LINUX SERVICES

Doporučení k zabezpečení datového úložiště

Draft

Z hlediska zákona o kybernetické bezpečnosti

Ing. Jiří Richter
Ing. Michal Vymazal

Leden 2016

Úvod

Tato doporučení se vztahují k bezpečnostní dokumentaci a bezpečnostním opatřením subjektů (právnické osoby, fyzické osoby) na něž se vztahuje zákon 181/2014 Sb. (Zákon o kybernetické bezpečnosti).

V textu jsou vždy uvedeny názvy jednotlivých dokumentů technického projektu, jednotlivá doporučení a odkazy na jednotlivé dokumenty (EU, NIST), dle kterých jsem doporučení zpracovával.

Obsah

Pojem „datové úložiště“

Datové úložiště je zařízení určené pro individuální uživatele nebo pro skupiny uživatelů umožňující vzdálené ukládání a skladování dat. Vlastní data (v nejrůznější digitální podobě – soubory, kontakty, odkazy, kalendáře, chat, konverzace apod.) je možné mezi uživateli (nebo skupinami uživatelů) sdílet. Vlastní přístup k úložišti je uskutečňován jednak prostřednictvím www prohlížeče jednak prostřednictvím tzv. „synchronizačních“ klientů, které dokáží automaticky synchronizovat data mezi různými počítači a mobilními zařízeními uživatele. Požadavkem doby je fakt, aby vlastní řešení bylo tzv. „platform independent“ a dále musí být umožněna propojitelnost mezi různými architekturami, řešeními, platformami. Výhodou je nezávislost na konkrétním prodejci či výrobci. Vhodné je rovněž řešení bez závislosti na komerční licenci produktu. Dostupnost zdrojových kódů programového vybavení je rovněž velmi významným faktorem a to z hlediska bezpečnosti, dostupnosti a transparentnosti celého řešení.

Důležitým faktorem je rovněž požadavek na umístění fyzických zařízení (včetně datových médií) vlastního datového úložiště.

Zákon o kybernetické bezpečnosti

Legislativa

http://www.govcert.cz/cs/legislativa/legislativa/

- Usnesení vlády ze dne 19.10.2011 č.781
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

  (http://www.nbu.cz/cs/aktuality/1262-vlada-2-ledna-2014-schvalila-navrh-zakona-o-kyberneticke-bezpecnosti/)
- Důvodová zpráva k zákonu
- Vyhláška k zákonu o kybernetické bezpečnosti
- Důvodová zpráva k vyhlášce
- Vyhláška o stanovení významných informačních systémů a jejich určujících kritériích

Metodiky

- Metodiky – Národní bezpečnostní autority EU

  https://www.bsi.bund.de/EN/Publications/BSIStandards/standards.html
- Implementační scénáře - Národní bezpečnostní autority EU, NIST

  https://gsb.download.bva.bund.de/BSI/ITGSKEN/IT-GSK-13-EL-en-all_v940.pdf

Legislativa

Gestorem oblasti kybernetické bezpečnosti je v ČR **Národní bezpečnostní úřad** (známý též pod zkratkou NBÚ). Stalo se tak usnesením vlády ze dne 19. října 2011 č. 781 o ustanovení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. NBÚ následně vypracoval **Návrh zákona o kybernetické bezpečnosti**, jež vláda schválila. NBÚ dále vypracoval návrh vyhlášky o kybernetické bezpečnosti a vydal prohlášení k vývoji legislativy v oblasti kybernetické bezpečnosti.

Zákon o kybernetické bezpečnosti byl podepsán prezidentem Milošem Zemanem dne 13.8.2014. Zákon nabyl platnosti dnem vyhlášení ve Sbírce zákonů, účinný je od 1. ledna 2015.

Prováděcí právní předpisy k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) jsou následující:

- NAŘÍZENÍ VLÁDY č. 315/2014 Sb. ze dne 8. prosince 2014, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
- VYHLÁŠKA ze dne 15. prosince 2014 č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
- VYHLÁŠKA ze dne 15. prosince 2014 č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích

Viz.
http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/provadeci-pravni-predpisy-k-zakonu-c-1812014-sb-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu/

V této souvislosti je dobré připomenout, že i Trestní zákoník zná trestné činy související s neoprávněnými přístupy do informačních systémů, konkrétně **§ 230** nazvaný "Neoprávněný přístup k počítačovému systému a nosiči informací".

Nový občanský zákoník pak pamatuje na škodu způsobenou informací nebo radou (§ 2950 NOZ).

Metodika / Národní autority

Dle prohlášení ředitele NCKB (Národní centrum kybernetické bezpečnosti, odbor NBÚ), NCKB do vlastního zákona zapracuje odkazy na související normy a metodiky (např. ISO 27032). Dále bude respektovat metodiky relevantní (např. metodiky národních autorit členských zemí EU, NIST atp.)

Implementační scénáře

Tato otázka zatím není řešena ani legislativně, ani metodicky. Předpokládáme, že zde se situace začne rychle měnit a implementační scénáře budou jednak veřejně dostupné, jednak budou navazovat na metodiku. K dnešnímu dni můžeme odkázat na vzorové implementační scénáře volně dostupné na stránkách německé národní autority (BSI).

Metodika / ISO

Dle prohlášení ředitele NCKB (Národní centrum kybernetické bezpečnosti, odbor NBÚ), NCKB do vlastního zákona zapracuje odkazy na související normy a metodiky (například ISO 27032). Dále bude respektovat metodiky relevantní (například metodiky národních autorit členských zemí, NBÚ – Česká národní bezpečnostní autorita, BSI – Německá národní bezpečnostní autorita, EU Council – poradní orgán EU, NIST - National Institute of Standards and Technology USA atp.).

Z již výše zmíněné řady ISO 27000 si dovoluji připomenout následující ISO normy:

- ISO/IEC 27031:2011 (Business Continuity)
- ISO/IEC 27032 (Cybersecurity)
- ISO/IEC 27033 (Network Security)
- ISO/IEC 27034 (Application Security)
- ISO/IEC 27035:2011 (Incident Management)
- ISO/IEC 27036 (Supplier Relationships)
- ISO/IEC 27037 (Guidelines for identification, collection, acquisition and preservation of digital evidence)
- ISO/IEC 27039 (IDS)
- ISO/IEC 27040 (Storage Security)

Bezpečnostní dokumentace / popis procesů

Vzhledem k faktu, že licence ISO dokumentů neumožňuje jejich „volnou“ distribuci a dále vzhledem k faktu, že ISO dokumenty nezahrnují tzv. „best practice“, rozhodli jsme se (v souladu s Č.j.: 1649/2013-NBÚ/41) využít pro jednotlivá doporučení metodik a dokumentů národních bezpečnostních autorit EU (BSI – Německá národní bezpečnostní autorita, *Bundesamt für Sicherheit in der Informationstechnik*) a NIST (National Institute of Standards and Technology, USA).

Níže uvedené dokumenty a procesy jsou v souladu s Přílohou č.4 Vyhlášky k ZKB (Vyhláška o kybernetické bezpečnosti).
http://www.govcert.cz/cs/legislativa/legislativa/

Primárními a podpůrnými aktivy jsou v tomto případě jednotlivé moduly datového úložiště. Vlastní topologie, zabezpečení a funkčnost datového úložiště jsou popsány dále v textu.

