu Gajdošíkovi, CSc. za cenné rady při vedení diplomové práce. Mé poděkování patří též kolektivu pracovníků Fakultní nemocnice Olomouc za umožnění zpracovat diplomovou práci z reálného informačního prostředí nemocnice.

Děkuji manželce a svému synovi, za podporu a trpělivost, kterou mi během studia poskytovali.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD **10**
I TEORETICKÁ ČÁST **11**
1 ODOLNOST ICT SLUŽEB VŮČI HAVÁRII **12**
1.1 SLUŽBY KRITICKÉ INFRASTRUKTURY 12
1.2 HW ZDROJE 13
1.3 OPERAČNÍ SYSTÉM A JEHO SLUŽBY 13
1.4 OBNOVA PO HAVÁRII 14
2 SLUŽBA ZÁLOHOVÁNÍ **17**
2.1 ZÁLOHOVÁNÍ JAKO OCHRANA PŘED UDÁLOSTMI 17
2.2 ZÁLOHOVÁNÍ JAKO PROCES 17
2.3 LIDSKÉ ZDROJE A JEJICH ROLE V PROCESU ZÁLOHOVÁNÍ 19
2.3.1 Technický personál 19
2.3.1.1 Operátoři a pracovníci podpory (backup operators) 19
2.3.1.2 Správci zálohování (backup adminstrators) 19
2.3.1.3 Systémoví administrátoři (system administrators) 20
2.3.1.4 Aplikační administrátoři (applications administrators) 21
2.3.2 Management 21
2.3.2.1 Týmový vedoucí 21
2.3.2.2 Vyšší management 22
2.3.3 Uživatelé 22
2.3.3.1 Klíčoví uživatelé 22
2.3.3.2 Koncoví uživatelé 22
3 KONCEPCE ZÁLOHOVÁNÍ **23**
3.1 TOPOLOGIE 23
3.1.1 Decentralizovaná zálohovací topologie 23
3.1.2 Centralizovaná zálohovací topologie 24
3.2 ÚROVEŇ ZÁLOHOVÁNÍ 26
3.2.1 Plná záloha (full backup) 26
3.2.2 Inkrementální záloha (incremental backup) 26
3.2.3 Rozdílová záloha (differencial backup) 28
3.2.4 Konsolidovaná úroveň (consolidated level) 30
3.2.5 Ruční zálohování 30
3.3 DOSTUPNOST ICT SLUŽBY / APLIKACE BĚHEM PROCESU ZÁLOHOVÁNÍ 31
3.3.1 Offline zálohování 31
3.3.2 Online zálohování 31
3.4 VÝBĚR ZÁLOHOVANÝCH DAT 31
3.4.1 Zahrnuté do zálohy (inklusive backup) 31
3.4.2 Vyloučené ze zálohy (exklusive backup) 32
3.5 RETENČNÍ POLITIKA 32
3.5.1 Jednoduchý retenční model 32
3.5.2 GFS retenční model 32
3.6 ZÁLOHOVACÍ ZAŘÍZENÍ 33
3.6.1 Magnetická pásková jednotka 34

3.6.2 Diskové datové úložiště 35
3.6.3 Flash datové úložiště 36
3.6.4 Optická datová úložiště 36
3.6.5 Cloudové datové úložiště 36
3.7 UŽITEČNÉ RADY K ZÁLOHOVÁNÍ 37
3.7.1 Pravidlo 3-2-1 37
3.7.2 Paranoia 38
3.7.3 Testování, testování, testování 38
4 PŘEHLED DOSTUPNÝCH ZÁLOHOVACÍCH SYSTÉMŮ VIRTUALIZOVANÉHO PROSTŘEDÍ 39
4.1 ZÁLOHOVACÍ SOFTWARE 39
4.1.1 Acronis Backup Advanced 39
4.1.2 Altaro VMBACKUP 39
4.1.3 IBM Spectrum Protect for Virtual Environments 40
4.1.4 Veritas NetBackup 40
4.1.5 Veeam Backup & Replication 40
4.2 SHRNUTÍ 41
II PRAKTICKÁ ČÁST 43
5 ANALÝZA SOUČASNÉHO STAVU ZÁLOHOVÁNÍ VIRTUALIZOVANÉ INFRASTRUKTURY 44
5.1 POPIS APLIKAČNÍHO VIRTUÁLNÍHO PROSTŘEDÍ 46
5.2 POPIS SYSTÉMOVÉHO VIRTUÁLNÍHO PROSTŘEDÍ 46
5.2.1 Klastr CLS-ISS2009 46
5.2.2 Klastr CLS-APP2014 46
5.2.3 Klastr CLS-IDMZ 47
5.2.4 Klastr CLS-EDMZ 47
5.2.5 Zálohovací plán 48
6 NÁVRH IMPLEMENTACE ZÁLOHOVACÍHO SYSTÉMU SPOLEČNOSTI VEEAM SOFTWARE 50
6.1 NÁVRH IMPLEMENTACE SYSTÉMU ZÁLOHOVÁNÍ 50
6.1.1 Konfigurace klastru CLS-APP2016 52
6.1.2 Příprava diskového úložiště 53
6.1.3 Příprava virtuálního serveru BCK-12 55
6.2 PŘÍPRAVA PŘED ZAHÁJENÍM INSTALACE ZÁLOHOVACÍHO SERVERU 56
6.2.1 Příprava Hyper-V hostů pro zařazení do zálohování 58
6.2.2 Příprava systémových účtů 59
6.2.3 Příprava SQL databází 61
6.2.4 Příprava notifikačních e-mailových zpráv 61
7 POSTUP INSTALACECE ZÁLOHACÍHO SYSTÉMU VEEAM BACKUP & REPLICATION 62
7.1 PŘÍPRAVA INSTALAČNÍCH MÉDIÍ 62
7.2 INSTALACE 62
7.3 KONFIGURACE 65
7.3.1 Přidání Hyper-V serverů 66
7.3.2 Vytvoření zálohovacího zařízení 68
7.3.3 Nastavení e-mailové notifikace 68

7.4 VYTVOŘENÍ ZÁLOHOVACÍ ÚLOHY 68
7.4.1 Denní zálohovací úlohy 69
7.4.2 Týdenní zálohovací úlohy 70
7.4.3 Měsíční zálohovací úlohy 70
7.4.4 Další typy zálohovacích úloh 71
7.5 ZMĚNA POČTU ZÁLOHOVANÝCH ICT SLUŽEB / APLIKACÍ V ZÁVISLOSTI NA NOVÉM SYSTÉMU ZÁLOHOVÁNÍ 71
7.5.1 Zasílání reportů o stavu zálohování 74
8 OBNOVENÍ VIRTUALIZOVANÝCH ICT SLUŽEB 76
8.1 OBNOVENÍ INSTANCE VIRTUÁLNÍHO SERVERU 76
8.2 OBNOVENÍ ADRESÁŘOVÝCH SLUŽEB 78
8.3 OBNOVENÍ SOUBOROVÝCH SLUŽEB 81
9 FORMULÁŘ PLÁNU OBNOVY 83
ZÁVĚR 84
SEZNAM POUŽITÉ LITERATURY 85
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 87
SEZNAM OBRÁZKŮ 89
SEZNAM TABULEK 91
SEZNAM GRAFŮ 92
SEZNAM PŘÍLOH 93

ÚVOD

Úkolem práce bylo zpracovat problematiku zálohování a obnovu IT služeb provozovaných ve virtualizované infrastruktuře Fakultní nemocnice Olomouc, včetně implementace nového zálohovacího systému, který bude splňovat požadavky kladené zástupci nemocnice. Výstupem práce je funkční zálohovací prostředí, které zajistí robustní bezpečnost informací zpracovávaných ve virtualizovaných informačních systémech, a to zejména po neočekávané havárii, konfiguračních chybách, nechtěnému smazání dat a podobně.

Práce rozvíjí moji bakalářskou práci na téma „Provoz systémových IT služeb v informačním systému Fakultní nemocnice Olomouc“. Z tohoto důvodu zde nebude detailně vysvětlena problematika provozu IT služeb, včetně technologie serverové virtualizace, protože se této problematice detailně věnuji v bakalářské práci. Základní informace o Fakultní nemocnici Olomouc, včetně rozsahu poskytované lékařské péče, jsou rovněž uvedeny v bakalářské práci.

Běžný provoz nemocnice je intenzivně provázán s informačními technologiemi, které se významně podílí na kvalitě poskytované zdravotnické péče. V případě dlouhodobé nefunkčnosti informačních systémů nemocnice hrozí riziko snížení kvality lékařského ošetření.

Pro zajištění podpory lékařské péče bylo rozhodnuto implementovat nový moderní zálohovací systém v IT prostředí nemocnice, který přinese významné zlepšení spolehlivosti služby zálohování. Díky novému zálohovacímu řešení byla zajištěna rychlá obnova ICT služeb / aplikací a současně zkrácena doba nutná pro obnovení služby do funkčního stavu po havárii.

Významným faktorem k zajištění správné funkce procesu zálohování a obnovení ICT služeb / aplikace je vytvoření zálohovacího plánu a provádění testů plánu obnovy, které byly pro některé důležité služby provedeny v produkčním IT prostředí Fakultní nemocnice Olomouc.

Všechny zpracovávané scénáře a implementační postupy byly prováděny a optimalizovány výlučně pro prostředí Fakultní nemocnice Olomouc. Během realizace implementace systému zálohování bylo postupováno dle dostupné dokumentace a doporučení výrobce zálohovacího softwaru Veeam Backup & Replication.

I. TEORETICKÁ ČÁST

1 ODOLNOST ICT SLUŽEB VŮČI HAVÁRII

Kapitola vytváří krátký úvod do problematiky kontinuity ICT (Informační a komunikační technologie) služeb. Má za úkol nastínit problematiku odolnosti ICT služeb /aplikací jako prevenci před procesem obnovení po havárii.

V rámci ICT je nativním jazykem angličtina, z důvodu krkolomných překladů do českého jazyka a správné srozumitelnosti problematiky se v textu budou vyskytovat i přesné anglické názvy.

Odolnost spočívá ve vytvoření robustní ICT infrastruktury, která je přizpůsobena k zajištění odolnosti vůči selhání individuálních IT (informační technologie) prvků. Infrastruktura, která tyto náležitosti splňuje, má předpoklady pro provozování vysoce dostupných aplikačních služeb. Ze strany byznysu a uživatelů je dostupnost aplikačních služeb důležitá v závislosti na míře elektronizace firemních procesů a působení na obchodním trhu. V případě ropných společností, které nejsou schopné bez funkčních ICT služeb zajistit logistiku ropy ke svým zákazníkům, se může jednat o finanční ztráty v řádech milionů korun za každý den nefunkčnosti byznys procesu. Dalším argumentem je poškození dobrého jména společnosti, která během výpadku ICT služeb nemůže poskytovat služby svým zákazníkům.

Aplikačními službami jsou uvažovány SW (software) nástroje, kterými uživatelé přeměňují zpracovávané informace na aktiva / data, která jsou v systémech zpracovávána. Pro ukázku můžeme jmenovat například nástroje pro podporu ekonomických procesů, skladového hospodářství, nemocničního informačního systému, atd.

Aplikační služby tvoří vrchol pyramidy ICT infrastruktury a jsou závislé na spolehlivosti ICT prvků v nižších vrstvách [3], [4].

1.1 Služby kritické infrastruktury

Prvky kritické infrastruktury z pohledu systémových IT služeb tvoří datové centrum, včetně technologie chlazení datového centra, připojení k elektrické rozvodné síti, UPS (Uninterruptible Power Supply) - krátkodobý zdroj náhradní elektrické energie, diesel agregát – zdroj náhradní elektrické energie.

Dle požadavku na robustnost infrastruktury jsou do objektu datového centra přivedeny např. dvě zcela nezávislé přípojky k elektrické rozvodné síti, nezávislé diesel agregáty, nezávislé systémy chlazení, atd. [3].

1.2 HW zdroje

Pojem HW (hardware) zdroje popisuje širokou skupinu zařízení, které jsou běžně v datovém centru osazené v rackových rozvaděčích. Servery, aktivní prvky, datová úložiště a další HW prvky jsou již běžně vybaveny systémy chránící prvek před neočekávaným selháním a tím odstavení aplikační služby z provozu.

Mezi základní systémy ochrany před havárií patří:

- redundantní napájecí zdroje,
- systémy ochrany diskového systému pomocí metody RAID (Redundant Array of Inexpensive / Independent Disks),
- operační paměť s kontrolou chyb ECC (Error Checking and Correcting),
- redundantní řadiče diskového subsystému,
- redundantní zapojení prvků do sítě LAN (Local Area Network),
- redundantní zapojení prvků do sítě SAN (Storage area network).

Díky výše zmíněným technologiím je riziko selhání HW potlačeno na velmi nízkou úroveň [3], [4].

1.3 Operační systém a jeho služby

Operační systém tvoří v prostředí ICT velmi důležitý element, bez kterého by bylo nesmírně složité a neefektivní budovat jednotlivé aplikační služby. Operační systém má za úkol přímo komunikovat s HW, provádí správu paměti, správu procesů, správu diskového systému, správu vstupního / výstupních zařízení, atd.

Společnost Microsoft u svých serverových operačních systémů nabízí možnost provozovat některé služby v režimu vysoké dostupnosti. Režim vysoké dostupnosti je zajištěn pomocí dvou a více instancí operačního systému, které společně využívají zdroje datové sítě a diskového úložiště. V případě selhání jedné z instancí operačního systému dochází k přepnutí služby na druhý nod klastru. Tím dochází pouze ke krátkodobému výpadku koncové ICT služby / aplikace.

Zajistit vysokou dostupnost ICT služeb / aplikací je díky technologii převzetí služby po havárii a virtualizaci ICT prostředí již zcela běžnou záležitostí. Velké množství podniků investuje nemalé prostředky na vybudování robustní infrastruktury. Bohužel z vlastních

praktických zkušeností mohu potvrdit, že nemalá část podniků zapomíná na řádné zálohování ICT služeb [3].

1.4 Obnova po havárii

Pojem obnova po havárii je v IT oblasti spíše povědomý pod označením disaster recovery. Obnova po havárii je sepsaný soupis procesů, které je nutné provést pro zajištění obnovení služby po havárii v ideálně geograficky odlišné lokalitě. V tomto případě se jedná o provozní stav, kdy není možné službu v primární lokalitě zprovoznit, například z následujících důvodů:

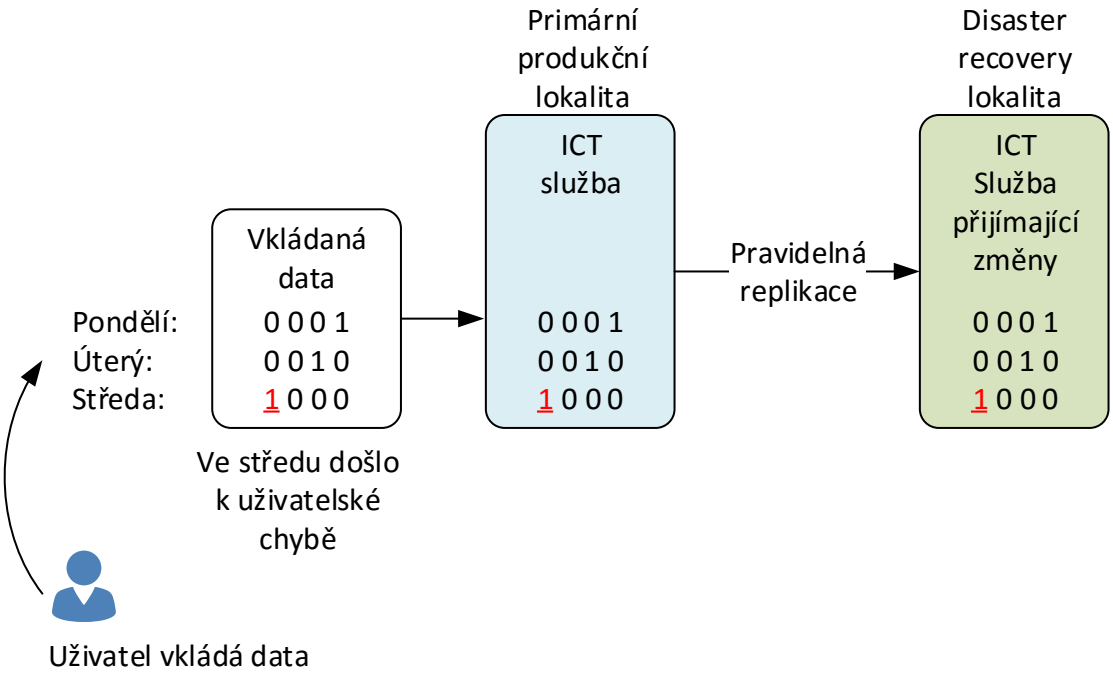
- přírodní katastrofy,
- úmyslné, neúmyslné havárie vzniklé lidským působením,
- hromadné poškození HW.

Samotná přítomnost disaster recovery lokality znamená zvýšení robustnosti a odolnosti ICT infrastruktury vůči neočekávaným událostem a rychlému obnovení služby. Organizace může v rámci oddělení lokalit snadněji provádět údržbu, testování služeb, nasazení změn konfigurace služeb, včetně reakce na plánované výpadky služeb od svých dodavatelů (služby připojení k síti Internet, dlouhodobé přerušení dodávek elektrické energie).

Vybudování samotné disaster recovery lokality je finančně náročně. Z tohoto důvodu se na ICT trhu množí nabídky na možnost vybudování disaster recovery jako služba. Softwarový gigant společnost Microsoft ve svých operačních systémech integruje rozhraní pro snadnou replikaci ICT služeb do prostředí svých cloudových služeb provozovaných v rámci Microsoft Azure cloudu. Funkčnost disaster recovery spočívá v pravidelné replikaci dat z primární do záložní lokality.

To může mylně zavádět k názoru, že funkční služba zálohování je v infrastruktuře v tomto případě zbytečná. Díky virtualizaci infrastruktury je v prostředí operačních systémů společnosti Microsoft používána replikační technologie Hyper-V replika, která zajišťuje přenesení obsahu primární instance virtuálního počítače do jiné lokality, nebo jiného Hyper-V serveru ve stejné lokalitě. Dojde tím tedy k vytvoření konzistentní kopie virtuálního počítače, která je vypnuta a v pravidelných intervalech přijímá změněné bloky dat. To je v případě běžného korektního stavu ICT služby v pořádku, ale v případě zanesení chyby do systému dojde v příští replikační iteraci k přenesení chyby do disaster recovery lokality. Problém je možné vyřešit přidáním dalšího replikačního řetězce, kde je časový

cyklus replikace o několik hodin opožděn. V závislosti na typu organizace je riziko objevení chyby různé a z tohoto důvodu nemůžeme disaster recovery technologie zaměňovat za službu zálohování [3].

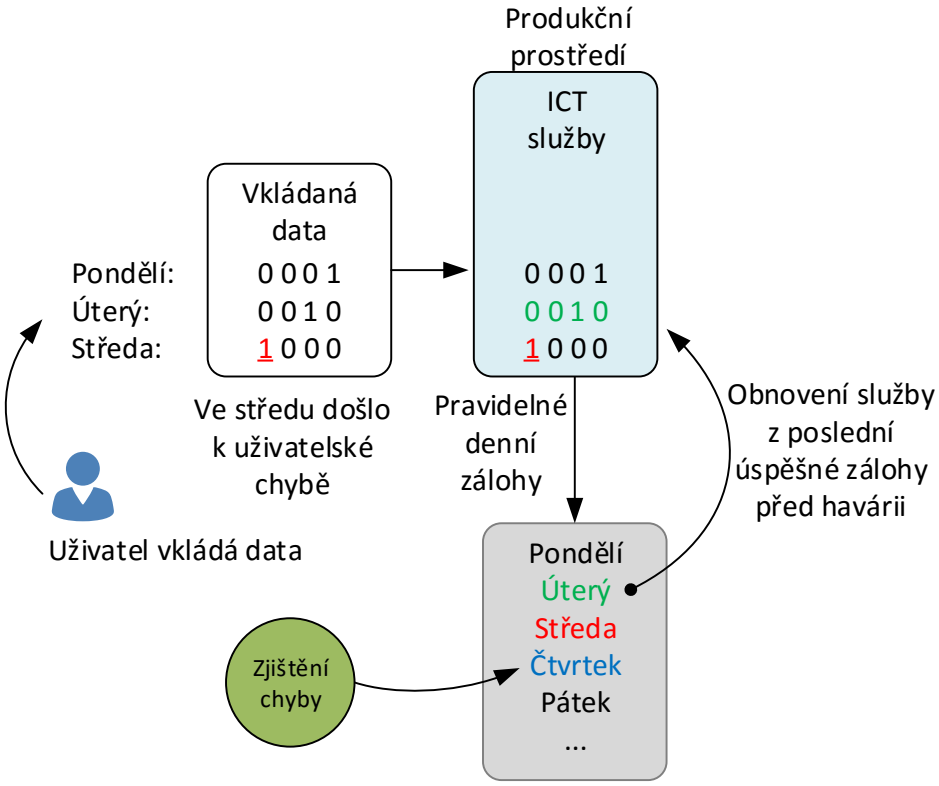


Obr. 1. Zanesení chyby z produkčního prostředí do disaster recovery lokality.

Služba zálohování nám má umožnit obnovení služby ve větším časovém horizontu v rozpětí dnů až týdnů. Časové rozpětí může být dáno specifickou potřebou organizace a IT službami, které využívá, eventuálně poskytuje svým zákazníkům. V organizaci by měl být definován zálohovací plán, který tvoří kompetentní osoby ze strany IT oddělení a garanta IT služby. Garant IT služby musí znát přesné požadavky organizace, strukturu aplikace a postup pro její obnovení do stavu před havárií.

Na obrázku číslo 2 je blokově znázorněn proces obnovy ICT služby ze zálohy. V rámci organizace je prováděno pravidelné zálohování na denní bázi. Ve středu uživatel informačního systému omylem zadal chybná data, která byla zpracována. Ve čtvrtek došlo ke zjištění, že je v systému chyba a bylo rozhodnuto obnovit službu do stavu před havárií. V případě replikace existuje riziko, že by již chyba mohla být přenesena do druhé lokality. V případě obnovení služby ze zálohy vybereme poslední úspěšně dokončenou úlohu, která byla provedena v úterý a obnovíme službu do tohoto stavu. V závislosti na typu ICT služby, většinou se jedná o databázové služby, můžeme s obnovenými daty a současnými poškozenými daty provádět různé operace a tím zajistit například nulovou ztrátu dat.

V tomto případě se již nejedná o problematiku zálohování, ale o aplikační zpracování dat [5].



Obr. 2. Obnovení ICT služby ze zálohy.

2 SLUŽBA ZÁLOHOVÁNÍ

2.1 Zálohování jako ochrana před událostmi

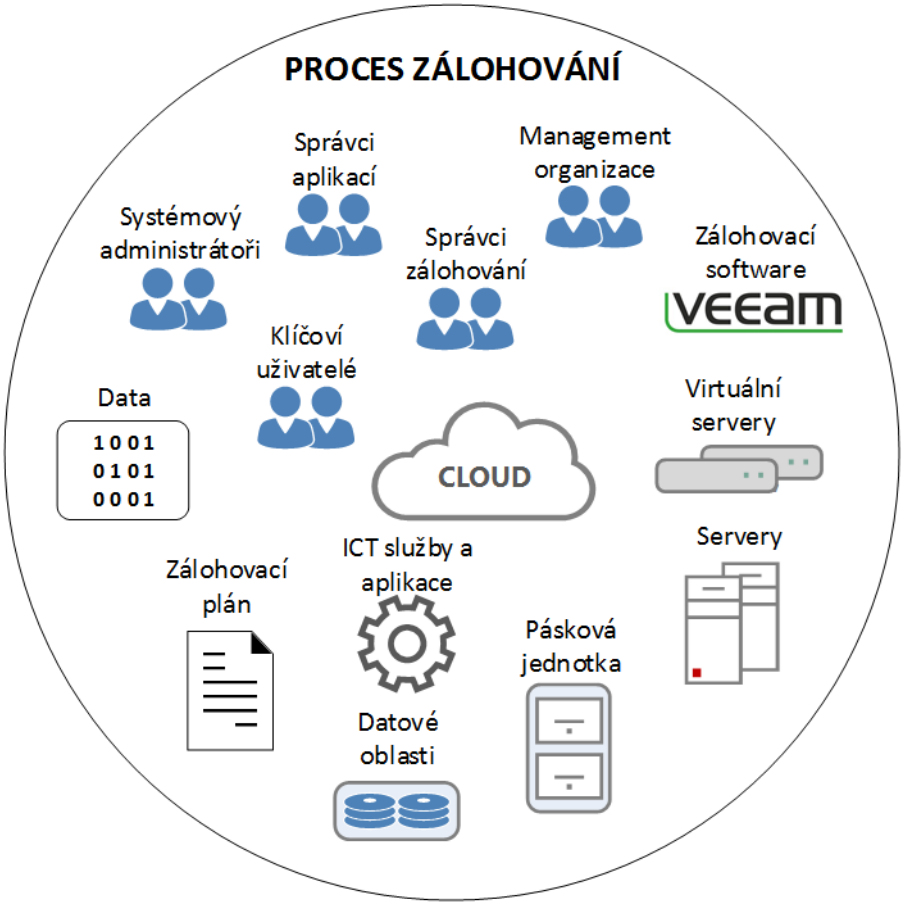
Zálohování může chránit informační systém před následujícími hrozbami:

- hardwarové chyby,
- softwarové chyby,
- úmyslné poškození,
- náhodné poškození,
- krádež,
- hacking,
- teroristický útok,
- přírodní katastrofy,
- počítačové viry,
- výpadek elektrického proudu.

2.2 Zálohování jako proces

Zálohování není pouze okamžik, kdy dochází k samotnému vytvoření kopie dat. Jedná se o komplexní proces, který má své zdroje, vstupy, výstupy, kontrolní mechanismy a prostor pro neustálé zlepšování. Cílem procesu je zajistit spolehlivou možnost, jak v co nejkratším časem a co nejmenší ztrátou dat zajisti obnovení chodu organizace z pohledu ICT. Pokud obdržíme otázku: Co je zálohování? Je možné na ni odpovědět pomocí následující definice. Zálohování je vytvoření kopie všech dat, která jsou nutná k obnovení původních dat. Pod pojmem data rozumíme:

- soubory,
- ICT služby,
- aplikace,
- operační systémy.



Obr. 3. Proces zálohování a jeho komponenty.

Rozsah procesu zálohování je velmi individuální a velmi záleží na míře zdravé paranoi jednotlivců, kteří do procesu zasahují. Dále je nutné provedené zálohovací úlohy (backup jobs) pravidelně ověřovat z důvodu čitelnosti médií pro případ možné obnovy, včetně nácviku scénářů obnovy jednotlivých aplikací a ICT služeb. Vedle samotných dat jsou do procesu zálohování integrovány HW, SW a personální zdroje. Nesmím opomenout na velmi důležitou skutečnost, kterou jsou znalosti pracovníků vstupující do problematiky zálohování [5].

Bohužel důležitost procesu zálohování se plně projeví až po výskytu první havárie, během které dojde ke zničení důležitých dat. Výrok platí v oblasti podnikového i domácího IT a uživatelé jsou bohužel stále nepoučitelní. Teprve po vlastní praktické zkušenosti svůj přístup k problematice zálohování velmi rychle přehodnotí. Je to velmi krutá daň, protože vlastní nezodpovědností můžeme přijít o veškeré digitální fotografie, zachycují zrození a růst našich dětí.

2.3 Lidské zdroje a jejich role v procesu zálohování

Systém ochrany podnikových dat je více než jen sbírkou hardwaru a médií. Lidé, kteří s ICT prostředím na sebe vzájemně působí, hrají v systému zálohování zásadní roli a jejich znalost prostředí je pro správné nadefinování procesu významná.

