VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

DATOVÉ ÚLOŽIŠTĚ SAN

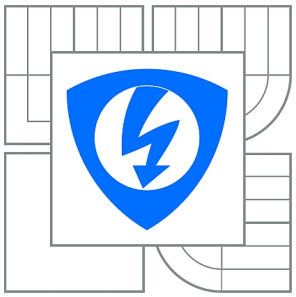
BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE JÁN PRUŽINSKÝ
AUTHOR

BRNO 2011

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

DATOVÉ ÚLOŽIŠTĚ SAN

SAN DATA STORAGE

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

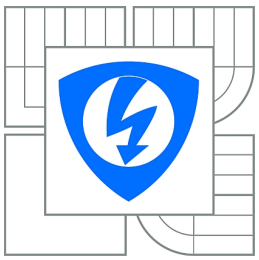
AUTOR PRÁCE — JÁN PRUŽINSKÝ

AUTHOR

VEDOUCÍ PRÁCE — Ing. RADIM PUST

SUPERVISOR

BRNO 2011



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Ján Pružinský	***ID:***	115262
Ročník:	3	***Akademický rok:***	2010/2011

NÁZEV TÉMATU:

Datové úložiště SAN

POKYNY PRO VYPRACOVÁNÍ:

Cílem bakalářské práce je stručný úvod do problematiky datových úložišť SAN (Storage Area Network) a jejich implementace v síti. Následně by měl být popsán protokol iSCSI, včetně zaměření na bezpečnost tohoto protokolu a jeho implementaci v OS Linux a MS Windows. Rovněž jsou požadovány instalace OS Linux s konfigurací iSCSI target a initiator. Dále je požadována instalace MS Windows Server jako iSCSI initiatoru a napojení na iSCSI target na platformě OS Linux. V rámci řešení by student měl vytvořit webové rozhraní pro správu a konfiguraci iSCSI targetu.

DOPORUČENÁ LITERATURA:

[1] Linux : Dokumentacní projekt, 4. aktualizované vydání. Brno : Computer Press, 2008. 1336 s. ISBN 978-80-251-1525-1.
[2] RUEST, Danielle; RUEST, Nelson. Virtualizace : Podrobný pruvodce. Brno : Computer Press, 2010. 408 s. ISBN 978-80-251-2676-9.

Termín zadání:	7.2.2011	***Termín odevzdání:***	2.6.2011

Vedoucí práce: Ing. Radim Pust

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Cieľom tejto práce bolo oboznámiť sa s protokolom iSCSI a s jeho implementáciou do SAN siete. Na začiatku je teoretický rozbor dátového úložiska SAN, popis jeho jednotlivých častí, k čomu slúži a jeho implementácia v sieti. V ďalšej časti je zahrnutý popis protokolu iSCSI spolu s vysvetlením jednotlivých skratiek a pojmov. Spracované sú jednotlivé možnosti zabezpečenia tohto protokolu, a tiež vysvetlená implementácia v OS Linux a OS MS Windows Server. Praktická časť práce je venovaná konfigurácii iSCSI targetu v OS Linux spolu s konfiguráciou iSCSI initiatora v OS Linux a OS Windows. Posledná časť je venovaná tvorbe webového rozhrania na ovládanie iSCSI targetu.

KĽÚČOVÉ SLOVÁ

iSCSI, SAN, initiator, target, LUN, IQN, iSNS, PHP

ABSTRACT

The main goal of this project is a familiarization with the protocol iSCSI and with its implementation into the SAN network. Firstly, the focus is aimed towards a theoretical analysis of the SAN data storage, description of its individual parts as well as its realization within the network. In the second part, the description of the protocol iSCI includes an explanation of particular abbreviations and terms. Every possibility of securing this protocol is fully processed and, moreover, the implementation in OS Linux and OS MS Windows Server is deeply explained. The practical part is devoted to configuring iSCSI Target in OS Linux and configuring iSCSI Initiator in OS linux and OS Windows. The last part is devoted to creating a Web interface to control the iSCSI Target.

KEYWORDS

iSCSI, SAN, initiator, target, LUN, IQN, iSNS, PHP

PRUŽINSKÝ, Ján *Dátové úložište SAN*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2011. 68 s. Vedúci práce bol Ing. Radim Pust,

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Dátové úložište SAN“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

Brno ....

(podpis autora)

Poďakovanie
Ďakujem vedúcemu mojej práce Ing. Radimovi Pustovi za užitočnú metodickú pomoc a cenné rady pri spracovávaní tejto práce.

V Brne dňa . . . .
podpis autora

OBSAH

ZOZNAM OBRÁZKOV

ÚVOD

Pred niekoľkými rokmi vznikol koncept, ktorého cieľom bola možnosť pristupovať k dátam na počítači z iného počítača v sieti. K tomu bolo potrebné vytvoriť určitý štandard (protokol), ktorý by dokázal dáta prepravovať po sieti.

V roku 1984 spoločnosť SUN Microsystems vyvinula protokol Network File System (NFS), ktorý fungoval na IP vrstve a bol vhodný na takýto prenos. V tom čase tiež spoločnosti Microsoft a IBM spolu definovali protokol, ktorý bol založený na technológii Server Message Block (SMB). Microsoft si tento štandard pomenoval ako „LAN Manager“ a spoločnosť IBM nazvala svoju verziu ako „LAN Server“. No táto technológia (SMB) dokázala fungovať iba v malej lokálnej sieti (LAN). Microsoft preto danú verziu upravil na takú, ktorá bola schopná fungovať aj cez internet a nazval ju Common Internet File System (CIFS).

Neskôr sa pre potreby organizácií vyvinul systém zdieľania dát pomocou NAS (Network Attached Storage) siete. Táto sieť podporovala práve spomínané protokoly NFS a CIFS.

V roku 1994 bol schválený protokol Fibre Channel, ktorý mal taktiež slúžiť na prenos dát po sieti. Svoje uplatnenie našiel Fibre Channel protokol v SAN (Storage Area Network) sietiach. SAN siete slúžia na prenos dát medzi serverom a zdieľaným diskovým priestorom. Oproti NAS poskytuje Fibre Channel SAN vyššie prenosové rýchlosti ale jej nevýhodou je to, že nepracuje na TCP/IP vrstve ethernet protokolu čo znamená že potrebuje mať vybudovanú vlastnú komunikačnú sieť.

V roku 2001 spoločnosť Intel predstavila prvú verziu protokolu iSCSI, ktorý mal byť hlavným konkurentom Fibre Channel protokolu. Na rozdiel od Fibre Channel funguje na IP vrstve a môže fungovať na už vytvorenej ethernetovej lokálnej sieti (LAN). Vďaka svojím výhodám sa tento protokol stal plnohodnou variantou používanou v SAN sietiach a v dnešnej dobe je už používanejším v SAN sietiach ako Fibre Channel protokol.

Protokol iSCSI prepravuje príkazy používané SCSI protokolom po IP sietiach. SCSI protokol je protokol používaný na SCSI zberniciach, ktoré sa používajú na pripojenie zariadení (pevných diskov, páskových mechaník, tlačiarní, skenerov, CD/DVD mechaník) k serveru. SCSI zbernica je všeobecne považována za prepojovaciu techniku, ktorá umožňuje rôznym typom zariadení spolupracovať s počítačom.

Práve protokolu iSCSI je venovaná hlavná časť tejto práce. V jednotlivých častiach je vysvetlená terminológia týkajúca sa tohto protokolu spolu so základným popisom jeho funkcie, bezpečnosť protokolu a tiež praktická realizácia.

1 SAN - DÁTOVÉ ÚLOŽISKO

1.1 Čo je dátové úložisko SAN?

Skratka SAN je skratkou od slov Storage Area Network. Ak sa pokúsime preložiť dané slovné spojenie dostaneme niečo ako „Sieť skladovacích priestorov“. Z toho by sme mohli usúdiť že je to nejaká sieť zahrňujúca určitý dátový priestor. V podstate by sme neboli ani ďaleko od pravdy. Presnejšia definícia znie že SAN je sieť, ktorá má za účel uskladňovať dáta a chrániť ich pred zneužitím. Slúži na prepojenie serverov(pracovných staníc) s dátovým úložiskom cez vysoko rýchlostnú optickú alebo metalickú sieť. Zmyslom SAN úložiska je umožniť rôznym serverom pristupovať k rôznym dátovým jednotkám, resp. k jednotkám ku ktorým majú povolený prístup.

Existuje viacero dôvodov prečo zvoliť SAN sieť ako svoje dátové úložisko (spomenuté v knihe [12]). Spomeňme aspoň niektoré výhody SAN sietí.

