Zálohování virtuálních infrastruktur

Projekt fondu rozvoje CESNET 562R1/2015

Závěrečná zpráva

28. listopadu 2016

Úvod

V poslední letech proběhla virtualizace bezmála všech fyzických serverů provozovaných Centrem informačních technologií Vysoké školy baňské - Technické univerzity Ostrava (dále CIT). V návaznosti na tento vývoj došlo k výraznému rozšíření virtualizační infrastruktury a vybudování univerzitního datového centra spravované spravované CIT.

V rámci datového centra jsme začali uvažovat o změně zálohovacího systému tak, aby efektivně pracoval i v rámci nového prostředí. V období před virtualizací byl nasazen a provozován systém pro zálohování HP Data Protector. Zálohovány byly pouze důležité datové soubory a vybrané servery. Obnova dat ze záloh byla kapacitně i časově náročná, mnohdy i v řádech hodin. Bylo nutné provést reinstalaci operačního systému, pak instalaci zálohovacího agenta a až poté bylo možno přistoupit k obnově datových souborů.

Virtualizace umožňuje zcela jiný přístup k zálohám díky tomu, že celý server je reprezentován pomoci datových a popisných souborů virtualizačního prostředí. Cílem zálohování virtuální infrastruktury je tedy zálohovat pouze těchto několik souborů. Z těchto souborů lze poté poměrně jednoduše a rychle obnovit celý virtuální server, jeho disky nebo jednotlivé soubory na discích uložené.

Pojmy

Pro přehled uvádíme základní pojmy, které budou použity v tomto dokumentu.

Backup & Replication (B&R) produkt společnosti Veeam určený pro zálohovaní VI.

Data Protector (DP) produkt společnosti Hewlett Packard pro agentové zálohovaní serverů.

Virtualizační infrastruktura (VI) infrastruktura určena pro provoz virtuálních serverů (VM).

Volume Shadow Copy Service (VSS) je technologie společnosti Microsoft pro vytvoření konzistentních obrazů pevných disků. Tato funkce požádá služby na daném serveru, aby převedli své datové soubory do konzistentního stavu.

Prostředí před realizací projektu

Univerzitní datové centrum VŠB-TU Ostrava je rozloženo mezi dvě geograficky oddělené lokality. Obsahuje jednotnou infrastrukturu pro LAN i SAN postavenou na technologii konvergovaného Ethernetu realizovanou na síťových přepínačích Nexus 5500 společnosti Cisco. Jako primární úložiště je použita platforma Netapp FAS8000 zapojená v režimu Metro-cluster se synchronní replikou dat mezi lokalitami.

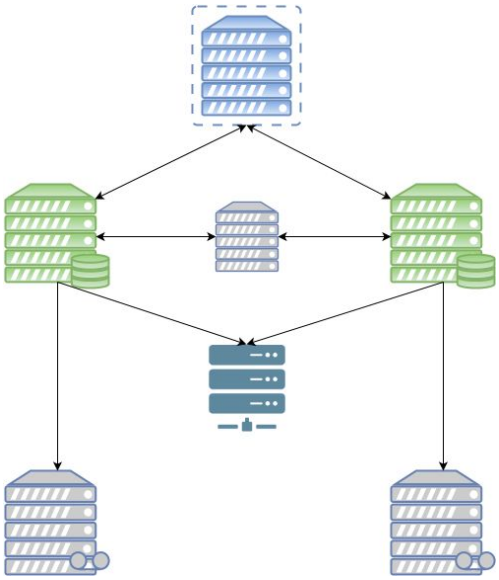
Pro serverovou část se používá řešení Cisco Unified Computing System (UCS). Na serverech provozujeme VMware vSphere ve verzi 5.5 v edici Enterprise Plus. Pro virtualizaci používáme 13 serverů s celkem 228 logickými jádry a 3,28 TB RAM na kterých běží přes 400 virtuálních serverů (dále VM).

Primární úložiště má výslednou kapacitu 135 TB. Pro ukládání záloh je k dispozici dedikované diskové pole s kapacitou 175 TB. Z původního zálohování máme k dispozici 2 páskové knihovny s LTO 4 a LTO 5 páskami, které plánujeme využít v novém zálohovací řešení.

HP Data Protector

Pro zálohování byl využíván plně agentový nástroj HP Data Protector A.08.00.

HP Data Protector je zálohovací software pro automatickou zálohu a obnovu dat pracující s jednotlivými servery, především v podnikovém prostředí, podporující ukládání dat na diskové pole či magnetické pásky. Agenti jsou multiplatformní s podporou především operačních systémů Windows / Windows Server a systémy na bázi Unix/Linux.



Obrázek 1.: Topologie zálohovaní HP Data Protector

Toto prostředí je demonstrováno na obr. 1. Zálohovací systém byl provozován na dvou fyzických linuxových serverech, na nichž byla provozována aplikace HP DP 8 Cell Manager.

Cell Manager je hlavní část platformy, která centrálně ovládá a řídí agenty. Obsahuje PostgreSQL databázi, ve které jsou uloženy veškeré informace o zálohovaných strojích včetně jejich historie, detailního nastavení zálohovacích procesů, licencí apod.

Jako nadstavbový prvek k našim cell managerů byla využívána aplikace HP DP Manager, která byla umístěna na virtuálním stroji s OS Windows Server. Manager má přívětivé GUI ve kterém jsme mohli jednoduše ovládat a konfigurovat oba cell managery, ale i diskové kapacity a páskové jednotky.

Z důvodů přehlednější evidence zálohovaných strojů jsme využívali virtuální server používající OS GNU/Linux. Na tomto stroji jsme evidovali, pomocí vlastních skriptů psaných v jazyce Python s podporou web2py frameworku, mimo jiné umístění serverů vůči cell manageru, jejich správce, předpokládané množství zálohovaných dat a skutečné množství odzálohovaných dat. Zároveň sloužil jako distributor nových strojů k jednotlivým cell managerům, kde automaticky vytvářel profily a nastavoval firewall pro správnou komunikaci klient-server. Databázi jsme s výhodou využívali také k následnému rozesílání reportů jednotlivým uživatelům, což současná verze HP DP, v takovém rozsahu neuměla. Součástí zálohovacích reportů bylo i upozornění při překročení předpokládaného limitu dat, což mohlo být způsobeno mnoha faktory (chyba ve scriptu, útok apod.).

Diskové kapacity

Jako primární diskové úložiště nám sloužil NetApp E2712 z něhož byly vypropagovány přes Fibre-channel LUNy (cca 2x 40 TB) k oboum cell managerům. Na těchto oddílech byl využíván souborový systém XFS. Pooly vytvořené pomocí HP DP měli velikost 1 TB.

Páskové jednotky

Sekundárním úložištěm se v původním prostředí staly páskové knihovny. Konkrétně se jedná o dvě zařízení typu MSL G3 Series. V prvním případě se jednalo o plně obsazenou knihovnu paskami HP LTO4 s kapacitou pásky 800 GB tedy 76 TB. V druhém případě byly využívány HP LTO5 s možností osazení opět 96 páskami s kapacitou tedy 1,5 TB/páska. Knihovna byla osazena 57 páskami s hodnotou kapacity 84 TB. Obě knihovny byly osazeny dvěma mechanikami. LTO4 knihovna se připojovala pomocí rozhraní SAS zatímco LTO5 knihovna pomocí 8 Gbps Fibre Channelu.

Trocha statistiky

Před realizací projektu se zálohovalo 118 vybraných serverů s průměrnou denní velikostí zálohy 1,1 TB. Níže uvedená tabulka ukazuje čísla za období 1.3. - 1.4.2016.