Množství lidí pohybujících se v oblasti správy a využívání IT služeb je závislá na velikosti podniku a mírou integrace ICT do byznysu procesů organizace. Pracovníci znají svoji roli, ale často jim chybí informace, že mají svůj podíl na samotném návrhu zálohování a obnovy. Spoléhají se vzájemně na své kolegy, případně na IT ředitele. Jen vzájemnou synergií může dojít ke vzniku spolehlivého systému zálohování a obnovy [5].

2.3.1 Technický personál

Pracovníci spadající do oblasti technických zaměstnanců jsou do oblasti zálohování a obnovy nejvíce zainteresováni. Technický personál musí přijmout odpovědnost za zálohování, jinak systém ochrany infrastruktury nebude správně zajištěn a bude vykazovat vážné nedostatky.

2.3.1.1 Operátoři a pracovníci podpory (backup operators)

Jedná se o skupinu pracovníků zajišťující operativní obsluhu zálohovacího systému. Musí být seznámeni se zálohovacím plánem organizace a poučeni o důležitosti jimi vykonávané práce. Jedná se například o následující operace:

- výměna páskových médií a uložení do trezoru,
- diagnostika běžných provozních problémů,
- restartování nedokončených zálohovacích úloh,
- spuštění mimořádné zálohovací úlohy dle potřeb aplikačních a systémových administrátorů,
- provádění obnovy souborů,
- pravidelné testování scénáře obnovení IT služby [5].

2.3.1.2 Správci zálohování (backup adminstrators)

Dle velikosti organizace a rozsahu ICT je role správce zálohování přiřazována různým profesím. Velké firmy se často specializují a drží si výhradně roli správce zálohování.

Pracovník se tedy zaobírá pouze jednou problematikou ICT, ve které je velmi profilován. Menší firmy s méně rozsáhlou ICT přiřazují zodpovědnost za zálohování roli Systémový administrátor. Takový pracovník je bohužel v situaci, že musí v rámci své práce zodpovídat za běžný provoz IT služeb, včetně zálohování a všech činností spadajících do tohoto okruhu.

Zaměstnanci s rolí správce zálohování musí být schopni zajistit všechny operace jako operátoři a pracovníci podpory. Dále musí splňovat následující požadavky:

- detailní znalost návrhu systému zálohování,
- detailní znalost konfigurace zálohovacích úloh,
- řešení chyb v systému zálohování,
- schopnost komunikace s ostatními zaměstnanci a spolupráce na vytvoření zálohovacího plánu,
- vytváření návrhu změn a optimalizace zálohovacího systému,
- zavádění nových technologií,
- aktualizace dokumentace – zálohovací plán,
- řídit se empirií – tedy zkušenosti plynoucí z testování scénářů obnovy jednotlivých IT služeb [5].

2.3.1.3 Systémoví administrátoři (system administrators)

V rámci přístupu ke správě ICT v organizaci můžeme systémové administrátory zařadit do dvou kategorií. První kategorii tvoří systémový administrátoři mající určitou znalost o všech ICT systémech v organizaci. Druhá kategorie se vyznačuje tím, že dělá jen to, co má primárně na správu. Pro zajištění funkčního IT v organizaci je nutné hledat kompromis mezi oběma skupinami. Naučit ICT tým sdílet informace a předávat zkušenosti. To může být náročné v organizacích, kde je IT personálně poddimenzované. Pokud mají problematiku zálohování na starost systémoví administrátoři, jsou na ně kladeny stejné nároky jako na správce zálohování. Navíc musí být zajištěna obnova na úrovni operačních systémů, aplikačních služeb, které jsou ve správě systémových správců. Na každou operaci týkající se obnovení ICT služby musí být zdokumentovaný postup, plán obnovy, kde je krok po kroku ukázáno, jak v případě havárie postupovat, případně jaké pracovníky kontaktovat z důvodu zajištění součinnosti během procesu obnovy. Plán obnovy se musí v pravidelných časových intervalech testovat a dle výsledku testů zdokonalovat [5].

2.3.1.4 Aplikační administrátoři (applications administrators)

Aplikační administrátoři musí mít detailní znalost architektury jednotlivých aplikací, např. Exchange Server, SAP, Lotus notes, SharePoint, atd. Skupinu mohou rozšířit i tzv. databázoví administrátoři spravující např. aplikace SQL Server, Oracle, DB2. Byly zde vyjmenovány aplikace světových softwarových gigantů, ale aplikační administrátoři servisují i aplikace méně známých společností působící na regionální úrovni.

Široká znalost architektury aplikace je důležitá z důvodu volby strategie zálohování. Ve spolupráci se správcem zálohování utvářejí správnou metodu a garantují konzistenci provedených záloh. Mají hluboké povědomí, kdy a jakým způsobem je aplikace v prostředí využívána. Z tohoto důvodu jsou schopni poskytnout expertní znalost pro vytvoření zálohovacího plánu, včetně časového rozvržení zálohovacích úloh. Ve spolupráci se správci zálohování provádí testování scénářů obnovy ICT služeb / aplikací, které garantují [5].

2.3.2 Management

Úlohou managementu v procesu zálohování je jednoznačně nastavit obchodní požadavky na dostupnosti jednotlivých ICT služeb / aplikací, včetně potřeby zajištění obnovy ICT po havárii. Koncepce musí být v průběhu životního cyklu společnosti dynamicky upravena.

2.3.2.1 Týmový vedoucí

Jasně předává požadavky na zálohování ICT, které specifikuje vyšší management. Konzultuje požadavky s technickým personálem a podílí se na vytvoření / provozování technického řešení. Od technického personálu přijímá požadavky na změny v procesu zálohování a musí je prosadit u vyššího managementu. V otázce financí musí být schopen zdůvodnit rozpočet na službu zálohování, včetně vyhodnocení možných rizik plynoucí ze stávajícího technického zajištění vůči představám a požadavku vyššího managementu. V případě krizových situací působí jako nárazník mezi technickým personálem a společností. Je zodpovědný za řízení vývoje, udržování a aktualizaci plánu obnovy po havárii. Provádění testovacího scénáře obnovení ICT, včetně písemného vytvoření záznamu o provedení. Z pozice technické musí mít hrubé představy o celém procesu zálohování. Měl by být schopen provádět operativní činnosti týkající se obsluhy zálohovacího systému. Velmi důležitá je důvěra technického personálu, tímto je potlačeno riziko nepředávání nepříznivých informací, které by mohly v konečném důsledku znamenat nenaplnění požadavku společnosti na dostupnost ICT [5].

2.3.2.2 Vyšší management

IT ředitel tvoří most mezi managementem, týmovými vedoucími a technickým personálem. Díky detailnímu povědomí o záměrech a cílech managementu dokáže jednoznačně nastavit koncepci procesu zálohování. Dokáže vedení společnosti ovlivnit a správně směrovat jejich požadavky na ICT. Má na starost zajistit potřebný rozpočet a jeho výši umět managementu zdůvodnit. Namátkově kontroluje způsob realizace plánu obnovy a případnou evoluci procesu zálohování. Zpracovává statistiky o jednotlivých nedostupnostech ICT služeb a časech potřebných pro obnovení služby po havárii. Zodpovídá za dodržování domluvené kvality ICT služeb SLA (Service Level Agreement), kterou společně s managementem určili [5].

2.3.3 Uživatelé

Nejdůležitější skupinou pracovníků vstupující do procesu zálohování jsou samotní uživatelé, kteří pomoci ICT služeb / aplikací zpracovávají různá firemní aktiva. Aktiva jsou specifická dle zaměření podniku.

2.3.3.1 Klíčoví uživatelé

Klíčoví uživatelé často komunikují s aplikačními / systémovými správci. Mají základní technické znalosti o aplikaci a dokáží srozumitelně a přesně diagnostikovat problémy koncových uživatelů, které poté předávají technickému personálu. Z pohledu zálohování je důležité s těmito uživateli aktivně spolupracovat, protože přesně ví, kdy je ICT služba / aplikace nejméně využívána. V případě obnovení služby po havárii jsou důležití pro ověření správné funkčnosti aplikace a všech jejich funkčností. Svoje specifické znalosti předávají koncovým uživatelům a podílejí se na jejich zaškolení v rámci využívání ICT [5].

2.3.3.2 Koncoví uživatelé

V rámci procesu zálohování je velmi důležité, aby koncoví uživatelé byli schopni přesně definovat data, které požadují obnovit a případně upřesnit časový horizont, kdy jimi spravovaná data byla funkční. Prostřednictvím klíčových uživatelů musí být koncoví uživatelé informováni a neustále vzděláváni, co vše je zálohováno a jak dlouho jsou tyto zálohy uchovávány. Je nutné odbourat názor, že díky procesu zálohování se mohou v ICT prostředí chovat nezodpovědně [5].

3 KONCEPCE ZÁLOHOVÁNÍ

V rámci zálohovacího prostředí využíváme několik pojmenování k charakteristice členů procesu zálohování.

- Zálohovací server (backup server) je zodpovědný za plánování zálohovacích úloh, konfiguraci, reportování, správu médii, která uchovávají zálohovaná data.
- Klient (client) je zdroj, který je v procesu zálohování zabezpečený. V rámci ICT poskytuje byznys služby / aplikace, které jsou pro podnik významné. Z názvosloví používané v ICT zde klient neznamená klientský (uživatelský) počítač, ale server, který využívá funkčnosti zálohovacího serveru. Z tohoto pohledu je tedy do procesu zálohování zaveden jako klient využívající službu zálohování.
- Server s úložištěm (media server / storage node) je zařízení, které svou funkčností spadá mezi zálohovací server a klienta. Obvykle je vybaven HW prostředky pro ukládání dat a v rámci zálohování umí obsloužit sám sebe nebo další servery [9].

3.1 Topologie

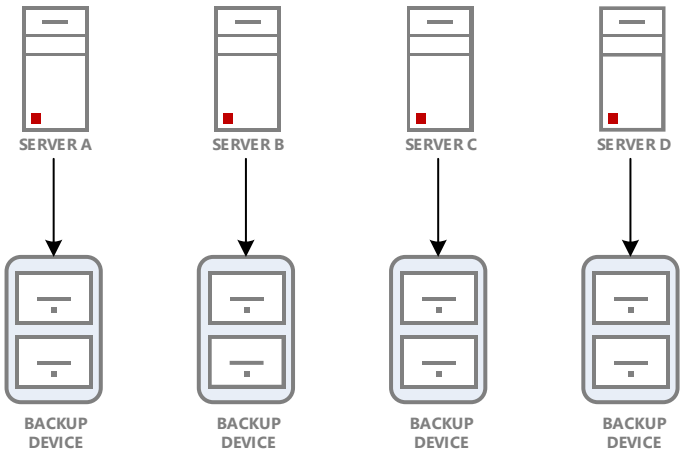
ICT architektura zálohovací topologie se dá rozdělit do dvou kategorií, a to na prostředí centralizované a decentralizované. Způsob využití jednotlivých typů je dán velikostí konkrétního ICT prostředí, které je zálohováno.

3.1.1 Decentralizovaná zálohovací topologie

Decentralizovaný způsob je hojně využíván v domácím prostředí, nebo v malých společnostech s nízkou integrací ICT. Spočívá v logice vyhrazeného systému zálohování pro každý server, který hostuje ICT služby / aplikaci. Na každém serveru je instalována zálohovací aplikace, která ukládá data na přímo připojené zálohovací zařízení (backup device). V některých případech může být zálohovací software nahrazen nativními prostředky pro zálohování, kterým disponuje ICT služba nebo aplikace. Častá jsou řešení, která využívají funkcionality skriptovacích jazyků. Díky znalosti místních aplikačních správců dochází tímto k vytvoření robustních a decentralizovaných systémů zálohování.

Výhodou decentralizované topologie zálohování je nezávislost jednotlivých serverů na centrálním zálohovacím serveru. Odpadá tím detailní časové plánování spouštění procesu zálohování a současně flexibilní možnost obnovování bez jakýchkoliv kompromisů. Další

výhodou je jednodušší konfigurace zálohovací úlohy, kdy je zálohovací úloha vytvořena pouze pro jeden server.



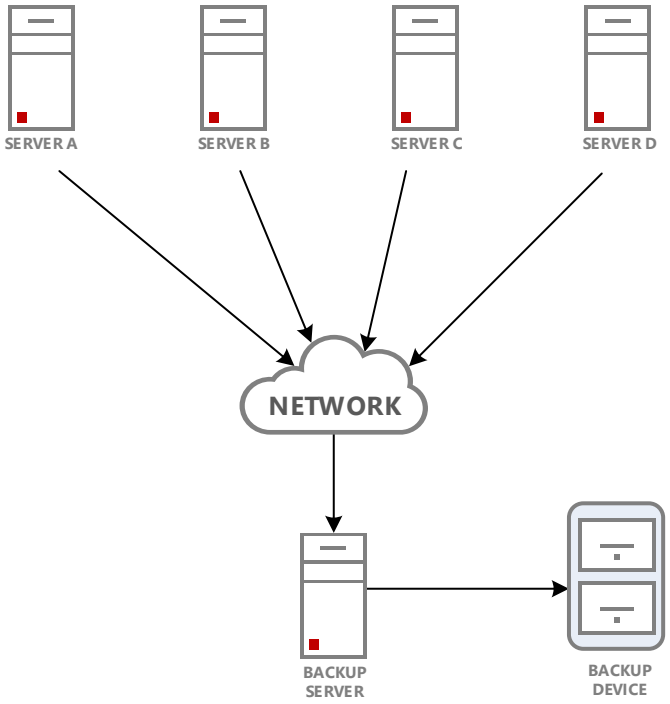
Obr. 4. Decentralizovaná topologie zálohování – upraveno autorem [5].

Nevýhody decentralizované metody spočívají v nutnosti mít pro každý server logicky izolované zálohovací zařízení. Nutnost většího počtu operátorů, který zajišťuje správu a výměnu páskových médií. Tím dochází k postupnému zvyšování nákladů na zajištění ochrany dat. Pozitiva jednodušší konfigurace jsou převážena nutností spravovat konfigurace pro několik serverů. Chybějící centrální správa a reportování stavu systému zálohování jsou zásadní v případě změny strategie zálohování, kterou určuje vedení společnosti. Pro zajištění mimořádné zálohy je třeba vykonat na všech serverech spadající do procesu stejnou změnu. To může být z časového hlediska velmi náročné. V případě využívání komerčního zálohovacího SW je částka vynaložená na zálohování vyšší, protože každá instalace obsahuje pouze zálohovací server a žádné klientské servery [5].

3.1.2 Centralizovaná zálohovací topologie

Centralizovaná topologie je využívána ve středních a velkých ICT řešeních. V rámci procesu zálohování je implementován minimálně jeden primární zálohovací server, který obsluhuje své klienty. V případě potřeby zvýšit výkonnost a modularitu zálohovacího řešení je možné přidat další sekundární zálohovací servery. V tomto případě je žádoucí využít zálohovací SW, který si umí s tímto poradit a zařadí všechny zálohovací servery pod jednotný management. Klienti služby zálohování jsou se zálohovacím serverem propojeni pomocí datové sítě, která může být dle použité technologie např. LAN, WAN (Wide Area Network), SAN, NAS (Network Attached Storage). Zálohovací server je zodpovědný za provedení

zálohy a následné uložení na zálohovací zařízení. V případě, kdy je nežádoucí přímá komunikace se zálohovacím serverem, je možné využít centralizovaný souborový server, který poskytuje dočasný prostor pro zálohy, které vytvoří klient zálohování, např. pomocí nativních prostředků ICT služeb / aplikací nebo skriptů. V rámci pravidelné zálohy jsou tyto data přenesena zálohovacím serverem do zálohovacího zařízení. Dojde tím k vytvoření hybridního řešení, které není centralizované ani decentralizované.



Obr. 5. Centralizovaná topologie zálohování – upraveno autorem [5].

Výhodou centralizované topologie jsou v celkovém důsledku nižší finanční nároky na zálohovací zařízení, zálohovací software a lidské zdroje, kdy není nutné velké množství operátorů. Podstatnou výhodou je flexibilita řešení spočívající ve snadné změně konfigurace, plánování doby provedení zálohy a souhrnného reportování stavu zálohovací infrastruktury. Pracovníci vstupující do procesu zálohování nemusí mít rozsáhlé znalosti několika jednotlivých systémů zálohování, ale rozvíjí své vědomosti v jednom nástroji, který je multiplatformní.

Nevýhodou centralizované topologie jsou vyšší náklady na zavedení procesu zálohování. V případě pořízení HW a SW je nutné počítat s finálním rozsahem nasazení služby, v rámci ICT prostředí se většinou plánuje na horizont pěti let. I přes vyšší pořizovací finanční

náročnost je centralizované řešení výhodnější, protože přidávání nových klientů již není finančně a personálně náročné [5].

3.2 Úroveň zálohování

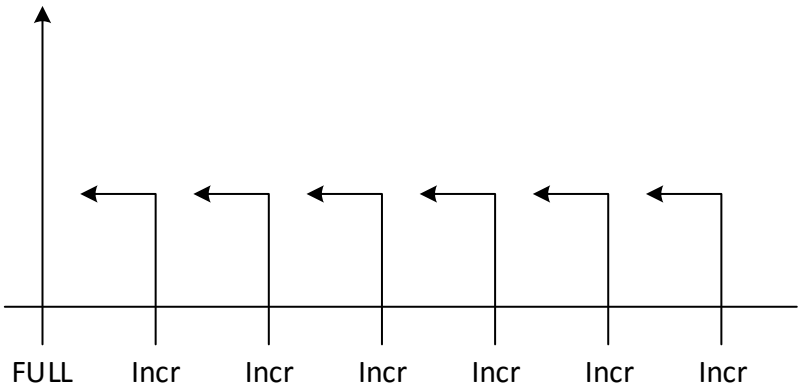
V závislosti na použitém zálohovacím softwaru jsou podporovány různé typy úrovně zálohování. Autoři zálohovacího softwaru mohou používat vlastní pojmenování úrovně zálohování. Úroveň popisuje, která data jsou zálohována v závislosti od poslední úspěšné zálohy. Pokud jsou některé ICT služby / aplikace vyjmuty z plánu záloh, nemá typ úrovně na tato data žádný vliv [5].

3.2.1 Plná záloha (full backup)

Nejzákladnější typ je plná záloha, kdy v průběhu zálohovací úlohy je provedeno zálohování všech dat umístěných na daném serveru. Tento typ je velmi spolehlivý z pohledu obnovy služby, kdy pro kompletní obnovu je nutný funkční set médií obsahující žádanou plnou zálohu. Dodatečné sety záloh nejsou požadovány, odpadá tím riziko nečitelnosti fyzického média. Výrazná časová náročnost provedení úlohy znemožňuje využívat tento režim pro ICT služby / aplikace, které vyžadují RPO (Recovery Point Objective) v řádu několika desítek minut až hodin. Pro provedení zálohy je nutné mít definováno dostatečně velké zálohovací okno. Periodické provádění úlohy nese velké kapacitní požadavky pro ukládání plných záloh. Kapacitní požadavky jsou neustále zvyšovány, a to i z důvodu nekonečného růstu dat v informačním systému. Znamená to tedy, že plná záloha není pro potřeby pravidelného zálohování na denní bázi vhodná. Bývá tedy doplňována jinými úrovněmi zálohování a tím dochází k optimalizaci celého procesu zálohování [5].

3.2.2 Inkrementální záloha (incremental backup)

Inkrementální záloha bývá často označována jako přírůstková. Během průběhu inkrementální zálohy dochází pouze k zálohování přírůstků dat, které byly změněny v čase od poslední zálohy. To má pozitivní dopad na množství zálohovaných dat a časový interval zálohovacího okna. Pro nekomerční produkty je tato úroveň možná pouze pro zálohování souborového systému. Využívá se možnosti změny atributu archivního bitu u každého souboru. Inkrementální záloha je využívána společně s plnou, kdy první záloha je provedena pomocí plné úrovně a poté následují jednotlivé inkrementální zálohy.



Obr. 6. Inkrementální zálohování – upraveno autorem [5].

U společností, kde je významně omezen víkendový provoz, může dojít ze strany osob zodpovědných za zálohování k deaktivaci provádění přírůstkových záloh. Není to správné řešení, protože zdánlivá úspora kapacity zálohovacího zařízení je zanedbatelně malá vůči riziku, že přes víkend došlo ke změnám velmi důležitých dat, která v případě mimořádné havárie budou ztracena. U zálohování platí jednoznačná poučka, zálohujte raději více než méně. V tabulce číslo 1 je uveden běžný příklad zálohovacího plánu, včetně použité úrovně zálohování [5].

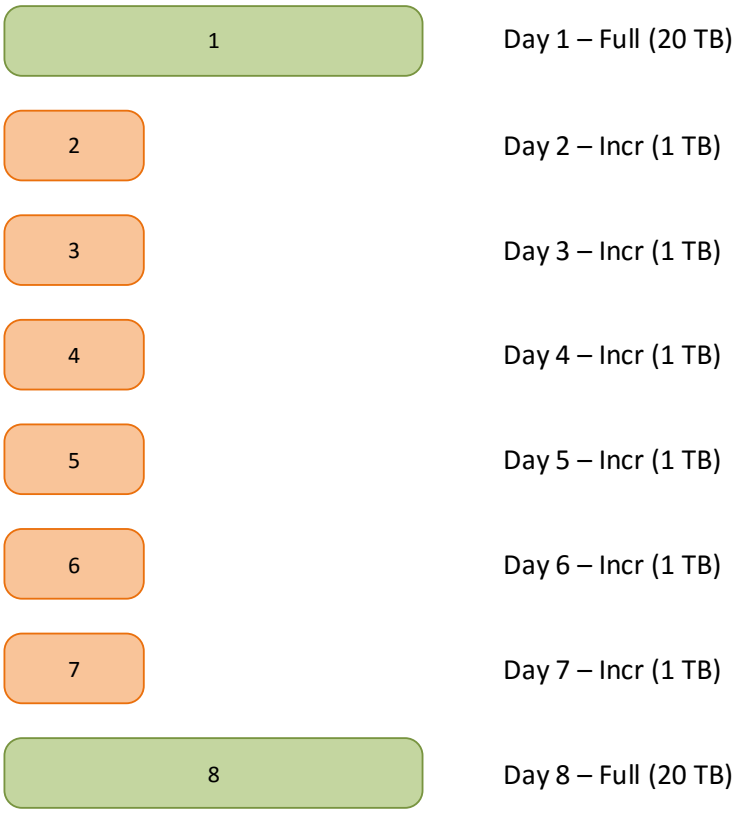
Tab. 1. Běžný týdenní inkrementální zálohovací plán – upraveno autorem [5].

Pátek	**Sobota**	**Neděle**	**Pondělí**	**Úterý**	**Středa**	**Čtvrtek**
Plná	Inkrement	Inkrement	Inkrement	Inkrement	Inkrement	Inkrement

Myšlenka vytvoření jedné plné zálohy a poté již „nekonečného“ inkrementu není zcela vhodná. Pro obnovení dat je nutné mít k dispozici veškeré předešlé zálohy od havárie vykonání po poslední plnou zálohu. Pokud požadujeme obnovit data ze středeční zálohy, potřebujeme k tomu následující média:

- pátek – plná záloha,
- sobota – inkrementální záloha,
- neděle – inkrementální záloha,
- pondělí – inkrementální záloha,
- úterý – inkrementální záloha,
- středa – inkrementální záloha.

Pokud je médium z pondělí nečitelné, můžeme poslední funkční obnovu provést z neděle. Detailnější představa o velikosti jednotlivých inkrementálních záloh v porovnání s plnou zálohou je znázorněna v obrázku číslo 7.



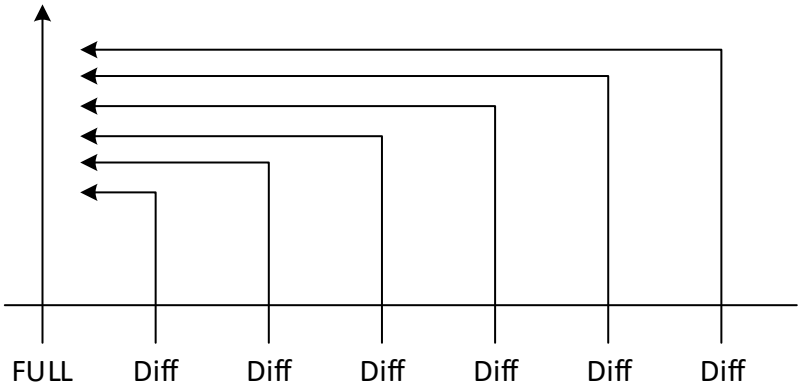
Obr. 7. Inkrementální zálohování – upraveno autorem [9].

Výrobci zálohovacích systémů doplňují možnosti přírůstkového zálohování o zpětnou inkrementální úroveň (reverse incremental backup). Výhodou zpětného inkrementu je integrace přírůstku do plné zálohy. Odpadá tedy nutnost periodického vytváření plné zálohy nebo ověření čitelnosti plné zálohy. Během integrace do plné zálohy dochází k přeskládání souboru plné zálohy. Samotné inkrementální zálohy jsou taktéž uchovávány, a to z důvodu možnosti vrátit se v čase po jednotlivých dnech. Další výhodou je rychlost obnovy, protože plná záloha obsahuje veškerá potřebná data, včetně posledního inkrementu. Nevýhodou může být větší časová náročnost zálohování a zatížení diskových subsystémů během přeskládání souboru s plnou zálohou [9].

3.2.3 Rozdílová záloha (differencial backup)

Rozdílová úroveň zálohuje veškerá změněná data od poslední plné zálohy. Odpadá zde nutnost čitelnosti řetězce provedených záloh v rámci zálohovacího plánu. Bohužel to nese negativum, v průběhu týdne se doba zálohování prodlužuje a potřebná velikost na uložení

záloh roste. V případě obnovy je nutné zajistit plnou kompatibilitu ICT služby / aplikace s rozdílovou zálohou. To může být problém u služeb, které využívají databázové prostředí.



Obr. 8. Rozdílová záloha – upraveno autorem [5].

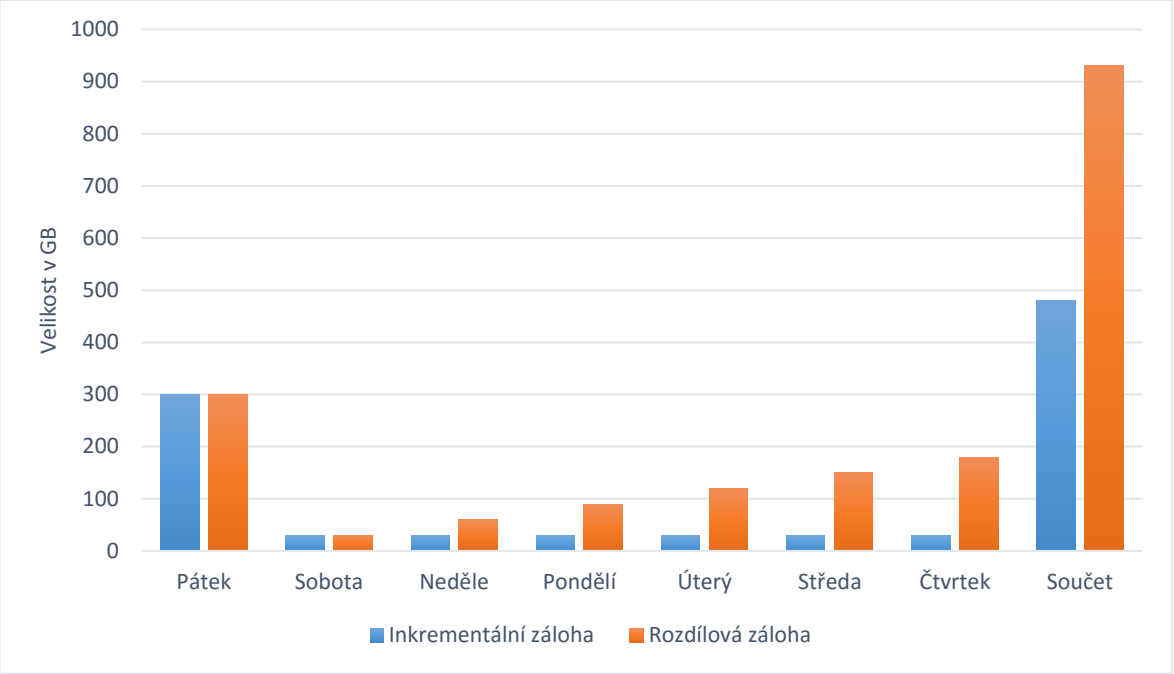
Zálohovací plán je obdobný s inkrementální zálohou.