- ***Odstraňuje vzdialenostný limit SCSI diskov***
  Maximálna vzdialenosť SCSI zbernice pri priamo pripojených diskoch môže byť okolo 25m. Pri použití SAN siete sa nám táto vzdialenosť podstatne zvýši.
- ***Vysoký výkon***
  Terajšie SAN siete umožňujú pristupovať k dátam rýchlosťou stoviek megabajtov za sekundu. Časom môžeme očakávať rýchlosti v giga alebo aj v tera bajtoch sa sekundu.
- ***Spoľahlivosť siete***
  Pokiaľ máme navrhnutú sieť iba s jednou cestou prístupu k dátam tak v prípade pádu tejto linky stratíme k nim celkový prístup. Tým že v SAN sieti možeme zriadiť viacero možných prístupov k dátam zvyšujeme tak jej spoľahlivosť. Správne navrhnutá SAN sieť s viacerými fyzickými cestami medzi servermi a diskami bude fungovať aj v prípade straty jednej či viacero liniek.
- ***Zlepšuje využitie diskov***
  V SAN sieti môže viacero serverov pristupovať k jednému fyzickému disku. Tým efektívnejšie využijeme diskový priestor a znížime náklady na nákupy nových diskov.
- ***Rýchle zotavenie siete po havárii***
  Jedna z hlavných výhod SAN. Vytvorením kópií diskov na iné nezávislé miesto získame zálohu dát, ktorá je v bezpečí v prípade havárie a je ľahké dáta následne obnoviť.
- ***Úložný priestor na požiadanie***
  Využitím virtualizácie môžeme v prípade potreby prideľovať ďalší diskový priestor serverom, ktoré o to požiadajú.

- ***Lepšia správa dát***
  V porovnaní so správou siete kde má každý server vlastné priamo pripojené disky sa SAN sieť spravuje jednoduchšie. Všetky dáta sú pohromade a potrebujeme menej ľudí na správu veľkého množstva dát.

SAN sieť je vhodné využiť v spoločnostiach s viacerými servermi. Môže poskytovať úložisko pre databázový či mailový server, server na zálohovanie alebo server zabezpečujúci streaming audia/videa. Všeobecne by sme mohli povedať že jej úložný priestor je vhodný pre servery, ktoré prevádzkujú služby závislé na rýchlom prístupu k dátam.

Naopak túto technológiu nieje veľmi vhodné používať ako úložisko napr. pre webový server alebo tie servery, ktoré nie sú až tak závislé na rýchlom prístupe k dátam. V prípade použitia optickej siete sú jednotlivé prvky dosť nákladné a pre malú firmu môžu znamenať zbytočne vyhodené peniaze.

1.2 Protokoly v SAN

Aby mohli jednotlivé prvky siete medzi sebou správne komunikovať musia mať spolu dohodnuté pravidlá na komunikáciu. Takýto súbor dohodnutých pravidiel nazývame protokol. V SAN sietiach existuje viacero protokolov ktoré je možné použiť.

Základným protokolom používaným v SAN sietiach je Fibre Channnel (FC) protokol. Vyžaduje na svoju komunikáciu špeciálny hardware čo niekedy nieje úplne najlacnejšie. Pomocou tohto protokolu sú dáta prepravované od servera ku dátovému úložisku alebo naopak. Spôsob akým budú tieto dáta prepravené (výber cesty a podobne) určuje zase iný použitý protokol, ktorý funguje na prepojovacích prvkoch. Medzi základné protokoly používané na prepojovacích prvkoch v FC SAN sieti patria FC-AL (Fibre Channel-Arbitrated Loop) a FC-SW (Fibre Channel-Switched Fabric).

Iné typy protokolov, ktoré môžeme v SAN sieti použiť sú založené na komunikácii cez ethernetovú IP (Internet Protokol) sieť. Tieto protokoly nevyžadujú špeciálne zariadenia na komunikáciu okrem tých, ktoré sa používajú v bežných ethernetových sietiach. Použitím týchto protokolov je možné komunikovať cez internet alebo cez iné siete založené na ethernetovom štandarde. Základným protokolom tejto skupiny je protokol iSCSI (Internet Small Computer System Interface), ktorý je popísaný v kapitole 2.

Existujú však aj iné protokoly komunikujúce cez ethernetovú sieť a využívané v SAN sieti. Medzi takéto protokoly patria : FCoE (Fibre Channel over Ethernet), iFCP (Internet Fibre Channel Protocol) a FCIP (Fibre Channel over IP).

1.3 Časti SAN siete

Tak ako väčšina sietí tak aj SAN sieť pozostáva z viacerých vrstiev. Logicky ju môžeme rozdeliť do troch vrstiev:

- Hosťovská vrstva
- Štruktúrna vrstva
- Úložná vrstva

Na obrázku 1.1 máme graficky znázornené rozdelenie jednotlivých vrstiev spolu s ukážkou prepojenia do lokálnej siete (LAN). Každá z týchto vrstiev má svoju funkciu, pričom rozdelenie do týchto jednotlivých vrstiev nám pomôže lepšie pochopiť ako systém funguje. Či už na prepojenie použijeme optickú alebo metalickú sieť tak na obe môžeme uplatniť toto rozdelenie.

1.3.1 Hosťovská vrstva

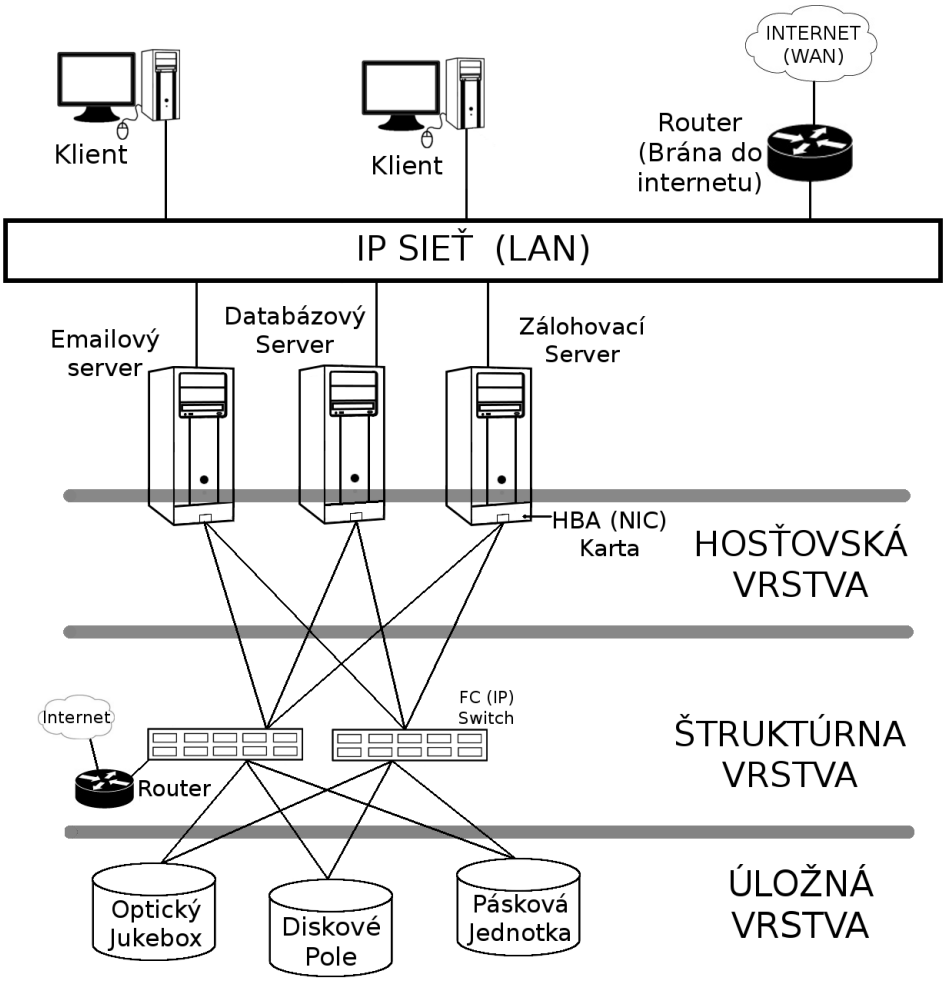
Do tejto vrstvy by sme mohli zaradiť fyzickú vrstvu serverov, káble a software potrebný na komunikáciu. Fyzickú vrstvu nám v tomto prípade predstavuje sieťová karta. Buď v prevedení HBA a GBIC modul, NIC karta spolu s integrovaným HW klientom alebo NIC karta a SW klient na aplikačnej vrstve.