Data jsme zálohovaly resp. plné zálohy byly prováděny zpravidla ve 14 denních cyklech mezi kterými byly prováděné klasické rozdílové zálohy.

Server	Počet zálohovaných serverů	Velikost dat celkem [GB]	Průměrná velikost dat / server [GB]	Průměrná velikost dat / den [GB]	Počet objektů	Průměrný počet objektů na server
Jelen	57	25 610	12 833	826	1 915 487 123	33 605 037
Žabka	61	8 980	4 520	289	2 323 230 499	38 085 745
Celkem	118	34 590	17 354	1 115	4 238 717 622	71 690 783

Tabulka č.1 - Statistika zálohovaných dat pomocí HP DP za březen 2016

Požadavky cílového řešení

Před výběrem nového zálohovacího systému bylo potřeba definovat požadavky, které by mělo nové řešení splňovalo. Požadavky jsme rozdělili do tří skupin.

Co

Rozšíření zálohovaní na všechny servery dostupné ve VI. V případě selhání primárního úložiště je nutné mít zálohu celé VI pro její obnovení. Pro rychlé obnovení služeb je potřeba mít zálohu kompletních virtuálních serverů včetně pomocných souboru virtualizační platformy.

Kdy

Zálohované data mohu být staré (RPO) maximalně 1 den. Je tedy nutné každý den vytvořit nový bod obnovení. Zálohovací infrastruktura musí být schopna udělat během 24 hodin zálohu veškerých produkčních dat. Jednou týdně musí být provedena plná záloha důležitých dat.

Zálohování nesmí ovlivnit provoz služeb v pracovní dny v čase 8-15h. Důležité servery se musí zálohovat v noci v čase 20-5h.

Kam

Zálohovací infrastruktura musí být postavena pro minimalizaci rizika ztráty dat. Zálohovaná data musí být uložena na fyzicky jiném diskovém poli, které nebude obsahovat žádné primární data. Nesmí nastat situace, že jsou data zálohována na stejná disková pole s původními daty.

Chceme dodržet pravidlo 3-2-1. Což znamená mít zálohu na třech různých místech, dvou různých mediích a v jedné lokalitě mimo organizaci. Zálohy chceme mít uložené na vyhrazeném diskovém poli, na magnetických páskách a DÚ CESNET. Tímto splníme výše uvedená pravidla.

Zvolený nástroj

Při průzkumu dostupných nástroj pro zálohování s přihlédnutím k naším požadavkům jsme nakonec zvolili produkt společnosti Veeam s názvem Backup & Replication ve verzi 9. Kromě splnění naších požadavků bylo mezi dalšími důvody výborné hodnocení a zkušenosti stávajících uživatelů a také dobrý přístup technických pracovníků výrobce.

Zvolený produkt používá stejný licenční model jako společnost VMware u platformy vSphere. Licencují se tedy fyzické procesory bez omezení na počet jader nebo velikost RAM. Veeam je dostupný v edicích Standard, Enterprise a Enterprise plus. Pro nasazení jsme zvolili edici Standard. Za poplatek je možné edici povýšit, což je ovšem doprovázeno zvýšením ceny roční podpory.

Architektura

Každý ze serverů ve Veeam infrastruktuře může být provozován fyzicky nebo virtuálně. V našem případě, kdy se snažíme minimalizovat počet fyzických serverů, bude většina serverů virtuálních. Výjimkou jsou servery zajišťující práci s páskovými knihovnami a připojení diskových kapacit přes technologii Fibre Channel.

Důvod pro použití fyzických serverů nejsou jen výkonnostní nároky, ale také možnost obnovy dat v případě katastrofálního selhání (tzv. disaster recovery). Za této situace jsou data jednoduše dostupná přes fyzické servery nezávislé na celé VI, která ve svých závislostech není zcela jednoduchá. Stačí jen nainstalovat Veeam Backup Server, zadat údaje k fyzickému serveru s Veeam Backup Repository a VI. Celá tato záležitost se dá zvládnout za několik minut.

Role serveru

Každý server v rámci Veeam prostředí má přidělenou svou roli. Jeden server může mít i více rolí. Při spuštění instalátoru na prvním serveru bude nainstalována role Backup Server, Backup Proxy i Backup Repository na jeden server.

Rozšíření o další servery se realizuje prostřednictvím administrace Veeam Backup Serveru, kde se vytvoří nový server daného typu a zadají se přístupové údaje k cílovému systému. Veeam poté provede instalaci a nastavení patřičné role na novém serveru.

Backup Server

Hlavní částí Veeam prostředí je Backup Server, který slouží jako jednotné místo pro správu celého prostředí. Musí se jednat o server s OS MS Windows. Správa se provádí prostřednictvím desktopové aplikace, která může být provozována i mimo tento server. V této aplikaci se provádí veškerá konfigurace včetně správy přistupových údajů, licencí apod.

Backup Proxy

Další součásti prostředí je Backup Proxy, která zpracovává data během zálohy. Podporovaný OS je MS Windows. Pro větší propustnost zálohování je vhodné mít několik Backup Proxy serverů. Pro každou proxy se nastavuje počet paralelních úkolů a pro každou souběžnou úlohu se doporučuje 1 vCPU a 0,2 GB RAM. Proxy server je během zálohování nejvíce vytěžovaný server zálohovací infrastruktury.

Backup Repository

Poslední část prostředí tvoří server pro uložení dat Backup Repository. Tato komponenta nemusí být provozována na OS MS Windows, ale lze také použít i systém GNU/Linux. Jde o server který má přímo připojené cílové úložiště (dedikované diskové pole, pásková knihovna, připojená vzdálená úložiště). U Backup Repository se opět definuje počet paralelních úloh.

Režimy přenosu

Backup Proxy podporují několik metod přenosu dat pro vytvoření zálohy. Zdroj pro vytvoření zálohy je vždy hlavní diskové pole a cíl musí být dostupný přes nějakou Backup Repository.

Na výběr jsou 3 režimy. První je Direct storage access. Jedná se o rozšíření režimu Direct SAN známého z předchozích verzí Backup & Replication. V tomto režimu se bude snažit Backup Proxy přistupovat k datům přímo pomocí SAN nebo NFS. Zjednodušeně řečeno dochází k připojení potřebného svazku k Backup proxy. Jedná se o režim s největší propustností.

Druhý režim se jmenuje Virtual Appliance (v předchozích verzi pojemenován jako HotAdd). Backup proxy si k sobě přímo připojí virtuální disk zálohovaného serveru. V principu se jedná o zálohovaní lokálního disku dané proxy. Bohužel se v našem testovacím prostředí (vSphere 5.5 a Veeam v8) objevila chyba, která způsobovala výpadky v řádech desítek sekund při přepojovaní disku v rámci NFS úložišť. Museli jsme tedy dočasně přejít na režim Network. Tato chyba by se již neměla objevit ve Veeam v9.

Poslední možností je Network, kdy je v roli zdroje ESXi, kde běží zálohovaný virtuální server. Tento režim zatěžuje hypervizor, jelikož on poskytuje data pro zálohu. Jedná se o nejpomalejší způsob zálohování, který navíc vytěžuje CPU fyzických serverů VI.

Režimy zálohování

B&R umožňuje několik metod pro tvorbu záloh. Základní se jmenuje *Forward Incremental*. Při použití tohoto režimu na začátku vznikne plná záloha všech dat. Při každé další záloze se ukládá pouze seznam změn proti předchozímu stavu. Takto probíhá záloha až do naplnění počtu bodu obnovení. Poté nastane proces slučování, pří kterém dojde ke spojení plné zálohy s následnou rozdílovou zálohou. Tento postup se opakuje do doby, než vznikne nová plná záloha.