Tab. 2. Běžný týdenní rozdílový zálohovací plán – upraveno autorem [5].

Pátek	**Sobota**	**Neděle**	**Pondělí**	**Úterý**	**Středa**	**Čtvrtek**
Plná	Rozdílová	Rozdílová	Rozdílová	Rozdílová	Rozdílová	Rozdílová

Výhodou rozdílové úrovně je odolnost vůči čitelnosti jednotlivých záloh. Pokud chceme obnovit data ze středy, budeme potřebovat páteční plnou zálohu a středeční rozdílovou zálohu. Nevýhodou je mnohem vyšší kapacitní náročnost pro ukládání záloh. Pro praktickou ukázku si zvolíme ICT službu o velikosti 300 GB (Giga Byte) s průměrnou denní změnou 10 %. Počáteční plná záloha je vytvořena v pátek a má velikost 300 GB. Denní přírůstky a finální datový součet za týden je uveden v grafu číslo 1 [9].

Graf. 1. Porovnání kapacitní náročnosti inkrementální a rozdílové zálohy.



3.2.4 Konsolidovaná úroveň (consolidated level)

Moderní zálohovací systémy nabízí možnost konsolidovaných záloh, v odborných skupinách je zmíněná funkcionalita označována jako synthetic full backup. Konsolidované zálohy jsou užitečné pro systémy, kde není možné provádět pravidelnou plnou zálohu, ale je tu přísný požadavek na rychlé obnovení služby. To není možné zajistit pomocí přírůstkové úrovně, protože musí být načteny a obnoveny všechny přírůstky zálohovacího řetězce.

Konsolidovaná úroveň využívá strategii, kdy v určitý časový interval, například co každý pátý den, je na pozadí do nové plné zálohy provedena konsolidace poslední plné zálohy a všech následujících inkrementálních záloh. Výhodou konsolidované úrovně je eliminování potřeby plné zálohy během provozu ICT služby / aplikace a pozitiva plynoucí z obnovy pomocí plné zálohy [5].

3.2.5 Ruční zálohování

Technicky se nejedná o úroveň zálohování, ale podpora mimořádných záloh je v systému zálohování velmi důležitá. V rámci zálohovacích softwarů se jedná o tzv. ad-hoc zálohy, které jsou spouštěny správcem nad rámec zálohovacího plánu. Praktické využití scénáře je před provedením plánovaných změn (upgrade ICT služby, konfigurační změny, atd.).

V případě častého využívání může docházet ke kolizi s řádnou plánovanou zálohou a tím k zvýšení zátěže zálohovací serveru, datové sítě a zálohovacího zařízení [5].

3.3 Dostupnost ICT služby / aplikace během procesu zálohování

Dostupnost ICT služby / aplikace je závislá na typu provedené zálohy. Pro určité typy systému není typ zásadní, ale v prostředí s očekávanou dostupností služby v režimu 24/7 je správný typ zálohování nezbytný.

3.3.1 Offline zálohování

Při offline typu zálohování je ICT služba / aplikace pro potřeby uživatelů nedostupná. Časové období nedostupnosti je závislé na celkové době běhu zálohovací úlohy. Po ukončení zálohy je informační systém opět zpřístupněn uživatelům. To je pro potřeby běhu moderních ICT služeb a aplikací velice omezující, protože uživatelé / byznys očekává dostupnost v režimu 24/7 [9].

3.3.2 Online zálohování

Při online typu zálohování je ICT služba / aplikace během provádění zálohovací úlohy pro potřeby uživatelů neustále k dispozici. Tento typ zálohy je náročný na výkon hardwaru, je tedy možné, že jednotlivé úkony s právě zálohovanou aplikací budou odbavovány pomaleji. Tuto problematiku částečně řeší moderní disková pole, která jsou vybavena technologií otisků datových oblastí. Zálohovací systém provádí zálohu z „virtuálního úložiště“ a výkon koncové ICT služby / aplikace je procesem zálohování nepoznamenán [9].

3.4 Výběr zálohovaných dat

3.4.1 Zahrnuté do zálohy (inklusive backup)

V rámci zálohovacího plánu je nutné zvolit data, která jsou obsažena v rámci prováděné úlohy. Výběr zálohovaných dat je možné definovat na úrovni souborového systému, virtuálních serverů, atd. Pomocí zahrnutí do záloh je možné přesně definovat data, která budou zálohovací úlohou zpracována. Je možné např. vynechat systémové disky, datové oblasti, které je možné jednoduše získat z prostředí Internetu. V rámci komerčních zálohovacích softwarů je možné definovat zahrnuté cesty a zadávat je pomocí parametrů (vše, pouze lokální disky, atd.) [5].

3.4.2 Vyloučené ze zálohy (exklusive backup)

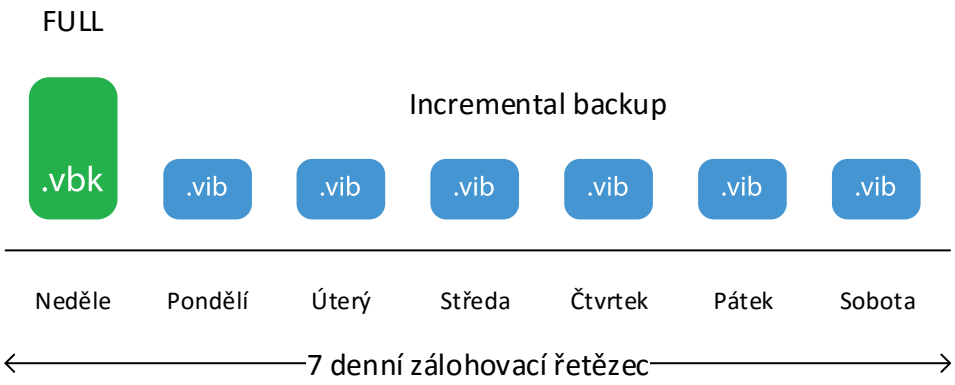
Výběr dat pomocí funkce vyloučení ze záloh stanoví jasně, že je zálohováno vše kromě striktně definovaných cest, které jsou v zálohovacím plánu uvedeny. Tímto způsobem je zajištěno doporučení raději zálohovat více než méně. Vyloučení ze záloh je užitečné v případě, kdy z objektivních důvodů je nežádoucí určitá data zálohovat. Může se jednat o dočasnou datovou oblast, úložiště s testovacími virtuálními počítači [5].

3.5 Retenční politika

Retenční politika definuje počet možných stavů ICT služby / aplikace v minulosti, ke kterým je možné se během procesu obnovení vrátit. Vychází z požadavku společnosti na dostupnost informačního systému. V případě požadavku na dlouhodobé uchovávání historie záloh je nutné počítat s vyšší kapacitou zálohovacího zařízení.

3.5.1 Jednoduchý retenční model

Jednoduchý retenční model je vhodný pro krátkodobé uchovávání záloh. V rámci zálohovací úlohy je definováno kolik bodů obnovy (restore points) je uchováváno. Dochází k vytvoření řetězce bodů obnovení, které po sobě následují. První bod obnovení je tvořen plnou zálohou, ostatní body jsou již přírůstkové. V případě přetečení počtu bodů obnovení je nejstarší bod přidán do plné zálohy a tím vzniká místo pro nový bod obnovení [16].



Obr. 9. Jednoduchý retenční model – upraveno autorem [16].

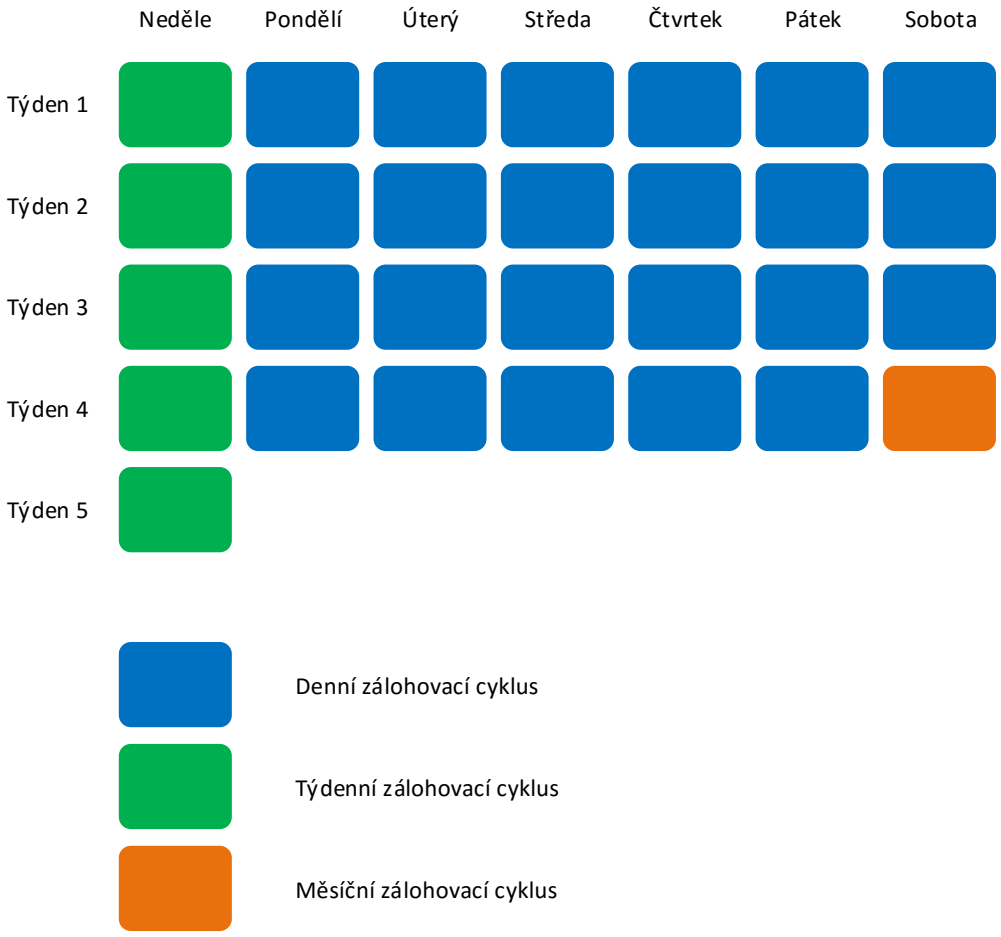
3.5.2 GFS retenční model

Jednoduchý retenční model je v určitých případech nedostatečný. V závislosti na použitém zálohovacím softwaru je množství bodů obnovy limitováno. Pro dlouhodobé uchování historie záloh slouží GFS (Grandfather-Father-Son) retenční model. Pro jednotlivé časové

periody je stanoveno různé množství bodů obnovení. GFS model pracuje v následujících pravidelných cyklech:

- denní (pravidelná) záloha,
- týdenní záloha,
- měsíční záloha,
- roční záloha.

Podmínkou pro nativní GFS rotaci je provádění záloh do páskového zálohovacího zařízení. U ostatních zálohovacích zařízení je možné GFS rotaci simulovat pomocí vhodně plánované zálohovací úlohy [11].



Obr. 10. GFS retenční model – upraveno autorem [11].

3.6 Zálohovací zařízení

Zálohovací zařízení představují skupinu hardwaru a cloudových služeb, které slouží pro cílové ukládání zálohovaných dat.

3.6.1 Magnetická pásková jednotka

V oblasti zálohování patří magnetická páska dlouhodobě mezi hlavní prostředky pro ukládání zálohovaných dat. V době magnetických a optických disků zní informace o neustálém vývoji páskových médií jako těžko uvěřitelná. Během neustálého vývoje vzniklo velké množství standardů pro magnetické pásky, kdy nejvíce používané jsou LTO (Linear Tape Open). O rozšíření standardu se zasloužily světové společnosti HP, IBM a Quantum. Současné verze pásek LTO generace 7 nabízí základní kapacitu 6 TB (Tera Byte) a v případě použití komprese až 15 GB. Magnetické pásky jsou vkládány do páskových jednotek. Vkládání provádí operátor případně automatický robot, který je součástí páskové knihovny. Dle celkového množství zálohovaných dat a retenční politiky je nutné vybrat správnou velikost páskové jednotky. Pásková knihovna IBM TS3310, která je určena do středně velkých organizací má možnost uložit a obsluhovat až 41 páskových médií [5], [8].

Obr. 11. Pásková knihovna IBM TS3310 [8].

Díky životnosti jsou pásková média vhodná pro archivní uchování záloh. Další velkou výhodou páskových médií je snadná přenosnost, to je důležité pro tzv. offline zálohy. Offline zálohy jsou vynášeny z datového centra a uchovávány na bezpečném místě pro případ obnovy pro disaster recovery. Nevýhodou páskových jednotek je nutnost mít pro obnovení dat kompletní set médií z dané zálohovací úlohy. V případě menších knihoven to znamená ruční vkládání médií, které má za následek pomalejší dobu obnovy.

Z těchto důvodů se doporučuje zálohovat pomocí strategie Disk to Disk to Tape [5].

3.6.2 Diskové datové úložiště

Diskové datové úložiště v oblasti zálohování přebírají od páskových jednotek první pozici v oblíbenosti ukládání souborů záloh. Má na to vliv nízká cena a vyšší kapacity SAS (Serial Attached SCSI), SATA (Serial Advancend Technology Attachment) a Nearline SAS pevných disků. Jednotlivé pevné disky jsou uloženy v diskových polích. Dle typu diskového pole je v rámci jedné expanze umístěno dvacetčtyři 2,5 palcových nebo dvanáct 3,5 palcových pevných disků. Počet disků se může dle výrobce lišit. Diskové pole společnosti IBM Storwize V7000 umožňuje v rámci jedné police nabídnout hrubou kapacitu až 96 TB při použití 8 TB nerline SAS pevných disků. Diskové pole umožňuje připojení až dvaceti diskových polic [5], [7].

Obr. 12. Diskové pole IBM Storwize V7000 [7].

Dle typu fyzického připojení datové oblasti k hostujícímu serveru rozeznáváme následující typy:

- SAN,
- NAS.

Z důvodu kompatibility zastaralých systémů zálohování s páskovými jednotkami a rozšíření oblíbenosti diskových datových úložišť pro potřeby zálohování bylo výrobci hardwaru vytvořeno hybridní řešení, které se nazývá virtuální pásková jednotka. Od páskové jednotky se liší tím, že místo páskových médií dochází k ukládání dat na pevné disky. V rámci zálohovacího SW se toto zařízení tváří jako pásková mechanika a umožňuje tím využít GFS retenčního modelu.

Diskové datové úložiště, včetně flashových datových úložišť nabízí pokročilé funkcionality, které jsou pro oblast zálohování prospěšné. Jedná se o funkcionalitu replikace diskových polí, deduplikace, zálohování pomocí otisku datových oblastí, komprimace, atd. Bohužel

jsou tyto funkcionality dodatečně licencovány, a to přináší další nemalé náklady spadající na oblast zálohování [5].

3.6.3 Flash datové úložiště

Flashové datové úložiště vychází z běžných diskových datových úložišť. Zásadní změnou je jiný typ datového média, který se označuje jako SSD (Solid State Drive). Médium typu SSD neobsahuje žádné rotační části, ale je tvořeno flashovou pamětí. V porovnání s rotačními disky umožňují SSD několikrát rychlejší zápis / čtení dat na médium. Nevýhodou SSD disků je vysoká cena, nízká datová kapacita a omezený počet zápisů do paměťové buňky. Zálohovat na flashové datové úložiště není z finančních důvodů v současnosti běžné. Nicméně se častěji vyskytují implementace, kdy je flashové datové úložiště využíváno jako rychlé dočasné úložiště pro zajištění co nejrychlejší zálohy a tím co nejnižší omezení produkčního informačního systému.

Do flashových datových úložišť dále spadají veškeré typy paměťových karet a USB (Universal Serial Bus) flash disky [9].

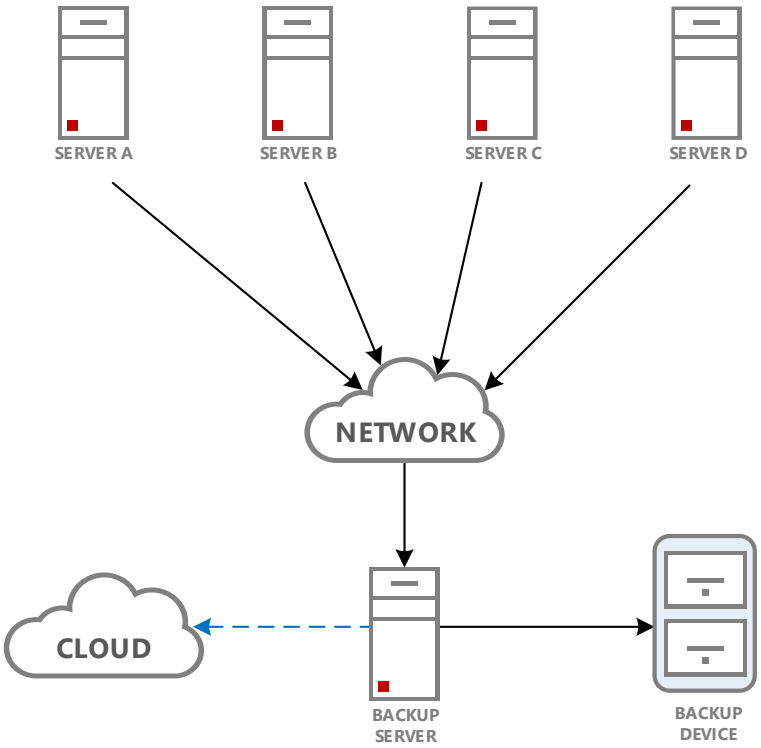
3.6.4 Optická datová úložiště

Optická datová úložiště jsou reprezentována médiem typu CD-R (Compact Disc - Recodable), CD-RW (Compact Disc - Rewritable), DVD-R (Digital Versatile Disc – Recordable), DVD+R (Digital Versatile Disc + Recordable), DVD-RW (Digital Versatile Disc - Rewritable), DVD+RW (Digital Versatile Disc + Rewritable), BD-R (Blu-ray Disc - Recodable), BD-RE (Blu-ray Disc – Recodable Erasable). Optická média jsou pro potřeby v pokročilých zálohovacích scénářích nevhodná. Jejich využití může být vhodné v domácím prostředí [9].

3.6.5 Cloudové datové úložiště

V době rozmachu cloudových služeb nabízí poskytovatelé v rámci cloudu stále nové služby. Jednou ze služeb je možnost vybudování disaster recovery lokality pro ukládání záloh. V rámci měsíčního předplatného, které je závislé na množství uložených dat, dochází k platbě za využívání služby. Odpadá budování disaster recovery, které může být pro řadu společností z finančních důvodů nedosažitelné. Dále je tu značná výhoda v rychlosti použitelnosti disaster recovery. Již za několik málo minut je možné začít zálohovat do offline lokality. Bohužel staré zálohovací nástroje nepodporují tyto nové technologické možnosti.

Je tedy nutné hledat zálohovací SW, které umožňují přímou integraci s cloudovými službami [9].



Obr. 13. Zálohování do cloudové služby – upraveno autorem [5].

V rámci procesu zálohování probíhá zálohovací úloha ve dvou fázích. V první fázi proběhne zálohování na přímo dostupné zálohovací zařízení. Tím je zajištěno, že provedení zálohy je provedeno v co nejkratším zálohovacím okně. Po dokončení zálohování úlohy proběhne operace kopírování souborů záloh do cloudového umístění. Tento postup se může lišit od technických parametrů konektivy k veřejné síti Internet a možnostech zálohovacího softwaru.

3.7 Užitečné rady k zálohování

3.7.1 Pravidlo 3-2-1

Pravidlo 3-2-1 je dobré mít neustále na paměti a pokud možno se jím neustále řídit. Jedná se o velmi jednoduchou pomůcku jak správně zálohování provozovat.

Význam čísla 3 udává, že veškerá data v organizaci mají být minimálně ve třech kopiích. Tyto kopie jsou ukládány na 2 různé typy zálohovacích zařízení. A konečně číslo 1 udává,

že aspoň jedna záloha musí být umístěna v jiné geografické lokalitě vůči produkčnímu prostředí [19].

3.7.2 Paranoia

V problematice zálohování je nutné ctít pravidlo raději zálohovat nadbytečná data než zálohovat méně. Během fáze nasazení nové ICT služby / aplikace do zálohování je nutné ve spolupráci s garanty služby definovat postup během obnovy. Tento postup jasně popisuje co, jak a kdy se má zálohovat. Pokud ze strany garanta není snaha o nastavení řádu, raději zálohujme vše [5].

3.7.3 Testování, testování, testování

Po dokončení zálohy nelze spoléhat, že jsou zálohy připraveny pro budoucí obnovování. Proces obnovení je nutné v pravidelných obdobích testovat. Dochází tím k nacvičení a zdokonalování postupů obnovy ICT služby / aplikace a ověření čitelnosti a komplexnosti zálohovaných dat. Nácvik plánů obnovy přináší benefit v podobě rychlejší obnovy během skutečné havárie [5].

4 PŘEHLED DOSTUPNÝCH ZÁLOHOVACÍCH SYSTÉMŮ VIRTUALIZOVANÉHO PROSTŘEDÍ

Na současném IT trhu je k dispozici velké množství komerčních zálohovacích softwarů určených k zálohování virtualizované infrastruktury. Tradiční výrobci jako IBM, Symantec, EMC, atd. museli reagovat na změny ve způsobu provozování IT infrastruktury. Nové společnosti např. Veeam využily změny na trhu a uvedly na trh produkty, které se staly konkurenty softwarů velkých hráčů v oblasti zálohování. V rámci kapitoly si základně představíme několik softwarových produktů. Ve většině případů výrobci softwaru poskytují nástroje v několika edicích, které se mezi sebou liší cenou a funkcionalitou. Informace jsou čerpány z webových stránek výrobců. Je jisté, že výrobci v rámci aktualizací zálohovacích systémů budou funkcionalitu programu rozvíjet. Informace, které jsou zde uvedeny, mohou být v určitém období nepřesné.

4.1 Zálohovací software

4.1.1 Acronis Backup Advanced

Řešení společnosti Acronis je určeno pro středně velké společnosti. Nabízí možnost zálohování širokého spektra virtualizačních technologií (VMware, Hyper-V, Citrix XenServer, Oracle VM Server, Linux KVM). Správa nástroje je prováděna pomocí centrálního managementu. Je podporováno zálohování do různých typů zálohovacích zařízení (disk, páska, cloud). Zajištěna ochrana podnikových aplikací typu Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint, Microsoft Active Directory. Kapacitní datová náročnost ukládání záloh je optimalizována pomocí kompresní a deduplikační technologie. Podporuje přírůstkové a rozdílové metody zálohování, včetně retenčních politik. Jednotlivé zálohy je možné chránit pomocí asymetrického šifrování [1].

4.1.2 Altaro VMBACKUP

Společnost Altaro nabízí zálohovací řešení pro virtualizaci VMware a Hyper-V. Správu nástroje je možné provádět pomocí centrálního managementu. Nativně je podporováno konzistentní zálohování Microsoft Exchange Serveru a Microsoft SQL Serveru, včetně obnovy na úrovni jednotlivých položek. Není podporováno zálohování na páskovou jednotku a chybí možnost deduplikace a komprese dat během vytvoření záloh. Podpora pro zabezpečení záloh pomocí asymetrického šifrování je umožněna [2].

4.1.3 IBM Spectrum Protect for Virtual Environments

Společnost IBM je tradičním výrobcem rodiny zálohovacích řešení, které se původně jmenovaly IBM Tivoli Storage Manager. Aplikace nabízí podporu virtualizace VMware a Hyper-V. K dispozici je centrální správa a automatické prohledávání virtualizovaného prostředí, které zajišťuje přidání nově vytvořených virtuálních serverů. Nativně je podporováno konzistentní zálohování Microsoft Exchange Serveru a Microsoft SQL Serveru, včetně obnovy na úrovni jednotlivých položek. Přítomna je deduplikace, ale chybí možnost komprimace. V rámci zálohovacích metod je možné využít možnost nekonečných inkrementů. Pro ukládání záloh je možné uložit diskové jednotky, páskové mechaniky. Chybí možnost zálohovat do cloudového prostředí [6].

4.1.4 Veritas NetBackup

Produkt společnosti Veritas podporuje virtualizační technologie VMware a Hyper-V. Umožňuje zálohy ukládat na diskové jednotky, páskové jednotky a do cloudových služeb. Podporuje konzistentní zálohu aplikačních služeb Microsoft SQL Server, Microsoft Exchange Server, Microsoft Active Directory, Microsoft SharePoint. Je umožněno zálohování na diskové jednotky, páskové jednotky a cloudové služby. Zabezpečení dat je možné pomocí asymetrického šifrování. Pro nasazení nástroje není nutné instalovat agenty na zálohované virtuální servery. Umožňuje pokročilou deduplikaci a technologickou integraci s diskovými poli [20].

4.1.5 Veeam Backup & Replication

Pro velké společnosti nabízí společnost Veeam zálohovací řešení Backup & Replication v edicích Standard, Enterprise a Enterprise Plus. V oblasti obnovení virtuálních počítačů je k dispozici:

- Úplné obnovení virtuálních počítačů – obnova na původním, nebo jiném hostiteli. Obsahuje funkci rychlého vrácení změn z důvodu provedení obnovy pouze u změněných bloků dat.
- Instant VM (Virtual Machine) Recovery – rychlé obnovení služby spuštěním virtuálních počítačů ze souboru zálohy v úložišti pro zálohování.
- Obnovení souboru VM a virtuálního disku.

Podporováno je obnovení na úrovni souborů – obnovení souborů ze 17 souborových systémů využívanými běžnými operačními systémy např. Windows, Linux, BSD, Mac OS, Novell, Solaris, Unix.

Obnova na úrovni jednotlivých položek, včetně konzistentní zálohy u následujících aplikací:

- Veeam Explorer pro Microsoft Active Directory – obnova všech typů objektů, např. uživatel, skupina, účet počítače, kontakt, obnova hesel.
- Veeam Explorer pro Microsoft Exchange server – obnova jednotlivých položek (e-mailů, položek kalendáře, poznámek, kontaktů.
- Veeam Explorer pro Microsoft SQL server.
- Veeam Explorer pro Microsoft SharePoint.
- Universal Application Item Recovery – obnovení jednotlivých objektů virtualizovaných aplikací.

Je podporováno rozdílové a přírůstkové zálohování, včetně možnosti nekonečného inkrementu. Možnost vytvořit mimořádné zálohy. Během zálohování je možné nastavení maximální rychlosti čtení a zápisu z důvodu zajištění dostatečné odezvy produkčního systému. Je umožněno zálohování na diskové jednotky, páskové jednotky a cloudové služby. Zálohy je možné chránit pomocí asymetrického šifrování. Během ukládání záloh umožňuje deduplikaci a kompresi. Zálohovací software umožňuje replikaci virtuálních počítačů pro potřeby zajištění disaster recovery, včetně vytvoření disaster recovery plánů. Velmi užitečnou vlastností je funkcionalita SureBackup, která spočívá v automatickém testování a prověření obnovitelnosti každého zálohovaného virtuálního počítače spuštěním po dokončení zálohy. Dále je možné využít On-Demand Sandbox, který zajišťuje spuštění virtuálních počítačů v izolovaném testovacím prostředí za účelem testování změn a odstraňování problémů během nasazení nových funkcí. To je velmi důležité pro zajištění vyšší dostupnosti a spolehlivosti produkčního prostředí [18].

