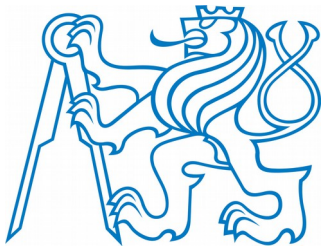
České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra počítačové grafiky a interakce



Zpráva k projektu 493/2013/1

Konsolidace zálohování a archivace dat
Ukládání a zálohování dat s využitím služeb CESNET

Martin Vaňko, Jan Kubr

Prosinec 2014

Úvod

Při řešení projektu bylo nutné navrhnout a implementovat pracoviště usnadňující zálohování a archivaci dat na Katedře počítačové grafiky a interakce. Při návrhu pracoviště bylo nutné zohlednit připojení k datovým úložištím CESNET. Během řešení jsme navrhli několik přístupů k realizaci, které jsme otestovali a poté zvolili a implementovali optimální řešení.

Infrastruktura

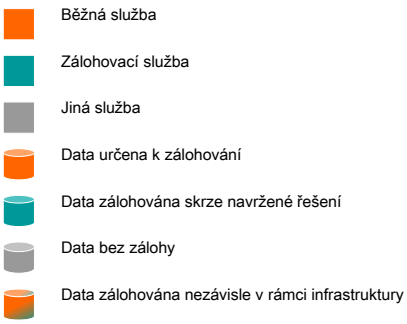
Jedním z cílů tohoto projektu je prozkoumání možností využití datového úložiště sdružení CESNET pro ukládání a zálohování dat. Dále pak bylo cílem návrh a realizace zajišťovací infrastruktury pro zálohování dat a služeb. Výsledkem je služba, nebo-li rozhraní, umožňující snadnou integraci možnosti zálohování do úložiště CESNET pro různorodé jiné infrastruktury, služby či navazující projekty. Z tohoto důvodu byl brán zřetel na co možná nejjednodušší implementaci a konfiguraci, umožňující snadnou přenositelnost a instalaci.

Z pohledu zálohování dat do CESNET se nabízí 3 přístupy realizace:

1. Uložení všech dat přímo v úložišti CESNET
2. Přímé zálohování dat do úložiště CESNET
3. Nepřímé, vrstvené zálohování dat do úložiště CESNET

Každý z těchto přístupů nabízí jisté výhody, ale i nevýhody - jak technologické, tak administrativní, či ekonomické. Našim cílem bylo analyzovat a případně vyzkoušet více možností.

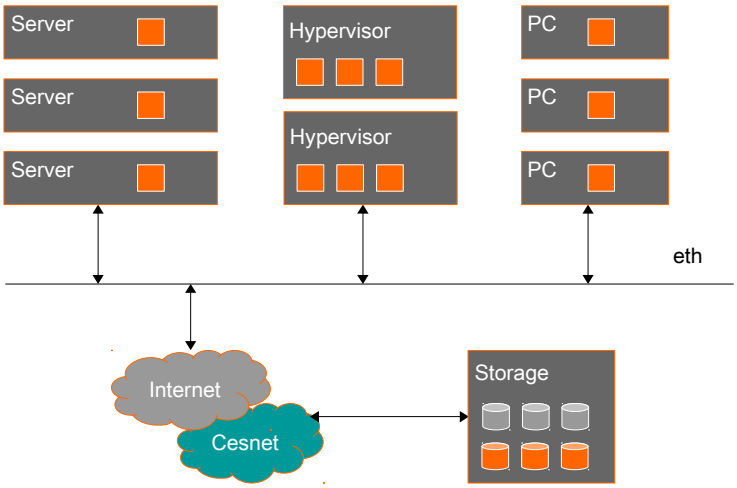
Legenda ke schématům uváděným níže:



Uložení všech dat přímo v úložišti CESNET

Schématický návrh uveden na obrázku níže, popisuje z datového hlediska minimalistickou infrastrukturu, jejíž všechna data, jsou uložena mimo lokalitu klienta. Lokálně jsou uložena pouze provozní data operačních systému nutných pro bootování. V ideálním případě by i tyto mohly být uloženy vzdáleně, ale v současné době je toto z technologického hlediska a možností poskytujících sdružením CESNET neproveditelné.

Z pohledu zálohování dat se jedná o optimální řešení jelikož veškerá uložená data jsou automaticky a transparentně zálohována službami CESNET v rámci jejich technologicky pokročilého systému pro ukládáni dat.