Výchozí dokumenty EU / NIST

Pro potřeby tohoto dokumentu jsem vycházel z těchto metodik a dokumentů národních bezpečnostních autorit EU:

BSI

BSI-Standards

https://www.bsi.bund.de/EN/Publications/BSIStandards/standards.html

BSI: Private Cloud: Sicherer Betrieb von ownCloud

https://www.bsi.bund.de/DE/Themen/CloudComputing/Dossiers/Anwender/AnwenderProfessionals/AnwenderProfessionals.html;jsessionid=E28E520B1538B09193E8707291A15F93.2_cid286?notFirst=true&docId=6259948

BSI: IT-Grundschutz-Kataloge

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

Moduly

S 2.5 Data media archives
S 2.9 Computer centre

BSI: Security Recommendations for Cloud Computing Providers

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.html

BSI: B 3.303 Storage systems and storage networks - 9. EL Version 2007 - moduleb03303_pdf

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/moduleb03303_pdf.pdf?__blob=publicationFile

BSI: Preliminary Version of Module Cloud Management

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/PreliminaryVersions/Module_Cloud_Management.html

NBU

Národní strategie kybernetické bezpečnosti české republiky na období let 2015 – 2020

http://www.govcert.cz/cs/informacni-servis/strategie-a-akcni-plan/

Výkladový slovník kybernetické bezpečnosti

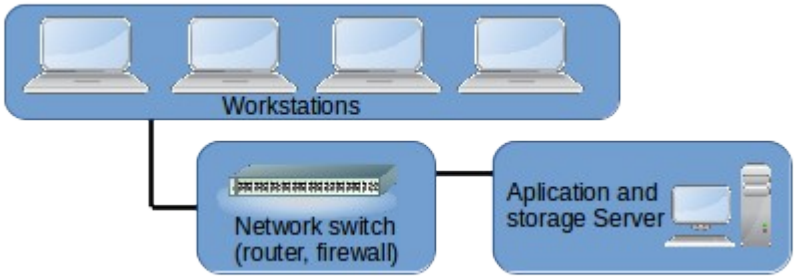
http://www.govcert.cz/cs/informacni-servis/vykladovy-slovnik/

Zařízení pro ukládání dat (Data Storage)

Jsou dva přístupy k ukládání dat na pevné disky: jedním je mít uložiště — pevný disk(-y) — připojený přímo k serveru, na kterém běží aplikace. Druhý přístup je oddělit řešení datového úložiště od serveru, který provozuje aplikaci.

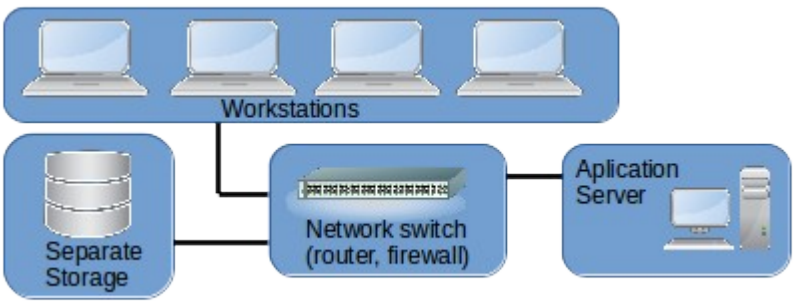
- Přímo připojené úložiště (DAS - Direct Attached Storage)
- Oddělené úložiště: Ukládací prostor připojený k síti (NAS) a Síť ukládacích prostorů (SAN)
- RAID (Redundant Array of Independent Disks)

Přímo připojené úložiště (DAS)



Tento způsob představuje nejběžněji používané řešení pro ukládací prostor na pevných discích pro instalace malé a střední velikosti. Pevný disk(-y) je umístěn ve stejném počítači, na kterém běží aplikační software (aplikační server). Dostupný prostor určuje počítač, respektive počet disků, které pojme. Většina počítačů pojme dva pevné disky, některé až čtyři. Každý disk může mít objem až kolem 4000 GB. To přináší celkovou kapacitu úložiště kolem 8 TB (Terabytu - 1000 Gigabytů).

Oddělené úložiště



V aplikacích, ve kterých požadavky na objem uložených dat a nástroje pro správu

překračují omezení přímo připojeného ukládacího prostoru, je vhodné použít systém odděleného úložiště. Ta dělíme na ukládací prostor připojený k síti (**NAS**) a Síť ukládacích prostorů (**SAN**).

NAS (Network Attached Storage)

Ukládací prostor připojený k síti tvoří jedno ukládací zařízení, které je přímo připojeno k síti a nabízí společný ukládací prostor všem uživatelům sítě. Zařízení typu NAS se jednoduše instaluje a spravuje, poskytuje levné řešení požadavků na ukládací prostor, ale má omezenou propustnost pro příchozí data.

SAN (Storage Area Network)

Síť ukládacích prostorů (**S**torage **A**rea **N**etwork) je vysokorychlostní síť, která je určena pro ukládání a je propojena s jedním nebo více servery pomocí optického vlákna. Uživatelé mají přístup k jakémukoli zařízení v SAN přes server(-y). Ukládací prostor typu SAN lze **rozšířit na stovky terabytů**. Centralizované úložiště snižuje nároky na administrační čas a poskytuje výkonný, flexibilní ukládací prostor pro použití v prostředí více serverů.

Rozdíl mezi NAS a SAN je v tom, že NAS je zařízení, kde je celý soubor uložen na jednom pevném disku, zatímco SAN se skládá z mnoha zařízení, kde může být jeden soubor uložen blok po bloku na několika pevných discích. Tento typ konfigurace pevných disků umožňuje vytvořit rozsáhlé a škálovatelné řešení, kde je možné bezpečně uložit velké množství dat.

RAID (Redundant Array of Independent Disks)

RAID je metoda využívající standardní pevné disky tak, že je operační systém vidí jako jeden velký logický disk.

Jsou různé úrovně RAID, které nabízí různé úrovně replikování dat - od téměř žádné až po "hot swap" řešení, kde výpadek jednoho pevného disku nezpůsobí žádný problém v chodu systému ani žádnou ztrátu dat.

Nejběžnější úrovně RAID ukazuje následující tabulka.

Druh RAID	Popis
RAID-0	Data se rozdělují na dva nebo více pevných disků, což zrychluje zápis a čtení, ale také zvyšuje riziko ztráty dat.
RAID-1	Také známý jako zrcadlení (mirroring) disků. Dva nebo více pevných disků ukládají stejná data. Jde tedy o čistou replikaci dat. Rychlost zápisu je stejná jako při jednom fyzickém disku.

Druh RAID	Popis
RAID-5	Obsahuje pole disků s měnící se úlohou, což umožňuje překrývání všech operací čtení a zápisu. RAID-5 uchovává informace pro rekonstrukci souborů v případě výpadku jednoho disku. RAID-5 potřebuje minimálně 3 pevné disky a běží až s 16 disky v poli. Zvušuje jak rychlost čtení tak bezpečnost uložení.

Fyzický návrh datového úložiště

Volba hardware závisí na několika faktorech:

1. Potřebná celková kapacita úložiště
2. Požadovaná doba odezvy
3. Počet realizovaných spojení
4. Rychlost přenosu dat

Požadovaná maximální kapacita úložiště bude první určující faktor pro výběr vhodného šasi úložiště. Bude však ještě rozhodovat požadovaná rychlost přenosu dat a počet realizovaných spojení během provozu.

Při volbě maximální kapacity bereme v úvahu, že pro způsob ukládání dat do pole RAID1, potřebujeme dvojnásobný počet fyzických pevných disků oproti vypočítané kapacitě.