4.2 Shrnutí

V rámci zajištění zálohování a obnovy virtualizované infrastruktury disponují sledované aplikace velmi podobnými vlastnostmi. Všechny nástroje umožňují zálohovat obě hlavní virtualizační platformy. Zálohování probíhá během běžného provozu a je bez výpadku podnikových ICT služeb / aplikací. V přehledu jsou uvedeny dva nástroje spadající do

segmentu velmi velkých IT prostředí. Jedná se o produkty společností IBM a Veritas. Bohužel na webových stránkách obou společností nejsou uvedeny přesné detaily funkcionalit produktů a celkově informační hodnota webové prezentace je slabší. Nicméně oba produkty jsou funkční a spolehlivé, ale v porovnání s Acronis a Veeam je implementace mnohem náročnější. Cena těchto řešení je v porovnání s konkurencí vysoká.

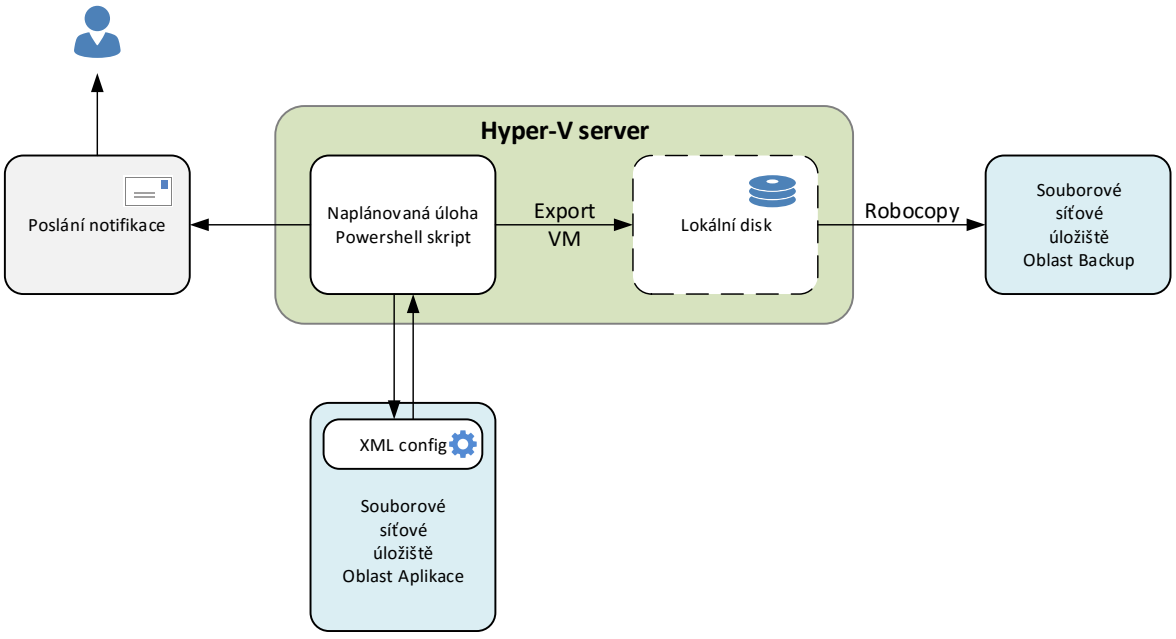
Do segmentu středně velkých IT prostředí spadají nástroje společností Acronis a Veeam. Acronis nabízí nejširší podporu virtualizovaných prostředí a nabídka funkcionalit je velmi rozsáhlá. Řešení společnosti Veeam je v současnosti považováno za jedno z nejoblíbenějších. Nabízí široké možnosti v oblasti zálohování a navíc přináší komplexní řešení pro vysokou dostupnost datových center pomocí integrované replikace. Obě společnosti mají výbornou prezentaci na webových stránkách.

V segmentu malých IT prostředí je možné využít funkcionality produktu společnosti Altaro. Nabízí všechny funkce potřebné pro jednoduché zálohování a obnovování dat. Z důvodu chybějících doplňkových technologií je produkt lehce ovladatelný.

II. PRAKTICKÁ ČÁST

5 ANALÝZA SOUČASNÉHO STAVU ZÁLOHOVÁNÍ VIRTUALIZOVANÉ INFRASTRUKTURY

V prostředí Fakultní nemocnice Olomouc byla provedena analýza stávajícího stavu zálohování virtuálního prostředí. V nemocnici je využíváno virtualizované řešení od společnosti Microsoft v rámci produktů Windows Server 2008 R2 a Windows Server 2012 R2. V rámci Windows Serveru 2008 R2 jsou v režimu vysoké dostupnosti provozovány čtyři klastry. Aplikační klastr sloužící pro hostování nemocničních služeb a systémový klastr sloužící pro potřeby infrastruktury. Zálohování virtuálních serverů bylo realizováno pomocí nativních prostředků technologie Hyper-V a nástroje robocopy. Oba nástroje byly obsluhovány pomocí powershell skriptu, který byl spouštěn pomocí naplánované úlohy na jednotlivých nodech klastru. Skript byl parametrizován pomocí XML (Extensible Markup Language) souboru, kde správce zálohování definoval způsob provedení zálohy. Pro jednotlivé virtuální počítače bylo umožněno definovat denní časový plánovač a nastavit ignorované virtuální disky.



Obr. 14. Proces zálohování pomocí Powershell skriptu.

V rámci naplánované úlohy došlo na jednotlivých nodech ke spuštění skriptu, který z Hyper-V získal informaci o běžících virtuálních serverech. Poté v rámci skriptu proběhlo zpracování XML a zjištění, které virtuální servery se mají zálohovat. Pokud došlo ke zjištění, že se nemá nic zálohovat, došlo k ukončení skriptu a odeslání e-mailu s informací, že žádný virtuální server nebyl zálohován. V opačném případě skript pomoci Hyper-V powershell

modulu požádal o vytvoření otisku virtuálního serveru a jeho export na lokální disk nodu klastru. Po ukončení exportu došlo ke spuštění nástroje robocopy, který provedl kopírování souborů exportovaného virtuálního počítače na centrální síťové úložiště. Po ukončení kopírování došlo ke smazání exportovaných dat z lokálního disku a pokračování v dalším virtuálním serveru. Celý proces byl z časového a kapacitního hlediska náročný. Záloha jednoho virtuálního počítače trvala přibližně 45 minut v závislosti na velikosti virtuálního disku. Řešení má celou řadu problémů, kdy mezi nejzávažnější patří závislost provedení zálohy na volné kapacitě lokálního disku serveru. Starší servery byly vybaveny pevnými disky o kapacitě 74 GB. Pro potřeby zálohování zbývalo cca 40 GB prostoru, a to pro některé virtuální počítače nestačilo. V rámci skriptu byla ošetřena podmínka na dostatečné volné místo. Do té doby hrozilo zaplnění systémového disku a vyřazení serveru z provozu. Zálohování pomocí skriptu bylo dostačující v době, kdy v prostředí nemocnice bylo provozováno maximálně dvacet virtuálních serverů. Během postupné migrace virtuálních serverů na nový operační systém Windows Server 2012 R2 bylo rozhodnuto, že funkcionalita zálohování pomocí skriptů nebude již dále rozvíjena. U virtuálních serverů, které byly ze systémového hlediska pro funkci nemocnice důležité, proběhla implementace replikování do druhé lokality pomocí technologie Hyper-V replika. U systémových virtuálních serverů, které zůstaly provozované v rámci operačního systému Windows Server 2008 R2 docházelo ke změně zálohovacího plánu, kdy automatické zálohování nahradilo ruční zálohování. Aplikační servery důležité z hlediska zajištění lékařské peče, byly zálohovány v týdenním režimu. Data zpracovaná těmito systémy byla uchovávána v SQL (Structured Query Language) databázích, které byly hostovány na fyzických serverech a do dnešního dne jsou zálohovány pomocí zálohovacího systému IBM Tivoli Storage Manager.

Nemocnici tedy reálně nehrozila ztráta dat a informací o pacientech. Z pohledu znovu zavedení služby po havárii, z důvodu ztráty aplikačního virtuálního serveru, nebylo možné u většiny ICT aplikací dosáhnout RTO (Recovery Time Objective) v řádu několika hodin. Tím by jednoznačně došlo ke snížení poskytované kvality péče o pacienty.

V rámci přehlednosti a ovlivňování výkonu byly virtuální servery rozděleny na aplikační a systémové Aplikační servery zajišťují funkci některých nemocničních systémů, např. laboratoře, analyzátory, skladové hospodářství, atd. Servery pro infrastrukturu zajišťují systémový provoz ICT služeb, např. autentizační služby, update služby, souborové služby, atd.

5.1 Popis aplikačního virtuálního prostředí

Aplikační virtuální servery byly provozovány na čtyřech nodech klastru CLS-APP2009. Každý nod disponoval následující konfigurací:

- 2x Intel Xeon X5560 @ 2.8 GHz (Giga hertz),
- 40 GB operační paměti,
- Operační systém Windows Server 2008 R2 edice datacenter.

Všechny nody byly připojeny ke sdílenému diskovému poli pomocí technologie Fibre Channel. V rámci tohoto klastru byly provozovány ICT aplikace zajišťující chod nemocnice v rozsahu od specializovaných lékařských systémů až po rezervační systém závodní jídelny. Z důvodu stáří všech serverů a nízkému počtu procesorových jader bylo i s ohledem na způsob licencování komerčního zálohovacího systému dohodnuto nahrazení klastru novým dvou nodovým klastrem.

5.2 Popis systémového virtuálního prostředí

Systémové servery byly provozovány ve čtyřech dvou nodových klastrech.

5.2.1 Klastr CLS-ISS2009

Oba nody disponují následující konfigurací:

- 2x Intel Xeon E5-2670v2 @ 2.5 GHz,
- 24 GB operační paměti,
- operační systém Windows Server 2008 R2 edice enterprise.

Všechny nody byly připojeny ke sdílenému diskovému poli pomocí technologie Fibre Channel. V rámci klastru jsou provozovány služby zajišťující běh ICT infrastruktury, např. adresářové služby Active Directory, interní certifikační autorita, interní windows update služba. V rámci analýzy došlo k závěru virtuální servery přesunout do klastru CLS-APP2014 a klastr CLS-ISS2009 zrušit.

5.2.2 Klastr CLS-APP2014

Oba nody disponují následující konfigurací:

- 2x Intel Xeon E7-4830 @ 2.2 GHz,

- 128 GB operační paměti,
- operační systém Windows Server 2012 R2 edice datacenter.

Všechny nody byly připojeny ke sdílenému diskovému poli pomocí technologie Fibre Channel. V rámci klastru jsou provozovány služby zajišťující běh ICT infrastruktury, např. monitoring služby, souborové služby, poštovní služby, atd. Z důvodu zajištění provizorní zálohy byly všechny servery v klastru jednou denně replikovány do druhé lokality. V rámci analýzy bylo rozhodnuto o zrušení replikace a zavedení pravidelného zálohování.

5.2.3 Klastr CLS-IDMZ

Oba nody disponují následující konfigurací:

- 2x Intel Xeon E5530 @ 2.4 GHz,
- 24 GB operační paměti,
- operační systém Windows Server 2008 R2.

Všechny nody byly připojeny ke sdílenému diskovému poli pomocí technologie Fibre Channel. V rámci klastru jsou provozovány bezpečnostní služby a služby zajišťující publikování informací do sítě Internet v interní demilitarizované zóně např. interní firewall služby, vzdálený přístup pomocí technologie společnosti Citrix, VPN koncentrátor, brána pro videokonference, atd.

5.2.4 Klastr CLS-EDMZ

Oba nody disponují následující konfigurací:

- 2x Intel Xeon E5420 @ 2.5 GHz,
- 8 GB operační paměti,
- operační systém Windows Server 2008 R2.

Všechny nody byly připojeny ke sdílenému diskovému poli pomocí technologie Fibre Channel. V rámci klastru jsou provozovány bezpečnostní služby a služby zajišťující publikování informací do sítě Internet v externí demilitarizované zóně např. externí DNS (Domain Name System) překlady, vzdálený přístup pomocí technologie společnosti Citrix, FTP (File Transfer Protokol) služba, reverzní webová proxy. atd.

V rámci IDMZ / EDMZ klastru bylo rozhodnuto neprovádět žádné konfigurační změny. Servery budou nahrazeny v průběhu roku 2017. Stávající servery byly zahrnuty do nového systému zálohování.

Tab. 3. Přehled zálohování virtuálního prostředí v době analýzy.

Typ klastru	**Název klastru**	**Verze operačního systému Windows Server**	**Počet běžících virtuálních serverů**	**Počet zálohovaných virtuálních serverů**
Aplikační	CLS-APP2008	2008 R2	34	16
Systémový	CLS-ISS2009	2008 R2	6	0
Systémový	CLS-IDMZ	2008 R2	6	0
Systémový	CLS-EDMZ	2008 R2	6	0
Systémový	CLS-APP2014	2012 R2	27	0

5.2.5 Zálohovací plán

Zálohovací plán pro virtuální prostředí nebyl v organizaci zaveden. Veškeré zálohy probíhaly pouze na týdenní bázi.

Tab. 4. Zálohovací plán v době analýzy.

Název Serveru	**Denní záloha**	**Týdenní záloha**	**Měsíční záloha**
SRV-01		x	
SRV-42		x	
SRV-44		x	
SRV-46		x	
SRV-53		x	
SRV-55		x	
SRV-59		x	
SRV-76		x	

Název Serveru	Denní záloha	Týdenní záloha	Měsíční záloha
SRV-80		x	
SRV-86		x	
SRV-87		x	
SRV-89		x	
SRV-90		x	
SRV-95		x	
SRV-98		x	
SRV-99		x	

6 NÁVRH IMPLEMENTACE ZÁLOHOVACÍHO SYSTÉMU SPOLEČNOSTI VEEAM SOFTWARE

Ve spolupráci s pracovníky informatiky Fakultní nemocnice Olomouc bylo rozhodnuto o nutnosti zkvalitnit problematiku zálohování virtualizované infrastruktury, a to z následujících důvodů:

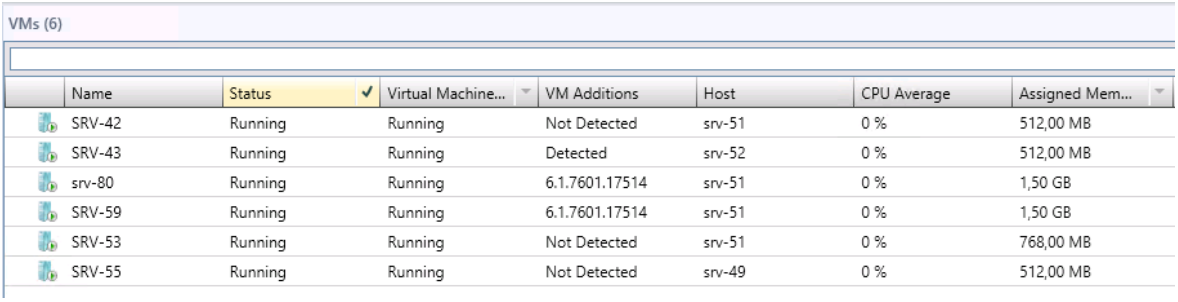
- snížit riziko nedostupnosti ICT služeb / aplikací,
- snížit RTO čas při obnově ICT služeb / aplikací po havárii,
- zajistit možnost obnovy dat z adresářových a poštovních služeb na úrovni jednotlivých objektů,
- zajistit možnost kontinuální replikace virtuálních serverů, které z pohledu nemocnice hostují kritické služby.

Po provedení průzkumu trhu, zjištění referencí a testovacího provozu byl pro potřeby zálohování vybrán zálohovací systém Veeam Backup & Replication v aktuální verzi číslo 9, který byl dodán včetně podpory.

Fakultní nemocnice souběžně připravovala veřejnou soutěž na dodávku nového blade řešení LENOVO Flex systém, včetně dodávky čtyř serverů. V rámci této soutěže bylo soutěženo rozšíření diskového pole IBM Storwize V7000 v záložní lokalitě, pro potřeby primárního uložení záloh virtualizované infrastruktury. Z důvodu zpoždění výroby a dodávky serverů byly HW prostředky předány až v průběhu měsíce dubna.

6.1 Návrh implementace systému zálohování

Zálohovací systém je licencován dle počtu fyzických procesorů. Na jeden server se dvěma procesory je nutné pořídit dvě licence. Je tedy finančně výhodnější disponovat s menším počtem výkonných serverů. Z tohoto důvodu bylo rozhodnuto, že klastr CLS-APP2009 bude nahrazen novým klastrem CLS-APP2016. Většina virtuálních serverů byla přesunuta na nově vytvořený klastr. Bohužel se nepodařilo provést migraci všech virtuálních serverů, a to z důvodu nutného odstavení ICT aplikace, které nebylo z provozních důvodů možné provést. Dokončení migrace bude probíhat postupně a nemá vliv na předmět práce.



VMs (6)

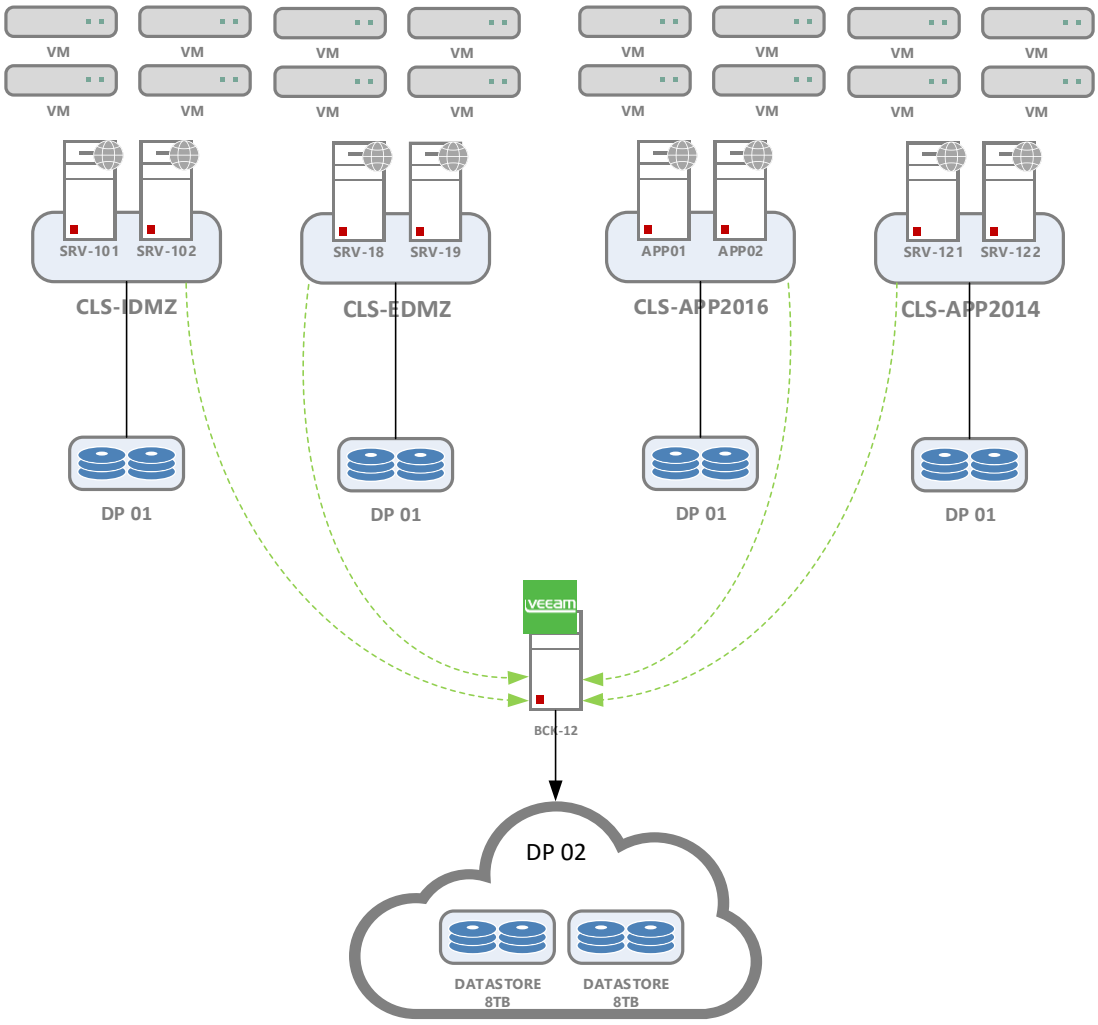
Name	Status	Virtual Machine...	VM Additions	Host	CPU Average	Assigned Mem...
SRV-42	Running	Running	Not Detected	srv-51	0 %	512,00 MB
SRV-43	Running	Running	Detected	srv-52	0 %	512,00 MB
srv-80	Running	Running	6.1.7601.17514	srv-51	0 %	1,50 GB
SRV-59	Running	Running	6.1.7601.17514	srv-51	0 %	1,50 GB
SRV-53	Running	Running	Not Detected	srv-51	0 %	768,00 MB
SRV-55	Running	Running	Not Detected	srv-49	0 %	512,00 MB

Obr. 15. Servery, které nebylo možné přesunout z klastru CLS-APP2009.

Scénář implementace softwaru Veeam Backup & Replication byl konzultován přímo s výrobcem softwaru. Z důvodu chybějícího fyzického serveru, který by hostoval služby zálohovacího systému, bylo zvoleno řešení v rámci virtuálního prostředí. Na funkčnost zálohování neměl tento scénář žádný vliv. Pouze bylo dosaženo menší optimalizace výkonu Hyper-V serverů, protože musí zajistit i režijní činnosti během procesu zálohování. V době až bude k dispozici dedikovaný fyzický server, bude provedena úprava scénáře a nahrazení virtuálního serveru BCK-12 serverem fyzickým. Produkční ICT služby / aplikace mají datové úložiště v primárním datovém centru. Diskové pole pro zálohování bylo umístěno do záložního datového centra, které je umístěno v jiné části nemocnice. V případě živelné události je riziko současného poškození obou datových center relativně nízké. Pro splnění pravidla 3-2-1 byly diskutovány tři možnosti řešení:

- připojení páskové jednotky a vynášení týdenních záloh do trezoru organizace,
- replikace záloh na NAS zařízení umístěné v areálu nemocnice,
- replikace záloh do cloudového úložiště.

Nemocnice připravuje upgrade zálohovacího řešení fyzických serverů. Je tedy možné, že dojde k zakoupení páskové jednotky s více nezávislými mechanikami, kdy jedna bude vyhrazena pro offline zálohování virtuální infrastruktury [10].



Obr. 16. Logické znázornění implementace zálohovacího systému.

6.1.1 Konfigurace klastru CLS-APP2016

Oba nody disponují následující konfigurací:

- 2x Intel Xeon E5-2660v3 @ 2.6 GHz,
- 256 GB operační paměti,
- operační systém Windows Server 2012 R2 edice datacenter.

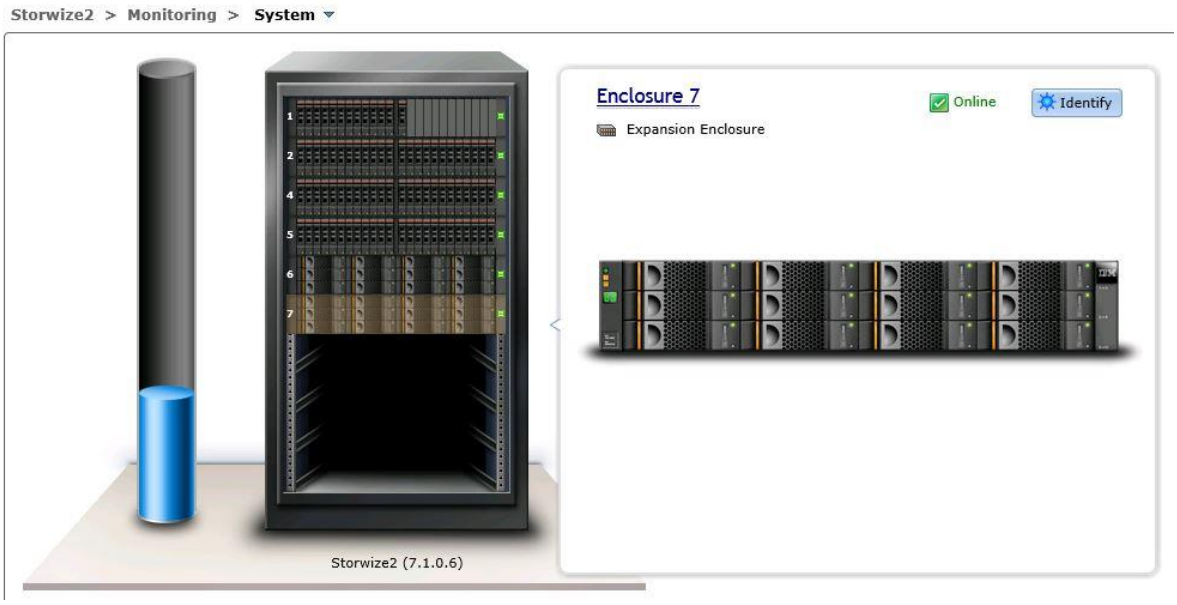
VMs (28)

Name	Status	Virtual Machine...	VM Additions	Host	CPU Average	Startup Memory
SRV-34	Running	Running	6.3.9600.16384	APP02	0 %	12,00 GB
SRV-129	Running	Running	6.3.9600.16384	APP02	0 %	6,00 GB
SRV-95	Running	Running	6.3.9600.16384	APP02	0 %	4,00 GB
SRV-38n	Running	Running	6.3.9600.16384	APP02	0 %	2,00 GB
SRV-87	Running	Running	6.3.9600.16384	APP02	0 %	4,00 GB
SRV-02	Running	Running	6.3.9600.16384	APP02	0 %	2,00 GB
SRV-99	Running	Running	6.3.9600.16384	APP02	0 %	2,00 GB
SRV-86a	Running	Running	6.3.9600.16384	APP02	0 %	4,00 GB
SRV-78	Running	Running	6.3.9600.16384	APP02	0 %	2,00 GB
SRV-45	Running	Running	6.3.9600.16384	APP02	0 %	2,00 GB
SRV-77	Running	Running	6.3.9600.16384	APP02	0 %	1,50 GB
SRV-59n	Running	Running	6.3.9600.16384	APP02	0 %	1,50 GB
SRV-97	Running	Running	6.3.9600.16384	APP02	0 %	1,25 GB
SRV-01	Running	Running	6.3.9600.16384	APP02	0 %	1,25 GB
SRV-128	Running	Running	6.3.9600.16384	APP02	0 %	1,00 GB
SRV-76	Running	Running	6.3.9600.16384	APP02	0 %	1,00 GB
SRV-86	Running	Running	6.3.9600.16384	APP02	0 %	1,00 GB
SRV-127	Running	Running	6.3.9600.16384	APP02	0 %	1,00 GB
SRV-88	Running	Running	6.3.9600.16384	APP02	16 %	2,00 GB
SRV-98	Running	Running	6.3.9600.16384	APP02	0 %	1,00 GB
SRV-07	Running	Running	6.3.9600.16384	APP02	0 %	768,00 MB
SRV-89	Running	Running	6.3.9600.16384	APP02	0 %	1,00 GB
SRV-44	Running	Running	6.3.9600.16384	APP02	0 %	512,00 MB
SRV-84	Running	Running	6.3.9600.16384	APP02	0 %	1,00 GB
SRV-85	Running	Running	6.3.9600.16384	APP02	0 %	6,00 GB
SRV-54	Running	Running	6.3.9600.16384	APP02	0 %	1,00 GB
SRV-75	Running	Running	6.3.9600.16384	APP02	0 %	2,00 GB
SRV-48	Running	Running	6.3.9600.16384	APP02	0 %	2,00 GB

Obr. 17. Průběh migrace do nového klastru CLS-APP2016.