Výhody řešení

Dlouhodobá masivní finanční úspora na technologiích a lidských zdrojích

- Z ekonomického hlediska se jedná o optimální variantu, umožňující drastickým způsobem snížit náklady na provozování vlastního řešení. V tomto konceptu je totiž pro jakýkoli klientský, či infrastrukturní HW potřebné zakoupit pouze minimální diskové řešení a to s ohledem na výkon a kapacitu neboť jakékoli současné nejlevnější diskové řešení dostačuje pro instalaci a provoz všech běžných OS.

Toto řešení tedy umožňuje ušetřit krátkodobé i dlouhodobé náklady za:

- pořízení diskového prostoru
- lidské zdroje potřebné ke konfiguraci, udržování a provozu
- lidské zdroje potřebné k výběru a pořizování včetně veškeré administrativy s tím spojené (obzvláště užitečné pro státní sektor)
- časové a materiální ztráty spojené s poruchami a následnými opravami
- spotřebu elektrické energie
- pronájem prostoru
- chlazení
- budoucí investice související zejména s pravidelnou obnovou

Vysoká kapacita a spolehlivost

- Úložiště CESNET disponuje díky zakoupené technologii robustním řešením pro masivní ukládání dat s kapacitou úložiště v jednotkách PB. Technologie a lidské zdroje jimiž také disponuje umožňují zabezpečení provozu tohoto úložiště na úrovni 24/7, včetně zálohování a archivování dat. Toto řešení je pro univerzitní sektor bezkonkurenční a žádná univerzita si jej interně nemůže dovolit nahradit v takovém rozsahu a zabezpečení.

Nevýhody řešení

Úplná závislost na službách sdružení CESNET

- Provoz klienta je úplně závislý na poskytování těchto služeb. V případě výpadku na straně CESNET, nebo mezilehlého propoje je infrastruktura úplně ochromena po celou dobu výpadku. Dále v případě vypovězení poskytování těchto služeb nastává pro klienta nutnost nahradit všechny aspekty této služby u sebe, nebo jiného, komerčního provozovatele, což bude mít za následek enormní finanční a časové náklady jenž pravděpodobně nebude možné existenčně ustát.

Propustnost a rychlost odezvy dat

- Vzhledem k dislokaci diskového úložiště zde nastává problém s množstvím a rychlostí jednotlivých prvků na aktivní datové cestě od klienta k úložišti. Se zvyšováním počtu prvků na této cestě tedy dochází k výraznému zpoždění v reakčním čase což se vzhledem k velikosti sítového paketu projeví i na celkové propustnosti. Je také dobré si uvědomit, že prvky na této cestě pravděpodobně nebudou dedikovány pouze pro přenos dat klienta, ale budou současně sloužit více klientům najednou a pro více různých účelů. To samé platí přímo i pro diskové úložiště CESNET.

Přetížení provozní konektivity

- Vzhledem k uložení všech dat mimo lokalitu jsou kladeny velké nároky na obsazení pásma klientových uplinků, čímž dochází k degradaci ostatní komunikace poskytované službám a uživatelům. Pro zachování rozumné míry přenosového pásma je klient nucen investovat více finančních zdrojů do své telekomunikační infrastruktury.

Flexibilita a možnosti optimalizace na základě uživatelských potřeb

- Z praxe často vychází potřeba poskytovat data různými způsoby a různými protokoly pro správné fungování na straně uživatele. Někdy může dokonce vyvstat potřeba použití proprietární technologie pro poskytování dat. Toto se sice dá nahradit intermediárními službami poskytovanými na straně IT klienta, nicméně je potřebné si uvědomit, že to přispívá k dalšímu stupni degradace výkonu při přístupu k datům.

Geografická dislokace

- I když se obecně sdružení CESNET považuje za důvěryhodnou autoritu v rámci ČR, může být klient donucen z pohledu svých závazků k požadavku nad plnou kontrolou nad daty. Obecně se může jednat např. o smlouvu o utajení dat mezi klientem a jeho odběratelem jenž ukládá klientovi odpovědnost za omezení nahlížení do dat pouze oprávněným osobám, či službám. Toto však není možné splnit při ukládáni dat do úložiště CESNET bez šifrování, jenž opět degraduje výkon a vytváří zvýšené finanční nároky na práci s daty.