Plná záloha se může vytvářet periodicky. Pro udržení nastaveného množství bodů obnovy Veeam nebude mazat plnou zálohu, pokud je potřebná alespoň jedna z navazujících rozdílových záloh. Tudíž bude docházet k existenci více bodu obnovení, než je nastaveno.

Pro tvorbu rozdílových záloh B&R používá API poskytované VMware pro použití technologie Change Block Tracking (CBT). Pro vytvoření rozdílové zálohy Veeam dostane jen změněná data od poslední zálohy. Nemusí tedy načít obsah poslední zálohy a dělat porovnání proti současnému stavu.

Veeam nabizí i obracené rozdílové zálohy tzv. *Reverse Incremental*, kdy se poslední záloha vždy tváří jako plná. Tento přístup má výhodu pro rychlou obnovu velkého množství dat. Při obnově není nutné načíst plnou zálohu a do ní pak promítnout všechny následné rozdílové. Je k dispozici rovnou plná záloha, která se dá obnovit. Nevýhodou je, prodloužení doby každé zálohy. Prodloužení je přibližně stejné jako v případě slučování záloh.

Při dosažení nastaveného počtu bodu obnovení dochází jen ke smazání nejstaršího bodu obnovení. Mazaní je výrazně rychlejší než slučování.

Ukládaní záloh

B&R ukládá zálohy na úložišti do binárních souboru .vbk (plné zálohy), .vib (dopředné rozdílové zálohy) a .vrb (zpětné rozdílové zálohy). V základním nastavení jsou tyto soubory vytvářeny na úrovni úlohy. V rámci úlohy také probíhá deduplikace a komprese zálohovaných dat.

U vyšších edic (Enterprise a Enterprise plus) lze nastavit vytváření souboru zvlášť pro každý zálohovaný server. Tato funkce se nastavuje na úrovni Backup Repository a je výhodná pro velké virtuální stroje s různorodými daty.

Konzistence záloh

Zálohováním VM může vytvořit několik možných typů konzistence zálohy. Konzistence se projeví až v případě obnovy z této zálohy. Základním typem je tzv. *crash consistent* záloha. Obnovený server se chová stejně jako by během zálohy došlo k náhledu výpadku napájení. Do tohoto stavu se může dostat VM u kterého neproběhlo tzv. *quiesce*, kdy dojde k ukončení zápisu do souboru, vyprázdnění vyrovnávací paměti, zapsaní čekajících příkazu a jiných operaci související s integritou souborového systému.

Veeam dokáže vytvořit tzv. *transactionally consistent* zálohy, kde je použita funkce Microsoft VSS pro převedení souborového do konzistentního stavu. U serveru bez podpory Microsoft VSS se použijí nástroje obsažené ve VMware Tools plnící stejnou funkci. U této zálohy nedochází k poškození souboru na souborovém systému. Převedení do konzistentního stavu prodlužuje dobu zálohy a nemusí proběhnout správně.

VMware umožňuje vytvořit skripty uvnitř OS, které se volají při převodu souborového systému do konzistentního stavu. Správce serveru tak může zajistit v případě potřeby

potřebné kroky. Lze tedy jednoduše zařídit těsně před vytvořením obrazu disku zastavení databáze a opětovné spuštění po vytvoření obrazu.

Nejvyšší úroveň konzistence zajišťuje tzv. *Application-aware processing*, kdy Veeam zálohuje server s ohledem na běžící aplikace. Tato možnost je dostupná jen pro vybrané aplikace (Microsoft Exchange, Microsoft SQL Server a další). Veeam po úspěšné záloze umí například udělat tzv. *truncate* logů. Pro obnovu je poté dostupná separátní aplikace, jenž umožňuje obnovit jednotlivé aplikační položky (např. e-mail u Exchange serveru). V edici standard jsou možnosti omezené. E-mail se třeba musí exportovat do .eml místo obnovení přímo do původního umístění. Případně se musí obnovit celá databáze a ta se připojí k Exchange serveru.

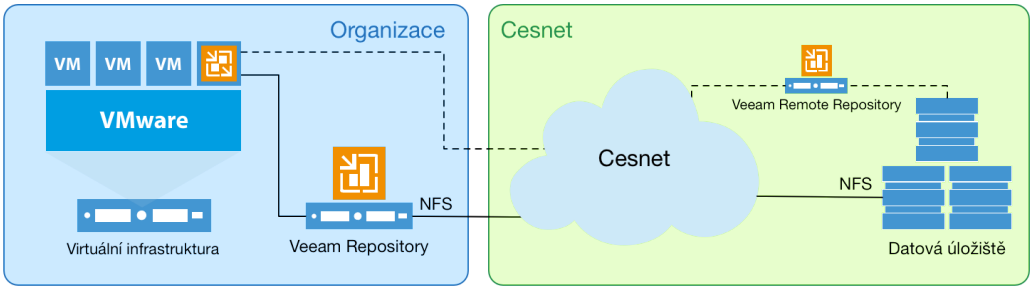
Podpora páskových knihoven

Veeam B&R umí využívat páskové knihovny LTO4 a novější. Práce s knihovnami se liší podle edice. Edice standard umí pracovat pouze na úrovni souborů. Je tedy nutno kopírovat jednotlivé .vbk a .vib soubory. Vyšší edice umí práci na úrovní záloh, takže je evidované na které pásce jsou které body obnovení.

Příklady použití

Vzorový scénář 1 - Záloha na DÚ CESNET

První scénář je nejjednodušší variantou zálohování VI. Nevyžaduje dodatečné diskové kapacity na straně organizace a je vhodná pro malá prostředí, které nemají vlastní zálohovací řešení a dedikované kapacity pro zálohování. Zálohy jsou prováděny z prostředí organizace přímo na DÚ CESNET.



Obrázek 2.: Topologie přímého zálohování na DŮ CESNET

Toto řešení je určeno k jednosměrnému zálohování za účelem obnovení VI v případě selhání primárního úložiště VI. Je velice závislý na spolehlivosti připojení organizace do sítě CESNET. Na straně DÚ CESNET dochází k migraci nepoužívaných dat na úložiště s delší dobou přístupu (MAID). Doba zpřístupnění dat se tedy může se stářím dat prodlužovat. Topologické znázornění toho scénáře naleznete na obrázku 2.

Čerpání služeb DÚ se realizuje pomocí protokolu NFSv4. Veeam potřebuje vidět cílové úložiště jako umístění v rámci souborového systému Veeam Backup Repository. NFSv4 svazky je problematické připojit do prostředí MS Windows (vyžadované Veeamem), proto jsme použili serverový systém s OS GNU/Linux, který má připojené patřičné svazky a provozuje službu Veeam Backup Repository.

Datová úložiště CESNET nabízí dobře zpracovaný návod pro připojení svazku přes protokol NFS, který lze najít na adrese https://du.cesnet.cz/cs/navody/nfs/start .

Server s připojenými svazky z DÚ může být umístěn uvnitř i mimo organizaci. Instalace serveru mimo organizaci může být vhodná s ohledem na eliminaci závislosti na vlastní infrastruktuře. Pro Veeam Backup Repository umístěnou mimo organizaci jsme zvolili pojem Veeam Remote Repository.