HBA (Host Bus Adaper) – Host Bus adapter slúži ako vstupno/výstupná adaptérová karta pomocou ktorej je server pripojený do ostatnej časti siete.

- **GBIC (Gigabit Interface Connector)**
  Toto zariadenie sa nachádza na HBA adaptéri a slúži ako prípojné miesto pre optický kábel. Jeho úlohou je konvertovať optické pulzy na elektronické dáta alebo naopak. Toto zariadenie nieje iba súčasťou HBA ale nachádza sa aj v iných častiach SAN siete. GBIC môžeme nájsť na každom zariadení do ktorého je pripojený optický kábel.

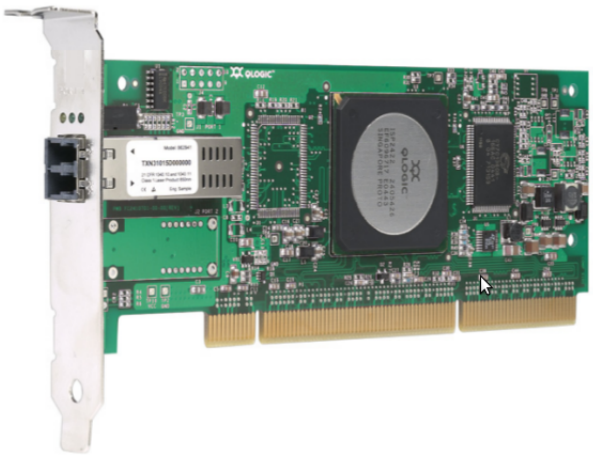
NIC (Network Interace Card) – Je to sieťová karta slúžiaca na pripojenie počítača do siete. Zabezpečuje komunikáciu medzi zariadeniami vrámci fyzickej vrstvy. Má v sebe od výrobcu napálené 48-bitové číslo označované ako MAC adresa. Každá NIC karta má vlastnú MAC adresu, ktorá je v sieti jedinečná. Najčastejšie NIC karta slúži na pripojenie počítača do ethernetovej IP siete. V súčastnosti je táto karta pridávaná do vybavenia počítača ako základné zariadenie slúžiace na pripojenie do internetu.

- **SW Klient (Software Client)**
  U softwarového klienta sa jedná o program bežiaci na serveri, ktorý vykonáva určitú svoju funkciu. Na svoju činnosť spotrebuváva výkon procesoru a tým znižuje výkon servera.
- **HW Klient (Hardware Client)**
  Hardwarový klient je zariadenie, napr. čip, ktorý je naprogramovaný na vykonávanie svojej funkcie. Vykonáva svoju činnosť svojpomocne, čiže nespotrebuváva procesorový výkon. Pokiaľ by sme použili iSCSI protokol na komunikáciu medzi SAN zariadeniami tak by nám tento klient generoval SCSI príkazy.



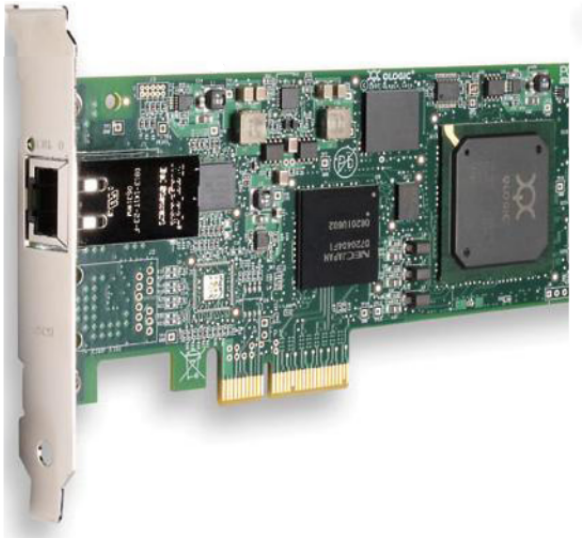
Obr. 1.1: Rozdelenie SAN siete do vrstiev a implementácia do lokálnej siete

Na obrázku 1.2 je zobrazený HBA adpatér spolu s GBIC modulom, ktorý môže byť napevno umiestnený v adaptéri alebo vyhotovený ako samostatná a výmenná jednotka. Táto sieťová karta sa používa pokiaľ použijeme na komunikáciu FC protokol.



Obr. 1.2: Host Bus Adapter spolu s integrovaným GBIC modulom [11]

Druhá varianta je NIC karta spolu s hardwarovým klientom, obr. 1.3. Táto varianta sa používa pokiaľ implementujeme SAN úložisko pomocou ethernetovej siete (použijeme napr. iSCSI protokol). NIC karta nám zabezpečí fyzické spojenie so sieťou a hardwarový klient generuje príkazy pre procesor. V prípade použitia iSCSI protokolu slúži na generovanie SCSI príkazov.



Obr. 1.3: NIC karta so zabudovaným hardwarovým klientom [11]

Jednou z najdôležitejších častí hosťovskej vrstvy a tiež celej SAN siete sú káble. Slúžia na prepojenie jednotlivých častí siete do jednotného celku. Pri SAN sietiach môžeme využiť ako optické tak metalické káble.

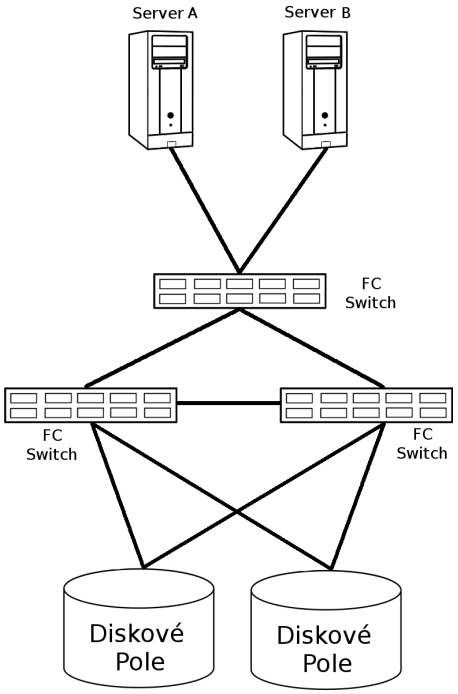
1.3.2 Štruktúrna vrstva

Štruktúrna vrstva tvorí časť, do ktorej su pripojené všetky prvky SAN siete. Je to prostredná časť siete obsahujúca prvky, ktoré spájajú jednotlivé časti SAN úložiska do jednotnej fyzickej siete. Úlohou týchto prvkov je zabezpečiť aby boli dáta prepravené od jedného zariadenia k druhému. Ako prepojovacie zariadenia môže slúžiť:

- ***Hub***
  Huby predstavujú jednu z lacnejších možností prepojenia SAN siete. No ich cena je na úkor výkonu. Poskytujú nižšie prenosové rýchlosti a ich veľkou nevýhodou je, že dokážu naraz obsluhovať iba jedno spojenie. V praxi to znamená že naraz môže komunikovať iba jeden server s dátovým úložiskom. Huby sa zväčša používajú iba vo FC SAN sieti. Čo sa týka ethernetových IP sietí tak tam sa huby už skoro nepoužívajú. Miesto nich sú používané switche, ktoré sú oproti nim výkonnejšie a bezpečnejšie.
- ***Switch***
  Pri použití optickej siete sú switche najčastejšie používané centrálne spojovacie body SAN úložiska. Oproti hubom poskytujú vyššie prenosové rýchlosti a dokážu naraz obsluhovať viacero spojení. To má ale za následok že ich cena je oproti hubom o dosť vyššia. Pre vyššiu spoľahlivosť siete sa zapája viacero switchov aby vytvorili dva alebo viacero možných ciest prístupu k serverom alebo dátam a tým predišli pádu siete. Príklad takéhoto zapojenia nájdeme na obrázku 1.4. Obdobnú topológiu môžeme vytvoriť aj pri použití IP switchov a ethernetovej siete. V ethernetovej IP sieti sú switche veľmi používané. Ich cena je oproti optickým switchom nižšia. Pokiaľ chceme prepájať prvky SAN úložiska iba vrámci jednej, povedzme firemnej, siete tak si vystačíme iba so switchom. Pokiaľ ale chceme prepájať úložné zariadenia z rôznych sietí tak budeme potrebovať ešte ďalšie zariadenie, ktoré nám bude slúžiť ako brána do inej sieti, poprípade do internetu. K týmto úcelom sa používa router.
- ***Router***
  Router, tiež nazývaný smerovač, je zariadenie, ktoré nám slúži na prepojenie viacerých sietí navzájom aby boli schopné komunikovať medzi sebou. Použitím routerov a internetovej siete sme schopný navzájom spojiť siete z hociakých krajín sveta. Jednotlivé routery používajú medzi sebou smerovacie protokoly

na určenie správnej cesty k cieľu. Príklad prepojenia dvoch SAN sietí pomocou routerov nájdeme na obrázku 1.5.