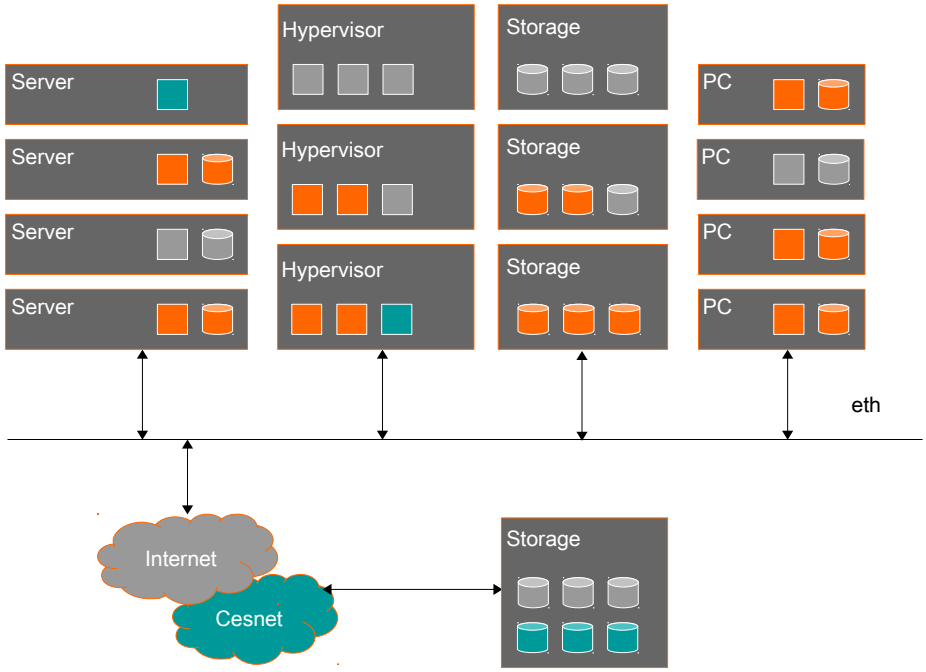
Závěr

Od realizace toho řešení jsme upustili z důvodu výše zmíněných nedostatků. Takovéto řešení představuje de-facto outsourcing úložiště, jenž pro nás také představuje překážku.

Řešení je lákavé jak z ekonomického, kapacitního tak i provozního hlediska. Nicméně není vhodným kandidátem pro prostředí s dynamickými požadavky na IT a zvýšenými nároky na rychlou odezvu a výkon, jaké uživatelé ČVUT FEL požadují v rámci interního provozu. Řešení se spíš jeví vhodné pro organizace s pomalu se měnícím IT a s nízkými nároky na její flexibilitu, jaký představují např. úřady veřejné správy. Nehodí se do prostředí, kde probíhá různorodý aktivní vývoj a výzkum, jakým je ČVUT FEL.

Přímé zálohování dat do úložiště CESNET

Tato varianta řešení spočívá v plné lokalizaci provozních dat u klienta s využitím jeho interní infrastruktury. Všechna data se následně replikují na stranu CESNET, čímž dochází ke geograficky oddělené záloze. Vzhledem k prostorovým možnostem úložiště CESNET je zde také možnost vytvářet i jednodušší zálohy definované v čase a také data archivovat. Níže uvedená schéma tento koncept graficky nastiňuje.



Toto řešení se jeví optimální pro klienta z hlediska flexibility a zvyšování zabezpečení dat se současným snižováním nákladů na dosažení této ochrany. Jelikož jsou operační data provozována na straně klienta, jeho uživatelé získávají flexibilitu jakou od své povahy práce požadují. Navíc jsou data chráněna proti náhodnému smazání, či jejich poškození v důsledku fatálního selhání HW, přírodní katastrofy či jiných neočekávaných okolnostech na straně klienta. To vše za minimální cenu a s nulovými náklady na HW a jeho provoz.

Výhody řešení

Dlouhodobá finanční úspora na technologiích a lidských zdrojích

- Pro standardní zálohování dat je nutné mít stejnou velikost zálohovacího prostoru, než jakou mají samotná data. V případě rozšíření této funkcionality o časové zálohy, případně archivaci vybraných dat tato potřeba ještě vzrůstá. Tím vzrůstá i finanční náročnost na realizaci a udržování takovéto funkcionality.
- Při využití služeb CESNET však nemusí klient investovat do pořízení a provozu těchto zařízení, ani do lidských zdrojů nutných pro jejich provoz. Současně také odpadá nutnost obnovy v čase, což představuje nemalé investice. Také nemusí klient investovat čas a peníze na přizpůsobování zálohovacího řešení reflektující změny produkčního provozu.