Veeam Repository neumožňuje sdílení jednoho serveru pro více instancí Veeamu. Z toho vyplývá podmínka, aby pro každou instanci běžel jeden server. Alternativou k tomu řešení je využít produkt Veeam Cloud Connect Backup. Jedná se o multitenantní repository určené pro cloud poskytovatele. Tento produkt je licencován podle počtu chráněných virtuálních

serverů. Cena je závislá na počtu zálohovaných strojů. Pro představu dle ceníku platného k 30.6.2016 je cena do 300 virtuálních serveru přibližně 4,5 Euro za 1 VM měsíčně.

V první fázi jsme pro Veeam Reposiotry použili fyzických server v konfiguraci 128 GB RAM a 2x AMD Opteron(tm) 6176 SE.

Pro otestování byl také zprovozněn Veeam Remote Repository běžící jako virtuální server ve virtualizační platformě CESNET v lokalitě Brno. Tento server měl konfiguraci 4 vCPU 16 GB RAM a 20 GB HDD.

Provoz

Pro představu o rychlosti jsme provedli několik desítek měření doby zálohy. Rozhodli jsme se měřit dobu zálohy místo přenosové rychlosti, jelikož doba zálohy zahrnuje více položek a je více objektivní. Zálohování totiž není pouze kopírování dat, ale zahrnuje jejich přípravu a zpracování.

Pro měření rychlosti jsme vytvořili zálohovací úlohu s 75 virtuálními servery s celkovou kapacitou okolo 11 TB. Velikost plné zálohy po deduplikaci a kompresi byla 4,3 TB. Medián velikosti rozdílové zálohy je 172,3 GB. Úloha měla nastavených 5 bodů obnovení.

Jako alternativu k NFS jsme použili pro připojení k DÚ CESNET i připojení přes SSHFS.

Režim	Repository	Medián času plné zálohy	Medián času rozdílové zálohy
Rozdílové bez periodické plné	Lokální	39:04:31	22:59:28
Rozdílové s periodickou plnou	Lokální	15:09:23	2:37:37
Rozdílové s periodickou plnou	Vzdálené	14:10:53	2:18:24
Rozdílové s periodickou plnou při použití SSHFS	Vzdálené	17:02:01	1:52:00

Tabulka č.2 - Statistika doby zálohovaní při zálohovaní na DÚ CESNET

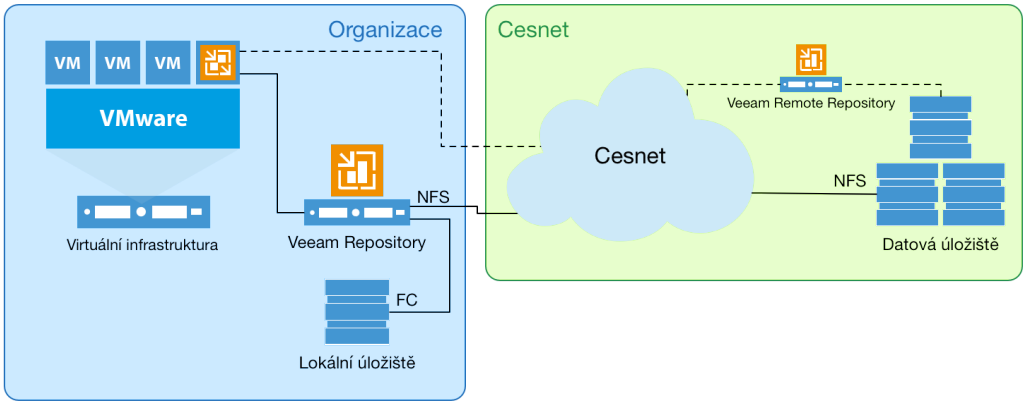
Každá situace v tabulce 2 byla testovaná přibližně měsíc. U první možnosti byla ovšem jen jedna plná záloha. Každá záloha byla prováděna v časech, kdy byl minimalizován provoz tvořen ostatními zálohami.

Z tabulky lze vyčíst, že je výhodnější používat periodické plné zálohy, než načítat stará data a ty poté spojovat. Časově není téměř rozdíl mezi lokální a vzdálenou repository.

Při použití NFS jsme pociťovali problémy se stabilitou. Jednalo se především o nárazové problémy, kdy jeden týden se objevil problém co druhý den a pak několik týdnů nebyl žádný problém. Při použití SSHFS jsme během měsíčního testování zaznamenali méně problémů než na NFS. Toto pozorovnání může být ovšem zkresleno kratší délkou testování.

Vzorový scénář 2 - Záloha na lokální úložiště a DÚ CESNET

Druhá varianta je zálohovat na vyhrazené diskové pole a poté hotové zálohy kopírovat mimo organizaci na prostředky DÚ CESNET. Diskové pole určena pro zálohovaní by neměla obsahovat provozní data. Diskové pole pro zálohy jsou zatěžovány primárně sekvenčním čtením a zápisem. Nejdůležitější parametr je kapacita, protože zálohy původních dat jsou uloženy v několika verzích. Kapacita zálohovacího diskového pole by měla být větší než kapacita primárního úložiště.



Obrázek 3.: Topologie zálohování na diskové pole a kopírovaní dat na DŮ CESNET

Toto nasazení má za úkol zrychlit dobu zálohy a zajistit spolehlivost vytváření záloh. Navíc obnovu dat lze provést přímo z lokálního úložiště i v případě nedostupnosti DÚ CESNET.

DÚ CESNET v tomto scénáři budou využívána k odkládání starších záloh a uložení dat mimo lokalitu organizace, čímž jsou data chráněny proti ztrátě v případě poruše zálohovacího diskového pole.

Scénář je vhodný pro nasazení ve středních a velkých prostředí, kde organizace investuje do hardwarových prostředků vyhrazených pouze pro zálohování.

V našem konkretní případě jsme použili diskové pole Netapp E2712 s 4 TB disky, které je pomocí Fibre Channel připojeno k našemu již existujícímu Veeam Repository serveru. Výhoda také je, že v případě následného kopírování dat na DÚ CESNET jsou data dostupná na jednom serveru. Celková kapacita je rozdělena do několika menších částí, které umožňují flexibilnější práci na straně serveru.

Na serveru je použit souborový systém ZFS, který umožňuje oddíly v rámci desítek TB složených z několika LUNů. Celková kapacita je rozdělena na 2 části, aby v případě selhání jednoho svazku nedošlo ke ztrátě všech dat. Původně byla zapnuta deduplikace a komprese na úrovní ZFS. Později se však ukázalo, že tato nastavení jen zpomalují proces zálohovaní bez větších úspor místa, protože Veeam již sám provádí deduplikaci a kompresi dat.

Tento scénář umožnil eliminovat závislost na dostupností k DÚ CESNET. Záloha proběhla vždy korektně na zálohovací diskové pole a až poté se hotová záloha překopírovala na DÚ. Když kopírování selhalo, pořád byla záloha dostupná ze zálohovacího diskového pole a všechny body obnovení se zkopírovaly při dalším kopírovacím cyklu.