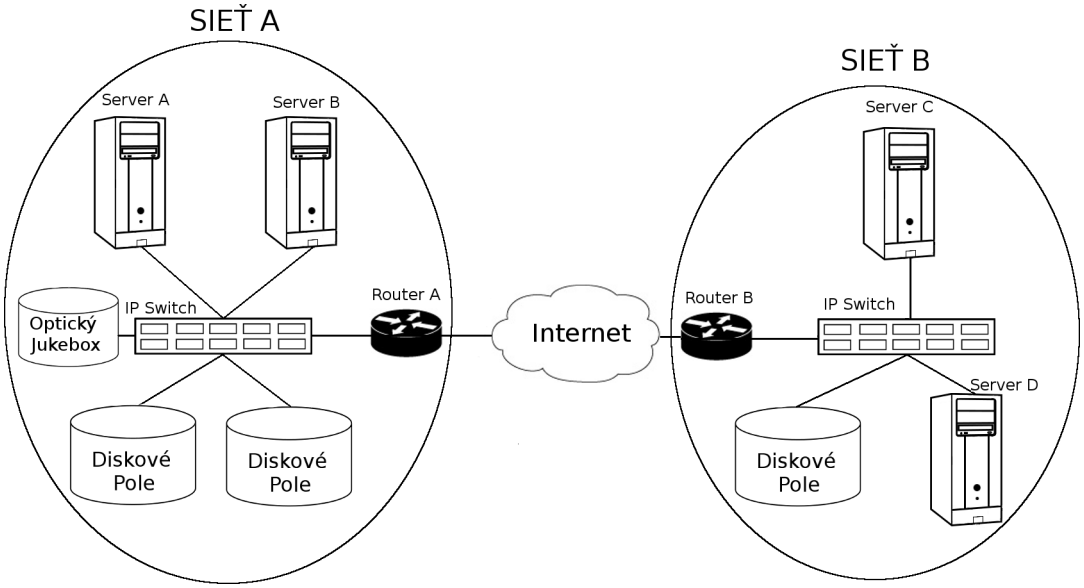
- ***Bridge***
  Vo Fibre Channel SAN sieti sa nám môže stať že budeme do nej chcieť pripojiť zariadenie komunikujúce iným protokolom, napr. SCSI. K tomuto účelu slúži prvok bridge. Obsahuje vstupy pre zariadenia komunikujúce ako SCSI tak aj FC protokolom. Tým dosiahneme preklad SCSI protokolu na FC protokol a naopak, a tým pádom vzájomnú komunikáciu týchto prvkov.



Obr. 1.4: Spoľahlivejšia SAN sieť vytvorená z viacerých switchov

V určitých prípadoch môže štruktúrna vrstva obsahovať iba prepojovacie káble. To je v prípade, že máme malé množstvo serverov a dátových úložísk a ich počet prípojných portov [1] postačuje na priame prepojenie. Toto prepojenie je vhodné pokiaľ chcem prepojiť servery a dátové úložiská vrámci jednej miestnosti poprípade jednej budovy, nakoľko použité káble majú svoj vzdialenostný limit. V takomto prípade nepotrebujeme žiaden switch ani router.

[1] Port - vstupno-výstupný externý konektor, ktorý je presne definovaný po mechanickej stránke (rozmery, rozmiestnenie kontaktov...), elektrickej stránke (napäťové úrovne, prúdové zaťaženie...) a komunikačnej stránke (použitý komunikačný protokol).



Obr. 1.5: Prepojenie dvoch SAN sietí cez internet za pomoci routerov

1.3.3 Storage vrstva

Všetky úložné zariadenia použité v SAN sieti patria do storage vrstvy. V tejto vrstve sú ukladané všetky naše dáta. V SAN sietiach sa na ukladanie dát využívajú diskové polia, páskové jednotky alebo optické jukeboxy.

Diskové polia sú zariadenia, ktoré obsahujú všetky disky pohromade spolu s vyvedenými prípojnými portami. Pomocou týchto portov je potom jednoduché disky pripojiť do switchu, hubu, routeru alebo priamo do servera. Pre efektívnejšie využívanie diskového priestoru sú jednotlivé disky spájané do RAID poľa. Tým môžeme dosiahnuť zrkadlenie dát a mať tak zálohu v prípade pádu disku alebo tým môžeme zvýšiť rýchlosť čítania a zapisovania dát.

Optický jukebox je zariadenie určené skôr na archiváciu dát než na uskladňovanie. Obsahuje prepisovaciu optickú mechaniku spolu s optickými diskami, na ktoré je pomocou aplikácie možno zapisovať a archivovať dáta.

Páskové jednotky sú najčastejšie používané na zálohovanie. Sú založené na princípe magnetického záznamu dát na páskovú mechaniku.

2 ISCSI

Protokol iSCSI patrí medzi protokoly používané v ethernetovej IP SAN sieti. Má architektúru typu klient/server, pričom pre server sa používa pomenovanie Target a pre klienta sa používa Initiator. Je popísaný v štandarde RFC 3720[13].

Initiator predstavuje klientskú časť iSCSI spojenia, ktorá má za úlohu iniciovať komunikáciu. Posiela SCSI príkazy cez IP sieť. Môže byť v prevedení ako : softwarový initiator (implementovaný v systéme vo forme kódu) alebo hardwarový initiator (používa na generovanie SCSI príkazov vlastné zariadenie).

Target zase predstavuje serverovú časť spojenia. Neslúži na iniciovanie spojenia ale iba čaká na požiadavok od initiatora a následne poskytne požadované vstupno/ výstupné dáta. Jeho úlohou je poskytovať úložné zariadenia klientom.

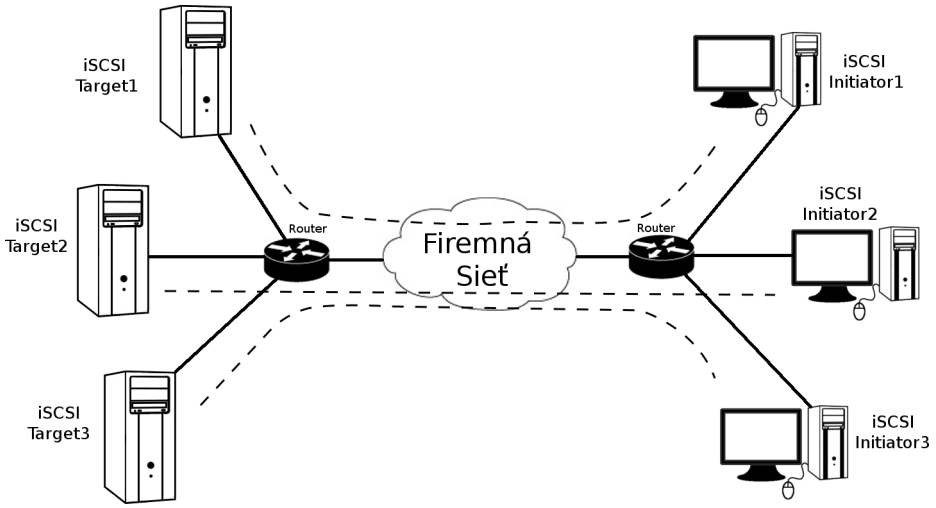
Komunikácia medzi iSCSI zariadeniami začína asi tak, že initiator vygeneruje SCSI príkaz pre target. Následne vytvorí paket [1], do ktorého vloží vygenerovaný SCSI príkaz a obalí ho IP obalom. Potom ho už môže vyslať do lokálnej siete alebo do internetu, ktoré fungujú na IP protokole. Po doručení paketu sa IP obal odstráni a target obdrží pôvodný SCSI príkaz.

Tým že iSCSI poskytuje prepojenie prostredníctvom ethernetových IP sietí môžu sa initiator a target spojiť cez viacero sietí alebo cez internet. Ako môžeme vidieť na obrázku 2.1, jednotlivé target servery môžu byť umiestnené v jednej firemnej sieti a pomocou routera pripojené do ostatným firemných sietí. Aby mohol initiator nadviazať spojenie s targetom tak musí mať k danej sieti prístup.

Smery komunikácie sú určované s ohľadom na initiator. Odchádzajúce spojenia sú definované ako spojenia od initiatora smerom k targetu. Naopak prichádzajúce spojenia sú spojenia odchádzajúce od targetu k initiatoru.