Vysoká kapacita a spolehlivost

- Výhodou využití úložiště CESNET je jeho možnost rychle se kapacitně přizpůsobit jakékoli současné infrastruktuře a dokáže téměř okamžitě reflektovat i její nové požadavky a případné změny. V běžné praxi je toto finančně náročné dosáhnout jelikož to při větších změnách obvykle vyžaduje kompletní nahrazení aktuálního zálohovacího řešení.

Nezávislost na službách CESNET

- Jelikož jsou data uložena na straně klienta, není v případě výpadku konektivity, či služeb CESNET nijak omezen jeho běžný provoz. Také v případě vypovězení služeb CESNET klientovi nejsou pro zachování provozu klienta nutné okamžité drastické investice do jeho interní infrastruktury.

Propustnost a rychlost odezvy dat

- Ke zpomalení propustnosti, či odezvy na data v důsledku komunikace s CENSNET nedochází, protože data si spravuje klient sám. Pro zálohování se navíc kriterium rychlosti odezvy stává irelevantní a směrodatná je pouze propustnost sítě. Tento parametr však tolik netrpí počtem prvků na aktivní cestě, či její vzdáleností.

Flexibilita a možnosti optimalizace na základě uživatelských potřeb

- Uživatelské potřeby na si klient reguluje sám. CESNET je využit pouze pro zálohování.

Geografická dislokace

- Jelikož se úložiště CESNET vždy nachází mimo lokalitu klienta, jsou data lépe chráněna proti přírodním katastrofám, či jiným geograficky závislým hrozbám.
- Jako problém se může jevit vystavení citlivých dat třetí straně a tím porušení klientových závazků. Nicméně, jelikož se jedná pouze o zálohy dat je možné tato data bezpečně kryptovat na straně klienta a zašifrovaná je přenášet do úložiště CESNET k záloze. Takovéto omezení navíc není nijak zásadně finančně či časově náročné.

Nevýhody řešení

Zvýšené zatížení provozní konektivity v době zálohování

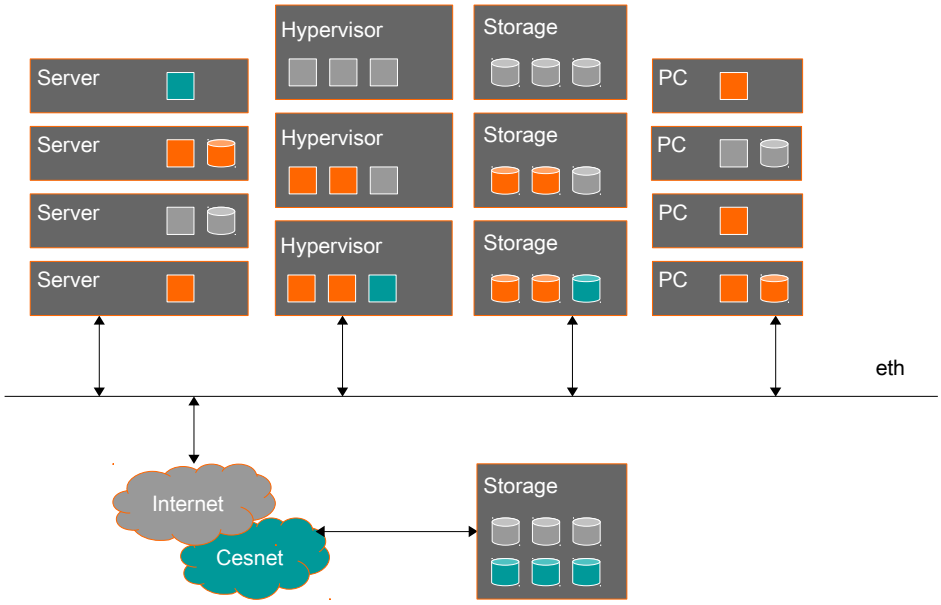
- Jediná nevýhoda spočívá v nutnosti data přenést do vzdálené lokality, čímž automaticky dochází k zatížení konektivity. Toto omezení lze spolehlivě obejít pouze dedikovanou linkou.
- Nicméně v běžných infrastrukturách a při běžných požadavcích na zálohování (obvykle 1x denně) lze toto vyřešit inkrementálním, nebo diferenčním zálohováním a tyto rozdíly navíc přenášet v průběhu noci, kdy běžní uživatelé linku nevyužívají. Pokud toto není možné, je zde ještě varianta omezení přenosového pásma. Praxe ukazuje, že běžné rozdíly v datech v intervalu jednoho dne bývají řádově kolem desítek, maximálně však stovek GB.