Např. pro úložiště s maximální kapacitou 12TB budeme potřebovat 2x 3ks 4TB HDD, tedy celkem 6ks HDD s kapacitou 4TB.

Dnešní disky pro servery mají kapacity zhruba v tomto rozsahu kapacit:

SATA disky pro pole RAID od 250GB do 6TB

SAS disky pro výkonnější pole od 300GB do 1,2TB

Celkovou kapacitu úložiště musíme vždy stanovit s dostatečnou rezervou.

Blokové schéma

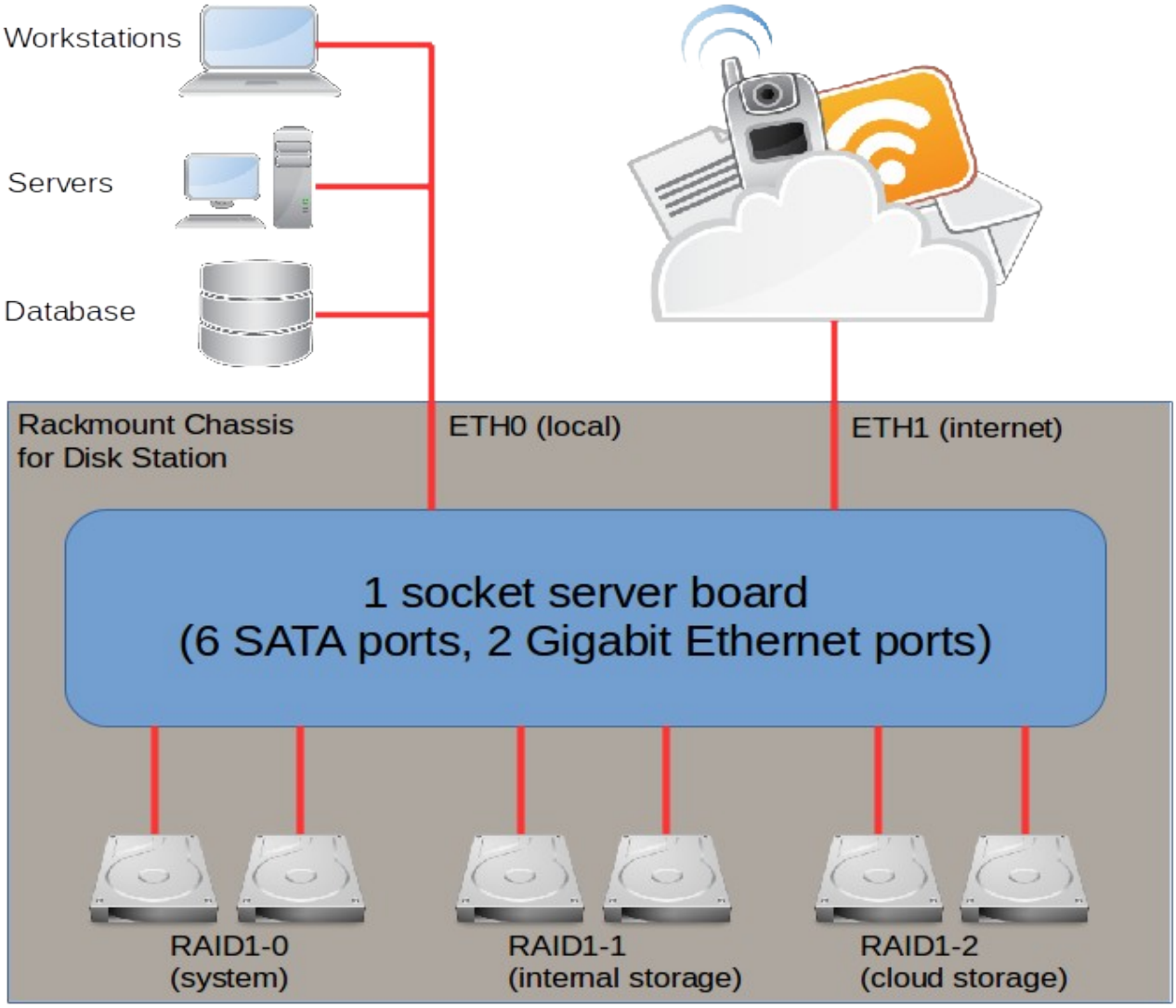


Schéma znázorňuje obvyklé zapojení jednoho fyzického datového úložiště. Toto rozdělení se dvěma oddělenými porty pro připojení k síti vyhovuje menším i středně velkým nasazením úložiště.

Standardy síťových protokolů

Pro přístup k úložiště po síti používáme některý z protokolů, který umožňuje připojení vzdáleného úložiště tak, jako kdybychom pracovali s lokálním diskem. Prvním představitelem takového protokolu je standard NFS. Dále je možno instalovat protokoly iSCSI, CIFS apod.

NFSv3

Verze 3 (RFC 1813, červen 1995) přinesla:

podporu pro 64-bitové velikosti souborů a offsety, což umožnilo použití souborů větších než 2 GB;

podporu asynchronního zápisu na server, pro zlepšení výkonu zápisu;

dodatečné atributy souborů v mnoha odpovědích, aby se zamezilo nutnosti je znovu dohledávat;

operace READDIRPLUS, umožňující získat souborové deskriptory a atributy při prohledání adresáře;

řadu dalších vylepšení.

V době představení verze 3 se výrazně zvýšila podpora výrobců protokolu TCP jako transportní vrstvy.

Viz https://en.wikipedia.org/wiki/Network_File_System

NFSv4

Verze 4 (RFC 3010, prosinec 2000; poslední revize v RFC 7530, březen 2015)

V dnešních moderních distribucích se téměř výhradně setkáme s nástupcem NFS verze 4, který se, ačkoli z uživatelského hlediska vypadá téměř totožně, přece jen od svého předchůdce hodně liší. Základní odlišnosti jsou:

Pseudo file systém - NFSv4 vyžaduje exportovat nějaký adresář jako kořen. To se provádí dodatečným parametrem fsid=0

Stavový protokol - na rozdíl od svého předchůdce, který byl v jádru bezestavový (démony rpclockd a spol mu sice dodávají stavovost ale nejsou definovány v RFC a nejsou součástí protokolu NFS) je NFSv4 protokol stavový, což mu dodává, kromě nevýhody větší složitosti i pár výhod, jako například delegování čtení nebo zápisu na klienta, nebo například zamykání souborů. NFSv4 nepotřebuje portmapper.

Přenos ACL - NFSv3 přenos přístupových práv neřeší. Naproti tomu jsou ACL nedílnou součástí protokolu NFSv4. Nutno ale říci, že protokol NFSv4 definuje vlastní formát ACL, který je odlišný (lepší) od formátu Posix ACL, který ale nebyl nikdy standardizován.

Jednodušší tunelování přes firewall - na rozdíl od svého předchůdce vyžaduje NFSv4 pro svůj běh mezi klientem a serverem otevřen jen jediný, předem definovaný port.

mapování uživatelů - NFSv4 byl vyvíjen primárně jako multiplatformní síťový souborový systém, takže na rozdíl od svého předchůdce nepřenáší User ID (UID, typické pro unix), ale doménové jméno ve formátu username@doména. Z tohoto důvodu je nutné, aby na Unixových systémech (klientu i serveru) běžel pomocný program starající se o překlad jmen na UID - obvykle je to démon rpc.idmapd

větší bezpečnost - kromě klasické "systémové" bezpečnosti, která je notoricky nebezpečná, protokol NFSv4 umožňuje využití i silnějších bezpečnostních mechanismů, jakým je např. Kerberos.

iSCSI

Internet Small Computer System Interface (zkratka iSCSI) je v informatice síťový protokol, který umožňuje připojovat úložný prostor (např. diskové pole) pomocí počítačové sítě.