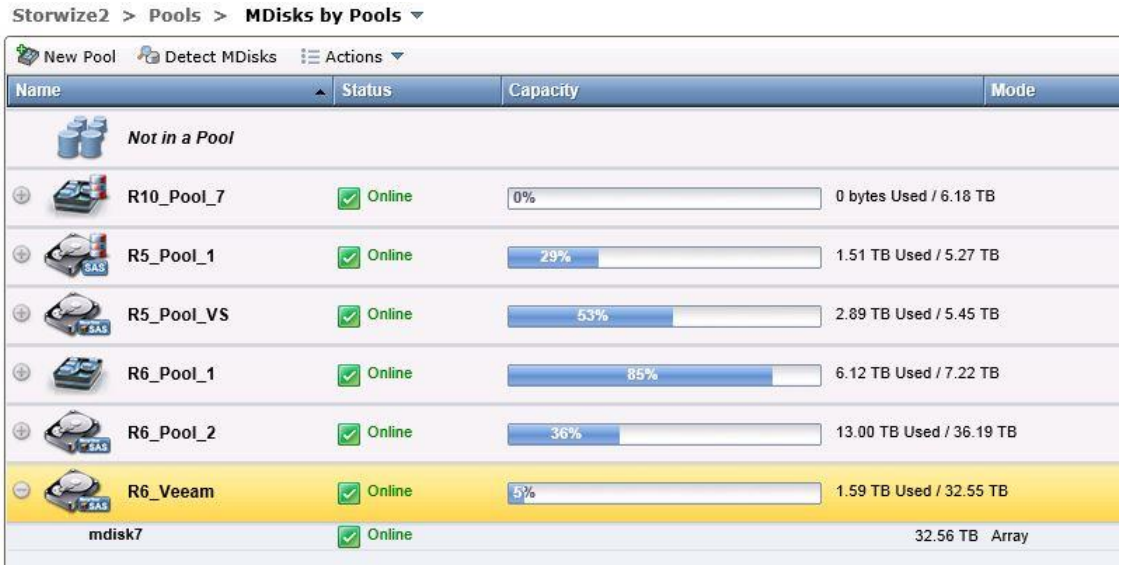
6.1.2 Příprava diskového úložiště

Diskové pole IBM Storwize V7000 v záložní lokalitě bylo rozšířeno o jednu diskovou expanzi. Expanze byla osazena dvanácti pevnými disky typu IBM 4 TB 6GB 3.5 Inch 7.2K SAS HDD. V rámci diskové police bylo vytvořeno RAID 6 pole složené z jedenácti disků. Dvanáctý disk byl označen jako tzv. hot spare disk, který je do RAID pole začleněn v případě selhání některého z disků v rámci diskového pole.

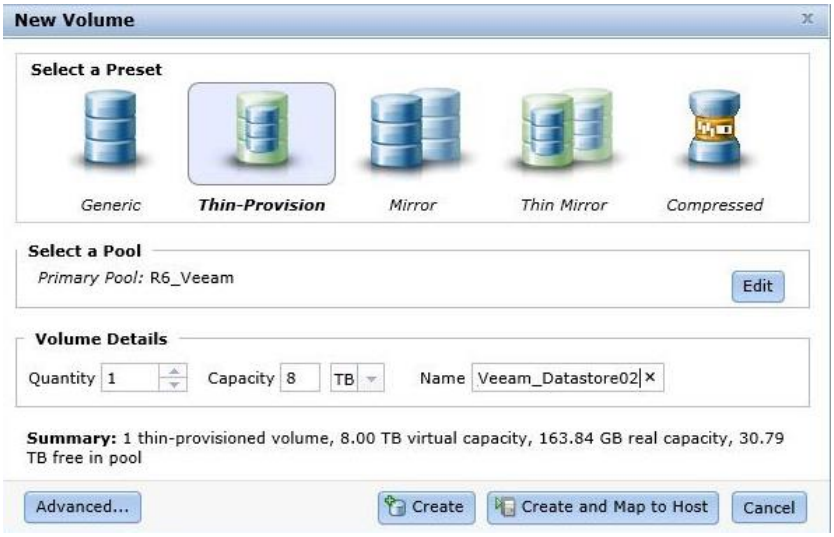


Obr. 18. Diskové pole v záložní lokalitě a detail expanze pro potřeby zálohování.

Po odečtení kapacitní režie RAID 6 pole zbývá pro potřeby zálohování kapacita 32 TB. Na obrázku číslo 19 jde vidět Mdisk R6_Veeam. V rámci této datové oblasti byly vytvořeny dvě logické diskové jednotky pojmenované Veeam_Datastore01 a Veeam_Datastore02. Obě logické diskové jednotky mají kapacitu 8 TB a byly vytvořeny v režimu Thin-provision. Režim Thin-Provision zaručí, že pro operační systém se disková jednotka prezentuje plnou velikostí 8 TB, ale ve skutečnosti na diskovém poli zabírá pouze reálně spotřebovanou velikost. Na obrázku 19 jde vidět, že v době pořízení otisku konfigurace to bylo 1,59 TB. Logické diskové jednotky byly připojeny pomocí SAN k Hyper-V serverům SRV-121 a SRV-122 tvořící klastr CLS-APP2014. V rámci Hyper-V byly disky připojeny k serveru BCK-12.



Obr. 19. MDisk R6_Veeam.



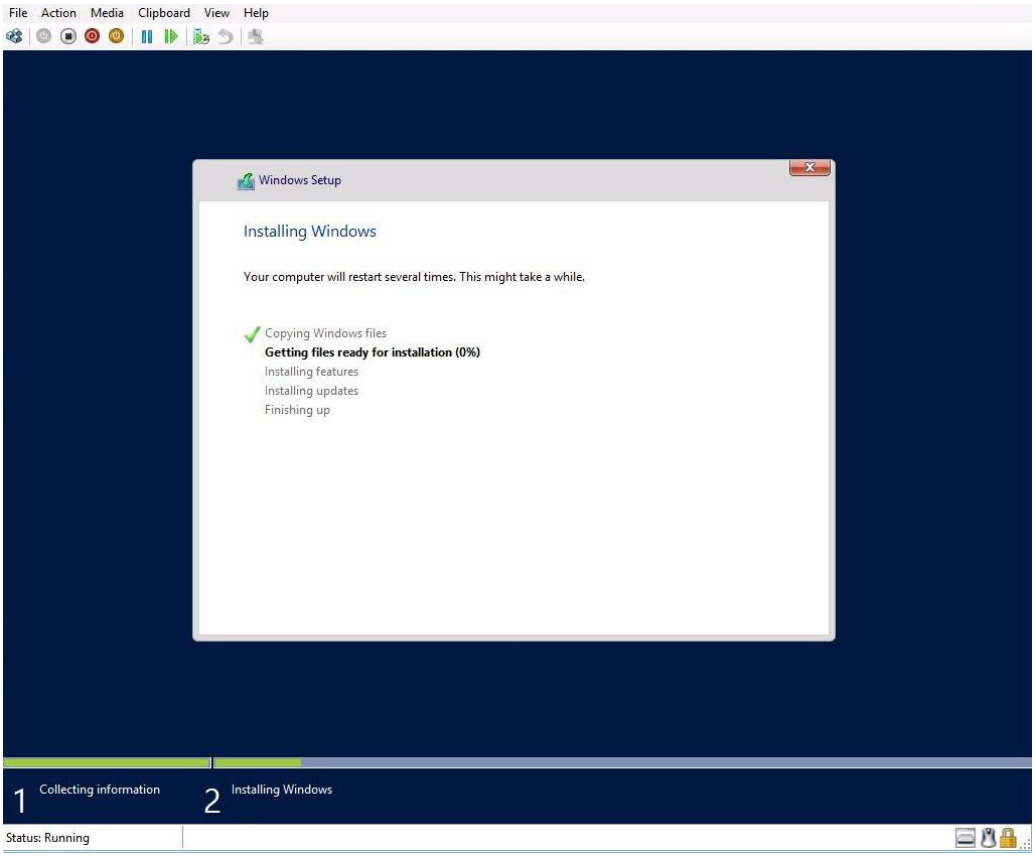
Obr. 20. Vytvoření logické jednotky

Obr. 21. Připojení k Hyper-V hostům.

6.1.3 Příprava virtuálního serveru BCK-12

V rámci klastru CLS-APP2014 byl vytvořen nový virtuální server BCK-12 v následující konfiguraci:

- 2x virtuální procesor,
- 8 GB operační paměti,
- 1x 100 GB pevný disk pro operační systém,
- 2x 8 TB pevný disk pro potřeby ukládání záloh,
- operační systém Windows Server 2012 R2 edice datacenter.



Obr. 22. Průběh instalace operačního systému Windows Server 2012 R2.

Po dokončení instalace serveru bylo provedeno nastavení síťového adaptéru a zařazení počítače do domény fnol.loc. Po restartování serveru bylo provedeno dokončení inicializace a formátování datových oblastí. Proběhla instalace chybějících aktualizací operačního systému.

6.2 Příprava před zahájením instalace zálohovacího serveru

Před zahájením instalace bylo nutné zkontrolovat infrastrukturu FNOL a ověřit, že splňuje veškeré požadavky pro úspěšnou implementaci zálohovacího softwaru.

Minimální HW požadavky zálohovacího serveru:

- 1x procesor x86-64,
- operační paměť 4 GB RAM (Random Access Memmory) + 500 MB (Mega Byte) pro každou souběžně běžící zálohovací úlohu,
- systémový disk - 20 GB volného prostoru pro instalaci aplikace,
- konektivita do sítě LAN – 1 Gbps (Gigabit per second).

Minimální požadavky na operační systém:

- Microsoft Windows Server 2012 R2,
- Microsoft Windows Server 2012,
- Microsoft Windows Server 2008 R2 SP1,
- Microsoft Windows Server 2008 SP2,
- Microsoft Windows 10,
- Microsoft Windows 8.x,
- Microsoft Windows 7 SP1,

Všechny podporované edice operačního systému musí být pouze v 64 bitové verzi.

Minimální požadavky na potřebný software:

- Microsoft .NET Framework 4.5.2,
- Microsoft Windows Installer 4.5,
- Microsoft SQL Server Management Objects,
- Microsoft SQL Server System CLR Types,
- Microsoft Visual C++ 2010 Service Pack 1 redistributable package.

Pokud není požadovaný software na serveru instalován, provede se jeho instalace v rámci spuštění instalátoru aplikace.

Minimální požadavky pro SQL databázi:

- Microsoft SQL Server 2014,
- Microsoft SQL Server 2012,
- Microsoft SQL Server 2008 R2,

- Microsoft SQL Server 2008,
- Microsoft SQL Server 2005.

Je podporováno lokální i vzdálené připojení k SQL instanci. Během instalace je možnost instalovat Microsoft SQL Server 2012 v edici express.

Veškeré požadavky na hardware a software v prostředí FNOL byly splněny [10].

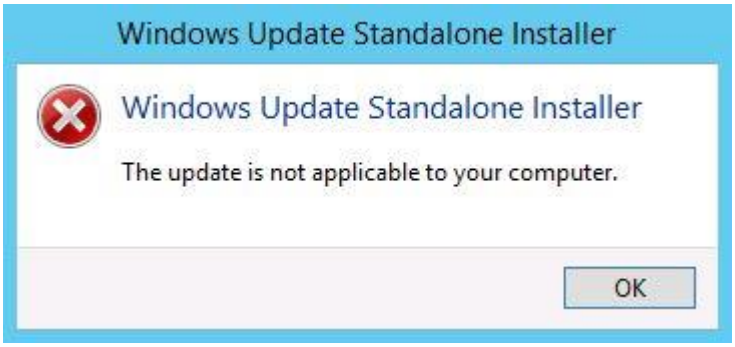
6.2.1 Příprava Hyper-V hostů pro zařazení do zálohování

Společnost Veeam doporučuje na jednotlivé Hyper-V hosty instalovat hotfix balíčky pro zajištění spolehlivosti procesu zálohování [14]. Tyto hotfix aktualizace nejsou společností Microsoft automatizovaně šířeny pomocí služby windows update. Bylo tedy nutné jednotlivé hotfix stáhnout z webových stránek společnosti Microsoft a provést ruční instalaci.

Tab. 5. Soupis doporučených hotfix balíčků – upraveno autorem [14].

Název Hotfix balíčku	**Staženo**	**APP01**	**APP02**	**SRV-121**	**SRV-122**
KB3090343	x	x	x	x	x
KB3072380	x	x	x	x	x
KB3068445	x	x	x	x	x
KB3068444	x	x	x	x	x
KB2919355	x	x	x	x	x

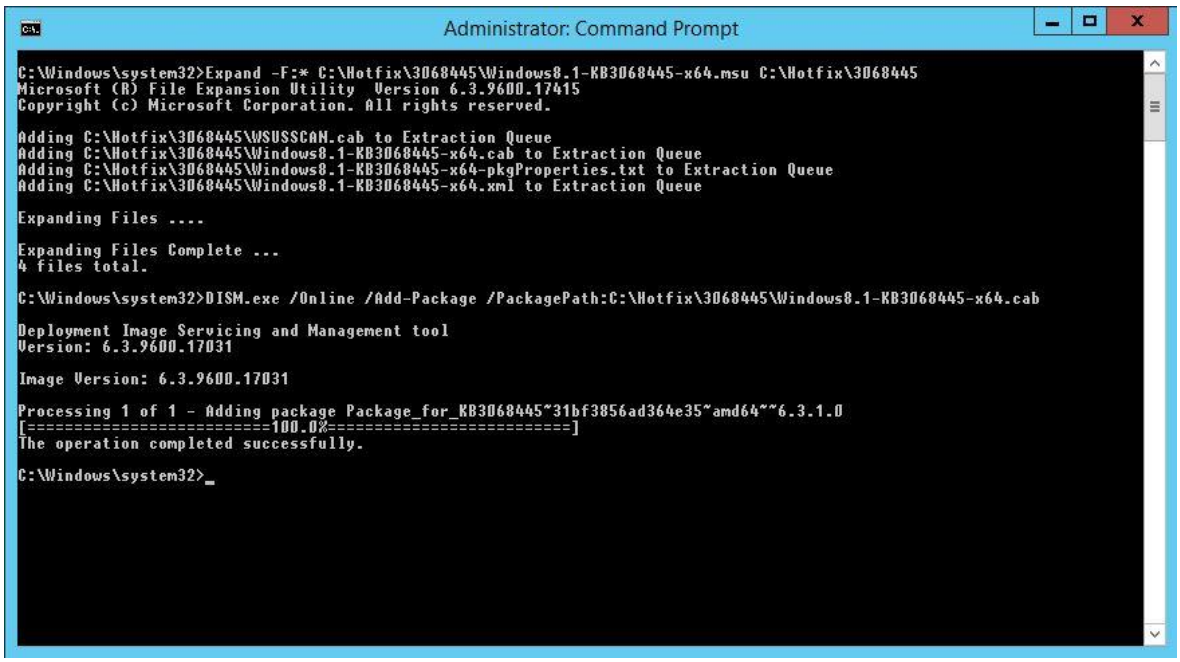
Během instalace jednotlivých balíčků bylo nutné provést několik restartů Hyper-V serverů. Díky funkci přesunu virtuálních serverů za provozu byly veškeré virtuální počítače v klastru přesunuty na jeden nod. Druhý nod byl přepnut do stavu údržby. Poté došlo k provedení instalace jednotlivých hotfix balíčků. Tento proces byl opakován na všechny nody klastrů s operačním systémem Windows Server 2012 R2. Během instalace se na některých serverech objevil problém s instalací některých balíčků. Operační systém po spuštění instalace balíčku informoval, že daný balíček není určen pro tento počítač a ukončil instalaci.



Obr. 23. Chyba v průběhu instalace hotfix balíčku.

Při řešení problému bylo zjištěno, že by balíček měl jít na operační systém nainstalovat. Byla vytvořena nová testovací čistá instalace operačního systému Windows Server 2012 R2, kde instalace hotfix balíčku proběhla v pořádku.

Bylo tedy vyzkoušeno hotfix balíček rozbalit a provést instalaci pomocí aplikace DISM (Deployment Imaging Servicing Management), která je určena k instalaci balíčků při implementaci operačních systémů. Instalace pomocí DISM aplikace již proběhla v pořádku.



Obr. 24. Postup instalace hotfix balíčku pomoci aplikace DISM.

6.2.2 Příprava systémových účtů

Pro úspěšnou instalaci softwaru bylo nutné připravit systémové účty, které zálohovací program využívá pro svoji činnost.

Tab. 6. Přehled systémových účtů pro potřeby zálohování Veeam Backup & Replication – upraveno autorem [12].

Název účtu	**Funkce účtu**	**Oprávnění účtu**
VeeamBackupService	Instalace softwaru zálohování. Běh systémových služeb aplikace Veeam. Přístup do SQL databází VeeamBackup a VeeamBackupReporting.	Lokální administrátor – BCK-12. Oprávnění pro databáze db_datareader, db_datawriter.
VeeamBackupHyper-V	Přístup k virtuálním počítačům.	Lokální administrátor – Hyper-V server.
VeeamEmailNotification	Odesílání notifikačních e-mailových zpráv.	Odeslat e-mail.
VeeamBackupGuestFile	Přístup do virtuálního počítače z důvodu možnosti obnovy po jednotlivých položkách.	Lokální administrátor na virtuálních serverech.

Názvy účtů v tabulce neodpovídají skutečným názvům použitých v infrastruktuře FNOL. Pro přiřazení účtu VeeamBackupHyper-V do skupiny lokálních administrátorů bylo využito systémových politik a cílení pomocí WMI (Windows Management Instrumentation) filtru, který zajistil vyfiltrování aplikování politiky pouze na servery hostující Hyper-V roli.

Z pohledu bezpečnosti informačního systému je rizikové použití účtu VeemBackupGuestFile, protože má být členem lokálních administrátorů ve všech virtuálních počítačích, kde chceme zajistit možnost obnovy po jednotlivých položkách. Někoho by mohlo napadnout vložit tento účet do skupiny doménových administrátorů, ale to je velmi riskantní, pokud na některém ze zálohovaných serverů má z důvodu správy práva lokálních administrátorů dodavatel ICT aplikace. Lokální administrátor má možnost přístupu do obsahu operační paměti. Během provádění zálohy může získat identitu účtu, včetně hesla, nebo jeho hash. Mohlo by poté dojít ke kompromitaci celé doménové struktury.

Z tohoto důvodů bylo použití účtu VeeamBackupGuestFile omezeno pouze na servery, které jsou výhradně ve správě informatiky FNOL.

6.2.3 Příprava SQL databází

FNOL disponuje vysoce dostupným SQL klastrovým řešením. V rámci tohoto klastru byly vytvořeny dvě databáze VeeamBackup a VeeamBackupReporting. K těmto databázím byly pro účet VeeamBackupService přiřazeny role db_datareader a db_datawriter [12].

6.2.4 Příprava notifikačních e-mailových zpráv

V prostředí Microsoft Exchange Serveru byla zřízena poštovní schránka VeeamEmailNotification s e-mailovou adresou sloužící pro odesílání notifikačních reportů. Pro příjemce notifikací byla vytvořena distribuční skupina s e-mailovou adresou. Do skupiny byly zařazeny osoby spadající do seznamu správců zálohování v prostředí nemocnice [12].

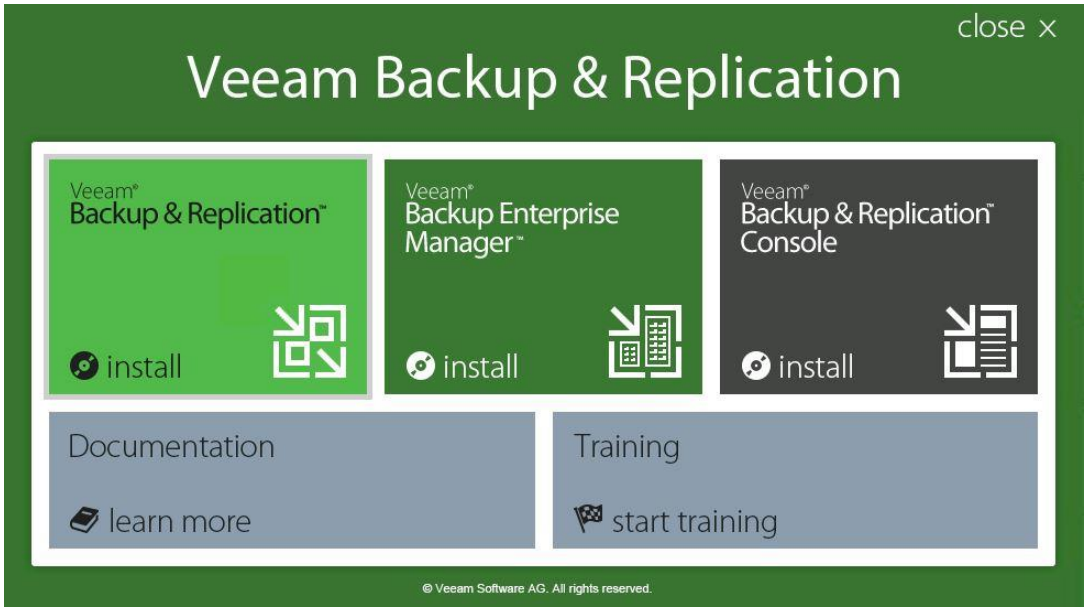
7 POSTUP INSTALACECE ZÁLOHACÍHO SYSTÉMU VEEAM BACKUP & REPLICATION

7.1 Příprava instalačních médií

Instalační média, včetně licenčních klíčů, byla stažena z webového portálu společnosti Veeam. Instalační médium je distribuováno pomocí obrazu DVD disku ve verzi 9.0.0.902. Pro verzi 9 již byla uvolněna první aktualizace označená update 1 s přesným označením 9.0.0.1491, která byla také ve formě obrazu DVD disku stažena [12].

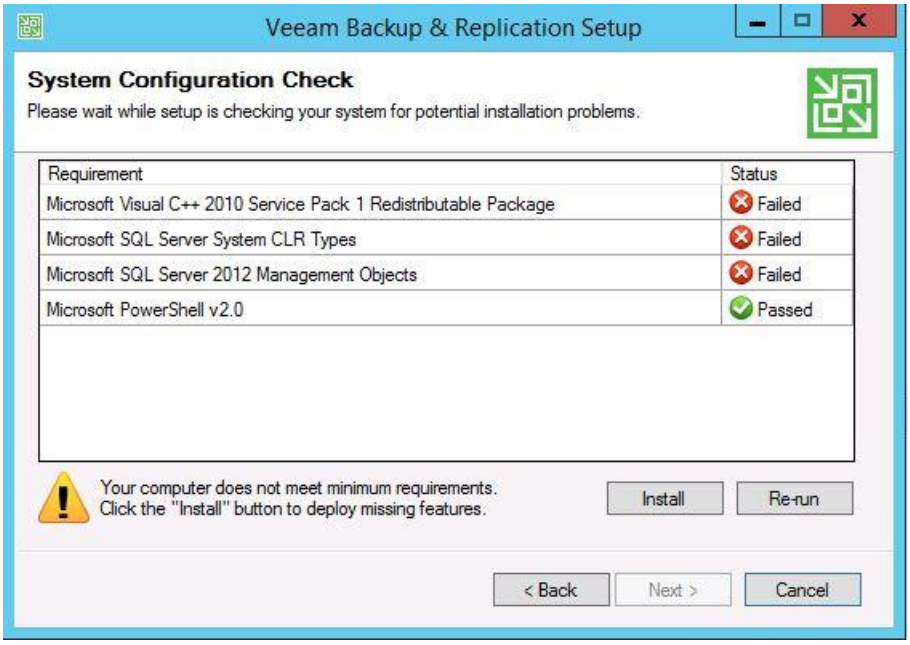
7.2 Instalace

Instalační médium bylo připojeno do operačního systému a byl spuštěn pomocí aplikace Setup.exe průvodce instalací Veeam Backup & Replication.



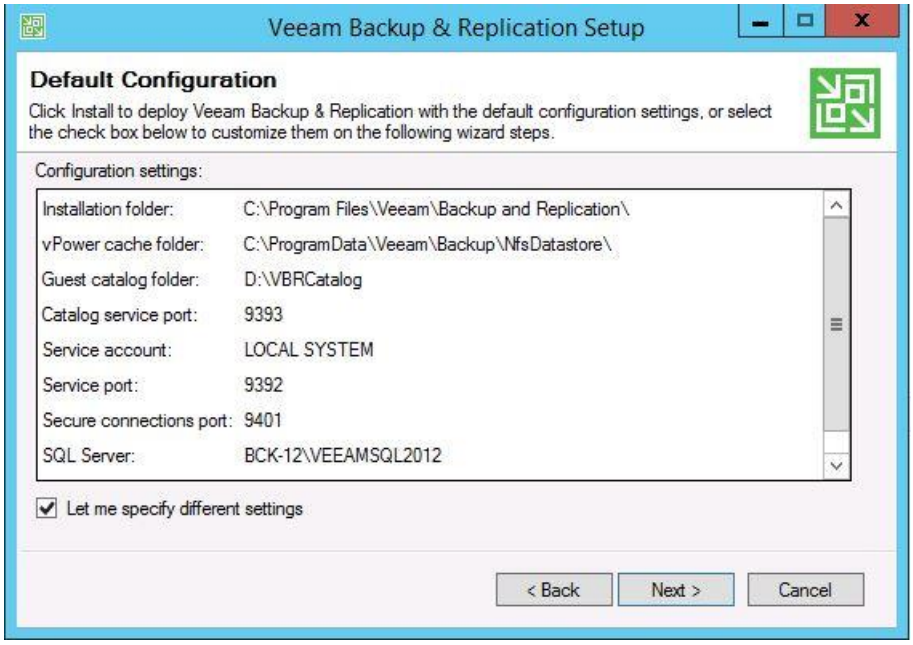
Obr. 25. Průvodce instalace Veeam Backup & Replication.

Po potvrzení licenční smlouvy byl do instalačního průvodce vložen licenční klíč. V dalším kroku byly vybrány komponenty, které se budou na serveru používat. Mimo samotný zálohovací software byla provedena instalace konzole pro správu zálohovacího prostředí. Další konzole byla instalována na terminálový server a počítače IT správců. Součástí průvodce je kontrola přítomných softwarových komponent. V případě, kdy některá z komponent není na serveru instalována, umožní průvodce pomocí tlačítka Install provést instalaci.



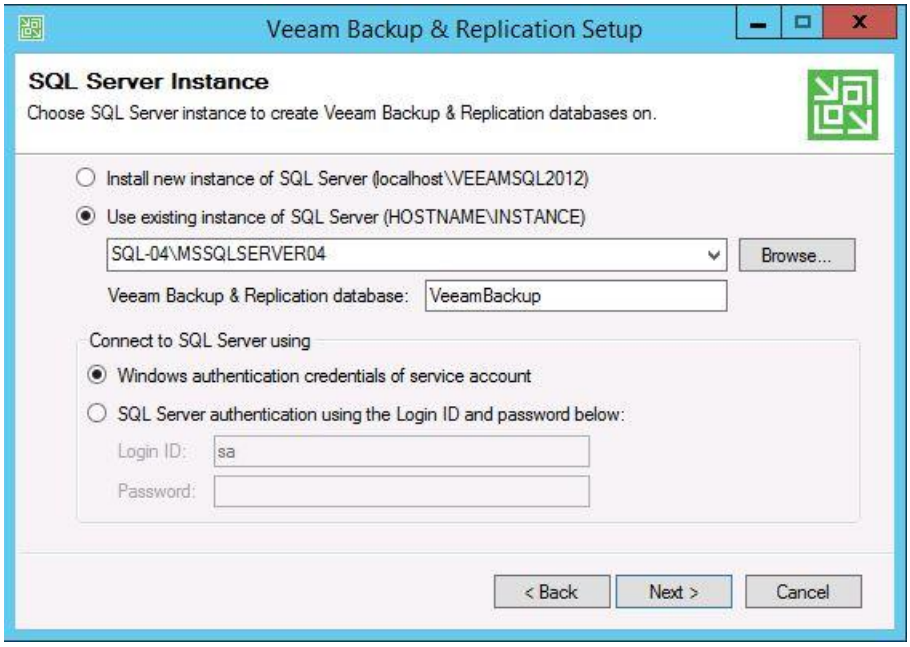
Obr. 26. Kontrola potřebných softwarových komponent.