Závěr

V době zadávání projektu se nám tato možnost perspektivně jevila jako nejvýhodnější vzhledem k disponující konektivitě a možnostech a parametrech tehdejších úložišť. Nicméně v čase jsme tuto variantu rozšířili o vrstvené zálohování – tzv. zálohovací tiering, jenž popisujeme níže.

Nepřímé, vrstvené zálohování dat do úložiště CESNET

Tento typ zálohování má nevetší smysl tam, kde má klient specifické požadavky na zálohování a je tak nutné jistou úroveň záloh provozovat přímo u klienta. To může být dáno třeba požadavkem na časté zálohovací cykly, kapacitně náročnou fluktuaci změn, nebo obojím současně. Jedná se o finančně nejméně efektivní řešení, nicméně poskytující nejvyšší stupeň rychlosti, flexibility a bezpečnosti dat s nejnižším stupněm zatížení konektivity.



Toto řešení poskytuje prakticky stejné výhody a důvody pro provoz jaké má přímé zálohování. Stírá však do značné míry problém se zatížením konektivity, jelikož si může dovolit optimalizovat zálohovací přenosy a jejich prováděcí časy. Jedinou a značnou nevýhodou je jeho náročnost na finanční, energetické a lidské zdroje.

Závěr

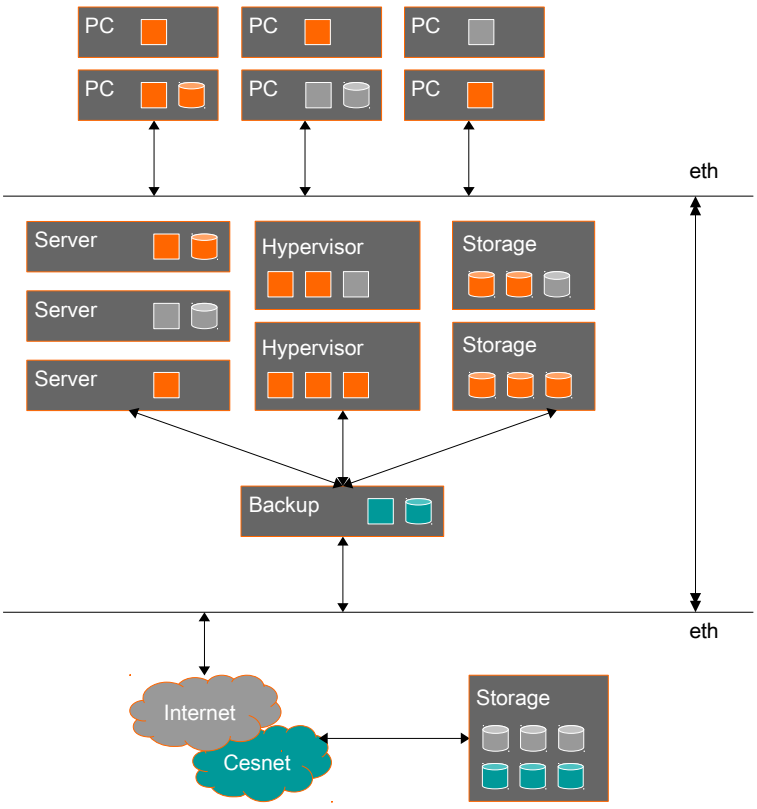
Vzhledem k možnostem jimiž disponujeme jsme se přiklonili k realizaci této varianty. Jelikož se jedná o nadmnožinu přímého zálohování, tak veškerá zjištění při řešení problémů budou uplatnitelná i pro přímé zálohování. Navíc zde můžeme rozebrat a pokrýt náročnější koncepty a myšlenky.