Protokol iSCSI má oproti Fibre Channel protokolu výhodu v tom, že je cenovo menej náročný, poskytuje neobmedzené vzdialenosté limity a koncové stanice nepotrebujú pri pripájaní do siete žiadne špeciálne vybavenie. Väčšina firiem pri zavádzaní SAN siete už má zavedenú svoju lokálnu sieť (LAN) fungujúcu na ethernetovom IP protokole, a tým že použijú ako protokol iSCSI nemusia investovať do tvorby novej siete ale môžu využiť stávajúcu. Tým sa dá ušetriť na správe kedže je to všetko implementované v jednej sieti nepotrebujeme ďalších správcov a stávajúci správcovia nemusia študovať nové technológie potrebné pre správu.

[1] Paket - ucelený blok dát, ktorý slúži na prenos dát po sieti. Má svoju štruktúru (hlavička, adresa odosielateľa a prijímateľa, dáta a kontrolný súčet) a nieje už deliteľný na menšie časti.



Obr. 2.1: Prepojenie iSCSI targetu a initiatora pomocou internetu

Protokol iSCSI môžeme používať na ethernetovej sieti o rôznych rýchlostiach. Celkový výkon nami vytvorenej SAN siete bude závislý na tom, akú verziu ethernet protokolu použijeme resp. na akú rýchlosť navrhneme jednotlivé prepojovacie prvky. Väčšina firemných sietí je tvorená UTP káblami kategórie 5 o ethernetovom štandarde 100Base-T. Takáto sieť nám dovolí komunikovať maximálnou rýchlosťou 100 megabitov za sekundu. To nám ale pre naše potreby nemusí vždy postačovať. V takomto prípade môžeme použiť vyššie štandardy ethernet protokolu. Najviac používaná verzia u IP SAN sietí v súčastnosti je 1 alebo 10 Gbit/s (10GBase-T). Pri využití týchto štandardov dokážeme dosiahnuť rýchlosť až 10 gigabitov za sekundu.

2.1 LUN - Logical Unit Number

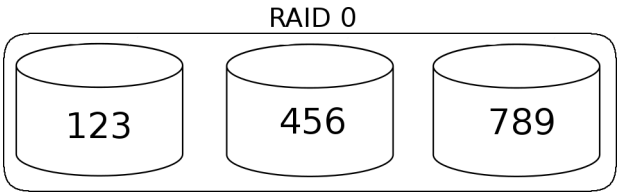
Hlavnou úlohou iSCSI targetu je poskytovanie úložného priestoru pre iSCSI initiator. Úložný priestor je identifikovaný skratkou LUN (Logical Unit Number) čo v preklade znamená Logická jednotka.

Logická jednotka (LUN) môže predstavovať buď jeden fyzický pevný disk alebo iba jeho určitú časť. Vezmime si ku príkladu target, ktorý obsahuje tri 100GB veľké pevné disky. V prípade, že je ako logická jednotka považovaný jeden fyzický disk, tak target môže ponúkať tri úložné priestory (LUNy). Povedzme, že každý LUN si pripojí iný initiator takže všetky tri logické jednotky budú obsadené. Dostaneme target, ktorý v prípade potreby nemôže zásobiť ďalší initiator úložným priestorom. V prípade, že potrebujeme zásobiť ďalší initiator tak nám neostáva nič iné iba zakúpiť ďalší fyzický disk a ten nastaviť ako ďalšiu LUN jednotku.

Čo však v prípade, že máme 100GB fyzický disk no initiatoru postačuje jednotka o veľkosti 20GB? Pridelením tomuto initiatoru 100GB jednotku budeme zbytočne plytvať úložným priestorom. Riešenie takéhoto problému je jednoduché. Stačí spojiť niekoľko pripojených fyzických diskov do jedného logického celku a ten si potom nakúskovať na menšie logické celky, ktoré budú initiatorom postačovať. Tým dokážeme efektívnejšie prerozdeliť úložný priestor a ušetriť pri nákupe stále nových a nových diskov. Aby sme toto dosiahli musíme potrebné pripojené disky spojiť do RAID poľa, ktoré zabezpečí že sa nám disky budú javiť ako jeden veľký disk.

RAID (Redundant Array of Independent Disks) je technológia, pomocou ktorej môžeme zlepšiť dostupnosť dát alebo zvýšiť výkon disku. To ako budú jednotlivé disky spojené nastavujeme správnym typom RAID poľa. Jednotlivé typy sú reprezentované číslami. Medzi základné typy patria RAID0, RAID1 a RAID5. Jednotlivé typy sa môžu aj kombinovať takže dostaneme pole RAID0+1, RAID1+0 alebo RAID5+0. Niekedy sa tieto kombinované typy označujú bez znamienka + takže sa môžeme stretnúť s označením ako RAID10 alebo RAID50. Bližšie informácie je možné nájsť v knihe [12].

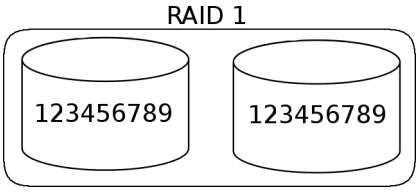
- ***RAID0***
  Pri tomto type sa nám dáta zapisujú po blokoch do všetkých diskoch, ktoré pridáme do RAIDu. Povedzme že máme v RAID poli 3 spojené fyzické disky, na ktoré chceme zapísať údaj „123456789“. Pole RAID0 nám zabezpečí to, že sa tento údaj rozkúskuje a rozdelí do diskov. V našom prípade sa „123“ zapíše do prvého disku, „456“ do druhého a „789“ do tretieho, obr. 2.2. Týmto dosiahneme vyšší výkon disku nakoľko pri čítaní údajov sa čítajú dáta z viacerých diskov naraz. Pole RAID0 poskytuje vyššý výkon no žiadnu odolnosť voči pádu disku. Pri páde hociktorého jedného disku stratíme dáta.



Obr. 2.2: Spôsob zápisu dát pri použití RAID0 poľa

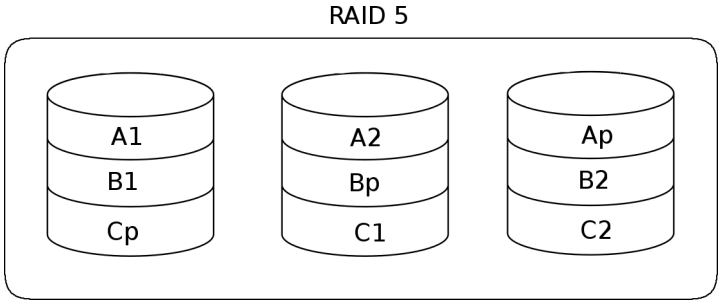
- ***RAID1***
  Tiež označovaný ako mirroring alebo zrkadlenie. Pri tomto zapojení sa dáta kopírujú na všetky (minimálne dva) disky čo nám vytvára zálohu v prípade pádu jedného disku. Poskytuje väčšiu rýchlosť čítania dát(číta z viacerých diskov naraz), no na druhej strane pomalší zápis (zapisuje sa na viacero diskov

naraz). Celková kapacita takéhoto poľa je rovná kapacite najmenšieho disku. Názornú ukážku nájdeme na obr. 2.3.



Obr. 2.3: Spôsob zrkadlenia dát pri použití RAID1 poľa

- ***RAID5***
  Obrázok 2.4 nám znázorňuje spôsob zápisu dát pri použití RAID5 poľa. Tento typ používa rozdeľovanie a zapisovanie dát po blokoch spolu s paritou na každom disku. Toto zapojenie vyžaduje minimálne 3 fyzické disky, pričom celková využiteľná kapacita je rovná $(n-1)*S$, kde n je počet použitých diskov a S je kapacita najmenšieho z nich. Takéto RAID pole vydrží pád jedného z diskov, nakoľko chýbajúce dáta sú dopočítavané z parity, ktorá je striedavo zapisovaná na jednotlivé disky. Vďaka tomu, že poskytuje vysokú rýchlosť a tiež odolnosť voči pádu patrí pole RAID5 medzi najviac používané v súčastnosti.



Obr. 2.4: Spôsob zapisovania dát spolu s paritou v RAID5 poli

2.2 Adresovanie

Aby mohli v sieti zariadenia spolu komunikovať potrebujú mať jednoznačne určené adresy. Pri použití iSCSI protokolu musia mať koncové body komunikácie (initiator a target) nastavené iqn alebo eui meno. Tieto mená slúžia ako adresa, pomocou ktorej dokážu initiator a target nadviazať spojenie. Viac ohľadom iSCSI mien je možné sa dočítať v knihe [5] a v RFC 3721[4].

iQN - iSCSI qualified name

V iSCSI protokole môžeme ako adresy použiť iqn mená. Jednotlivé tieto mená majú svoju štruktúru a sú konštruované tak, aby boli vrámci celého sveta jedinečné.