Po dokončení kontroly softwarových komponent byla průvodcem nabídnuta běžná konfigurace instalace, která není pro prostřední nemocnice vhodná. Byla tedy zvolena volba vlastního nastavení instalace.



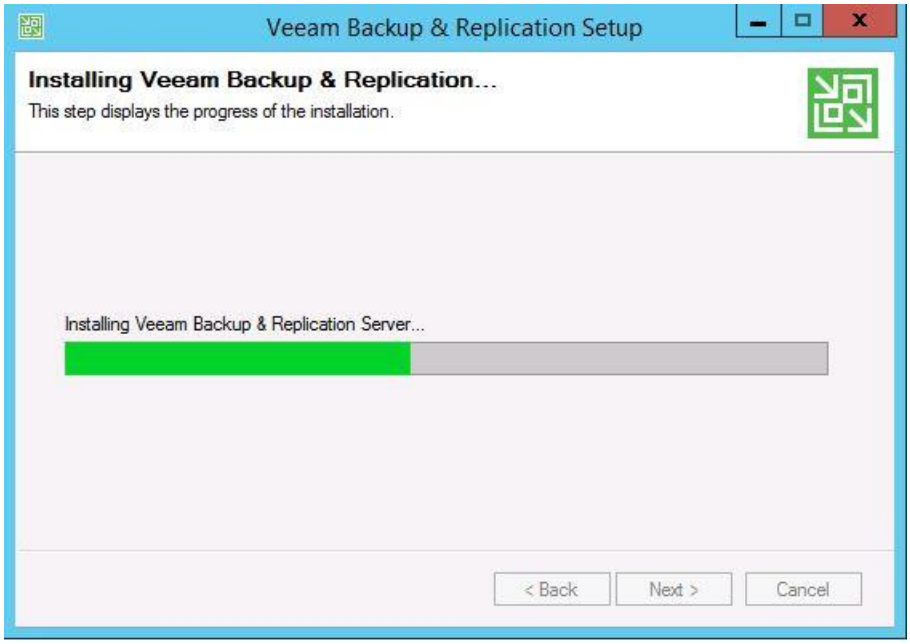
Obr. 27. Preferovaná nabídka defaultní konfigurace.

Po zvolení vlastního nastavení bylo umožněno vložit uživatelské jméno pro servisní účet a jeho heslo. V našem případě to byl VeeamBackupService. V dalším kroku bylo zvoleno umístění SQL databází.



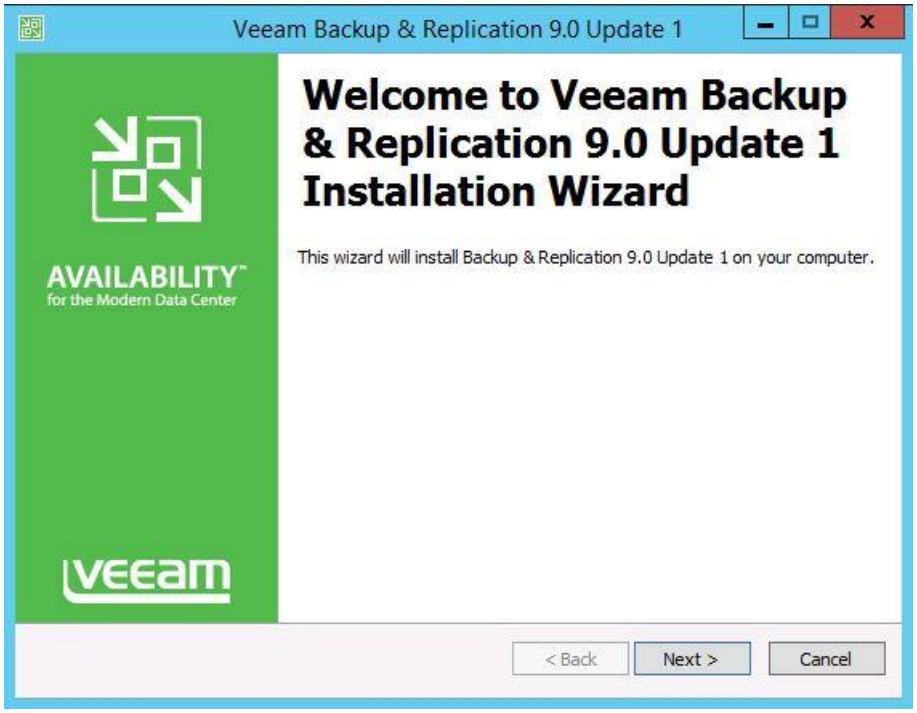
Obr. 28. Volba umístění databáze.

Poté již byla provedena samotná instalace aplikace.



Obr. 29. Průběh instalace Veeam Backup & Replication.

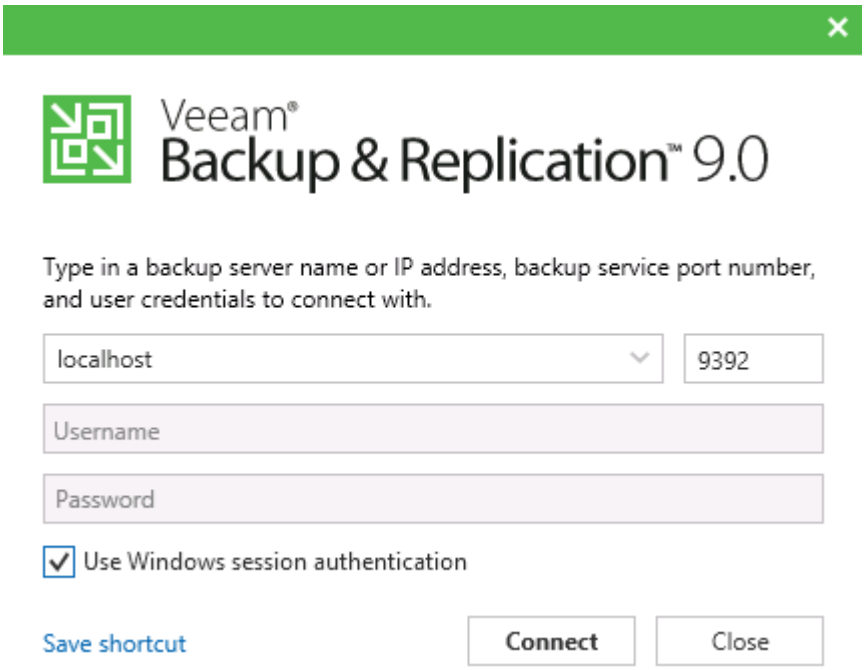
Po ukončení průvodce byla provedena instalace aktualizace update 1. Během instalace aktualizace nebylo nutné do průvodce zadávat žádné informace [12].



Obr. 30. Instalace update 1.

7.3 Konfigurace

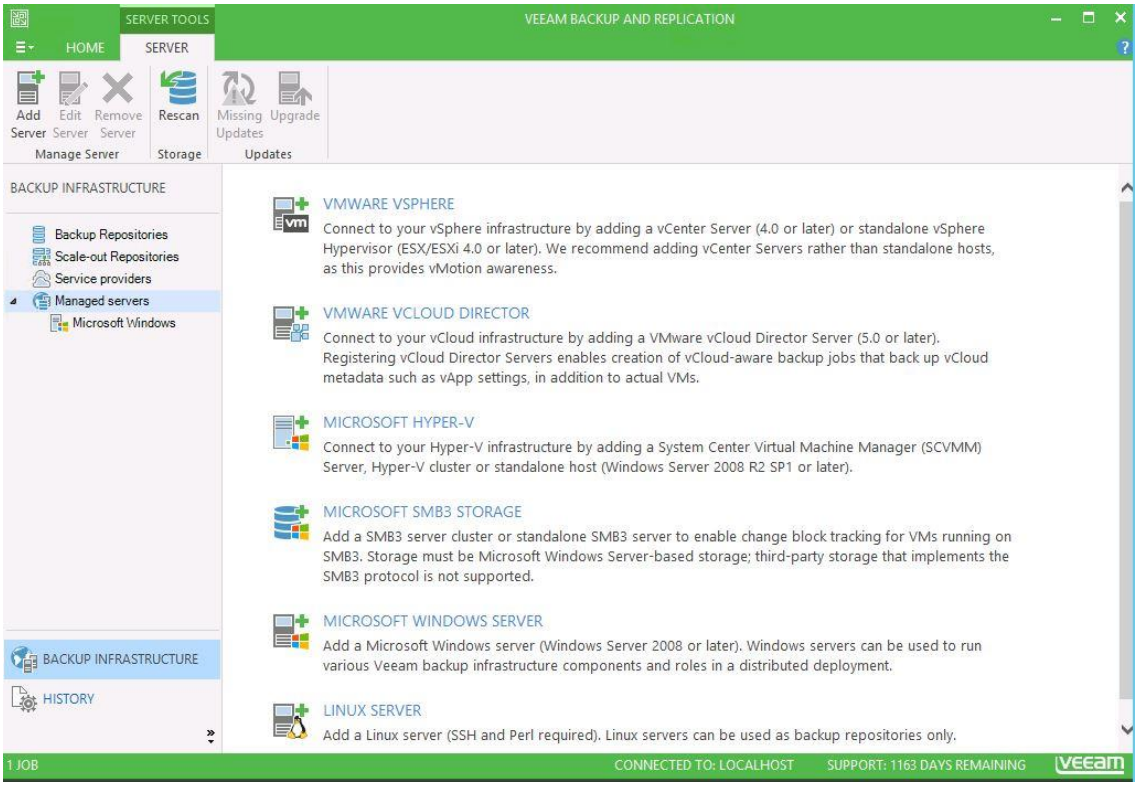
Po dokončení instalace bylo provedeno první spuštění aplikace pomocí konzole Veeam Backup & Replication. Aplikace pro ověření identity uživatele využila Windows autentizaci.



Obr. 31. Autentizace do konzole Veeam Backup & Replication.

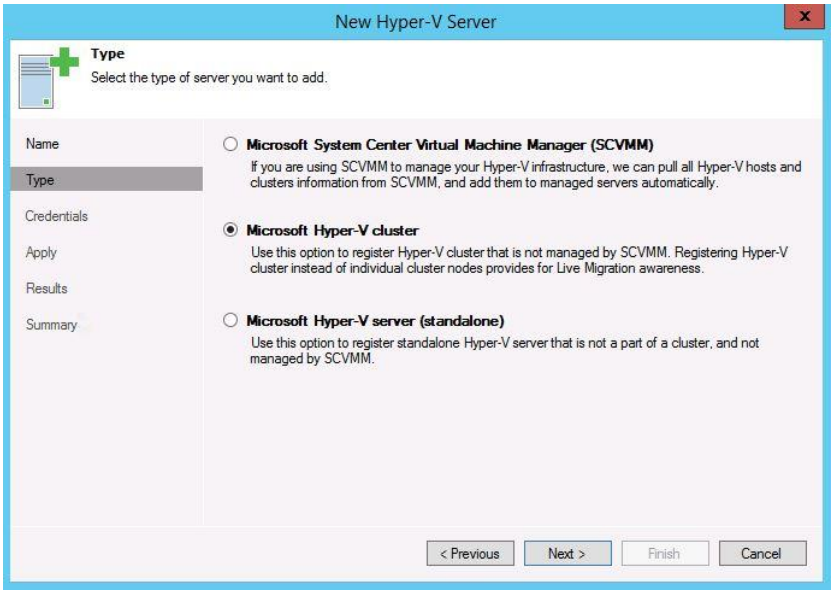
7.3.1 Přidání Hyper-V serverů

Po spuštění konzole bylo nutné do zálohovacího softwaru připojit jednotlivé Hyper-V servery.



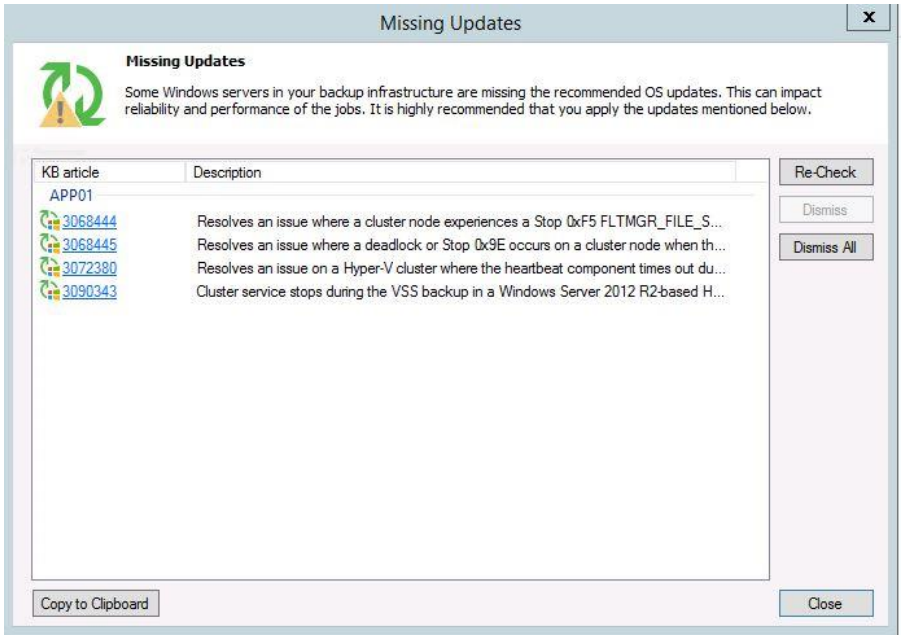
Obr. 32. Přidání Hyper-V serveru do systému zálohování.

Byla zvolena volba Microsoft Hyper-V, která spustila průvodce přidání nového Hyper-V serveru. Do průvodce bylo vloženo DNS název Hyper-V klastru CLS-APP2016. V dalším kroku bylo průvodci oznámeno, že se jedná o Hyper-V klastr.



Obr. 33. Výběr typu Hyper-V serveru.

Dále je nutné průvodci sdělit účet s oprávněním lokálního administrátora, pomocí kterého jsou zálohovány virtuální počítače. Byl zvolen připravený doménový účet VeeamBackupHyper-V. Průvodce poté provedl identifikaci klastru CLS-APP2016 a prozkoumal jednotlivé nody klastru APP01 a APP02. Průvodce na serverech provedl kontrolu potřebných instalovaných oprav typu hotfix. Pokud by některá oprava chyběla, provedl by informování operátora, ale bylo by možné dále pokračovat v instalaci. Opravy typu hotfix nejsou vynucené, ale doporučené.



Obr. 34. Ukázka informace o chybějících hotfix opravách.

Po dokončení průvodce byl klastr CLS-APP2016 přidán do systému zálohování. Proces přidání byl proveden pro zbývající Hyper-V klastry [10].

7.3.2 Vytvoření zálohovacího zařízení

Aby bylo možné začít virtuální infrastrukturu zálohovat, bylo nutné vytvořit zálohovací zařízení. V rámci zálohovacího systému Veeam je používán název Backup repository.

Byly vytvořeny dvě Backup repository sloužící pro ukládání záloh.

Tab. 7. Backup repository.

Název Backup repository	**Popis využití**
Daily Backup Repository	Slouží pro ukládání denních záloh Hyper-V klastrů.
Weekly and Monthly Backup Repository	Slouží pro ukládání týdenních a měsíčních záloh Hyper-V klastrů.

Během vytváření repository bylo nutné specifikovat diskový oddíl pro vytvoření repository. Dále bylo možné nastavit limit datové propustnosti během průběhu zálohování a omezení počtu současně probíhajících zálohovacích úloh. Každá z uvedených repository má startovací diskovou kapacitu 8 TB.

7.3.3 Nastavení e-mailové notifikace

Pro zajištění možnosti zasílání e-mailových notifikací po dokončení zálohy bylo provedeno nastavení e-mailového klienta. Byl nastaven SMTP (Simple Mail Transfer Protocol) server, kterým je v prostředí nemocnice Microsoft Exchange Server. V rámci nastavení bylo nutné definovat e-mailovou adresu příjemců notifikací. V případě FNOL to bylo zajištěno distribuční skupinou, která obsahuje e-mailové adresy správců zálohování.

7.4 Vytvoření zálohovací úlohy

Všechny potřebné přípravy byly provedeny a nyní je možné v zálohovacím systému nastavit co, jak, kdy se má zálohovat. Pro klastry CLS-APP2016 a CLS-APP2014 byly vytvořeny tři zálohovací úlohy. Pro klastry CLS-IDMZ a CLS-EDMZ pouze dvě zálohovací úlohy.

Tab. 8. Přehled zálohování Hyper-V klastrů.

Název klastru	**Denní záloha**	**Týdenní záloha**	**Měsíční záloha**
CLS-APP2014	x	x	x
CLS-APP2016	x	x	x
CLS-IDMZ	x	x	
CLS-EDMZ	x	x	

7.4.1 Denní zálohovací úlohy

Denní zálohy byly nastaveny, aby se prováděly pravidelně každý den. Ukládány jsou do backup repository Daily. Spuštění zálohovací úlohy bylo nastaveno dle tabulky číslo 9. Virtuální servery byly do zálohovací úlohy přidány na základě informací z nového zálohovacího plánu.

Tab. 9. Konfigurace spouštění denní zálohovací úlohy.

Název úlohy	**Repository**	**Den spuštění**	**Čas spuštění**	**Počet bodů obnovy**
CLS-APP2014-Daily	Daily	Každý den	0:00	7
CLS-APP20016-Daily	Daily	Každý den	20:00	7
CLS-IDMZ/EDMZ-Daily	Daily	Každý den	22:00	7

Denní zálohovací úloha využívá přírůstkový model zálohování. Každou sobotu je vytvořena syntetická plná záloha. U virtuálních serverů zařazených do úlohy je možné provést obnovení dat za poslední týden, vždy po kroku jednoho dne [10].

7.4.2 Týdenní zálohovací úlohy

Týdenní zálohy byly nastaveny, aby se prováděly pravidelně každou sobotu. Ukládány jsou do backup repository Weekly and Monthly. Spuštění zálohovací úlohy bylo nastaveno dle tabulky číslo 10. Virtuální servery byly do zálohovací úlohy přidány na základě informací z nového zálohovacího plánu.

Tab. 10. Konfigurace spouštění týdenní zálohovací úlohy.

Název úlohy	**Repository**	**Den spuštění**	**Čas spuštění**	**Počet bodů obnovy**
CLS-APP2014-Weekly	Weekly and Monthly	Sobota	3:00	4
CLS-APP20016-Weekly	Weekly and Monthly	Sobota	1:00	4
CLS-IDMZ/EDMZ-Weekly	Weekly and Monthly	Sobota	22:00	4

Týdenní zálohovací úloha využívá přírůstkový model zálohování. U virtuálních serverů zařazených do úlohy je možné provést obnovení dat za poslední čtyři týdny, vždy po kroku jednoho týdne.

7.4.3 Měsíční zálohovací úlohy

Měsíční zálohy byly nastaveny, aby se prováděly pravidelně každou první a poslední neděli v měsíci. Ukládány jsou do backup repository Weekly and Monthly. Spuštění zálohovací úlohy bylo nastaveno dle tabulky číslo 11. Virtuální servery byly do zálohovací úlohy přidány na základě informací z nového zálohovacího plánu.

Měsíční zálohovací úloha využívá přírůstkový model zálohování. U virtuálních serverů zařazených do úlohy je možné provést obnovení dat za posledních šest měsíců, vždy po kroku jednoho měsíce.

Tab. 11. Konfigurace spouštění měsíční zálohovací úlohy.

Název úlohy	Repository	Den spuštění	Čas spuštění	Počet bodů obnovy
CLS-APP2014-Monthly	Weekly and Monthly	První neděle v měsíci	23:00	6
CLS-APP20016-Monthly	Weekly and Monthly	Poslední neděle v měsíci	21:00	6

7.4.4 Další typy zálohovacích úloh

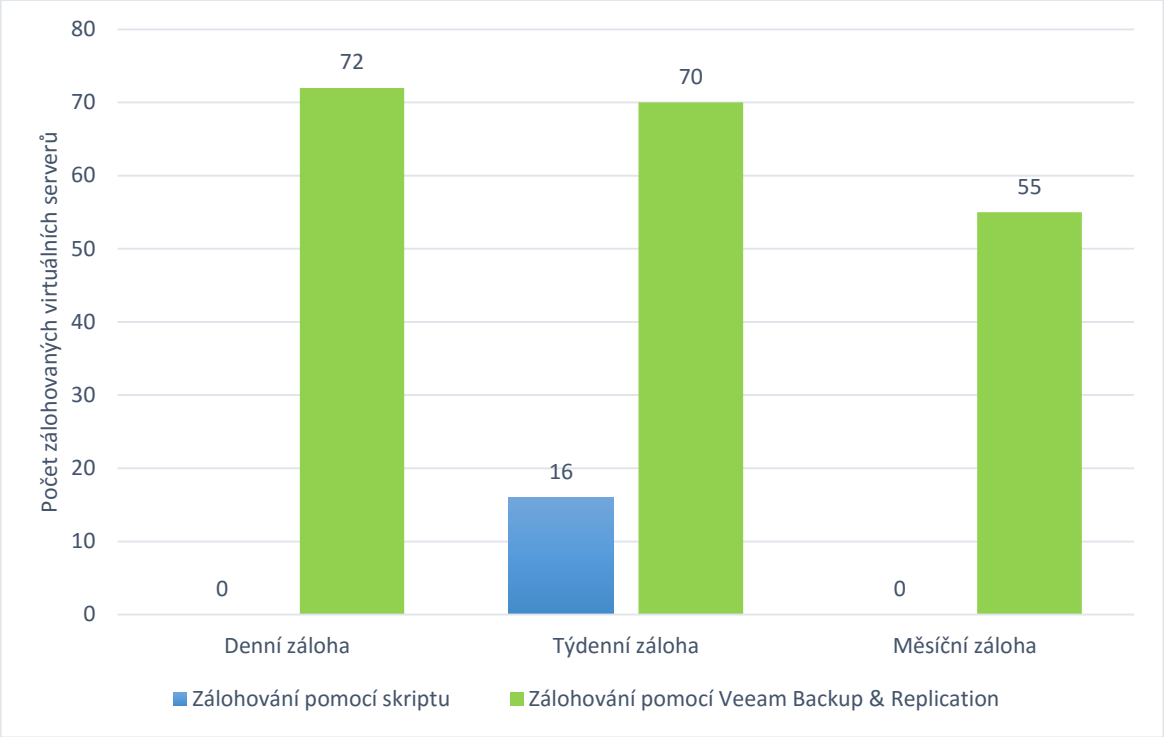
V rámci prostředí Veeam bylo vyzkoušeno provést mimořádnou úlohu typu Add-hoc, která byla nastavena v režimu automatického smazání po 24 hodinách. Možnost nastavení doby bylo možné individuálně změnit. Takový typ zálohy je vhodné provést před začátkem aktualizace ICT služby / aplikace.

Zálohovací software disponuje možnost kontinuálního zálohování. Ze strany garantů aplikací nebyly dodány detailnější požadavky na nastavení této funkčnosti [10].

7.5 Změna počtu zálohovaných ICT služeb / aplikací v závislosti na novém systému zálohování

Po nasazení nového systému zálohování byla vytvořena statistika porovnání starého systému zálohování a nového systému zálohování z pohledu počtu chráněných virtuálních serverů, které poskytují ICT služby / aplikace.

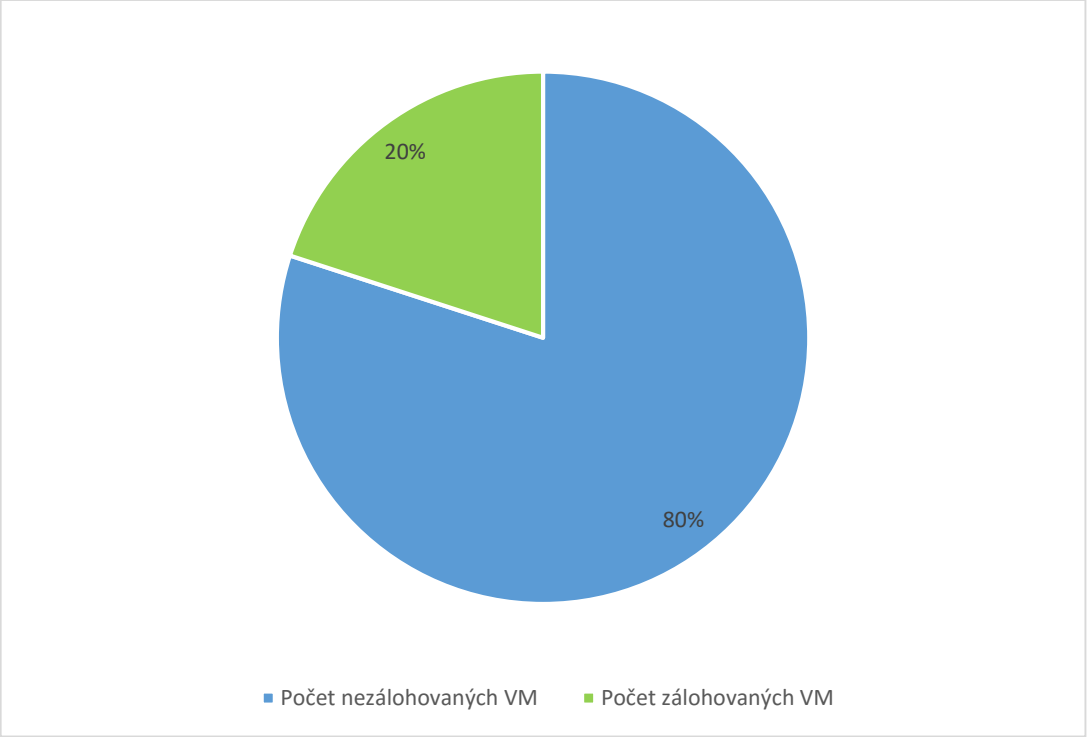
Graf. 2. Porovnání počtu virtuálních serverů ve vazbě na typ zálohovací úlohy.



Graf číslo 2 zobrazuje porovnání jednotlivých zálohovacích úloh a počtu zálohovaných virtuálních serverů. Implementací zálohovacího softwaru Veeam Backup & Replication došlo k významnému nárůstu počtu zálohovaných ICT aplikací / služeb. Původní režim zálohování nebyl schopný zajistit zálohování na pravidelné denní bázi.

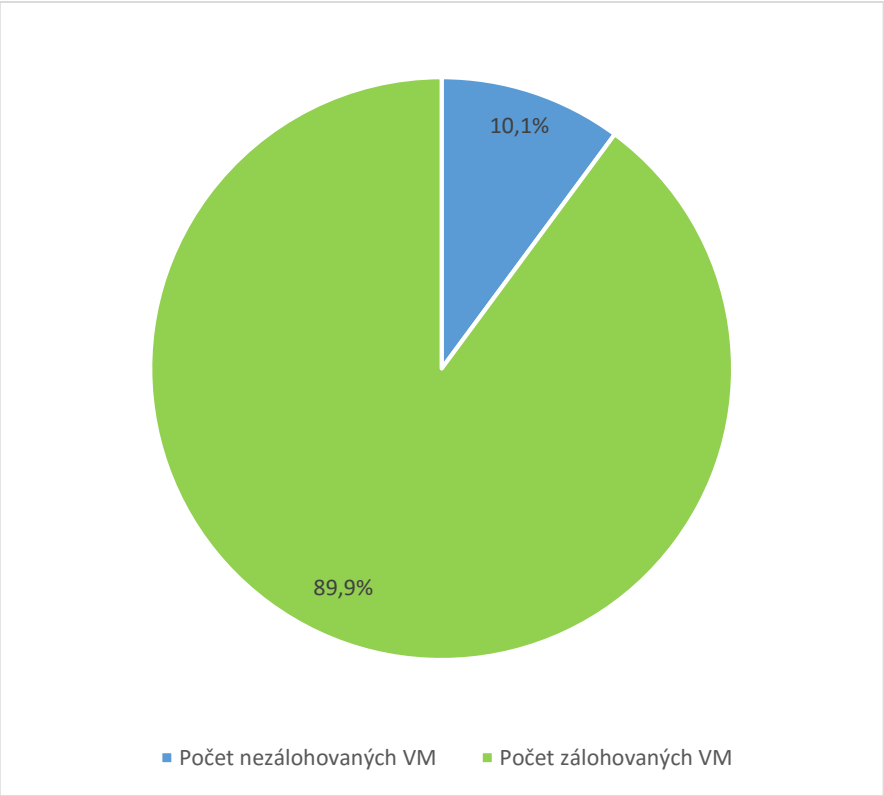
V grafu číslo 3 je pomocí výsečového grafu zobrazen poměr zálohovaných a nezálohovaných virtuálních serverů v období, kdy bylo využíváno zálohování pomocí automatizovaného skriptu. Je jasně viditelné, že u 80 % produkčních virtuálních serverů a na nich provozovaných ICT službách / aplikacích hrozilo velmi vysoké riziko dlouhé nedostupnosti po havárii.