Skutečná realizace a zapojení

Původní koncept

Řešení projektu prošlo několika iteracemi, jež jej tvarovaly různými vstupy od systémů až po uživatele a z nichž zde popisujeme hlavně počáteční a finální fázi. V počátku byla myšlenka na vytvoření komplexního zálohovacího řešení s připojením do CESNET. Nicméně složitost implementace všech postupů do jediného funkčního celku se ukázala spíše jako kontraproduktivní, protože mnoho systémů vyžaduje vlastní specifickou správu a závislosti a současně je nutné se podvolit i parametrům připojujících se infrastruktur. Tím tedy postupně došlo k osvobození zatížené myšlenky na dokonalé zálohovací řešení a na jeho postupné zjednodušování a přenášení jistých odpovědnosti na přímo se připojující infrastruktury.

Původní záměr vycházel z konceptu vytvoření zálohovacího serveru dostupného ve všech sítích a s povoleným přístupem pro jakékoli prvky sítě od úložišť v SAN, přes blade-servery a klasické servery až po jednotlivé uživatele a jejich zařízení. Hned po jeho zavedení narazil tento koncept na bezpečnostní problémy s autorizací, jelikož sdružoval přístup všech oblastí sítě do centrálního místa, ze kterého bylo možné číst data ze všech připojených zdrojů. Běžný uživatel, který z principu není považován za důvěryhodnou entitu, tedy získal de-facto přístup do segmentu infrastruktury kam by se zavedenými bezpečnostními politikami jinak nedostal.



Pokud by se v takovéto konfiguraci vyskytla jakákoli bezpečnostní mezera mohli by být kompromitovány všechny systémy všech infrastruktur na všech úrovních najednou, což není z hlediska utajení některých dat přijatelné. Navíc tímto značně vzrůstá složitost systému, protože ten musí reflektovat bezpečnostní politiky každé připojené infrastruktury.

Řešením tedy bylo navrhnout systém jenž omezí uživatele od přímého přístupu a tím zjednoduší veškerou autorizaci. Hlubší analýzou požadavků a několika interních infrastruktur v našem akademickém okolí a současně i několika komerčních infrastruktur jsme dospěli ke zjištění, že každá námi prozkoumaná infrastruktura vždy provozuje pro uživatele sdílené úložiště pro běžný provoz. Současně jsme zjistili, že každé takového úložiště má již vyřešenou autorizaci vlastních uživatelů a to vždy po svém a různě vzhledem k ostatním.

Abychom tedy dosáhli nejvyšší možné efektivity při zprostředkovávání našeho řešení bylo potřebné nastavit systém tak, aby se mu ostatní nemuseli zásadním způsobem přizpůsobovat. Bylo tedy potřebné minimalizovat problém s autorizací a vymyslet, jakým způsobem budou uživatelé a služby jednotlivých různých systému moct zálohovat svoje data.

Řešení tedy spočívalo ve vystavění zjednodušeného intermediárního systému s agregací jednotlivých datových úložišť a datových služeb. Autorizace přístupu se převedla a zjednodušila z různých možných systémů na správce zálohovacího řešení, jenž se pak musí smluvně definovat jako důvěryhodní, nebo zpětně na správce zálohovaného systému. V druhém případě je takovému správci z našeho systému pouze poskytnuta kapacita pro přímé zálohování. Zálohovací proces si v takovémto případě správce úložiště řeší sám. Dále se tímto správa systému centralizovala do jediného místa a tím i zpřehlednila.

Finální řešení

Realizace výše uvedeného konceptu spočívá v nainstalování stabilní linuxové distribuce s možností importu a exportu různých protokolů pro přenos dat a vybraných datových služeb. Jako základ jsme tedy zvolili linuxovou distribuci Debian ve verzi 7. Bližší analýzou jednotlivých infrastruktur jsme dospěli k rozhodnutí o zprovoznění datových protokolů:

- SMB/CIFS
- NFS
- iSCSI

V žádné z prozkoumaných infrastruktur jsme nenašli službu, jíž by některý z uvedených protokolů nevyhovoval, nebo jehož připojení by nebylo možné jednoduše bez narušení interního provozu dosáhnout. Tyto protokoly s výjimkou iSCSI je možné provozovat obousměrně, tedy jak se na zálohované datové úložiště připojovat, tak mu poskytovat zálohovací prostor pro přímé zálohování.