Príklad iqn mena môže byť napr. takýto : *iqn.2010-11.sk.priklad:nazov.disku.*

Slovo iqn na začiatku nám indikuje že sa jedná o iqn meno. Čísla 2010-11 nám predstavujú dátum spustenia daného servera, kde 2010 predstavuje rok a 11 je mesiac, v ktorom bol spustený. Ďalej nasleduje DNS [2] meno, ktoré však musí byť v obrátenom poradí, napr. doménové meno projekt.sk prevedieme do sk.projekt. Nakoniec nasleduje iSCSI unikátny reťazec znakov, ktorý jasne identifikuje konkrétne zariadenie v sieti. Doménové meno a unikátny reťazec sú oddelené zankom „:“.

EUI - enterprise unique identifier

Eui predstavuje takisto ako iqn adresu (meno) zariadenia používajúceho iSCSI protokol. Oproti iqn sa líši štruktúrou podľa ktorej je konštruované, no stále platí že musí byť vrámci sveta jedinečné.

Príklad eui mena : *eui.abcd12345678aaab.*

Eui používa EUI-64 formát, ktorý pozostáva zo 64 bitov. Syntax eui mena je zložený z „eui.“ slova, za ktorým nasleduje 16 hexadecimálnch čísel (64 bitov). Týchto 64 bitov môžeme zložiť z dvoch častí. Prvých 24 bitov obsahuje identifikačné číslo (ID) inštitúcie ktorá prevádzkuje daný server. Identifikačné čísla prideľuje organizácia IEEE [3], ktorá zabezpečuje jedinečnosť prideľovaných eui. Zvyšných 40 bitov doplní prevádzkovateľ serveru podľa vlastného uváženia. Celkovo dostaneme 64 bitové číslo zapísané v hexadecimálnom tvare.

[2] DNS (Domain Name System) - hierarchický systém, ktorý prekladá IP adresy na doménové názvy, ktoré sú ľahšie na zapamätovanie. Namiesto pamätania si napr. adresy 74.125.87.99 stačí si pamätať projekt.sk

[3] IEEE (Institute of Electrical and Electronics Engineers) - nezisková profesionálna organizácia zameraná na poskytovanie technickej inovácie v oblasti elektriny.

3 BEZPEČNOSŤ PROTOKOLU ISCSI

Pri každej komunikácii, ktorá prebieha cez sieť nám vzniká potenciálne bezpečnostné riziko. Pokiaľ sa jedná o komunikáciu cez internet musíme byť zvlásť opatrní nakoľko nevieme cez koľko sietí náš paket prechádza. Aj pri použití iSCSI protokolu musíme dbať na bezpečnosť dát ktoré prenášame. Existuje viacero spôsobov ako môže útočník odpočúvať našu komunikáciu a následne zneužiť získané dáta. No proti všetkému je možné sa brániť pokiaľ máme dostačujúce znalosti.

3.1 CHAP Autentifikácia

CHAP (Challenge Handshake Authentication Protocol) autentifikáciu používame v prípade, ak chceme aby sa najprv initiator a target autentifikovali a až potom zahájili komunikáciu. Používa sa pri spojení typu bod-bod, to znamená medzi dvomi koncovými zariadeniami siete. Touto metódou zabránime útočníkovi použiť útok nazývaný „Snoofing“, pri ktorom sa útočník vydáva za zariadenie s ktoým komunikujeme. Overovanie pomocou CHAP protokolu prebieha v 3 fázach. V prvej fáze vyšle autentifikátor (koncové zariadenie, ktoré vyžaduje overenie a špecifikuje overovací protokol) správu, ktorou vyzve peera (zariadenie na druhom konci spojenia, ktoré má byť overené autentifikátorom) aby sa identifikoval. Peer odpovie správou, v ktorej pošle číselnú hodnotu vypočítanú pomocou určitého hash algoritmu. Autentifikátor po prijatí správy danú hodnotu porovná so svojim výpočtom a pokiaľ sa zhodujú tak daného peera autentifikuje. CHAP autentifikácia je popísaná v odporúčaní RFC 1994[14]. CHAP autentifikácia môže byť dvojaká :

Jednoduchá autentifikácia slúži na overenie initiatora targetom. Tým že nastavíme autentifikáciu (meno a heslo) obmedzíme prístup iba na initiatory, ktorí poznajú dané údaje.

Obojstranná autentifikácia slúži na vzájomné overenie initiatora a targetu. Initiator musí poznať údaje potrebné pre autentifikáciu u targetu a naopak target musí poznať údaje pre autentifikáciu u initiatora.

Podľa RFC 3720[13] musí byť heslo použité pri CHAP autentifikácii väčšie než 96 bitov. Nami zadávané heslo pozostávajúce z písmen, čísel alebo znakov je pomocou ASCII tabuľky prevedené na bity. 96 bitov predstavuje 12 znakov, takže pri nastavovaní hesla musíme zadať minimálne 12 miestny reťazec. V prípade, že chceme použiť heslo kratšie než je 96 bitov (12 znakov) musíme použiť IP Security protokol (IPsec).

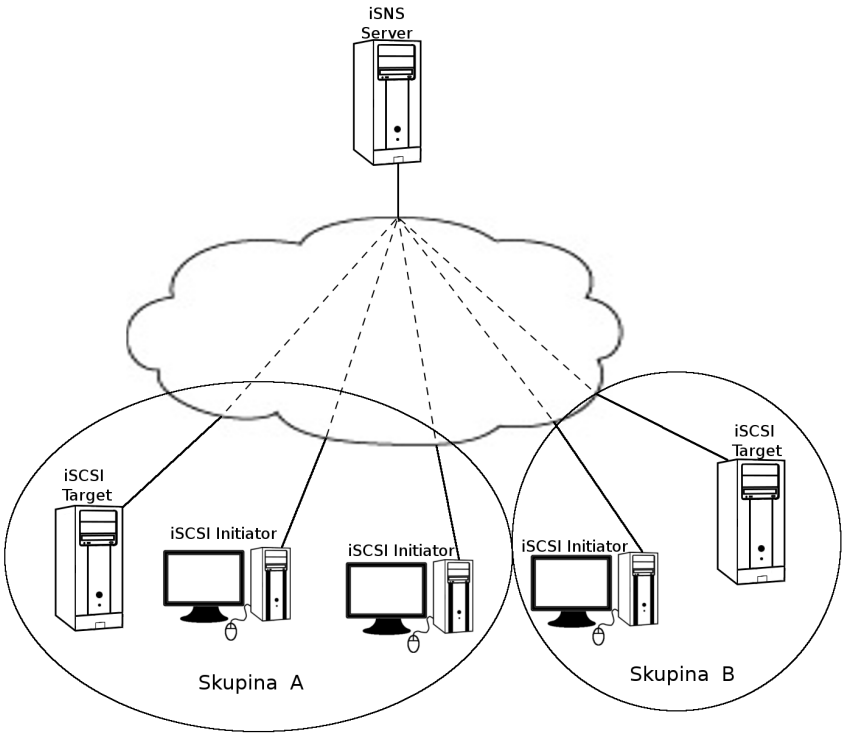
IPsec je protokol, ktorý slúži na zabezpečenie komunikácie na IP vrstve pomocou overovania a šifrovania paketov. Šifrovanie paketov je vhodné preto, aby nikto

kto sa nachádza medzi koncovými zariadeniami našeho bod-bod spojenia nemohol odpočúvať túto komunikáciu. Týmto zabezpečením vyradíme útočníka, ktorý chce použiť útok nazývaný „man-in-the-middle“ kde útočník odpočúva komunikáciu medzi koncovými bodmi. Útočník síce dáta odchytí ale kedže sú zašifrované nieje schopný prečítať ich obsah. Overovanie pravosti paketov je vhodné použiť aby sme si boli istí, či paket ktorý sme prijali je naozaj od odosielateľa s ktorým komunikujeme.

3.2 iSNS - Internet Storage Name Service

Ďalšou metódou, ktorú môžeme použiť pre zvýšenie bezpečnosti iSCSI protokolu je použitie iSNS servera, obr. 3.1. Používaním iSNS servera môžeme zoskupovať jednotlivé targety a initiatory do skupín, a tým zabezpečiť aby initiator mohol komunikovať iba s targetom, ktorý je pre neho určený. Jednotlivé initiatory a targety sa zaregistrujú u iSNS servera, ktorý zabezpečí ich prvotné spojenie. Po spojení už komunikácia prebieha priamo medzi initiatorom a targetom. iSNS server môže byť umiestnený buď priamo v sieti, v ktorej sa nachádzajú ostatné zariadenia alebo v inej, ku ktorej sa majú možnosť pripojiť.