Graf. 3. Procentuální vyjádření počtu zálohovaných VM při použití skriptu.



Po provedení implementace nástroje Veeam Backup & Replication se dle grafu číslo 4 poměr mezi zálohovanými a nezálohovanými systémy otočil. V době vzniku grafů nejsou ještě všechny virtuální servery zmigrovány do nového klastru. Celkové procento zálohovaných VM bude tedy ještě o pár jednotek procent vyšší. Do grafu jsou zahrnuty i virtuální servery, které běží v rámci Hyper-V klastru a jedná se např. o testovací servery. Z pohledu provozu informačního systému není cílem dosáhnout 100 % stavu zálohování provozovaných virtuálních počítačů.

Graf. 4. Procentuální vyjádření počtu zálohovaných VM při použití Veeam.



7.5.1 Zasílání reportů o stavu zálohování

Významným zlepšením je i pravidelné zasílání informačních reportů po dokončení zálohovací úlohy. Operátoři díky tomu mají k dispozici přehledné informace o stavu zálohovacího systému. Dokáží operativně řešit problémy v případě, kdy se vyskytnou. To je důležité, protože se často stává, že jsou operátoři o funkci systému zálohování přesvědčeni. Až v případě nutnosti obnovení ICT služby / aplikace je zjištěn skutečný stav, že potřebné zálohy se z nějakých důvodů neprovedly.

Backup job: CLS-APP2016-Weekly
Týdenní záloha - 4 restore point

7. května 2016 1:00:01

Success	29	**Start time**	1:00:01	**Total size**	2,9 TB	**Backup size**	76,4 GB
Warning	0	**End time**	1:25:43	**Data read**	341,6 GB	**Dedupe**	1,1x
Error	0	**Duration**	0:25:42	**Transferred**	76,3 GB	**Compression**	2,6x

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration
SRV-54	Success	1:01:18	1:04:16	120,0 GB	9,9 GB	3,3 GB	0:02:57
SRV-07	Success	1:01:18	1:05:34	120,0 GB	17,4 GB	2,2 GB	0:04:16
SRV-75	Success	1:05:55	1:06:51	45,0 GB	3,1 GB	422,5 MB	0:00:55
SRV-98	Success	1:06:21	1:07:46	65,0 GB	9,9 GB	2,3 GB	0:01:25
SRV-95	Success	1:08:52	1:09:53	127,0 GB	2,2 GB	180,6 MB	0:01:00
SRV-02	Success	1:10:03	1:12:04	15,0 GB	10,1 GB	1,6 GB	0:02:01
SRV-86	Success	1:14:05	1:16:32	50,0 GB	3,7 GB	446,9 MB	0:02:27
SRV-88	Success	1:05:40	1:06:56	170,0 GB	4,8 GB	513,3 MB	0:01:16
SRV-38n	Success	1:08:57	1:10:00	45,0 GB	4,8 GB	882,2 MB	0:01:02
SRV-65	Success	1:08:57	1:10:01	730,0 GB	2,2 GB	185,4 MB	0:01:03
SRV-127	Success	1:01:18	1:04:00	45,0 GB	8,4 GB	609,7 MB	0:02:41
SRV-78	Success	1:10:03	1:14:18	45,0 GB	17,4 GB	5,8 GB	0:04:14
SRV-34	Success	1:13:34	1:24:50	200,0 GB	42,3 GB	10,5 GB	0:11:15
SRV-01	Success	1:03:19	1:06:01	30,0 GB	10,3 GB	1,3 GB	0:02:42
SRV-86a	Success	1:07:06	1:09:00	45,0 GB	7,1 GB	1003,3 MB	0:01:54
SRV-89	Success	1:07:16	1:08:57	15,0 GB	7,9 GB	1,4 GB	0:01:40
SRV-94	Success	1:10:48	1:20:51	220,0 GB	82,1 GB	18,5 GB	0:10:02
SRV-77	Success	1:14:20	1:18:53	165,0 GB	11,0 GB	3,4 GB	0:04:33
SRV-76	Success	1:07:21	1:08:57	45,0 GB	4,3 GB	598,8 MB	0:01:35
SRV-44	Success	1:12:04	1:14:22	45,0 GB	4,4 GB	879,1 MB	0:02:18
SRV-97	Success	1:18:52	1:20:52	127,0 GB	4,1 GB	444,1 MB	0:01:59
SRV-87	Success	1:16:56	1:19:33	50,0 GB	3,4 GB	471,7 MB	0:02:37
SRV-45	Success	1:09:58	1:10:52	60,0 GB	2,3 GB	160,8 MB	0:00:54
SRV-99	Success	1:19:22	1:21:24	45,0 GB	9,2 GB	2,0 GB	0:02:01
SRV-48	Success	1:03:54	1:05:43	95,0 GB	10,2 GB	2,2 GB	0:01:48
SRV-84	Success	1:20:48	1:25:28	60,0 GB	33,8 GB	13,7 GB	0:04:40
SRV-128	Success	1:10:03	1:11:13	60,0 GB	3,1 GB	493,5 MB	0:01:09
SRV-59n	Success	1:07:51	1:09:14	45,0 GB	3,8 GB	661,1 MB	0:01:22
SRV-129	Success	1:05:45	1:07:36	50,0 GB	8,6 GB	435,0 MB	0:01:50

Obr. 35. Ukázka reportu po ukončení zálohovací úlohy.

8 OBNOVENÍ VIRTUALIZOVANÝCH ICT SLUŽEB

Výhodou virtualizace je možnost zajistit zálohování / obnovení ICT služby / aplikace pomocí obnovení celé instance operačního systému, ve kterém jsou ICT služby / aplikace provozovány.

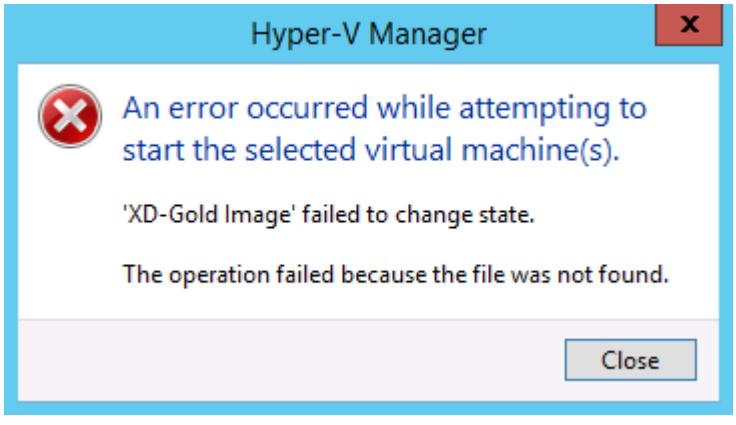
Zcela to neplatí pro služby, kde je nutné zajistit kompletní konzistenci zálohy. Většinou se jedná o služby typu:

- Microsoft Active Directory,
- Microsoft SQL Server,
- Microsoft Exchange Server,
- Microsoft SharePoint,
- ostatní systémy řízení báze dat.

8.1 Obnovení instance virtuálního serveru

Pro testování obnovení instance virtuálního serveru byl vybrán virtuální počítač XD-Gold Image, který slouží jako vzor pro vytvoření uživatelských virtuálních desktopů, které jsou ve FNOL používány v rámci počítačové učebny.

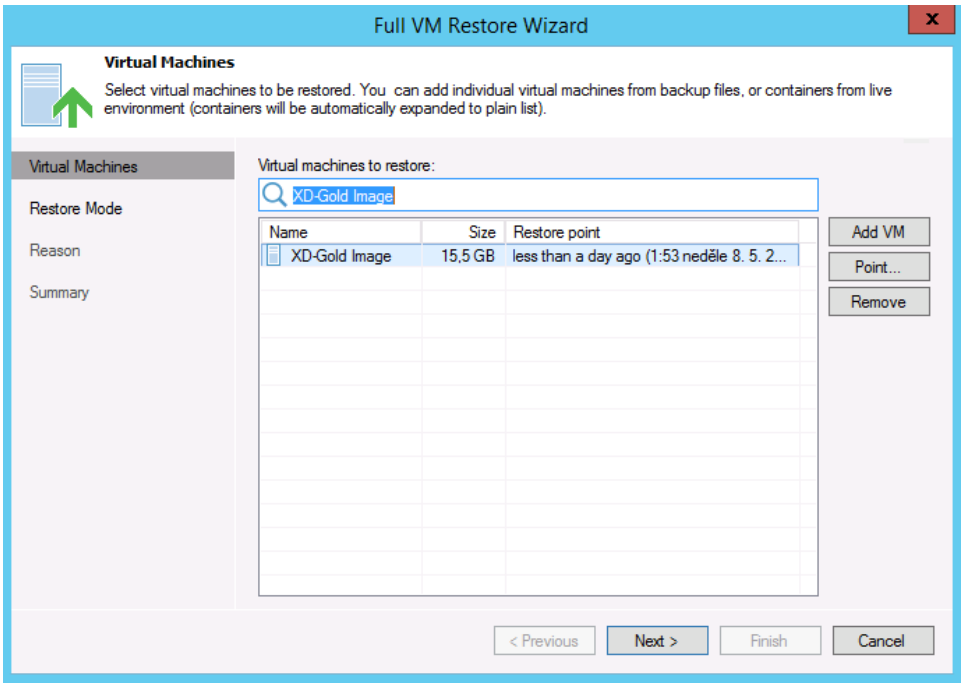
Server byl vypnut a poté došlo ke smazání souboru virtuálního disku. Poté bylo vyzkoušeno spuštění serveru, které bylo samozřejmě neúspěšné.



Obr. 36. Chyba po zapnutí VM po smazání disku.

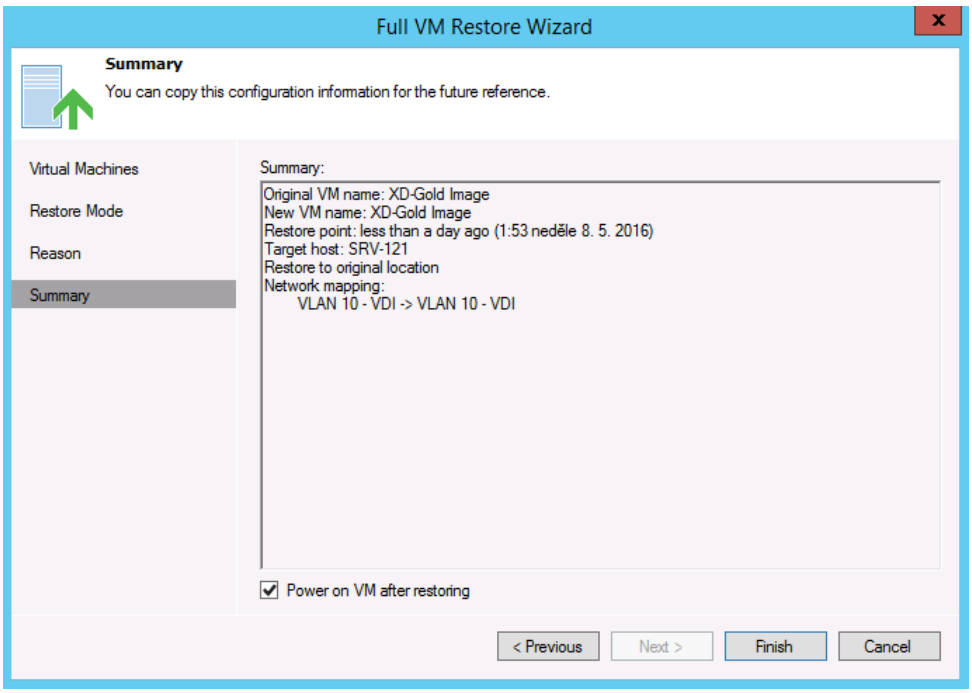
Bylo tedy nutné obnovit virtuální server. Během požadavku na provedení obnovy serveru se aplikace Veeam dotázala, zda požadujeme server spustit přímo ze zálohy souboru nebo obnovit do původního umístění. Možnost spustit server přímo ze zálohy je výhodné u služby,

kterou je nutné zprovoznit v co nejkratším čase. Finální přenesení do původního umístění by bylo provedeno v rámci časového úseku určeného pro údržbu ICT služby / aplikace.



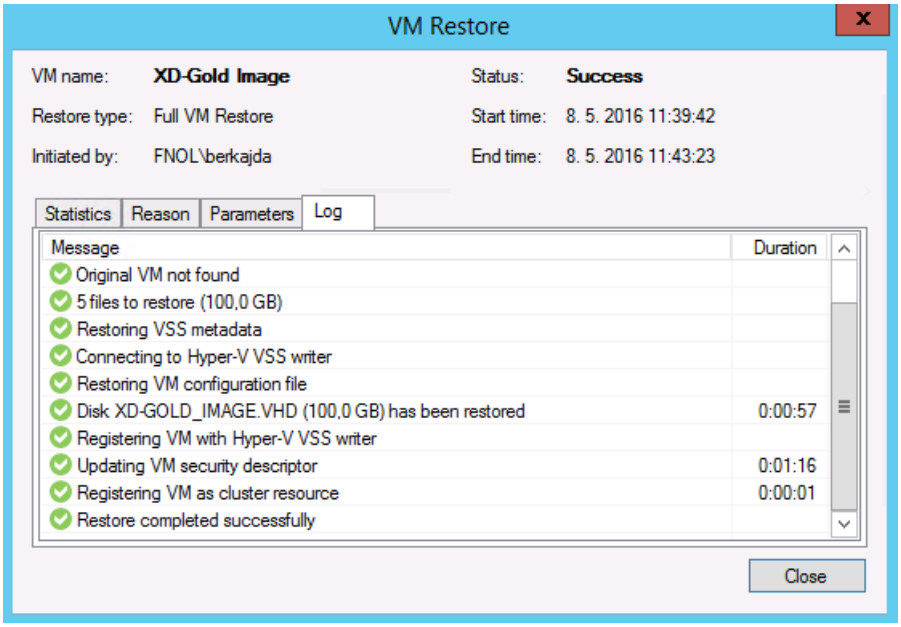
Obr. 37. Výběr bodu obnovení.

V závěrečném kroku byla vložena informace o důvodu provedení obnovení virtuálního počítače.



Obr. 38. Sumář obnovení virtuálního počítače.

Na první pokus se obnovení nepodařilo. Zálohovací systém zahlásil obecnou chybu, ze které nebylo možné identifikovat důvod neprovedení obnovy. Po ověření prohlížečů událostí v rámci Hyper-V serverů byl zjištěn nekonzistentní stav instance virtuálního počítače po smazání virtuálního disku. Bylo provedeno smazání prostředků virtuálního počítače z klastru CLS-APP2014 a restartován pokus o obnovení instance virtuálního počítače.



Obr. 39. Úspěšné obnovení instance virtuálního počítače.

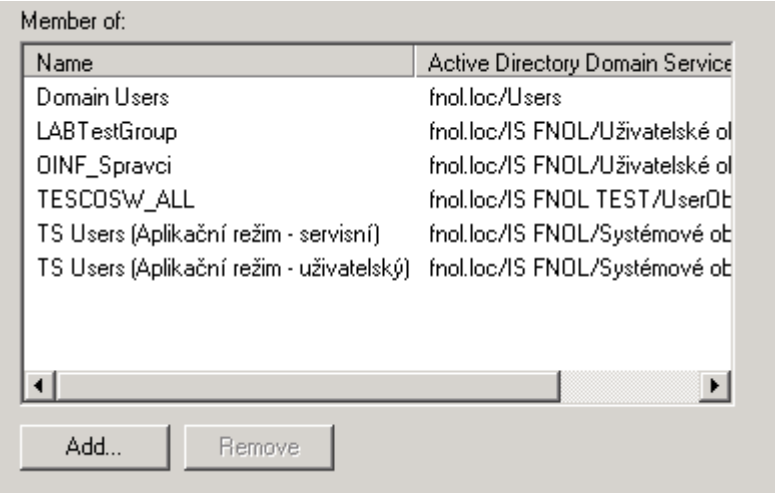
Instance virtuálního serveru byla automaticky přidána do klastru a bylo provedeno spuštění virtuálního serveru. Funkčnost byla ověřena úspěšným přihlášením do operačního systému [13].

8.2 Obnovení adresářových služeb

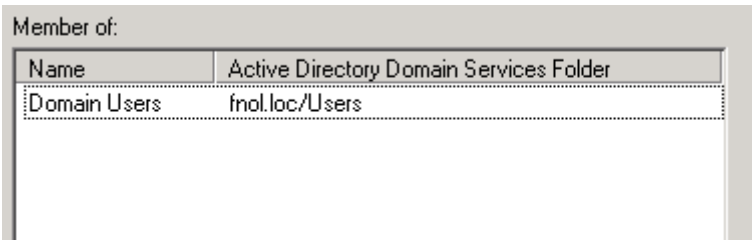
Pro testování obnovení adresářových služeb byly v doméně fnol.loc vytvořeny testovací objekty:

- organizační jednotka VeeamLAB,
- objekt uživatele berkajveeam,
- doménová skupina LABTestGroup.

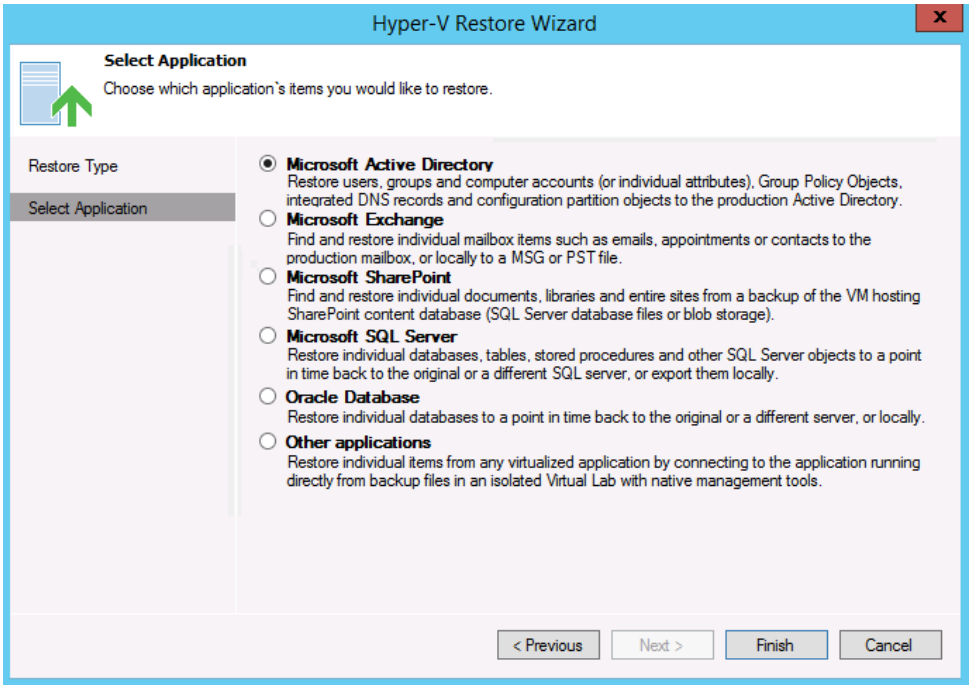
Byl proveden test obnovení členství ve skupinách, který simuluje úmyslné / neúmyslné smazání. Původní soupis členství doménových skupin pro uživatele berkajveeam je zobrazen na obrázku číslo 40. Proběhlo odebrání členství ze všech doménových skupin mimo skupiny Domain Users. Detail je zobrazen na obrázku číslo 41.



Obr. 40. Původní soupis členství v doménových skupinách.



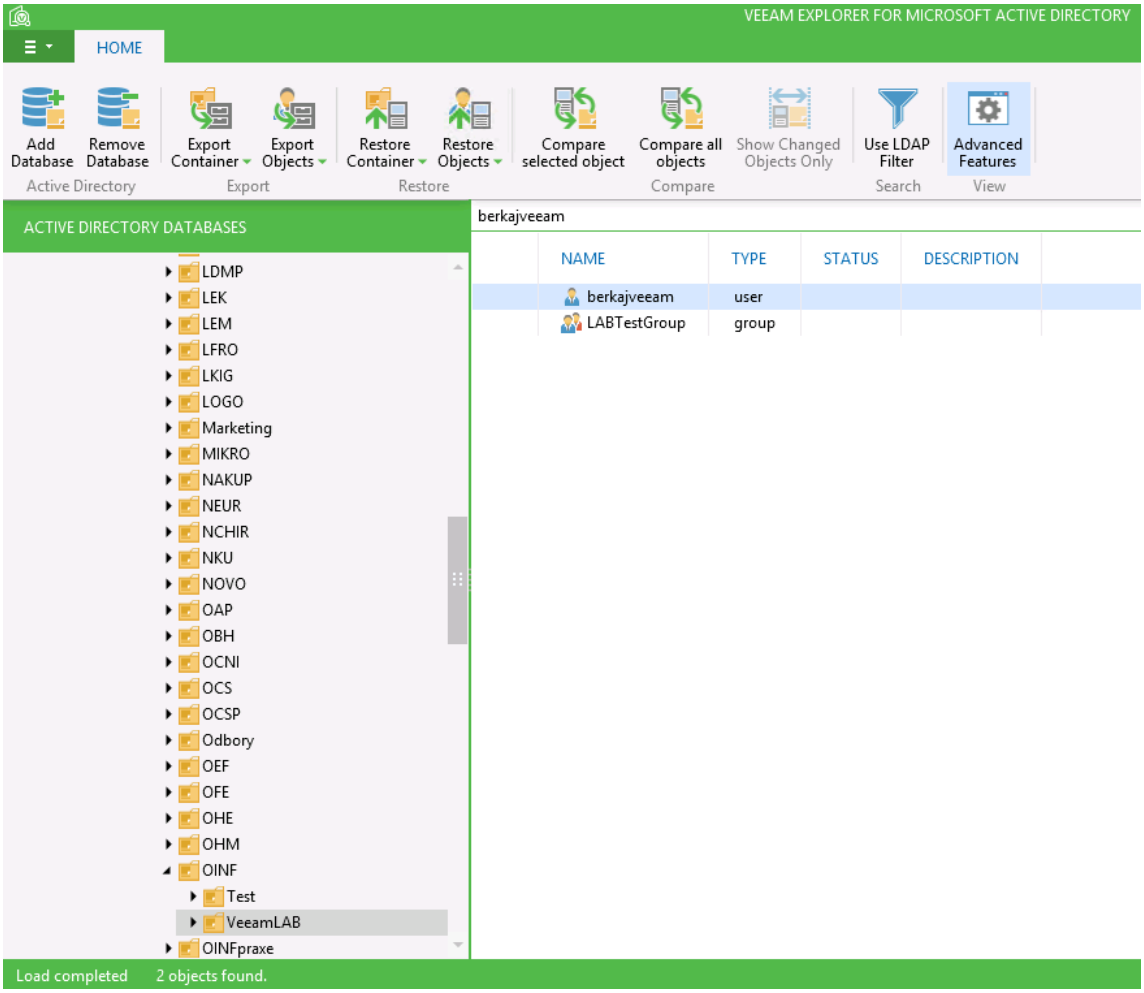
Obr. 41. Členství v doménových skupinách po havárii.



Obr. 42. Průvodce obnovení objektu Active Directory.

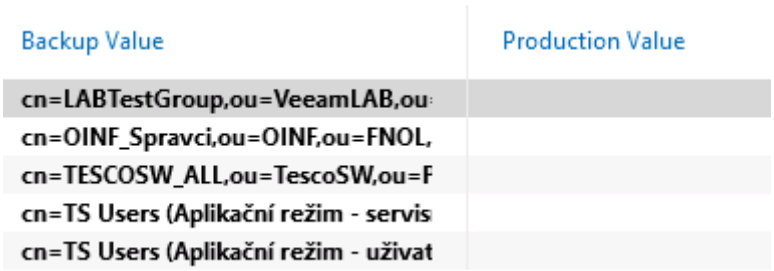
Pro spuštění procesu obnovení adresářových služeb bylo nutné v aplikaci Veeam spustit aplikační obnovení Microsoft Active Directory. Průvodce obnovení našel automaticky

ze seznamu zálohovaných virtuálních serverů hostitele adresářových služeb. V rámci obnovení bylo možné uvést informaci, proč byla úloha obnovení spuštěna. Veeam automaticky spustil nástroj k obnovení adresářové služby Veeam Explorer For Microsoft Active Directory. V rámci aplikace byla vidět struktura domény fnol.loc, ze které byl vybrán objekt k obnovení.

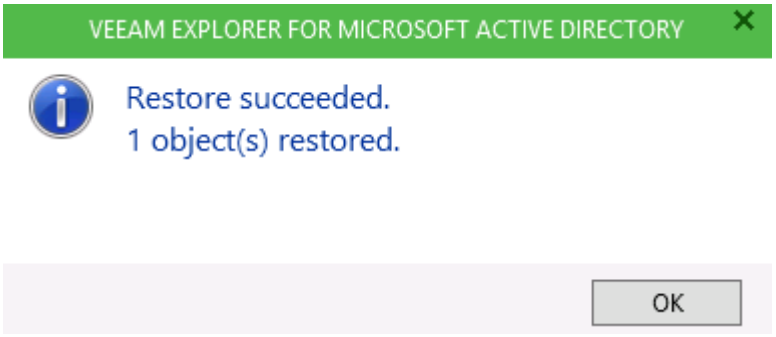


Obr. 43. Aplikace Veeam Explorer For Active Directory.

Aplikace nabídla možnost porovnání vlastností objektu mezi produkčním stavem a stavem uloženým v záloze.



Obr. 44. Porovnání vlastností objektu.



Obr. 45. Informace o úspěšném obnovení objektu.

Úspěšné obnovení bylo ověřeno pomocí kontroly v Active Directory.

Stejný způsob byl opakován pro obnovení organizační jednotky a objektu uživatelského účtu. U uživatelského účtu bylo provedeno kompletní smazání objektu. Po ukončení procesu obnovení byla ověřena možnost přihlášení se do domény fnol.loc [17].