Režim	**Repository**	**Medián času plné zálohy**	**Medián času rozdílové zálohy**
Rozdílové bez periodické plné	Lokální	39:04:31	22:59:28
Rozdílové s periodickou plnou	Lokální	15:09:23	2:37:37
Rozdílové s periodickou plnou	Vzdálené	14:10:53	2:18:24
Rozdílové s periodickou plnou při použití SSHFS	Vzdálené	17:02:01	1:52:00
Rozdílové s periodickou plnou na vyhrazené diskové pole	**Lokální**	**8:06:04**	**0:38:24**

Tabulka č.3 - Statistika rozšířena o zálohovaní na vyhrazené diskové pole

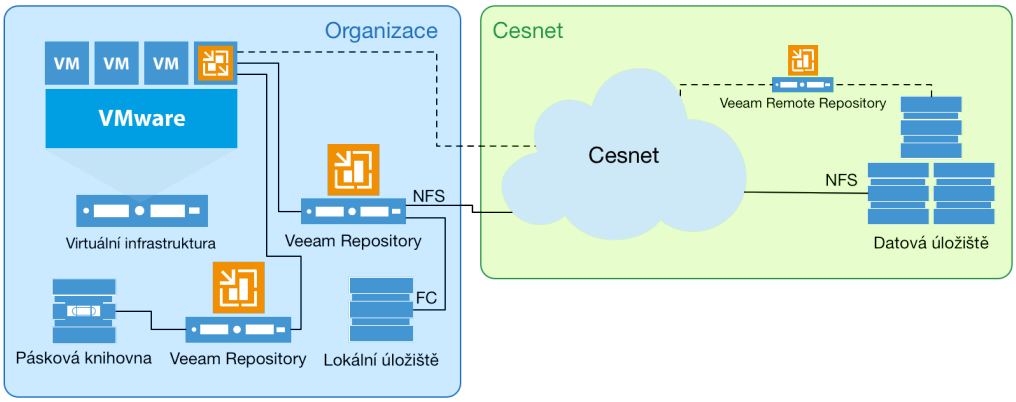
Pro srovnání s předchozím scénářem jsme rozšířili statistiku z tabulky 2 o data při zálohovaní stejné úlohy na vyhrazené diskové pole. Výsledná tabulka 3 zobrazuje, že na lokální vyhrazené diskové pole se záloha provede za přibližně polovinu času než na DÚ CESNET. U rozdílových záloh je časová úspora výraznější a záloha trvá přibližně čtvrtinu času.

Vzorový scénář 3 - Záloha na lokální úložiště, pásky a DÚ CESNET

Poslední scénář je o proti předchozímu rozšířen o zálohovaní na magnetické pásky. Jde o druhý typ media pro splnění podmínky 3-2-1 uvedené dříve.

Shrneme-li to, tak zálohovaní probíhá na vyhrazené diskové pole a následně probíhá kopírování záloh na prostředky DÚ CESNET a na magnetické pásky.

Tento scénář již plně pokrývá pravidlo 3-2-1, kdy máme 3 kopie dat (vyhrazené diskové pole, DÚ CESNET a magnetické pásky) na 2 typech medií (pevné disky a magnetické pásky) a 1 kopie dat je mimo organizaci (DÚ CESNET).



Obrázek 4.: Topologie zálohování splňující pravidlo 3-2-1

Topologie celého prostředí je znázorněna na obrázku 4. Celé řešení bylo rozšířeno o jeden server, ke kterému jsou připojeny páskové knihovny. Opět je lepší mít tento server jako fyzický pro jednodušší obnovu v případě výpadku. Do našeho řešení jsme integrovali páskové knihovny využívané původním zálohovacím systémem.

Páskové knihovny řeší problém s kapacitou pro trvalejší zálohy. Problém je ovšem v rychlosti zápisu na magnetické pásky. Přenosová rychlost je závislá na typu pásek a naměřili jsme hodnoty rychlosti 35 MB/s u LTO4 a 45 MB/s u LTO5 pro jednu mechaniku. Rychlost je konstantní a nezahrnuje výměnu pásek. Veeam umí paralelizovat přístup na úrovni úloh. Tedy dvě úlohy mohou pracovat se dvěma mechanikami v jedné knihovně.

Omezená rychlost zápisů na pásky nás donutila také k omezení množství zálohovaných dat pouze na plné zálohy. Tento stav je dočasný a řešením bude nasazení páskové knihovny podporující LTO7 s rychlejším zápisem.

Edice Standard umí pracovat s páskami pouze na úrovni souborů. Tedy pro obnovu jednoho stroje je potřeba obnovit celý soubor obsahující plnou zálohu a z něj poté obnovit jeden konkrétní server. Edice Standard navíc neumožňuje vytvořit repository, kde jsou zálohy serverů rozdělené pro každý server. Toto omezení by se dalo obejít vytvořením zvláštní úlohy pro každý server.

V našem nasazení se předpokládá obnova z pásek v případě selhání primárního úložiště, selhání zálohovacího diskového pole a porušení dat na DÚ CESNET. Tato situace je tak málo pravděpodobná, že pokud nastane tak ten jeden velký soubor obnovíme jako celek z magnetických pásek.

Systém pro evidenci záloh

U předchozího systému zálohovaní se po vytvoření zálohy každému správci vytvořil e-mail, který ho informoval o provedení zálohy. Z tohoto důvodu musel mít zálohovací systém svou databázi serveru a jejich správců, kterou bylo nutné udržovat.

Veeam B&R má možnost posílat e-mail jen na úrovni zálohovací úlohy obsahující souhrnné informace za všechny zálohované servery v dané úloze. Takováto forma výstupu je spíše vhodná pro správce zálohování, aby měli přehled o průběhu záloh.

Chtěli jsme však správcům serverů umožnit jednoduchou formou zjistit, stav zálohování jejich serveru. Pro tento účel jsme vytvořili systém pro evidenci zálohovaní, který sbírá data z prostředí Veeam i VMware vSphere.

Při tvorbě tohoto řešení jsme chtěli eliminovat dodatečnou evidenci, kterou lze získat z jiných zdrojů. Evidence správců virtuálních serverů chceme mít pouze na jednom místě a to na straně VI. Všechny služby, které tyto informace potřebují, je mohou získat z VI.

Obrázek 5.: Náhled systému pro evidenci zálohování

Systém se skládá z dvou části. První se periodicky spouští v plánovači úloh na Veeam Backup Serveru a je napsaná v Powershellu. Tento skript přes dostupné API Veeamu získá informace o zálohovacích serverech a všech dostupných bodu obnovené daného serveru.

V druhé fázi se skript připojí k VI a získá informace o správcích serveru uložené jako Tagy u VM. Nakonec skript spojí získaná data do jednoho celku a udělá export ve formátu JSON. Tento export je pak dostupný přes HTTP druhém serveru, který s ním dále pracuje. Jako webový server jsme použili aplikaci Mongoose a pomocí firewallu omezili přístup pouze na server, kde běží zbytek systému.

Druhou část tvoří webová prezentace napsaná pomocí skriptovacího jazyka PHP s podporou jQuery knihovny.

Po stažení exportního JSON souboru přes HTTP se provede jeho parsování a následné nahrání dat do MySQL databáze. Tato součinnost s DB nám následně umožní lepší a rychlejší práci s daty. V budoucnu plánujeme rozšíření aplikace o statistickou vrstvu, tak abychom analyzovali nejčastější požadavky obnov a případně tak upravili zálohovací specifikace.

Systém vyzve uživatele, aby se ověřili proti centrálnímu školnímu LDAP. Po jeho ověření se zobrazí seznam serverů (viz obr. 5), kde je uživatel uveden jako správce a to včetně lokality umístění dostupných bodu obnovení. Při kliknutí na daný bod obnovy se předvyplní formulář pro vytvoření požadavku do našeho IT Helpdesku (obr. 6) - uživatel zde dodá jen cestu k obnovovaným souborům, a případně poznámku kde mají být data obnovena.

Obrázek 6. - Ukázka předvyplnění tiketu do HelpDesku

Obě části tohoto systému jsou licencovány pod GNU GPLv3 a jsou součásti elektronické přílohy této zprávy.

Poznatky z nasazení

Úvodní nasazení produktu Veeam je velice rychlé a bez-problémové. Pomocí absence agentů, lze téměř okamžitě začít zálohovat veškeré virtuální servery.