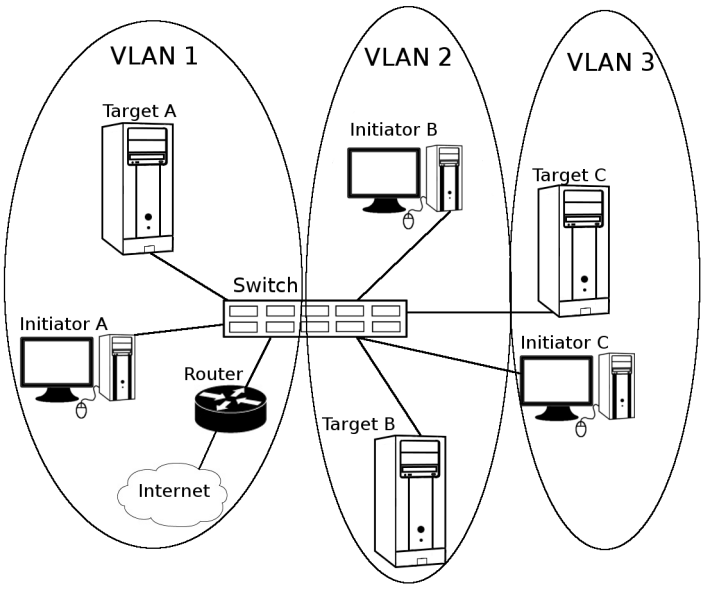
Nevýhodou používania iSNS servera je to, že pri jeho výpadku nebude môcť initiator nájsť svoje targety a nebude sa k nim môcť pripojiť.



Obr. 3.1: Prepojenie iSCSI targetu a initiatora pomocou iSNS servera

3.3 VLAN - Virtual LAN

Zabezpečenie pomocou VLAN spočíva v nakonfigurovaní IP Switcha tak, aby oddelil od seba initiatory a targety, ktoré medzi sebou nemajú komunikovať. Tým, že vytvoríme viacero virtuálnych lan sietí akoby vytvoríme z jedného switcha viacero menších (z menším počtom portov) pričom každý menší bude spravovať jednu sieť. Týmto rozdelením zabezpečíme, že prvky, ktoré nebudú v rovnakej sieti (VLANe) nebudú o sebe vedieť a tým pádom nebudú môcť spolu komunikovať. Príklad takéhoto rozdelenia nájdeme na obrázku 3.2.



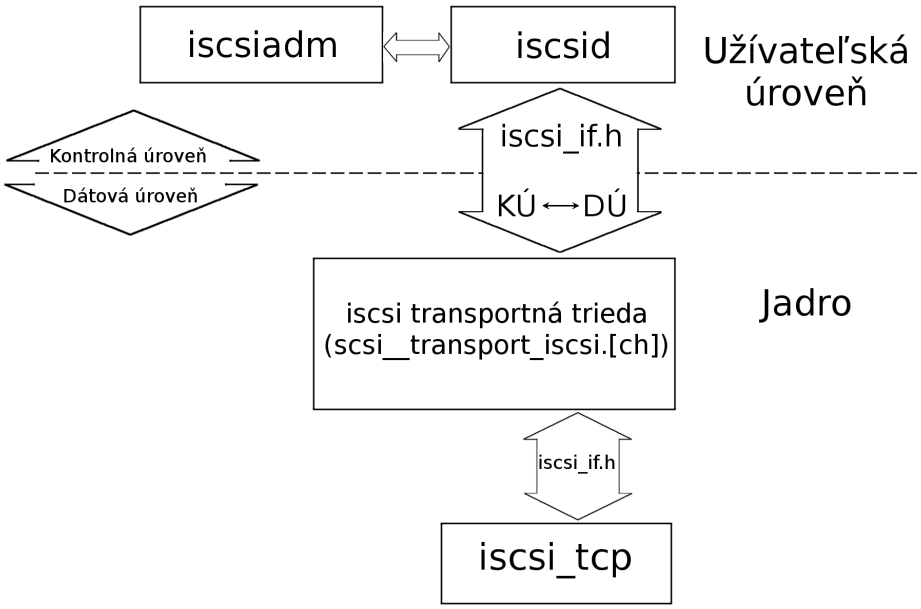
Obr. 3.2: Rozdelenie prvkov siete do virtuálnych sietí (VLAN)

4 IMPLEMENTÁCIA ISCSI V OS LINUX

Protokol iSCSI je v OS linux implementovaný prostredníctvom modulov stiahnuteľných pre jadro systému (kernel). Základné jadro nemôže z kapacitných dôvodov obsahovať ovládače na všetky druhy hardwaru. No potrebné ovládače je možné stiahnuť v podobe modulov.

Modul, alebo moduly sú časti kódu napísané v programovacom jazyku, ktoré môžu byť podľa potreby načítané, prípadne odstránené z jadra (kernelu). Jednoducho sa dá povedať, že moduly rozširujú funkcionalitu kernelu. Pridaním správneho modulu môžeme zabezpečiť správnu funkčnosť hardwaru či pridať podporu pre potrebný protokol alebo súborový systém.

Na obrázku 4.1 je možné vidieť blokovú schému, ktorá zobrazuje spôsob komunikácie iSCSI initiatora v operačnom systéme linux. Konkrétne sa jedná o program Open-iSCSI [10].



Obr. 4.1: Implementácia iSCSI protokolu v OS linux

Iscsiadm v tomto prípade predstavuje príkazové rozhranie, pomocou ktorého zadávame príkazy pre iSCSI protokol. Uchováva si výsledky vyhľadávania iSCSI zariadení v databáze a posiela príkazy pre iscsid. Iscsid zase predstavuje iSCSI démona [1] komunikujúceho s jadrom. Jeho úlohou je implementovať správy typu LOGIN, LOGOUT, TEXT atď. a komunikovať s iscsiadm aj s iscsi_if modulmi. Iscsi_if.h slúži ako medzi-procesové asynchrónne rozhranie špecifikované systémom. Predstavuje

[1] Démon - počítačový program bežiaci na pozadí.

rozhranie medzi užívateľskou úrovňou a jadrom a tiež medzi kontrolnou a dátovou úrovňou. Iscsi transportná trieda exportuje informácie o transporte, relácii a spojení cez sysfs (virtuálny súborový systém) z jadra do užívateľskej úrovne. Slúži tiež ako transportný prepínač pre viacero iSCSI realizácií. Spravuje zóny obsahujúce kontrolu prijatých PDU (protokolová dátová jednotka), úroveň chybovosti daného spojenia a odozvu na požiadavku pre nižšie vrstvy. Iscsi_tcp modul narozdiel od iscsi transportnej triedy kontroluje počet zón aby zabránil alokovaniu počas behu programu. Implementuje iSCSI dátovú cestu a zabezpečuje komunikáciu iSCSI cez TCP protokol a cez bežnú sieťovú kartu (NIC).

5 IMPLEMENTÁCIA ISCSI V OS MS WINDOWS SERVER

Operačný systém MS Windows nepatrí medzi systémy s otvoreným zdrojovým kódom ako Linux. Jeho zdrojové kódy niesú voľne prístupné pre verejnosť a nieje možné hlbšie zistiť ako je v ňom iSCSI protokol implementovaný. No aby bolo možné v OS Microsoft Windows komunikovať pomocou iSCSI protokolu, je potrebné mať nainštalované ovládače[1] zabezpečujúce správnu funkčnosť tohto protokolu. Viac ohľadom protokolu iSCSI v OS Windows je možné nájsť na stránkach spoločnosti Microsoft [9].

iSCSI Initiator

Aby bolo možné spravovať zariadenia komunikujúce iSCSI protokolom je potrebné mať nainštalovaný software na správu. V OS Microsoft Windows je možné ako iSCSI initiator použiť program priamo od spoločnosti Microsoft, a to Microsoft iSCSI Initiator [9]. V tomto programe sú obsiahnuté hneď ovládače pre iSCSI protokol potrebné pre správnu funkčnosť. V novších vydaniach operačného systému Microsoft je Microsoft iSCSI Initiator obsiahnutý už hneď po inštalácii a nieje nutné ho dodatočne doinštalovávať. Jedná sa o vydania Windows Server 2008 R2, Windows 7, Windows Server 2008 a Windows Vista. Staršie vydania systému ako Windows Server 2003, Windows XP a Windows 2000 tento program natívne neobsahujú a tiež neobsahujú ovládače pre iSCSI protokol. Aby bolo možné na týchto vydaniach prevádzkovať iSCSI initiator je potrebné tento software dodatočne doinštalovať.

iSCSI Target

Prevádzkovanie iSCSI targetu v OS Microsoft Windows je taktiež prevádzkované prostredníctvom programu, no jeho implementácia nieje však taká ako pri iSCSI initiatore. ISCSI target je implementovaný v špecializovaných serverových OS Microsoftu.