Charakteristika

Koncepce iSCSI vychází ze dvou technologií. SCSI rozhraní pro připojování disků v serverech a protokolu TCP/IP.

Z rozhraní SCSI se používá pouze protokol, kterým spolu zařízení komunikují a zcela opouští jeho fyzickou vrstvu (kabely, konektory, elektrickou specifikaci). Pro přenos paketů SCSI se použije jejich zapouzdření do protokolu TCP/IP.[1]

Norma iSCSI používá vlastní terminologii: Pokud u SCSI hovoříme o adaptéru a disku, adaptér nám nahradí komponenta, která se jmenuje Initiator, a cílové zařízení (disk/diskové pole, případně pásková jednotka) se nazývá Target.[1]

Rozhraní iSCSI je běžně dostupné na většině platforem. Lze tak snadno ukázat notebook s terabytovým diskem - disk připojený přes iSCSI se chová úplně stejně, jako disk připojený na lokální řadič, je vidět i ve Správci disků.[1]

Viz https://en.wikipedia.org/wiki/ISCSI

Operační systém

Jako operační systém je vhodná jedna z osvědčených linuxových distribucí, které jsou převážně šířeny pod nekomerční licencí GNU GPL 2.0, popřípadě LGPL 2.1.

Doporučené distribuce jsou např. UBUNTU Server LTS, Debian, CentOS.

http://www.ubuntu.com/server

http://www.debian.org/

http://www.centos.org/

HW, vhodný pro úložiště dat

Uvedené úložiště je určené pro menší skupinu uživatelů (záleží samozřejmě na četnosti přístupů k úložišti, ale obecně lze toto úložiště provozovat s desítkami připojených uživatelů) a cílová maximální kapacita je okolo 10TB. Pro tento účel plně vyhovuje šasi 2U do rack skříně s šesti pozicemi pro disky 3,5“. Je možno využít jak disky SATA, tak i SAS, to podle typu řadiče na základní desce. Výsledné zařízení bude sloužit samostatně jako úložiště typu NAS s podporou CLOUD.

Šasi bude osazeno zdrojem o maximálním výkonu 500W, průměrná spotřeba se však může pohybovat okolo 100W. Jeden disk SATA během provozu odebírá cca 10W, disky SAS mohou odebírat až 20W. Vyšší zatížitelnost zdroje je nutná kvůli celkové stabilitě zařízení. Pro zvýšení spolehlivosti se používají zdroje s menšími energetickými ztrátami (účinnost min.85%).

Protože je požadována spíše vyšší kapacita disků než jejich rychlost a krátká doba odezvy, zvolili jsme všechny disky SATA a základní deska tedy má pouze řadič SATA. Musí mít ale dvě Gigabitové síťové karty, jednu pro připojení do interní sítě a druhou pro připojení do veřejné sítě.

Disky budou pro zvýšení spolehlivosti a omezení vlivu chyb organizovány do pole typu RAID1, tedy mirroring, kdy dva identické disky obsahují stejná data. V případě výskytu chyby pak o data nepřijdeme a pouze musíme vyměnit jeden vadný disk. První pole, na kterém bude systém, je složeno ze dvou disků WD RAID SE 2TB, vhodných právě pro cloudová úložiště.

Na úložiště instalujeme OS Ubuntu 14.04 LTS, 64-bit, podporu pro NFS v4 a OwnCloud.

První pole RAID je rozděleno na oddíl pro systém, který má 100GB na formátu ext4. Na něm je nainstalován OS Ubuntu 14.04 LTS, 64-bit, s podporou pro NFS v4 a OwnCloud.

Další část je rozdělena na oddíl pro uživatelské složky a pro OwnCloud. Tyto oddíly jsou na formátu ext3, který je pro datové oddíly vhodnější.

Programové vybavení datového úložiště

Jak již bylo řečeno výše, velmi důležitým faktorem je dostupnost zdrojového kódu vlastního programového vybavení, dalším faktorem pak je vývojový cyklus kódu a samozřejmě podpora z řad sponzorů.

Níže si dovolíme představit řešení, které má podporu národních bezpečnostních autorit členských zemí EU, v našem případě se jedná o BSI (Německá národní bezpečnostní autorita, *Bundesamt für Sicherheit in der Informationstechnik*) viz. kapitola Výchozí dokumenty EU / NIST na straně 10.

Řešení ownCloud

Jedná se o programové vybavení na bázi klient-server pro vytváření a hostování datových úložišť na bázi „file-hosting service“.

https://en.wikipedia.org/wiki/OwnCloud
https://owncloud.org/

Ověřování uživatelů (klientů) vůči serveru se může dít na bázi adresářové struktury (zde LDAP) nebo na bázi samostatné databáze (součástí owncloud instalace), kde jsou uložena přihlašovací data (uživatelské jméno, hash hesla uživatele apod.).

Vlastní projekt owncloud je open source (konkrétně pod AGPLv3 licencí), je však možné dokoupit komerční podporu nebo se zapojit do owncloud komunity. Projekt je „platform-independent“, v současné době může jak klient, tak server běžet na řadě operačních systémů (viz. https://owncloud.org/install/).

Proti svým komerčním rivalům má balík ownCloud nepřehlédnutelné výhody, které lze rozepsat následovně:

- Jednoduchá instalace
- Možnost využití verze s nekomerční licencí
- Podpora aplikací třetích stran
- Textový editor
- Správce souborů
- Verzování
- Galerie
- Kontakty
- Kalendář
- Podpora více uživatelů
- Synchronizační klient pro Linux/Windows/Mac OS X
- Umístění dat dle vlastní vůle
- Aktivní vývoj
- Otevřený zdrojový kód (je myšlena větev kódu pod AGPLv3 licencí)

Velmi sympatické jsou zvolené technologie. Pro přístup k datům se používá WebDAV, ke kontaktům CardDAV, pro kalendář CalDAV. Pro přístup skrze www prohlížeč budete využívat protokol HTTPS. Vlastní jádro programového vybavení je napsané v široce podporovaném jazyce PHP.

Serverovou část datového úložiště můžete nainstalovat na stroj (nebo stroje) dle vlastního výběru a ve vámi zvolené lokalitě.

Serverovou část lze provozovat pouze na strojích s OS Linux, přesný výčet požadavků na server je uveden níže.