Dále jsme pro výběr datové zálohovací služby prozkoumali několik možností, jmenovitě to byl software:

- Rsync
- Rdiff-backup
- Duplicity
- Rsnapshot
- BackupPC
- Amanda
- Bacula

Po podrobné analýze jsme si zvolili jako hlavní datovou zálohovací službu agentní software Bacula jenž jsme pak zprovoznili a nakonfigurovali pro možnost zpětného zálohování serverů a služeb bez centrálního úložiště. Tento typ zálohy nevyužívá výhod zálohovacího mezistupně a je zálohován přímo do úložiště CESNET. Jelikož se ale jedná o technologii založenou na agentním přístupu zvolili jsme jako alternativní zálohovací software program Rsync pro podporu systémů, nebo řešení jenž nám provoz agentního zálohování neumožní. Jedná se o nejjednodušší avšak výkonnou variantu, jenž dokáže mezi úložišti přenášet pouze rozdíly v datech a vše bez složitých konfigurací.

Princip fungování služby spočívá v myšlence, že jednotlivé servery, či služby buďto dostanou přidělenou kapacitu pro přímé zálohování, nebo jsou jejich datová úložiště připojena k našemu serveru. V prvním případě si zálohování může provádět správce dotyčného systému sám, nebo může požádat o složitější zálohovací konfiguraci správce zálohovacího serveru, jenž mu skrze agentní technologii softwaru Bacula tuto službu poskytne. V ostatním případě nastavuje a provádí konfigurace záloh správce zálohovacího serveru.

Řešení zálohovacího serveru jsme původně plánovali jako dedikovaný server s rychlým síťovým připojením. Postupně v čase jsme ale dospěli k názoru, že by tato investice nebyla optimální. Proto jsme zálohovací server virtualizovali do infrastruktury určené pro projekt a zpřístupnili jeho používáni i některým externím infrastrukturám. Tím jsme navíc vyzkoušeli i reakce našeho systému na integraci externí infrastruktury. Virtualizace nám dále umožnila možnost využití bezvýpadkového provozu v případech poruchy, nebo servisního zásahu. Hlavně však umožnila jednoduchou, ale komplexní vzdálenou správu serveru a škálování výkonů a možností serveru. To vše včetně škálování CPU, RAM, interních disků, síťových prvků apod.

Infrastruktura

Současná infrastruktura pozůstává celkem ze 4 fyzických serverů a několika síťových prvků, zakoupených částečně z prostředků poskytnutých CESNET v rámci tohoto projektu. V základu se jedná o:

- Primární hypervisor
- Záložní hypervisor
- Primární úložiště
- Záložní úložiště
- 10GbE síťový propoj

Konfigurace primárního hypervisoru

- Fujitsu Primergy RX350 S8
- 2x CPU Intel Xeon E5-2650, 8-core @ 2.6GHz
- 192GB DDR3 RAM @ 1600MHz
- 5x 600GB SAS @ 15k rpm
- 2x 1GbE
- 2x 10GbE

Konfigurace záložního hypervisoru

- Supermicro X7DW3
- 2x CPU Intel Xeon E-5440, 4-core @ 2.8GHz
- 72GB DDR2 RAM @ 667 MHz
- 2x 120GB SATA @ 7200rpm
- 2x 1GbE
- 1x 10GbE

Konfigurace primárního storage

- DELL PowerEdge R515
- 2x CPU AMD Opteron 4184, 6-core @ 2.8GHz
- 32GB DDR3 RAM @ 1333 MHz
- 2x 146GB SAS @ 10k rpm
- 10x 4TB SAS @ 7200rpm
- 2x 128GB SSD SATA
- 2x 1GbE
- 2x 10GbE