Pokud se jedná o desítky VM, tak lze tímto nasazení ukončit. Pokud je ale zálohovaných serverů více, tak je potřeba proces zálohovaní optimalizovat.

Tvorba úloh

Jednu z otázek, kterou jsme začali řešit již na začátku byla tvorba zálohovacích úloh. U každé volby jsme museli jít cestou kompromisů. Například pro přiřazení serverů do úlohy jsme pro většinu serveru zvolili použití tagů uvnitř prostředí VMware. Našlo se ale několik serverů, které musí být zálohované samostatně. Zde jsme zvolili statickou definici v rámci úlohy.

Podobná situace nastala také u rozdělení VM do jednotlivých úloh. Není moudré mít všechny servery uvnitř jedné úlohy. Krom toho, že vznikají obrovské soubory záloh, se kterými se těžko pracuje, tak je celá záloha závislá na dokončení této úlohy. Navíc i v případě jednotné politiky zálohovaní je potřeba upravovat parametry zálohovaní pro jednotlivé skupiny serverů.

V první fázi jsme rozdělili servery podle důležitosti. Tím nám vznikly 4 kategorie (p1, p2, p3 a testing). Serverů s prioritou p1 a p2 nebylo mnoho, takže výsledný soubor nebyl příliš velký. Pro každou z priorit p1 a p2 vznikla samostatná úloha. Ovšem v kategorii p3 běží většina provozovaných virtuálních serverů a proto jsme přistoupili k rozdělení zálohovací úlohy na několik menších úloh.

Svou roli při návrhu také hrálo, že Veeam podporuje deduplikaci a kompresi pouze v rámci zálohovací úlohy. Pro ušetření místa je tedy nejlepší mít podobné servery v jedné úloze, proto jsme přistoupili k tvorbě zálohovacích úloh na základě OS (Debian, CentOS, Windows a ostatní).

Jakmile jsme začali avizovat, že ukládáme naše zálohy také mimo organizaci, tak se objevily aplikace, jejichž data nelze z právních důvodů umístit mimo technické prostředky nebo prostory naší univerzity. Vznikl tedy další zálohovací job, který nemá nastavené kopírování na DÚ.

V tomto případě nám přišlo vhodné kopírování na magnetické pásky, kdy jsme i u těchto rizikových dat mohli mít zálohu i lokálně na zvláštním mediu. Rychlost pásek je velmi omezená a nejsme schopni kopírovat veškerá data každý den na pásky. Kopírují se pouze plné zálohy jednou za týden.

Ve výsledku tedy máme ve VMware vSphere v kategorii zálohovaní vytvořeny tyto tagy:

- **priority** - servery z P1 a P2,
- **windows** - servery P3 s OS Microsoft Windows,
- **linux** - servery s OS GNU/Linux,
- **debian** - servery P3 s OS GNU/Linux Debian a jeho derivaty,
- **centos** - servery P3 s OS GNU/Linux CentOS a RedHat,
- **testing** - testovací servery,
- **vsb-only** - servery bez kopirování do DÚ CESNET,
- **special** - staticky definované servery ve Veeam,
- **exclude** - nezálohované servery (vypnuté a dočasné VM).

Dlouhodobé zálohy

Při kopírování záloh do DÚ CESNET je možnost zapnout zálohovaní typu GFS. Tato funkce vytváří v cílovém úložišti dlouhodobé zálohy. Záloha je rozdělena na týdenní, měsíční, čtvrtletní a roční. U každého typu lze zvolit počet bodů daného typu, které se mají držet. Dobu vytváření je možnost modifikovat. Měsíční zálohy se mohou třeba dělat první den v měsíci nebo třeba první pondělí.

Každá takto vytvořená záloha je plná záloha a je tedy nutné počítat s příslušnými nároky na diskové kapacity. Z počátku jsme optimisticky nastavili politiku na ukládání čtyř týdenních, dvou měsíčních, jedné kvartální a jedné roční zálohy. Následkem bylo rychlé vyčerpání přiděleného místa. Jedna plná záloha dané skupiny VM byla okolo 6 TB. Při našem nastavení jsme museli mít 8 plných záloh. Takže tato jedná zálohovací úloha zabrala 48 TB a to se jednalo o 58 VM z celkového počtu 400.

Následně jsme tedy politiku upravili na udržování pouze 2 měsíčních záloh. U převážné většiny zálohovaných systémů je toto nastavení plně vyhovující. Výjimku jsme udělali u hlavního souborového serveru, kde z důvodu šíření ransomware obnovujeme data i několik měsíců stará.

Velice důležité je zaškrtnout volbu pro vytváření GFS bodu obnovení pomocí plné zálohy. V opačném případě bude záloha vytvořena synteticky pomocí spojení poslední plné zálohy a všech následných rozdílových záloh. Tato operace může způsobovat problém hlavně ve spojení s architekturou DÚ CESNET, kde získání starších dat může být zdlouhavé.

Režim

Jak bylo popsáno výše, tak Veeam podporuje několik režimu ukládání. Zpočátku jsme používali výchozí režim nekonečných rozdílových záloh pro všechny úlohy. Problémy se však objevily, až se vytvořil maximální nastavený počet bodů obnovení.

Naše zálohovací diskové pole nebylo vybíráno s ohledem na maximální propustnost a výkon, ale hlavně s ohledem na velkou kapacitu. Proto jsme narazili na problém v případě, kdy všechny úlohy začali spojovat plné zálohy s následující rozdílovou zálohou. Toto slučování trvalo podobně dlouho jako plná záloha a probíhalo každý den.

Kdybychom nastavili periodické plné zálohy u všech úloh, nebudeme mít dostatek kapacit pro udržení definovaného počtu bodu obnovení. Proto jsme zvolili periodickou plnou zálohu pouze u úloh p1, p2 a vsb-only. Zbytek úloh se zvládá spojit v definovaném časovém okně.

Záloha fyzických serverů

Zálohovací služba je poskytována pro zálohování serverů běžících ve VI. V infrastruktuře však je potřeba zálohovat i některé fyzické servery. Jednalo se například o záložní fyzicky LDAP server nebo například monitorovací server, který jsme se z provozních důvodů rozhodli nevirtualizovat. Celkový počet těchto serverů není více než deset a na všech je instalován OS GNU/Linux.

Veeam ohlasil vydání aplikace pro agentové zálohovaní fyzických linuxových serverů s datem vydaní začátkem roku 2016. Vydání se ovšem opozdilo a protože jsme potřebovali nasadit nový systém zálohování dříve, tak jsme se rozhodli najít alternativní metodu.

Vytvořili jsme nový virtuální server sloužící jako úložiště pro zálohy fyzických serverů. Tento server přes NFS exportuje složky fyzickým serverům. Na fyzickém serveru je pote nastaven v cronu skript, který s využitím programu TAR archivuje souborový systém a uloží jej do připojené složky určené pro zálohovaní. Virtuální server se poté zálohuje jako každý jiný s tím rozdílem, že obsahuje i zálohu několika fyzických serverů.

Později v roce 2016 Veeam ohlásil vydaní agenta pro zálohovaní Windows i Linux serverů a jejich napojení do prostředí Veeam Backup & Repliaction. Po vydání těchto agentů a jejich otestování se předpokládá nahrazení našeho dočasného řešení pomocí prostředků Veeam.

Problémy

Během nasazení jsme samozřejmě narazili na překážky. Některé jsme byli schopni vyřešit s využitím zkušeností dalších uživatelů produktu Veeam, zejména v diskusních fórech. U systémovějších nebo zásadnějších změn jsme postup konzultovali se systémovou podporou společnosti Veeam.