Blíže zde:
https://doc.owncloud.org/server/9.0/admin_manual/installation/system_requirements.html

https://doc.owncloud.org/server/8.2/admin_manual/installation/system_requirements.html

Supported Platforms

- Server: Linux (Debian 7, SUSE Linux Enterprise Server 11 SP3 & 12, Red Hat Enterprise Linux/Centos 6.5 and 7 (7 is 64-bit only), Ubuntu 12.04 LTS, 14.04 LTS, 14.10)
- Webserver: Apache 2
- Databases: MySQL/MariaDB 5.x; Oracle 11g; PostgreSQL
- PHP 5.4 + required
- Hypervisors: Hyper-V, VMware ESX, Xen, KVM
- Desktop: Windows XP SP3 (EoL Q2 2015), Windows 7+, Mac OS X 10.7+ (64-bit only), Linux (CentOS 6.5, 7 (7 is 64-bit only), Ubuntu 12.04 LTS, 14.04 LTS, 14.10, Fedora 20, 21, openSUSE 12.3, 13, Debian 7 & 8).
- Mobile apps: iOS 7+, Android 4+
- Web browser: IE8+ (except Compatibility Mode), Firefox 14+, Chrome 18+, Safari 5+

Pro přístup k serverovému úložišti je možné volit buď www prohlížeč (který respektuje příslušné standardy) nebo samostatného klienta. Aplikace pro owncloud jsou psány převážně v jazyce PHP (kontakty, Kalendář, Sdílení souborů, Konverzace, Řízení projektů) a jsou rovněž vyvíjeny pod otevřenými licencemi
(viz. https://apps.owncloud.com/ a https://github.com/owncloud/core/wiki/Apps)

Vlastní stránky projektu owncloud pak obsahují velmi podrobné návody týkající se konfigurace serveru a jednotlivých serverových komponent (apache, php, ssh, ssl, memcache, apc a řady dalších).

https://doc.owncloud.org/server/9/admin_manual/configuration_server/index.html

Popis síťových služeb

V této kapitole jsou popsány implementované síťové služby, které jsou součástí úložiště dat.

TCP Wrapper

TCP Wrapper je mechanismus, který umožňuje v unixových operačních systémech řídit přístup ke službám serveru na základě adresy, ze které přicházejí požadavky klienta.[1]

Vkládá se do komunikace mezi spouštěnou službu a tzv. „*super-server*“ (např. inetd), který naslouchá požadavkům jím spravovaných služeb. Úkolem **TCP Wrapperu** je ochránit volanou síťovou službu před nepovoleným přístupem. Zavádí podporu pro vracení stavových zpráv klientovi při pokusu o připojení ke službě. Dále informuje správce operačního systému o příchozích požadavcích, které zapisuje do systémového logu. Dnes se nejčastěji používá jako knihovna (*libwrap*) připojená k libovolnému programu, která následně komunikuje s internetovým démonem. Při požadavku klienta na spuštění nějaké konkrétní služby, se namísto požadovaného démona spouští nejprve program `/usr/sbin/tcpd` (samotný **TCP Wrapper**), který na základě definovaných pravidel rozhodne, jestli má klient ke službě přístup. Po úspěšné autorizaci předává řízení požadovanému démonu *(programu)*, který klientovi službu poskytne. Binární kód cílového démona však musí být „slinkován“ s knihovnou libwrap (v řadě linuxových distribucí jsou takto „vybaveni“ démoni pro ftp-server, ssh-server nebo nfs-server). V těchto případech je „řízení přístupu“ pomocí **TCP Wrapper** mnohem efektivnější než např. pomocí firewallu (iptables).

Pro správnou funkci **TCP Wrapperu** jsou důležité 2 textové soubory: `/etc/hosts.allow` a `/etc/hosts.deny`. Obsah těchto souborů určuje, které služby ze kterých adres budou povolené resp. Zakázané.

Pořadí zpracování

1. jestliže požadavek určený dvojicí *démon – adresa klienta* vyhoví některému pravidlu v souboru `/etc/hosts.allow`, přístup bude

umožněn;

2. jestliže požadavek určený dvojicí *démon – adresa klienta* vyhoví některému pravidlu v souboru `/etc/hosts.deny`, přístup nebude umožněn;
3. v ostatních případech je přístup implicitně povolen!

V našem případě tedy volíme filosofii „uzavřeného systému“, kde jsou všechny služby a IP rozsahy implicitně zakázány v konfiguračním souboru `/etc/hosts.deny`. Ověřené služby a rozsahy IP adres jsou následně povoleny v konfiguračním souboru `/etc/hosts.allow`.

hosts.deny

Obsah souboru `/etc/hosts.deny`:

```
ALL : ALL
```

hosts.allow

Příklad obsahu souboru `/etc/hosts.allow`:

```
# APCUPSD
apcupsd: 127.0.0.0/255.0.0.0.

#MySQL
mysqld: 127.0.0.0/255.0.0.0

#NFS
portmap: 127.0.0.0/255.0.0.0
lockd: 127.0.0.0/255.0.0.0
mountd: 127.0.0.0/255.0.0.0
rquotad: 127.0.0.0/255.0.0.0
statd: 127.0.0.0/255.0.0.0

ALL: 127.0.0.1

# Interni sit
ALL: 192.168.10.0/255.255.255.0


# UPC CR
```

ALL: 84.42.128.0/255.255.128.0

CZ-DATTELKABEL-20080709 #2

ALL: 94.112.0.0/255.254.0.0

CZ.CZNET

ALL: 90.180.0.0/255.252.0.0

CZ.CZNET

ALL: 88.101.0.0/255.255.0.0

UPC Ceska Republika Broadband II

ALL: 89.176.0.0/255.254.0.0

BlueTone-CRa-CZ Fourth address block origin: AS25248

ALL: 85.207.0.0/255.255.0.0

fail2ban

Jedná se o velmi účinný adaptivní firewall, který je součástí prakticky každé linuxové distribuce.

https://en.wikipedia.org/wiki/Fail2ban
http://www.fail2ban.org/wiki/index.php/Main_Page

V systému (na serveru) běží démon fail2ban (napsáno v jazyce Python), který registruje změny v předem určených souborech log systému. Pokud nalezne v daném logu předem danou kombinaci textu (např. Invalid user, spoof syn - těch "varovných výrazů“ je celá řada - fali2ban je má předem dané v samostatnych konfiguračních souborech), pak fail2ban vydá pokyn k určité činnosti. Máme na

výběr z těchto kroků:

- Pokyn firewallu (integrovaném v jádru linuxu) a firewall IP adresu "útočníka" dočasně zablokuje.
- Pouze mailové hlášení, nedojde k zablokování IP adresy útočníka
- Spuštění jiného skriptu

Výše uvedené kroky je samozřejmě možné kombinovat. Vlastní „filtry“ pro fail2ban je možné samozřejmě upravovat, doplnit vlastní filtry apod.

Mail hlášení adminovi obsahuje:

- IP adresu utočníka
- Úplný popis IP rozsahu (CIDR) včetně identifikace providera
- Výpis z logu, kde se vyskytuje IP adresa útočníka

Ukázka hlášení administrátorovi:

Hi,
The IP 109.230.94.54 has just been banned by Fail2Ban after
6 attempts against ssh.
Here are more information about 109.230.94.54:
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf
% Note: this output has been filtered.
% To receive output for a database update, use the "-B" flag.
% Information related to '109.230.94.0 - 109.230.94.255'
inetnum: 109.230.94.0 - 109.230.94.255
netname: KFZO
descr: Kish Free Zone Organization
country: IR
admin-c: AV5398-RIPE
tech-c: AV5398-RIPE

status: ASSIGNED PA
mnt-by: mnt-boom
source: RIPE # Filtered
person: Afshin Vafaei
address: Kish Free Zone Organization-Kish Island
phone: +987644422048
nic-hdl: AV5398-RIPE
source: RIPE # Filtered
% Information related to '109.230.80.0/20AS50591'
route: 109.230.80.0/20
descr: Boomerang-Route2
origin: AS50591
mnt-by: MNT-BOOM
mnt-lower: MNT-BOOM
mnt-routes: MNT-BOOM
source: RIPE # Filtered
% This query was served by the RIPE Database Query Service version 1.67.4 (WHOIS1)
Lines containing IP:109.230.94.54 in /var/log/auth.log
Aug 7 19:16:36 server sshd[27434]: refused connect from 109.230.94.54 (109.230.94.54)
Aug 7 19:16:36 server sshd[27435]: refused connect from 109.230.94.54 (109.230.94.54)
Aug 7 19:16:36 server sshd[27436]: refused connect from 109.230.94.54 (109.230.94.54)
Aug 7 19:16:36 server sshd[27437]: refused connect from 109.230.94.54 (109.230.94.54)
Aug 8 23:08:56 server sshd[3386]: refused connect from 109.230.94.54 (109.230.94.54)
Aug 8 23:08:56 server sshd[3390]: refused connect from 109.230.94.54 (109.230.94.54)
Aug 8 23:08:56 server sshd[3388]: refused connect from 109.230.94.54 (109.230.94.54)
Aug 8 23:08:56 server sshd[3391]: refused connect from 109.230.94.54 (109.230.94.54)
Aug 8 23:08:56 server sshd[3387]: refused connect from 109.230.94.54 (109.230.94.54)
Aug 8 23:08:56 server sshd[3389]: refused connect from 109.230.94.54