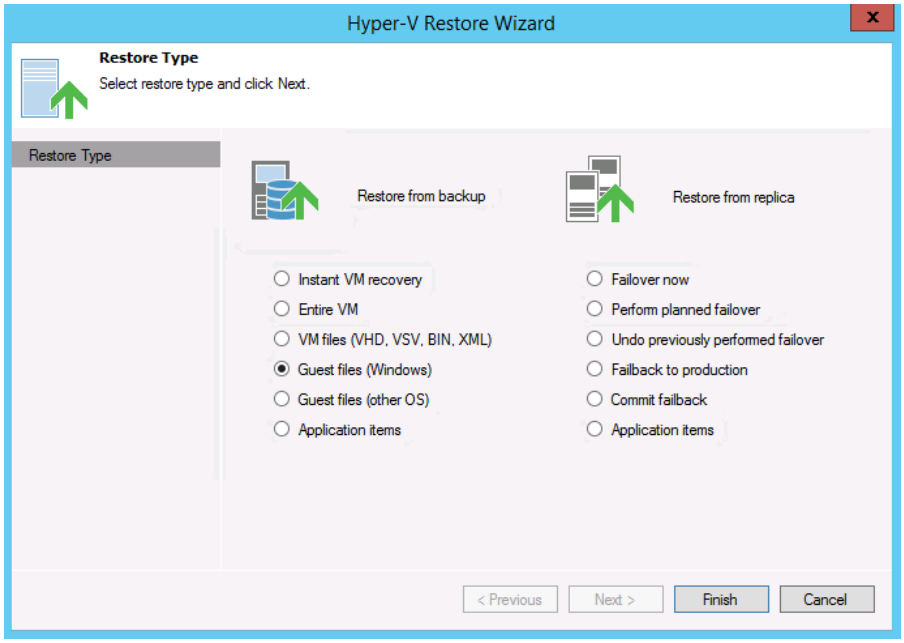
8.3 Obnovení souborových služeb

Souborové služby jsou ve velmi blízké interakci s uživateli informačního systému. Uživatelé do centrálního úložiště ukládají data různorodého typu. Díky tomu je riziko potřeby obnovení souborů velmi vysoké.

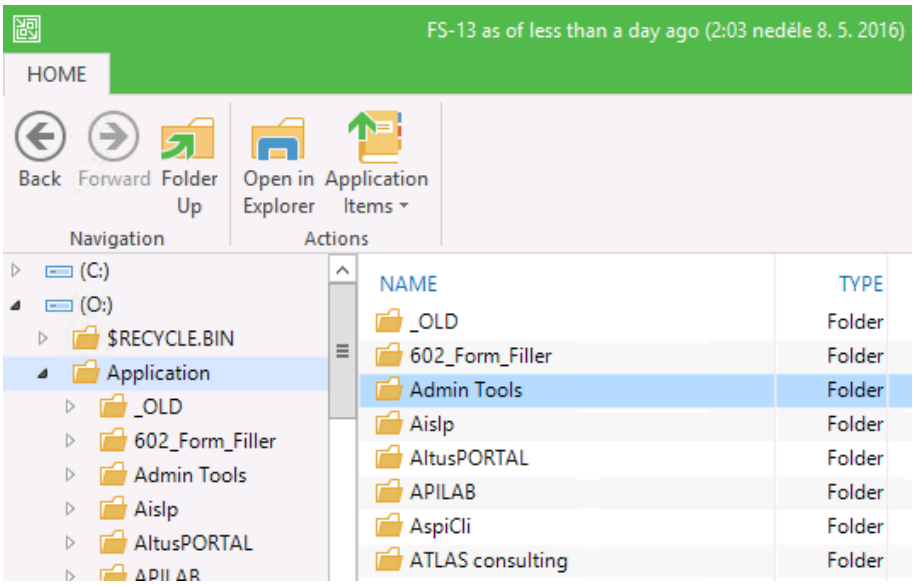
Je výhodné doplnit zálohovací proces o technologii volume shadow copy, která umožní samotným uživatelům provést obnovení vlastních souborů. Historii v rámci volume shadow copy není nutné volit příliš dlouhodobě. Z praxe je dostačující časový horizont maximálně jednoho týdne. Díky možnosti uživatelského obnovení nedochází ke zbytečnému vytěžování technického personálu.

Pro testování obnovení souborových služeb pomocí zálohovacího řešení Veeam Backup & Replication bylo provedeno smazání části souborů z centrálního souborového serveru. Z datové oblasti Applications byla smazána složka Admin Tools, která byla opět obnovena ze zálohy.

Po spuštění aplikace Veeam Backup & Replication byl vybrán virtuální server, který souborové služby hostuje. V rámci typu obnovy byla zvolena možnost obnovy souborů. Poté byl spuštěn prohlížeč souborů, pomocí kterého byla vybrána složka Admin Tools. Veeam nabízí možnost obnovení do původního nebo alternativního umístění. Bylo provedeno obnovení do původního umístění.

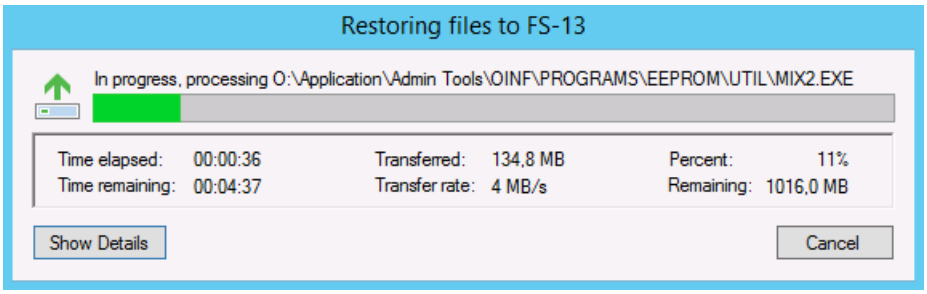


Obr. 46. Obnovení souborových služeb.



Obr. 47. Prohlížeč souborů v rámci aplikace Veeam.

Po potvrzení byl spuštěn proces obnovení do původního umístění [15].



Obr. 48. Průběh obnovení souborových služeb.

9 FORMULÁŘ PLÁNU OBNOVY

Formulář plánu obnovy je záznam, který může být reprezentován různými variantami provedení. Může to být záznam v informačním systému, nebo například textový dokument. Mnohem důležitější je informační hodnota záznamu. Význam plánů obnovy je důležitý z pohledu testování obnovení ICT aplikací a služeb po havárii. Nikdy nejde zajistit, že v průběhu procesu obnovení nedojde k nepředpokládaným problémům. Řešení problémů během ostrého procesu obnovení může celkovou nedostupnost informačního systému prodloužit i o desítky hodin. Proto je nutné testy obnovení nebrat na lehkou váhu a v rámci organizace je začlenit mezi pravidelné činnosti. V rámci testovacích plánů obnovy je očekáván proces neustálého zlepšování.

Na vytvoření a testování plánu obnovy musí spolupracovat:

- management organizace,
- technický personál,
- klíčoví uživatelé aplikace.

Plán obnovy obsahuje:

- hlavičku organizace,
- ICT služby / aplikace, kterých se plán týká,
- datum provedení testu plánu obnovy,
- dopad na provoz produkčního prostředí,
- seznam kroků, které byly v rámci plánu provedeny,
- doporučení pro zlepšení.

ZÁVĚR

Bylo vypracováno vypořádání požadavku odboru informatiky Fakultní nemocnice Olomouc na zajištění implementace nového systému zálohování virtuální infrastruktury provozované v rámci operačních systémů Windows Server 2008 R2 a Windows Server 2012 R2.

Byla zajištěna fyzická instalace a konfigurace expanze diskového pole IBM Storwize V7000. Proběhla instalace a konfigurace dvou nových virtualizačních serverů, které byly implementovány v režimu vysoké dostupnosti. Byla provedena migrace většiny virtuálních serverů ze starého aplikačního klastru do nově instalovaného aplikačního klastru.

Byl vypracován návrh zálohovacího plánu, který byl schválen zástupci odboru informatiky Fakultní nemocnice. Plán byl navržen s cílem zajistit v oblasti zálohování a obnovy po havárii ideální výstupy, které by byly v synergii s poskytovanou kvalitou léčby pacientů nemocnice. Změna v oblasti zálohování byla vůči předcházejícímu stavu statisticky znázorněna. Výsledek provedení implementace nástroje Veeam Backup & Replication byl zvýšení počtu zálohovaných serverů z původních 20 % na současných 90 %.

Návrh implementace byl úzce konzultován přímo s výrobcem aplikace společností Veeam. Během postupu implementace zálohovacího systému Veeam Backup & Replication verze 9 bylo postupováno dle doporučení výrobce. V průběhu implementace a konfigurace systému zálohování byly diagnostikovány různé chyby, které byly průběžně odstraňovány.

Úspěšně byly provedeny testovací plány obnovy pro některé důležité ICT služby. Bylo otestováno obnovení kompletní instance virtuálního serveru po havárii, která byla simulována smazáním virtuálního serveru z infrastruktury. Adresářové služby byly ověřeny simulací smazání uživatelského účtu, nebo odebrání členství z několika doménových skupin v rámci domény fnol.loc. Souborové služby byly ověřeny pomocí simulace úmyslného smazání několika adresářů z centrálního souborového serveru.

Bohužel se nepodařila kompletní migrace virtuálních počítačů z původního aplikačního klastru do nového prostředí. Bylo to zapříčiněno zamítnutím žádosti o dočasné odstavení virtuálních serverů z provozu. To mělo vliv na způsob implementace hlavního zálohovacího serveru, který musel být dočasně realizován jako virtuální server. Kvalita zálohování nebyla uvedenou vynucenou změnou poznamenána.

SEZNAM POUŽITÉ LITERATURY

[1] ACRONIS. Acronis Backup Advanced. *Acronis.com* [online]. [cit. 2016-04-12]. Dostupné z: http://www.acronis.com/en-us/business/backup-advanced

[2] ALTARO. Altaro VM Backup. *Altaro.com* [online]. [cit. 2016-04-12]. Dostupné z: http://www.altaro.com/vm-backup/features.php

[3] BERKA, J. *Provoz systémových IT služeb v informačním systému Fakultní nemocnice Olomouc.* Zlín, 2014. Bakalářská práce. Univerzita Tomáše Bati, Fakulta aplikované informatiky. Vedoucí práce Miroslav Matýsek.

[4] BRUCKNER, Tomáš, Jiří VOŘÍŠEK a Alena BUCHALCEVOVÁ. *Tvorba informačních systémů: principy, metodiky, architektury*. 1. vyd. Praha: Grada, 2012, 357 s. Management v informační společnosti. ISBN 978-80-247-4153-6.

[5] DE GUISE, Preston. *Enterprise systems backup and recovery: a corporate insurance policy*. Boca Raton: CRC Press, c2009. ISBN 142007639.

[6] IBM. IBM Spectrum Protect for Virtual Environments. *IBM.com* [online]. [cit. 2016-04-20]. Dostupné z: http://www-03.ibm.com/software/products/en/spectrum-protect-for-virtual-environments

[7] IBM. IBM Storwize V7000 Unified and Storwize V7000. *IBM.com* [online]. [cit. 2016-03-16]. Dostupné z: http://www-03.ibm.com/systems/storage/disk/storwize_v7000/overview.html

[8] IBM. IBM TS3310 Tape Library. *IBM.com* [online]. [cit. 2016-03-16]. Dostupné z: http://public.dhe.ibm.com/common/ssi/ecm/ts/en/tsd01449usen/TSD01449USEN.PDF

[9] NELSON, Steven. *Pro data backup and recovery*. New York: Distributed to the book trade worldwide by Springer Science+Business Media, c2011. Expert's voice in data management. ISBN 1430226625.

[10] VEEAM. Administration. *Veeam.com* [online]. [cit. 2016-04-23]. Dostupné z: https://helpcenter.veeam.com/backup/hyperv/administration.html

[11] VEEAM. GFS Retention Policy. *Veeam.com* [online]. [cit. 2016-03-14]. Dostupné z: https://helpcenter.veeam.com/backup/hyperv/backup_copy_gfs.html

[12] VEEAM. Installing Veeam Backup & Replication. *Veeam.com* [online]. [cit. 2016-04-22]. Dostupné z: https://helpcenter.veeam.com/backup/hyperv/install_vbr.html

[13] VEEAM. Performing Instant VM Recovery. *Veeam.com* [online]. [cit. 2016-04-30]. Dostupné z: https://helpcenter.veeam.com/backup/hyperv/performing_instant_recovery.html

[14] VEEAM. Recommended hotfixes for Hyper-V servers. *Veeam.com* [online]. [cit. 2016-04-12]. Dostupné z: https://www.veeam.com/kb1838

[15] VEEAM. Restoring VM Guest OS Files (Microsoft Windows). *Veeam.com* [online]. [cit. 2016-04-30]. Dostupné z: https://helpcenter.veeam.com/backup/hyperv/performing_guest_restore.html

[16] VEEAM. Simple Retention Policy. *Veeam.com* [online]. [cit. 2016-03-14]. Dostupné z: https://helpcenter.veeam.com/backup/hyperv/backup_copy_simple_retention.html

[17] VEEAM. Using Veeam Explorer for Microsoft Active Directory. *Veeam.com* [online]. [cit. 2016-04-30]. Dostupné z: https://helpcenter.veeam.com/backup/hyperv/restore_vead.html

[18] VEEAM. Veeam Backup & Replication v9. *Veeam.com* [online]. [cit. 2016-04-22]. Dostupné z: https://www.veeam.com/cz/backup-replication-features.html

[19] VEEAM BLOG. The 3-2-1-0 Rule to High Availability. *Veeam.com* [online]. [cit. 2016-04-05]. Dostupné z: https://www.veeam.com/blog/the-3-2-1-0-rule-to-high-availability.html

[20] VERITAS. Veritas NetBackup 7.7. *Veritas.com* [online]. [cit. 2016-04-20]. Dostupné z: https://www.veritas.com/content/dam/Veritas/docs/data-sheets/21324986_GA_ENT_DS-Veritas-NetBackup_7-7_EN_R2.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Atd.	A tak dále
BD-R	Blu-ray Disc - Recodable
BD-RE	Blu-ray Disc – Recodable Erasable
CD-R	Compact Disc - Recodable
CD-RW	Compact Disc - Rewritable
DISM	Deployment Imaging Servicing Management
DNS	Domain Name System
DP	Diskové pole
DVD+R	Digital Versatile Disc + Recordable
DVD+RW	Digital Versatile Disc + Rewritable
DVD-R	Digital Versatile Disc - Recordable
DVD-RW	Digital Versatile Disc - Rewritable
ECC	Error Checking and Correcting
FNOL	Fakultní nemocnice Olomouc
FTP	File Transfer Protokol
GB	Giga Byte
Gbps	Gigabit per second
GFS	Grandfather-Father-Son
Graf.	Graf
HW	Hardware
ICT	Informační a komunikační technologie
IT	Informační technologie
LAN	Local Area Network
LTO	Linear Tape Open

MB	Mega Byte
NAS	Network Attached Storage
Obr.	Obrázek
RAID	Redundant Array of Inexpensive/Independent Disks
RAM	Random Access Memmory
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAN	Storage Area Network
SAS	Serial Attached SCSI
SATA	Serial Advancend Technology Attachment
SCSI	Small Computer System Interface
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSD	Solid State Disk
SW	Software
Tab.	Tabulka
TB	Tera Byte
Tzv.	Takzvaný
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VM	Virtual Machine
WAN	Wide Area Network
WMI	Windows Management Instrumentation
XML	Extensible Markup Language

SEZNAM OBRÁZKŮ

Obr. 1. Zanesení chyby z produkčního prostředí do disaster recovery lokality. 15
Obr. 2. Obnovení ICT služby ze zálohy. 16
Obr. 3. Proces zálohování a jeho komponenty. 18
Obr. 4. Decentralizovaná topologie zálohování – upraveno autorem [5]. 24
Obr. 5. Centralizovaná topologie zálohování – upraveno autorem [5]. 25
Obr. 6. Inkrementální zálohování – upraveno autorem [5]. 27
Obr. 7. Inkrementální zálohování – upraveno autorem [9]. 28
Obr. 8. Rozdílová záloha – upraveno autorem [5]. 29
Obr. 9. Jednoduchý retenční model – upraveno autorem [16]. 32
Obr. 10. GFS retenční model – upraveno autorem [11]. 33
Obr. 11. Pásková knihovna IBM TS3310 [8]. 34
Obr. 12. Diskové pole IBM Storwize V7000 [7]. 35
Obr. 13. Zálohování do cloudové služby – upraveno autorem [5]. 37
Obr. 14. Proces zálohování pomocí Powershell skriptu. 44
Obr. 15. Servery, které nebylo možné přesunout z klastru CLS-APP2009. 51
Obr. 16. Logické znázornění implementace zálohovacího systému. 52
Obr. 17. Průběh migrace do nového klastru CLS-APP2016. 53
Obr. 18. Diskové pole v záložní lokalitě a detail expanze pro potřeby zálohování. 54
Obr. 19. MDisk R6_Veeam. 55
Obr. 20. Vytvoření logické jednotky 55
Obr. 21. Připojení k Hyper-V hostům. 55
Obr. 22. Průběh instalace operačního systému Windows Server 2012 R2. 56
Obr. 23. Chyba v průběhu instalace hotfix balíčku. 59
Obr. 24. Postup instalace hotfix balíčku pomoci aplikace DISM. 59
Obr. 25. Průvodce instalace Veeam Backup & Replication. 62
Obr. 26. Kontrola potřebných softwarových komponent. 63
Obr. 27. Preferovaná nabídka defaultní konfigurace. 63
Obr. 28. Volba umístění databáze. 64
Obr. 29. Průběh instalace Veeam Backup & Replication. 64
Obr. 30. Instalace update 1. 65
Obr. 31. Autentizace do konzole Veeam Backup & Replication. 65
Obr. 32. Přidání Hyper-V serveru do systému zálohování. 66

Obr. 33. Výběr typu Hyper-V serveru. 67
Obr. 34. Ukázka informace o chybějících hotfix opravách. 67
Obr. 35. Ukázka reportu po ukončení zálohovací úlohy. 75
Obr. 36. Chyba po zapnutí VM po smazání disku. 76
Obr. 37. Výběr bodu obnovení. 77
Obr. 38. Sumář obnovení virtuálního počítače. 77
Obr. 39. Úspěšné obnovení instance virtuálního počítače. 78
Obr. 40. Původní soupis členství v doménových skupinách. 79
Obr. 41. Členství v doménových skupinách po havárii. 79
Obr. 42. Průvodce obnovení objektu Active Directory. 79
Obr. 43. Aplikace Veeam Explorer For Active Directory. 80
Obr. 44. Porovnání vlastností objektu. 80
Obr. 45. Informace o úspěšném obnovení objektu. 81
Obr. 46. Obnovení souborových služeb. 82
Obr. 47. Prohlížeč souborů v rámci aplikace Veeam. 82
Obr. 48. Průběh obnovení souborových služeb. 82

SEZNAM TABULEK

Tab. 1. Běžný týdenní inkrementální zálohovací plán – upraveno autorem [5]. 27
Tab. 2. Běžný týdenní rozdílový zálohovací plán – upraveno autorem [5]. 29
Tab. 3. Přehled zálohování virtuálního prostředí v době analýzy. 48
Tab. 4. Zálohovací plán v době analýzy. 48
Tab. 5. Soupis doporučených hotfix balíčků – upraveno autorem [14]. 58
Tab. 6. Přehled systémových účtů pro potřeby zálohování Veeam Backup & Replication – upraveno autorem [12]. 60
Tab. 7. Backup repository. 68
Tab. 8. Přehled zálohování Hyper-V klastrů. 69
Tab. 9. Konfigurace spouštění denní zálohovací úlohy. 69
Tab. 10. Konfigurace spouštění týdenní zálohovací úlohy. 70
Tab. 11. Konfigurace spouštění měsíční zálohovací úlohy. 71

SEZNAM GRAFŮ

Graf. 1. Porovnání kapacitní náročnosti inkrementální a rozdílové zálohy.....30
Graf. 2. Porovnání počtu virtuálních serverů ve vazbě na typ zálohovací úlohy. 72
Graf. 3. Procentuální vyjádření počtu zálohovaných VM při použití skriptu.....73
Graf. 4. Procentuální vyjádření počtu zálohovaných VM při použití Veeam. 74

SEZNAM PŘÍLOH

P I Zálohovací plán.

P II Formulář obnovy ICT služby / aplikace.

PŘÍLOHA P I: ZÁLOHOVACÍ PLÁN

Název Serveru	Denní záloha	Týdenní záloha	Měsíční záloha
ALEF0	x	x	x
BCK-12	x		
BYOD-DNS	x	x	x
DHCPSnooping	x	x	x
Flowmon	x	x	
FS-13	x	x	
FTP	x	x	
FWIPv6	x	x	
GoogleAuth	x	x	x
HotSpot	x	x	x
Monitoring	x	x	x
SeaFile	x	x	x
SRV-01	x	x	x
SRV-02	x	x	x
SRV-07	x	x	x
SRV-10	x	x	x
SRV-109	x	x	
SRV-110	x	x	
SRV-111	x	x	
SRV-127	x	x	x
SRV-128	x	x	x
SRV-129	x	x	x
SRV-140	x	x	x

Název Serveru	Denní záloha	Týdenní záloha	Měsíční záloha
SRV-16	x	x	x
SRV-17	x	x	
SRV-17n	x	x	
SRV-21	x	x	
SRV-28n	x	x	
SRV-29	x	x	
SRV-34	x	x	x
SRV-35N	x	x	x
SRV-36-SCCM	x	x	x
SRV-36-SCOM	x	x	x
SRV-36-SCVMM	x	x	x
SRV-37	x	x	x
SRV-38n	x	x	x
SRV-40	x	x	x
SRV-40A	x	x	x
SRV-44	x	x	x
SRV-45	x	x	x
SRV-48	x	x	x
SRV-54	x	x	x
SRV-56a	x	x	
SRV-58a	x	x	
SRV-59n	x	x	x
SRV-60	x	x	
SRV-65	x	x	x

Název Serveru	Denní záloha	Týdenní záloha	Měsíční záloha
SRV-73	x	x	x
SRV-74	x	x	x
SRV-75	x	x	x
SRV-76	x	x	x
SRV-77	x	x	x
SRV-78	x	x	x
SRV-84	x	x	x
SRV-85	x	x	x
SRV-86	x	x	x
SRV-86a	x	x	x
SRV-87	x	x	x
SRV-88	x	x	x
SRV-89	x	x	x
SRV-94	x	x	x
SRV-95	x	x	x
SRV-97	x	x	x
SRV-98	x	x	x
SRV-99	x	x	x
SysLog	x	x	x
TACACSa	x	x	x
TACACSb	x	x	x
XD-Gold Image	x		
XenController 5.6	x	x	x
Zabbix-Proxy	x	x	x

PŘÍLOHA P II: FORMULÁŘ OBNOVY ICT SLUŽBY / APLIKACE

REPORT PROVEDENÍ PLÁNU OBNOVY ICT SLUŽBY / APLIKACE V PROSTŘEDÍ FAKULTNÍ NEMOCNICE OLOMOUC

1 ÚČEL REPORTU

Tento dokument obsahuje základní informace o aktivitách a závěrech provedených v souvislosti s obnovou systému a dostupnosti ICT služby / aplikace v prostředí Fakultní nemocnice Olomouc, včetně provedení testování obnovy.

Obnovované ICT služby / aplikace	Instance virtuálního počítače XD-GoldImage.
Dopad na provoz produkčního prostředí	Ano
Datum provedení obnovy	08. 05. 2016
Obnovu prováděl	Berka Jaromír

2 POPIS VÝPADKU

Report dokumentuje: (nehodící se škrtněte).

Testování plánu kontinuity	~~Ostrý výpadek produkčního prostředí~~

3 ROZSAH VÝPADKU

Oblasti infrastruktury, které byly výpadkem ovlivněny:

ICT služby / aplikace výpadkem ovlivněné	**Doba trvání obnovy**	**Popis rozsahu výpadku**
Virtualizační služby	30 minut	Nefunkční virtuální počítač XD-GoldImage. Po dobu výpadku nebylo možné provádět centrální aktualizace virtuálních desktopů.

4 POPIS AKTIVIT A OPATŘENÍ PROVEDENÝCH V RÁMCI OBNOVY

Smazání instance virtuálního počítače z Hyper-V.
Přihlášení ke konzole zálohovacího systému Veeam.
Provedení obnovení virtuálního serveru ze zálohy – byl použit poslední bod obnovy.
Kontrola úspěšného provedení zálohy v prostředí Veeam.
Kontrola instance virtuálního počítače v prostředí Hyper-V.
Kontrola instance operačního systému, provedení úspěšného přihlášení k operačnímu systému.
Kontrola systémového logu operačního systému.

5 ZÁVĚRY A DOPORUČENÍ

Po smazání virtuálního počítače nebylo možné provést obnovu instance. Na úrovni klastrového prostředku došlo k neúplnému odstranění virtuálního serveru. Po smazání virtuálního serveru z konzole klastru proběhla obnova v pořádku.

REPORT PROVEDENÍ PLÁNU OBNOVY ICT SLUŽBY / APLIKACE V PROSTŘEDÍ FAKULTNÍ NEMOCNICE OLOMOUC

1 ÚČEL REPORTU

Tento dokument obsahuje základní informace o aktivitách a závěrech provedených v souvislosti s obnovou systému a dostupnosti ICT služby / aplikace v prostředí Fakultní nemocnice Olomouc, včetně provedení testování obnovy.

Obnovované ICT služby / aplikace	Adresářové služby – obnovení účtu berkajveeam.
Dopad na provoz produkčního prostředí	Ne
Datum provedení obnovy	08. 05. 2016
Obnovu prováděl	Berka Jaromír

2 POPIS VÝPADKU

Report dokumentuje: (nehodící se škrtněte).

Testování plánu kontinuity	~~Ostrý výpadek produkčního prostředí~~

3 ROZSAH VÝPADKU

Oblasti infrastruktury, které byly výpadkem ovlivněny:

ICT služby / aplikace výpadkem ovlivněné	**Doba trvání obnovy**	**Popis rozsahu výpadku**
Adresářové sužby	5 minut	Nemožnost využít doménový uživatelský účet fnol\berkajveeam.

4 POPIS AKTIVIT A OPATŘENÍ PROVEDENÝCH V RÁMCI OBNOVY

Smazání uživatelského účtu fnol\beerkajveeam pomocí konzole adresářových služeb.
Přihlášení ke konzole zálohovacího systému Veeam.
Provedení obnovení uživatelského účtu ze zálohy – byl použit poslední bod obnovy.
Kontrola úspěšného provedení zálohy v prostředí Veeam.
Kontrola přítomnosti účtu v Active Directory.
Provedeno úspěšné přihlášení pomocí obnoveného účtu, včetně ověření členství v doménových skupinách pomocí příkazu *whoami /groups*.

5 ZÁVĚRY A DOPORUČENÍ

Během obnovení účtu nedošlo k žádnému problému.

REPORT PROVEDENÍ PLÁNU OBNOVY ICT SLUŽBY / APLIKACE V PROSTŘEDÍ FAKULTNÍ NEMOCNICE OLOMOUC

1 ÚČEL REPORTU

Tento dokument obsahuje základní informace o aktivitách a závěrech provedených v souvislosti s obnovou systému a dostupnosti ICT služby / aplikace v prostředí Fakultní nemocnice Olomouc, včetně provedení testování obnovy.

Obnovované ICT služby / aplikace	Souborové služby – datová oblast Application.
Dopad na provoz produkčního prostředí	Ano
Datum provedení obnovy	08. 05. 2016
Obnovu prováděl	Berka Jaromír

2 POPIS VÝPADKU

Report dokumentuje: (nehodící se škrtněte).

Testování plánu kontinuity	~~Ostrý výpadek produkčního prostředí~~

3 ROZSAH VÝPADKU

Oblasti infrastruktury, které byly výpadkem ovlivněny:

ICT služby / aplikace výpadkem ovlivněné	**Doba trvání obnovy**	**Popis rozsahu výpadku**
Souborové služby	15 minut	Chybějící data na datové oblasti Application.

4 POPIS AKTIVIT A OPATŘENÍ PROVEDENÝCH V RÁMCI OBNOVY

Smazání adresáře Admin Tools z datové oblasti Application.
Přihlášení ke konzole zálohovacího systému Veeam.
Provedení obnovení serveru FS-13 na úrovni jednotlivých souborů. – byl použit poslední bod obnovy.
V rámci souborového prohlížeče Veeam byl vybrán adresář Admin Tools, který byl obnoven.
Kontrola úspěšného provedení zálohy v prostředí Veeam.
Kontrola přítomnosti obnoveného adresáře a jeho obsahu.

5 ZÁVĚRY A DOPORUČENÍ

Během obnovení adresáře Admin Tools nedošlo k žádným problémům.