Obnova souboru velkých VM

Na první problém jsme narazili při pokusu o obnovu souborů z našeho hlavního souborového serveru. Server používá operační systém SUSE, jehož součástí je souborový systém NSS od společnosti Novell.

Tento operační i souborový systém je plně podporován B&R. Problém ovšem způsobila velikost VM, která činí přibližně 7 TB. Navíc jsme obnovení prováděli ze starší zálohy, která byla dostupná pouze na DÚ CESNET.

Při obnově souborů z operačních systémů jiných než jsou MS Windows, používá Veeam pomocný virtuální server. Celý proces probíhá tak, že Veeam vytvoří NFS datastore ve VI, kde jsou dostupná data obnovovaného serveru. Poté vytvoří malý virtuální server (nazývaný

FLR Appliance), ke kterému připojí disky původního server. FLR Appliance se po náběhu spojí s Backup serverem a tam se zobrazí grafické rozhraní pro obnovu souboru.

Z preventivních důvodů má Veeam nastavenou dobu, kdy čeká na náběh. Výchozí hodnota je 10 minut. Po uplynutí této doby dojde k vypnutí a smazaní FLR Appliance. V našem případě však došlo k situaci, že při inicializaci NSS si FLR Appliance kontrolovala celý souborový systém. Kontrola téměř 7 TB souborového systému, který je uložen na druhém konci republiky, byla záležitost trochu delší než přednastavených 10 minut.

Situaci jsme řešili s podporou a bylo nám doporučeno vytvořit v registrech následující klíče s hodnotou 3600 v desítkové soustavě (1 hodina). Klíče je nutné vytvořit v umístění *Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication* s těmito jmény:

- remotingTimeout,
- FlrVmToolsWaitingTime,
- FlrApplianceIpWaitingTime.

Po tomto zásahu je nutné restartovat službu Backup Serveru. Při dalším pokusu již Veeam čekal déle jak 10 minut na náběh FLR Appliance. Náběh trval okolo 30 minut. Poté již byla dostupná možnost obnovy jednotlivých souborů uvnitř operačního systému.

Obnova včetně cesty

Během testování jsme narazili na situaci, kdy bylo potřeba obnovit řádově desítky složek včetně jejich cest. Přes grafické rozhraní se dá bez problémů obnovit jakákoliv složka do původního umístění, případně do určené cílové složky.

Problém nastává když má být obnoveno několik podsložek do jedné cílové složky. V takovém případě je nutné přes grafické rozhraní vytvořit v cílové složce patřičnou cílovou strukturu, poté ve stromě najít potřebný podadresář a překopírovat jej do cílového podadresáře. Tento krok se musí provést pro každou obnovovanou podsložku a je velice zdlouhavý.

Pro ušetření času při práci s grafickým rozhraním jsme použili jiný postup. Jak již bylo uvedeno dříve, Veeam používa FLR Appliance jako pomocný VM (GNU/Linux BusyBox), kde je připojený původní souborový systém.

FLR Appliance umožňuje přihlášení přes účet root a heslo se skládá z jména serveru poskytujícího data (většinou to bude Backup Server) a řetězce “_r”. Výchozí heslo se dá nastavit ve správě identit Veeam u položky s popisem “Helper appliance credentials”.

Tento virtualizovaný systém umožňuje přístup přes SSH. Pomocí unixového nástroje SED jsme z původního seznamu adresářů k obnově vytvořili seznam příkazů, které stačí spustit v cílové složce pro obnovu. Příkazy vytvoří patřičnou adresářovou strukturu a poté přes SCP zkopírují požadované soubory z FLR Appliance na cílový server. Lze použít i například RSYNC, FTP nebo SFTP.

Omezení FLR Appliance

Jelikož FLR Appliance z důvodů úspory běží na systému BusyBox, tak má svá omezení. První nás překvapil problém s podporou UTF-8 v příkazovém řádku. Původně jsme chtěli obnovu včetně cest provést ze strany FLR Appliance. Některé cesty ovšem obsahovali diakritiku a takovéto příkazy nešlo spustit. Toto omezení jsme vyřešili spouštěním příkazu pro kopírovaní přímo ze serveru, kde se mají data obnovit.

Na vážnější problém jsme narazili při pokusu obnovu jednoho souboru na cílový linuxový server přes grafické rozhraní. Obnova vždy skončila s chybou ověření na cílový server. Nejdříve jsme hledali problém v klíčích pro SSH.

Nakonec byl problém v navazování SSH. FLR Appliance totiž používala pro přístup k serveru algoritmus pro výměnu klíčů (KEX) diffie-hellman-group1-sha1. Na tom by nebylo nic špatného, kdyby OpenSSH server nepřestal z bezpečnostních důvodů tento algoritmus podporovat. Řešením je buď oslabit zabezpečení cílového serveru povolením daného algoritmu nebo spouštět kopírování přímo z cílového serveru.

Při řešení tohoto problému s podporou Veeam nám bylo doporučeno napsat na oficiální forum žádost o funkci. Provedli jsme kroky dle podpory, ale není jisté zda se v novějších verzích B&R objeví podpora pro bezpečnější algoritmy používané protokolem SSH.

Zpřístupnění obnovených dat

V rámci nasazení nového řešení jsme museli také vytvořit seznam postupů jak obnovit a zpřístupnit data. Nejjednodušší se ukázala situace v případě OS Microsoft Windows. Každý uživatel VŠB-TUO má kromě účtu v LDAP také zřízen účet v Microsoft Active Directory.

Obnovu jsme vyřešili zapojením Backup serveru do Active Direcotry. Máme lokálně vytvořenou složku, kde provádíme obnovu souborů. Tuto složku pomocí Active Directory můžeme zpřístupnit přes protokol SMB pouze vybraným uživatelům. Správce si může jednoduše připojit složku s obnovenými daty jako síťový disk a ověří se svým účtem v Active Directory. Cílový server nemusí být součásti Active Directory.

U OS GNU/Linux je situace rozdílná, protože Veeam používá pro obnovu pomocný VM FLR Appliance. Tento VM obsahuje značná omezení - viz. výše popsané problémy. Obnovu souboru tedy řešíme pouze spuštěním FLR Appliance a poté správci sdělíme síťovou adresu a heslo na uživatele root. Správce si sám zkopíruje data, která ho zajímají a nám jen ohlásí, že tak učinil a my ukončíme provoz FLR Appliance.

Tyto postupy mají jednu klíčovou výhod v porovnaní s předchozím řešením. Nyní totiž nemusí mít zálohovací systém přistup do operačního systému zálohovaných serverů. Není dokonce potřeba ani přístup zřizovat pro obnovu souborů. Jediná výjimka je Exchange server, kde musí mít Veeam lokální účet pro spuštění VSS a zpracovaní logů.

Přechod z HP Data Protectoru

(aneb ”byl to horor, ale nakonec jsme to dokázali!”)

Přechod na nové zálohovaní není jednoduchá záležitost. Po dodaní nového řešení probíhalo několikaměsíční testovaní funkcí a spolehlivosti nového řešení. Stále ovšem muselo být zachováno bez omezení provozu i původní řešení.

Hlavní omezení spočívalo v nedostatku diskových kapacit zálohovacího diskového pole, o které se dělil HP Data Protector i Veeam. I proto bylo nutné rozšířit kapacitu tohoto pole.

Před zrušením provozu HP Data Protectoru muselo být ohlášeno a vyjednáno ukončení provozu. Před tímto ohlášením jsme ještě museli připravit plně nový systém zálohování a to včetně návodů.