(109.230.94.54)

Regards,
Fail2Ban

Vlastní fail2ban lze samozřejmě dále upravovat. Velmi populární úpravou je rozšíření fail2ban o tzv. **ip.blacklist**, což je vlastně textový soubor obsahující seznam IP adres (nebo celých adresních rozsahů), které naše instalace fail2ban na firewallu (zde tedy iptables) zakáže a stroje s těmito IP adresami pak nemohou s naším serverem vůbec komunikovat.

Příslušné návody můžete nalézt např zde:

http://www.looke.ch/wp/list-based-permanent-bans-with-fail2ban

http://www.mauromascia.com/blog/fail2ban-set-permanent-ban-per-ip/

Stručný popis úprav vypadá asi takto:

/etc/fail2ban/jail.local

```
#
# ACTIONS
#
...
banaction = iptables-multiport
...
```

/etc/fail2ban/action.d/iptables-multiport.conf

```
...
actionstart = iptables -N fail2ban-<name>
              iptables -A fail2ban-<name> -j RETURN
              iptables -I INPUT -p <protocol> -m multiport
--dports <port> -j fail2ban-<name>
              # Persistent banning of IPs
              cat /etc/fail2ban/ip.blacklist | while read IP; do
iptables -I fail2ban-<name> 1 -s $IP -j DROP; done
...
actionban = iptables -I fail2ban-<name> 1 -s <ip> -j DROP
            # Persistent banning of IPs
            echo '<ip>' >> /etc/fail2ban/ip.blacklist
...
```

A konečně, obsah vlastního souboru */etc/fail2ban/ip.blacklist* bude vypadat následovně.

....

37.200.127.222

85.105.114.246

79.53.135.205

192.198.86.236

46.146.226.231

130.117.10.35

178.125.100.47

.....

Fail2ban doplňuje IP adresy „narušitelů“ do souboru */etc/fail2ban/ip.blacklist* automaticky. Následně pak stačí vlastní fail2ban restartovat (např. pomocí cron) a IP adresy „narušitelů“ budou na firewallu zakázány „navždy“ (tedy ne jen na onen přednastavený časový interval ve fail2ban).

Network File System

Network File System (NFS) je internetový protokol pro vzdálený přístup k souborům přes počítačovou síť. Protokol byl původně vyvinut společností Sun Microsystems v roce 1984, v současné době má jeho další vývoj na starosti organizace Internet Engineering Task Force (IETF). Funguje především nad transportním protokolem UDP, avšak od verze 3 je možné ho provozovat také nad protokolem TCP.

NFS protokol pro přístup k datové oblasti zařízení je vhodný zejména pro jeho rychlost a vysoký stupeň zabezpečení. Především ve verzi 4 byl výrazný nárůst prostředků pro zvýšení bezpečnosti. Verze 4 již byla vyvíjena ve spolupráci se skupinou IETF (Komise pro technickou stránku internetu), která vyvíjí a podporuje internetové standardy. Tato verze dostala označení mezinárodního standardu RFC3010.

V praxi si můžete prostřednictvím NFS klienta připojit disk ze vzdáleného serveru a pracovat s ním jako s lokálním. V prostředí Linuxu se jedná asi o nejpoužívanější protokol pro tyto účely.

V dnešních moderních distribucích se téměř výhradně setkáme s nástupcem NFS verze 4, který se, ačkoli z uživatelského hlediska vypadá téměř totožně, přece jen od svého předchůdce hodně liší. Základní odlišnosti jsou:

1. **Pseudo file system** - NFSv4 vyžaduje exportovat nějaký adresář jako kořen. To se provádí dodatečným parametrem *fsid=0*
2. **Stavový protokol** - na rozdíl od svého předchůdce, který byl v jádru bezestavový (démony *rpclockd* a spol mu sice dodávají stavovost ale nejsou definovány v RFC a nejsou součástí protokolu NFS) je NFSv4 protokol stavový, což mu dodává, kromě nevýhody větší složitosti i pár výhod, jako například delegování čtení nebo zápisu na klienta, nebo například zamykání souborů. NFSv4 nepotřebuje portmapper.
3. **Přenos ACL** - NFSv3 přenos přístupových práv neřeší. Naproti tomu jsou ACL nedílnou součástí protokolu NFSv4. Nutno ale říci, že protokol NFSv4 definuje vlastní formát ACL, který je odlišný (lepší) od formátu Posix ACL, který ale nebyl nikdy standardizován.
4. **Jednodušší tunelování přes firewall** - na rozdíl od svého předchůdce vyžaduje NFSv4 pro svůj běh mezi klientem a serverem otevřen jen jediný, předem definovaný port.
5. **mapování uživatelů** - NFSv4 byl vyvíjen primárně jako multiplatformní síťový souborový systém, takže na rozdíl od svého předchůdce

nepřenáší User ID (UID, typické pro unix), ale doménové jméno ve formátu username@doména. Z tohoto důvodu je nutné, aby na Unixových systémech (klientu i serveru) běžel pomocný program starající se o překlad jmen na UID - obvykle je to démon **rpc.idmapd**

6. **větší bezpečnost** - kromě klasické "systémové" bezpečnosti, která je notoricky nebezpečná, protokol NFSv4 umožňuje využití i silnějších bezpečnostních mechanismů, jakým je např. Kerberos.

Konfigurace serveru

NFS server se nastavuje pomocí konfiguračního souboru `/etc/exports`, který na jednotlivých řádcích obsahuje definice sdílených adresářů. Jako první je název adresáře a pak seznam povolených klientů (zde jsou uvedeny názvy *server*, *stanice* a IP adresa) s přidanými volitelnými parametry:

```
/usr 10.1.2.3(ro) stanice(ro)
/home 10.1.2.3(rw,no_root_squash) stanice(rw)
```

Parametry

- **ro** (read-only) – pouze pro čtení
- **rw** (read-write) – povoleno čtení i zápis
- **no_root_squash** – mapovat požadavky uživatele *root* na běžného uživatele (obvykle *nobody*)

Konfigurace klienta

Klient připojuje adresář ze serveru do svého adresářového stromu stejným způsobem, jako jsou připojovány jednotlivé systémy souborů. V současné době je obvykle nutné na klientovi spustit též démona portmap:

```
mount -t nfs server:/home /home
mount -t nfs server:/usr /mnt/usr-from-server
```

Od této chvíle může klient s daty v adresáři `/home` a `/mnt/usr-from-server` pracovat stejně, jako kdyby byly umístěny na lokálním počítači.