Konfigurace záložního storage

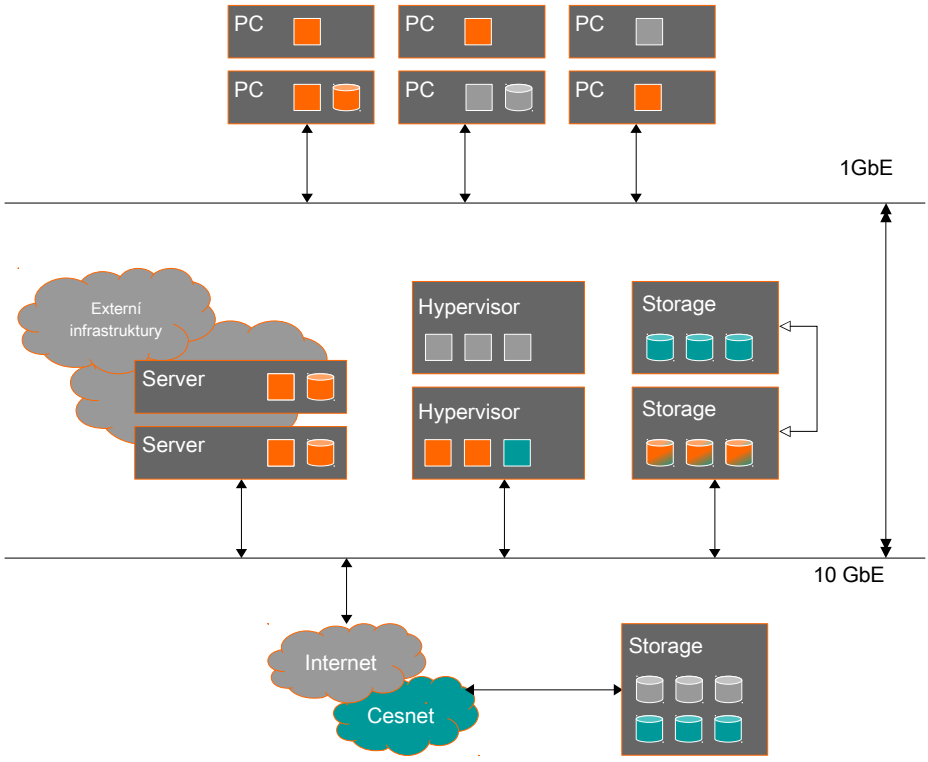
- 2x CPU AMD Opteron, 6-core @ 2.2GHz
- 32GB DDR3 RAM @ 1333 MHz
- 22TB SATA HDD
- 2x 1GbE

Propojovací switch

- Extreme networks Summit X670
- 48 x 10GbE SFP+
- Layer 3 switch

Realizace

Aktuální schéma reálného provozního zapojení je uvedena níže. Domovská infrastruktura v ní hostuje zálohovací řešení a díky její celkové virtualizaci a centralizaci dat může poskytovat naše řešení zálohovací služby přímo datovým úložištím a tím prakticky všem datům v infrastruktuře. Tímto dochází také k odlehčení komunikačních linek pro přístupy ke službám, jelikož datová linka je fyzicky oddělena do sítě SAN a propojení našeho řešení je díky virtualizaci bez-nákladové a rychlé.



Dále vzhledem k veliké fluktuaci objemu dat hostující infrastruktury (desítky GB za hodinu, nebo stovky GB za den) a naší snaze o snížení zatížení síťového provozu zde s výhodou využíváme konceptu vrstveného zálohování. Primární úložiště poskytuje zálohování veškerých dat domovské infrastruktury specifickým způsobem a dle jejích potřeb v častých intervalech několikrát za den. Navíc jsou datová úložiště sestavena v replikaci dat, z důvodu ochrany proti selhání HW a z výkonnostních důvodů propojena dedikovanou linkou.

Místo toho abychom tedy přenášeli tyto značné a časté objemy dat (navíc nad převážně stejnými daty), necháváme na hostující infrastruktuře zajistit si její lokální potřeby častých záloh individuálně. Pak jednou denně pomocí programu Rsync projdeme na blokové úrovni rozdíly v datech a tyto přeneseme do CESNET. Navíc abychom nezatěžovali již tak zatížený primární storage, se všechny tyto operace dějí nad úložištěm zálohovacím, jenž aktivně neparticipuje na operacích s daty.

Díky námi navrženému řešení nám nezáleží, které úložiště, nebo server budeme připojovat. Všechny tyto operace mají pro nás v realizovaném konceptu stejnou složitost. V tomto případě nám záložní úložiště poskytne veškerá svá data skrze NFS přes zabezpečenou linku v síti SAN. Naše řešení se pak pouze postará o pravidelné zazálohování poskytnutých dat do CESNET. Dále správce hostující infrastruktury poskytne svým uživatelům prostor pro zálohování svých zařízení na vlastní úložiště skrze vlastní autentizační a autorizační mechanizmus. Jelikož si však uživatelé nahrají svá data na úložiště jenž se zálohuje skrze naše řešení jsou tak i jejich data zálohována do CESNET.

V případě, že na centrálním úložišti infrastruktury připojené k našemu řešení nemá její správce dostatek místa pro takovéto uživatelské zálohování, bude mu poskytnut přímo prostor z úložiště CESNET skrze naše řešení exportem vyhrazeného adresáře. Ten si pak externí správce může integrovat do vlastního úložiště např. v podobě speciálních zálohovacích adresářů.