Jeden z hlavních kroků byl přesun páskových knihoven. Celý proces zahrnoval reinstalace serverů, které mají připojené páskové mechaniky a posléze smazání všech pásek. Šlo o nevratný krok a neměli jsme plně provozně ověřenou funkčnost na novém řešení. Rozhodli jsme se řešit celý problém postupně. Z první knihovny jsme přesunuli důležité servery na druhý server s druhou knihovnou. Posléze jsme zjistili, že nemůžeme původní server reinstalovat, protože bychom přišli i o zálohy na diskovém poli. Museli jsme najít další server kompatibilní s knihovnou.

Po přepojení první páskové knihovny jsme mohli vyzkoušet práci s páskovými knihovnami z prostředí Veeam. Po ověření funkce jsme se rozhodli pro přepojení i druhé páskové knihovny. Abychom nemuseli opět přijít o zálohy na diskovém poli, tak jsme připojili druhou knihovnu ke stejnému serveru jako předchozí.

Po těchto krocích probíhalo zálohovaní pomocí HP Data Protectoru pouze na diskové pole, kde byly zvětšena retence dat. Veeam již zálohoval na diskové pole a páskové knihovny. Stále ale Veeam neměl dostatek místa pro uchovaní požadovaného množství bodů obnovení. Na několika serverech již proběhlo zrušení zálohovaní pomocí HP Data Protectoru a díky tomu jsme v původní zálohovací infrastruktuře získali volné místo.

Získaní nevyužitého místa však nebylo triviální. Veškerá využitá data se totiž musela přesunout na dočasné místo, poté se zmenšil původní LUN na diskovém poli a všechna data se nakopírovala zpět. Celá operace proběhla během jednoho dne, kdy HP Data Protector neprovedl zálohy.

Zrušením původní služby proběhlo ve dvou krocích. Nejprve jsme přestali zálohovat a o týden později jsme smazali původní zálohy. Poté jsme hned přidělilo místo z původního řešení k Veeamu a rozšířili jsme počet bodů obnovení.

Spolupráce a využití DÚ CESNET

Nové řešením nám také otevřelo možnost využívat kapacit DÚ CESNET. Během řešení projektu jsme sice zažili problémy s nedostupností svazku přes protokol NFS. Přesto ale celkově zkušenosti s provozem této služby hodnotíme velice pozitivně. Kromě rozšíření kapacit nám DÚ CESNET vyřešila složitější práci s daty na magnetických páskách.

V rámci testu jsme zkoušeli někdy až extrémní scénáře, např. když jsme využili funkci B&R k přímému spuštění VM ze zálohy úložené na DÚ CESNET v Jihlavě. Spuštění sice nebylo v řádech sekund, ale VM byl spuštěn v rámci jednotek minut. Server určitě nedosahoval výkonu, jako by běžel na našem primárním úložišti, ale dokázal běžet a omezeně poskytovat služby.

Konzultovali jsme se správci DÚ CESNET výsledky našeho projektu. Hlavní diskuze se zabývala problému se stabilitou NFS. Z jejich strany padl návrh na přechod z NFS na jiný protokol nejlépe RSYNC. B&R umí ovšem pracovat s daty, které vidí lokálně na Veeam Repository.

Pokud bude docházet k dodatečnému kopírování dat přes RSYNC, tak je nemůže spravovat Veeam. Musí se vytvořit další aplikace, která se bude starat o případné kopírovaní dat na DÚ CESNET. Aplikace navíc bude muset mít evidenci, který soubor obsahuje jaká data a která záloha závisí na které. Poslední role aplikace je také mazání starých záloh, kde musí být dodržena závislost, protože když dojde ke smazání plné zálohy nebude možné obnovit data ze žádné navazující rozdílové zálohy.

Závěr

Zálohovaní je záležitost, která bývá občas řešena jako jedna z posledních. Je to také dáno tím, že nemá přímý přínos pro chod datového centra. Mnozí si uvědomí důležitost zálohování až v případě, kdy dojde k porušení dat a potřebě tato data obnovit. Navíc při masivním sdílení zdrojů v dnešních datových centrech tyto potíže mohou postihnout daleko větší množství systémů, aplikací i uživatelů než dřív.

S nasazením virtualizace se otevřely nové možnosti, které nyní můžeme využít. Celá služba zálohovaní během tohoto projektu prošla razantní změnou. Je technicky komplexnější ale přitom jednodušší na systémovou správu. Nyní se správa zálohovaných serverů provádí přímo ve VMware vSphere.

Nové řešení zálohovaní je pro správce virtuálních systémů zcela transparentní, protože z jejich strany nejsou nutné žádné technické kroky pro zřízení služby a do zálohovaného systému není potřeba instalovat žádného zálohovacího agenta. Zálohovací systém nyní nemusí mít přistup do zálohovaných systémů, což mj. zlepšuje i bezpečnost celého prostředí.

Jako podstatný problém se během řešení ukázala disková kapacita. Zpočátku byla disková pole sdílena mezi nové i staré řešení a bylo potřeba hlídat volné místo a upravovat počty bodů obnovení, když začalo docházet místo na zálohovacích diskových polích. Zároveň jsme si nemohli dovolit být v jakémkoliv okamžiku přechodu zcela bez záloh.

Rychlost zálohování je nyní omezena pouze výkonem primárního diskového pole. Veeam umí od edice Enterprise řídit rychlost zálohovaní podle odezvy zdrojového úložiště. Umí tedy v případě nadměrné zátěže omezit vytížení způsobené zálohou tak, aby nedošlo k ovlivnění chodu virtuálních serverů. V námi použité edici však tato funkce není, takže je potřeba vyzkoušet kolik paralelních záloh úložiště zvládne.

V rámci projektu bylo úspěšně nasazeno nové řešení zálohování Univerzitního datového centra VŠB-TU Ostrava a to včetně dokumentace, kterou jsme publikovali na dokumentačních serverech CIT VŠB-TU Ostrava. Úspěšně jsme ověřili také spolupráci a ukládání dat do DÚ CESNETu.

Další měsíce nám jistě přinesou další provozní zkušenosti a ukáže se, jakým přínosem by mohly být vlastnosti, které jsou dostupné ve vyšších edicích produktu Veeam.

Aktivní přístup k řešení a spolupráce s výrobcem se projevila i v tom, že Petr Havlíček, jako jeden z řešitelů, byl pozván na konferenci VeeamON fórum 2016, aby na něm prezentoval získané zkušenosti.

Z našeho pohledu tak lze konstatovat, že vytyčené cíle projektu byly splněny a mohou být přínosem zejména pro jiné akademické instituce připojené do infrastruktur sítě CESNET.

Tisková zpráva

Ve spolupráci Centra informačních technologií VŠB-TU Ostrava a Fondu rozvoje CESNETu byl úspěšně realizován projekt Zálohování virtuálních infrastruktur.

Cílem projektu bylo nasazení, zdokumentování a propojení zálohovaní virtuálního prostředí a Datových úložišť sdružení CESNET.

Poznatky získané v rámci tohoto projektu byly také prezentovány na největší české konferenci zaměřené na zálohovaní konané 14.9.2016 v Praze s názvem VeeamON Forum Czech Republic.

Související dokumenty:

- Závěrečná zpráva
- Elektronická příloha

Tato tisková zpráva byla publikována na webu VŠB-TU Ostrava na adrese:
https://www.vsb.cz/info/?reportId=32743&lang=cs&categoryId=45

V Ostravě dne 28. listopadu 2016

Ing. Petr Havlíček