OpenSSH_Server

OpenSSH (**OpenBSD Secure Shell**) je soubor počítačových programů poskytujících zašifrovaná komunikační sezení, která se používají pomocí ssh protokolu přes počítačovou síť. Je to produkt, zajišťující šifrovaný přístup k shellu operačního systému přes počítačovou síť. Má dvě části: ssh klienta (*Secure Shell Klient*) a ssh server (ten běží na našich serverech). SSH klient kromě zpřístupnění Shellu umí také vytvářet SSH tunely.

Instalace

Instalace OpenSSH klienta i serveru je jednoduchá. V případě linuxové distribuce Ubuntu nainstalujeme klienta z řádky takto:

sudo apt-get install openssh-client

Instalaci serveru a potřebných dodatečných balíků provedeme tímto příkazem:

sudo apt-get install openssh-server

Balíček openssh-server může být vybrán také v průběhu instalace Ubuntu Server Edition.

Nastavení

Můžete nastavit základní chování OpenSSH služby, sshd, upravením souboru /etc/ssh/sshd_config. Pro informace o konfiguračních příkazech tohoto souboru můžete nahlédnout do manuálu příkazem:

man sshd_config

Zde je mnoho příkazů v souboru konfigurace sshd, jako např. nastavení komunikace a způsoby ověřování. Následují příklady konfiguračních příkazů, které mohou být změněny editací souboru /etc/ssh/sshd_config file.

Doporučujeme nejprve vytvořit kopii originálu konfiguračního souboru a nastavit ho pouze pro čtení, abychom si uložili výchozí nastavení pro případ opětovného použití.

Zkopírujte soubor /etc/ssh/sshd_config a ochraňte ho proti zápisu pomocí příkazů:

sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.original

sudo chmod a-w /etc/ssh/sshd_config.original

Zde jsou příklady změny konfigurace:

Pro nastavení OpenSSH k naslouchání na TCP portu 2222 na rozdíl od výchozího TCP portu 22, změňte direktivu Port na:

Port 2222

Pokud chceme povolit sshd použití přihlašování pomocí veřejného klíče, přidáme nebo opravíme tento řádek:

PubkeyAuthentication yes

Pokud je řádek již vložen, přesvědčíme se, že není zakomentován.

Pro zobrazování obsahu souboru /etc/issue.net před přihlášením, přidejte nebo upravte řádek:

Banner /etc/issue.net

Poté, co provedeme úpravy a uložíme soubor /etc/ssh/sshd_config, musíme sshd server restartovat pomocí příkazu:

sudo service ssh restart

Konfigurace sshd má k dispozici ještě spoustu dalších direktiv pro přizpůsobení chování. Pokud se však k serveru připojujete pomocí SSH a uděláte chybu v konfiguraci, můžete zůstat od serveru odstřiženi a některá chyba v konfiguraci může způsobit i problém se spuštěním systému po restartu. Proto hlavně při editaci konfiguračního souboru na vzdáleném serveru buďte velmi opatrní.

SSH klíče

SSH klíče umožňují přihlašování bez použití hesla. Přihlašování pomocí SSH klíčů používá dva klíče, soukromý a veřejný.

Pro vygenerování klíčů použijte příkaz:

```
ssh-keygen -t rsa
```

Tím vygenerujete klíče s použitím algoritmu RSA. Během procesu budete vyzváni k zadání hesla. Jednoduše stiskněte Enter jakmile budete vyváni k vytvoření klíčů.

Veřejný klíč je standardně uložen do souboru ~/.ssh/id_rsa.pub, a soukromý do ~/.ssh/id_rsa. Nyní zkopírujte soubor id_rsa.pub do vzdáleného stroje a připojte ho do ~/.ssh/authorized_keys pomocí:

```
ssh-copy-id username@remotehost
```

Nakonec zkontrolujte oprávnění přístupu ke klíči, kde by pouze vlastník měl mít práva k čtení a zápisu. Pokud jsou oprávnění jinak, opravte je pomocí:

```
chmod 600 .ssh/authorized_keys
```

Nyní se můžete ke vzdálenému stroji připojovat i bez přihlašování heslem.

Postfix, SMTP server

Postfix byl vybrán jako výchozí mailer pro rozesílání logů hned z několika důvodů. Především se jedná o software s otevřeným kódem, tzv. „open source software“. Od začátku byl jeho vývoj sponzorován firmou IBM Research, která i nadále jeho vývoj podporuje (v její terminologii se nazývá Secure Mailer).
Postfix má hned několik výjimečných vlastností:
- spolehlivost (je velmi odolný proti přetížení jak sebe, tak i systému)
- vysoká bezpečnost (má k dispozici několik obranných vrstev proti útočníkům)
- vysoký výkon (je navržen pro vysoký výkon, neomezuje však ostatní procesy v systému)
- značná variabilita (v postfixu lze snadno konfigurovat větší množství modulů)
- kompatibilita se sendmailem (Sendmail můžeme snadno nahradit Postfixem, protože Postfix podporuje téměř všechny konvence a původní argumenty příkazové řádky Sendmailu)

Log server (Log collector)

Jedná se o samostatné zařízení určené pro sběr a vyhodnocování logů (ve formátu syslog), které je součástí určité DMZ zóny nebo vnitřní LAN sítě. Vlastní vyhodnocování logů pak provádí automat na základě předem daných šablon. Obsluha má samozřejmě možnost se k jednotlivým logům vracet a zpětně je podrobně analyzovat. Vlastní rozesílání upozornění na „podezřelé“ logy se děje pomocí e-mailu nebo SMS. Celé zařízení je možné provozovat na bázi open source a to s nekomerční licencí GPL.

Dle platné legislativy Log server slouží jako "Nástroj pro zaznamenávání činnosti kritické informační infrastruktury a vyznamných informačních systémů, jejich uživatelů a administratorů" dle §21 Hlavy II „Technická opatření“ vyhlášky o kyberneticé bezpečnosti ze sbírky zákonů 316/2014
a především jako "Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí" dle §23 téže vyhlášky.

> Dle výše uvedené vyhlášky musí toto zařízení zajišťovat
> a) integrovaný sběr a vyhodnocování kybernetických bezpečnostních událostí
> b) poskytování informací pro určené bezpečnostní role o detekovaných bezpečnostních událostech
> c) nepřetržité vyhodnocování kybernetických bezpečnostních událostí pro vyhodnocování bezpečnostních incidentů a včasné varování určených bezpečnostních rolí

Log server je zařízení, které musí být odděleno od internetu i od klientských stanic, proto je mu vyhrazeno samostatné připojení v DMZ rozsahu. Vyplývá to z povinnosti jeho správce, který dle §21 vyhlášky o kybernetické bezpečnosti musí zajistit ochranu získaných informací před neoprávněným čtením či změnou.

Logcheck

www.logcheck.org

Poměrně výkonný analyzátor logů šířený pod GNU GPL licencí. Analyzuje logy a podle předem nastavených pravidel je zařazuje a posílá např. mailem nebo prostřednictvím SMS předem určeným bezpečnostním rolím. Spouštěn je prostřednictvím CRON. Pravidla pro analýzu logů je samozřejmě možné upravovat, je možné spouštět logcheck s různými konfigračními soubory (a analyzovat tak pokaždé jinou množinu logů).

Apache

Apache HTTP Server je softwarový webový server s otevřeným kódem pro GNU/Linux, BSD, Solaris, Mac OS X, Microsoft Windows a další platformy. V současné době se jedná o nejrozšířenější www server. V zařízení je www server apache kombinován s CMS Drupal (Content Management System – redakční systém), který je rovněž šířen pod GPL licencí a vytváří zde „klamný cíl“ pro útočníka. Vlastní Drupal pak loguje veškerou svou činnost do syslog. Logy jsou samozřejmě ukládány jak lokálně, tak zasílány do samostatného syslog serveru (log server / log collector). Logy mohou být analyzovány nástroji jako **logcheck** (dávkové zpracování) nebo **fail2ban** (on-line zpracování s možností okamžité automatické reakce). Vlastní přístup k samotnému datovému úložišti lze pomocí direktiv apache (zde konkrétně prostřednictvím .htaccess) omezit na konkrétní IP adresy nebo vybrané adresní rozsahy.

Ukázka obsahu souboru .htaccess pro omezení přístupu k datovému úložišti owncloud z vybraných adresních rozsahů.

```
order deny,allow
deny from all
allow from 127.0.0.0/8
# Vnitrni rozsah
allow from 192.168.14.0/24
#UPC CR
allow from 84.42.128.0/17
#  CZ-DATTELKABEL-20080709 #2
allow from 94.112.0.0/23
```

MySQL

MySQL je databázový systém, vytvořený švédskou firmou MySQL AB, nyní vlastněný společností Sun Microsystems, dceřinou společností Oracle Corporation. Jeho hlavními autory jsou Michael „Monty“ Widenius a David Axmark. Je považován za úspěšného průkopníka dvojího licencování – je k dispozici jak pod bezplatnou licencí GPL, tak pod komerční placenou licencí.

MySQL je multiplatformní databáze. Komunikace s ní probíhá – jak už název napovídá – pomocí jazyka SQL. Podobně jako u ostatních SQL databází se jedná o dialekt tohoto jazyka s některými rozšířeními.

MySQL bylo od počátku optimalizováno především na rychlost, a to i za cenu některých zjednodušení: má jen jednoduché způsoby zálohování, a až donedávna nepodporovalo pohledy, triggery, a uložené procedury. Tyto vlastnosti jsou doplňovány teprve v posledních letech, kdy začaly nejčastějším

uživatelům produktu – programátorům webových stránek – již poněkud scházet.

Pro svou snadnou implementovatelnost (lze jej instalovat na Linux, MS Windows, ale i další operační systémy), výkon a především díky tomu, že se jedná o volně šiřitelný software, má vysoký podíl na v současné době používaných databázích. Velmi oblíbená a často nasazovaná je kombinace Linux, MySQL, PHP a Apache jako základní software webového serveru („technologie LAMP“).

PHP

PHP (rekurzivní zkratka PHP: Hypertext Preprocessor, česky „PHP: Hypertextový preprocesor“, původně Personal Home Page) je skriptovací programovací jazyk. Je určený především pro programování dynamických internetových stránek a webových aplikací například ve formátu HTML, XHTML či WML. PHP lze použít i k tvorbě konzolových a desktopových aplikací. Pro desktopové použití existuje kompilovaná forma jazyka.

Při použití PHP pro dynamické stránky jsou skripty prováděny na straně serveru – k uživateli je přenášen až výsledek jejich činnosti. Interpret PHP skriptu je možné volat pomocí příkazového řádku, dotazovacích metod HTTP nebo pomocí webových služeb. Syntaxe jazyka je inspirována několika programovacími jazyky (Perl, C, Pascal a Java). PHP je nezávislý na platformě, rozdíly v různých operačních systémech se omezují na několik systémově závislých funkcí a skripty lze většinou mezi operačními systémy přenášet bez jakýchkoli úprav.

PHP podporuje mnoho knihoven pro různé účely – např. zpracování textu, grafiky, práci se soubory, přístup k většině databázových systémů (mj. MySQL, ODBC, Oracle, PostgreSQL, MSSQL), podporu celé řady internetových protokolů (HTTP, SMTP, SNMP, FTP, IMAP, POP3, LDAP, …).

PHP je nejrozšířenějším skriptovacím jazykem pro web, v současnosti (listopad 2014) s podílem 82 %. Oblíbeným se stal především díky jednoduchosti použití, bohaté zásobě funkcí. V kombinaci s operačním systémem Linux, databázovým systémem (obvykle MySQL nebo PostgreSQL) a webovým serverem Apache je často využíván k tvorbě webových aplikací. Pro tuto kombinaci se vžila zkratka LAMP – tedy spojení Linux, Apache, MySQL a PHP, Perl nebo Python.

LDAP

LDAP (Lightweight Directory Access Protocol) je definovaný protokol pro

ukládání a přístup k datům na adresářovém serveru. Podle tohoto protokolu jsou jednotlivé položky na serveru ukládány formou záznamů a uspořádány do stromové struktury (jako ve skutečné adresářové architektuře). Je vhodný pro udržování adresářů a práci s informacemi o uživatelích (např. pro vyhledávání adres konkrétních uživatelů v příslušných adresářích, resp. databázích). Protokol LDAP je založen na doporučení X.500, které bylo vyvinuto ve světě ISO/OSI, ale do praxe se ne zcela prosadilo, zejména pro svou „velikost“ a následnou „těžkopádnost“.

Protokol LDAP již ve svém názvu zdůrazňuje fakt, že je „odlehčenou“ (lightweight) verzí, odvozenou od X.500 (X.500 - Mezinárodní standard, vyvinutý spolkem International Consultative Commitee of Telephony and Telegraphy, pro formátování elektronických zpráv přenášených přes sítě nebo mezi počítačovými sítěmi).

Aplikace funguje na bázi klient-server. V komunikaci využívá jak synchronní tak asynchronní mód. Součástí LDAP je autentizace klienta. Při provádění požadavku lze nedokončený požadavek zrušit příkazem abandon.

Slovníček pojmů

Zkratka	Vysvětlení zkratky
Audit IS	Vlastním auditem informačního systému rozumíme proces jehož výstupem je zdokumentování informačního systému, popis jeho vazeb na okolní informační systémy a prostředí.
	Metodika BSI pro audit informačního systému https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/ISRevision/guideline-isrevision_pdf.pdf?__blob=publicationFile
Analýza rizik	Metodika sloužící k rozpoznání, předpovězení a vyhodnocení jednotlivých hrozeb a jejich dopadů na daný informační systém. Analýza rizik navazuje na vlastní bezpečnostní proces a představuje zpětnou vazbu pro daný informační systém a oblasti tímto informačním systémem dotčené.
	Výstupní dokument je třeba periodicky aktualizovat https://www.bsi.bund.de/EN/Publications/BSIStandards/standards.html
BIA	Business Impact Analysis
	Analýza dopadů (BIA) je základem celého procesu řízení kontinuity činností organizace (Business Continuity Plan, BCP). http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.html
BSI	*Bundesamt für Sicherheit in der Informationstechnik*
	Německá národní bezpečnostní autorita (obdoba českého NBÚ). www.bsi.bund.de
DRP	Disaster Recovery Plan
	Jedná se o metodiky a postupy sloužící k obnově funkčnosti informačního systému po živelných pohromách a jiných zásadních událostech.
ISO	International Organization for Standardization
	Označení mezinárodní normy http://www.iso.org/iso/home.html
NBÚ	Národní bezpečnostní úřad
	www.nbu.cz
NIST	National Institute of Standards and Technology, USA
	http://www.nist.gov/

Penetrační testy	Cílem penetračních testů je odhalení zranitelností cílového informačního systému, stanovení způsobu jejich možného využití a doporučení vedoucí k jejich nápravě.
	http://www.linuxservices.cz/penetracni-testy