Microsoft Windows Storage Server je Microsoft Windows Server so špecializáciou na využitie so zariadeniami v NAS (Network-Attached Storage). Táto distribúcia obsahuje užívateľské rozhranie (Initial Configuration Tasks), pomocou ktorého je možné spravovať úložiská či zdielať zložky. Verzia 2008 obsahuje podporu pre iSCSI target v podobe implementovaného programu Microsoft iSCSI Software

[1] Ovládač - program, ktorý zabezpečuje spoluprácu medzi počítačovým programom a hardwarovým zariadením.

Target. Microsoft Windows Storage Server je možné nájsť aj vo verzii 2003. Microsoft Windows Storage Server 2003 je založený na verzii Windows Serveru 2003 a zase Microsoft Windows Storage Server 2008 na Windows Serveru 2008. Tieto verzie operačného systému sú predinštalovávané do zariadení, ktoré sa špecializujú práve na problematiku ohľadom spravovania úložísk.

Windows Unified Data Storage Server je platforma navrhnutá pre NAS systémy. Je pokračovaním Microsoft Windows Storage Server 2003 produktu spolu s novými funkciami ako je napr. Microsoft iSCSI Software Target zabezpečujúci prevádzkovanie iSCSI targetu.

6 KONFIGURÁCIA ISCSI TARGETU

Cieľom tohto bodu bolo nainštalovať a nakonfigurovať iSCSI target v prostredí OS linux. Jednotlivé konfigurácie boli prevádzané v OS, ktorý bol nainštalovaný vo virtuálnom prostredí programu Virtual Box [17].

6.1 Predinštalačné kroky

6.1.1 Výber linuxovej distribúcie

Ako prvý krok bolo nutné zvoliť vhodnú linuxovú distribúciu, na ktorej bude iSCSI target nainštalovaný. Pre potreby tejto práce bola zvolená serverová verzia distribúcie Ubuntu.

Ubuntu je distribúcia založená na Debian linuxe a je vydávaná každý polrok v novej verzii.

Dôvodov prečo bola vybraná práve distribúcia Ubuntu je niekoľko no hlavne preto, lebo:

- je to jednoduchá distribúcia na správu a používanie.
- má veľkú užívateľskú základňu s čím súvisí veľké množstvo dostupných návodov na internete.
- dostupnosť veľkého množstva inštalačných balíčkov, ktoré sú obsiahnuté v repozitároch [1].

Serverovú verzia bola zvolená preto, lebo neobsahuje grafické prostredie, ktoré by zbytočne zaťažovalo server a zaberalo úložný priestor. ISCSI target je možné nakonfigurovať za použitia konzoly (príkazového riadku) poprípade cez vzdialený prístup (SSH).

6.1.2 Výber iSCSI Targetu

Podobne ako linuxových distribúcií tak aj programov prevádzkujúcich iSCSI target existuje viacero. Aako iSCSI target bol vybraný program IET (iSCSI Enterprise Target).

ISCSI Enterprise Target (IET) je software, ktorý poskytuje úložisko pre klientov vrámci iSCSI protokolu. Je to open-source program, takže za jeho používanie nie je nutné platiť a je dostupný priamo z repozitárov Ubuntu ako inštalačný balíček, takže jeho inštalácia je jednoduchá.

[1] Repozitár - Server (najčastejšie), ktorý obsahuje balíčky rôznych softwarov, ktoré sú pripravené na inštaláciu. Jednotlivé balíčky je možné pomocou správcu balíkov jednoducho stiahnuť a nainštalovať.

Medzi ďalšie výhodi patrí napríklad to, že:

- je dosť rozšírený, odskúšaný a stabilný.
- nie je potrebné aplikovať žiadne dodatočné patche do kernelu [2].
- podporuje najnovšie používané kernely 2.6.xx.
- nastavovanie nových LUNov pre zdieľanie a pridávanie účtov pre autentifikáciu je možné prevádzať dynamicky.
- poskytuje porovnateľný alebo vyšší výkon v porovnaní s jeho konkurenciu.
- podporuje zapezpečenie pomocou iSNS servera.

6.1.3 Príprava pevných diskov

Pred inštalovaním a konfiguráciou IET bolo nutné pevné disky pripraviť, aby boli zdieľateľné ako logické jednotky (LUNy). Pre potreby tejto práce boli vytvorené 3 pevné disky v programe VirtualBox a pripojené pomocou SCSI radiča do nainštalovanej distribúcie Ubuntu.

Takto pridané disky je už možné používať ako logické jednotky (LUNy) ale pre lepšiu dostupnosť a výkon boli spojené do RAID poľa a následne rozdelené na virtuálne disky (partície).

Vytvorenie RAID poľa

Aby bolo možné inštalovať a následne konfigurovať nové veci v Ubuntu, je potrebné pracovať na počítači pod administrátorským účtom. Administrátorom v Ubuntu a celkovo v linuxových systémoch je užívateľ root, takže je potrebné zadávať všetky príkazy spojené s inštaláciou a konfiguráciou pod jeho právomocami.

RAID pole je možné vytvoriť pomocou viacerých programov. Pre tento účel bol zvolený program **mdadm** [15]. Po naformátovaní diskov podľa postupu uvedenom v literatúre [8] bolo RAID pole vytvorené zadaním nasledujúceho príkazu.

```
mdadm -C /dev/md0 --level=5 --raid-devices=3 /dev/sdb1 /dev/sdc1 /dev/sdd1
```

Tento príkaz vytvorí RAID pole md0 kategórie 5, ktoré pozostáva z 3 zariadení, a to /dev/sdb1, /dev/sdc1 a /dev/sdd1. Počet zariadení záleží na počte fyzických diskov, ktoré majú byť pridané do poľa čo v tomto prípade predstavuje práve 3 disky, vytvorené programom VirtualBox. Označenie a cestu k diskom je možné zistiť z výpisu príkazu **fdisk**. Jeho jednotlivé možnosti a nastavenia sú v manuálovej stránke [15].

[2] Kernel - centrálny komponent slúžiaci ako vrstva kompatibility medzi hardvérom a softvérom.

Vytvorenie logických diskov (partícií)

Aby bolo vytvorené RAID pole efektívnejšie využité je vhodnejšie ho prerozdeliť na menšie ale postačujúce časti. K tomuto účelu bol opäť použitý **fdisk** [15].

Program fdisk obsahuje textové menu pomocou ktorého je možné vytvárať jednotlivé partície o rôznej veľkosti. Zadaním príkazu

```
fdisk /dev/md0
```

sa vyvolá práve spomínané menu. Zadaním písmena „m“ v danom menu sa vyvolá pomocník obsahujúci zoznam funkcií.

Vytvorenie novej partície sa vykonáva pomocou písmena „n“. Jeho zadaním sa vyvolá ďalšie menu zobrazujúce možnosť výberu medzi primárnou a rozšírenou partíciou. Je potrebná primárna partícia, takže je potrebné zadať písmeno „p“ a následne podľa poradia zvoliť číslo partície.

V ďalšom kroku je potrebné zvoliť začiatok partície. Program automaticky doplní prvý voľný cylinder takže stačí iba potvrdiť stlačením klávesy ENTER. Koniec vytváranej partície je možné zvoliť pomocou viacerých jednotiek. Vytvorenie partície o veľkosti 500 MB sa zadáva ako „+500 MB“.

Výslednú partíciu stačí už iba zapísať na disk zadaním písmena „w“. V nasledujúcom výpise je názorne zobrazený celý postup.

Výpis kódu 6.1: Postup pri vytváraní logickej partície

```
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
 p
Partition number (1-4): 1
First cylinder (1-452, default 1): ENTER
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-452, default 452): +500MB

Command (m for help): w
The partition table has been altered!
Syncing disks.
```

6.2 Inštalácia a konfigurácia IET

Tak ako už bolo spomenuté tak IET je program obsiahnutý v repozitároch Ubuntu. To síce uľahčuje jeho inštaláciu ale je podmienkou mať pripojenie k internetu aby sa balíček mohol z repozitára stiahnuť.

Inštalácia iSCSI Enterprise Target (IET)

Inštalácia programu IET bola prevádzaná pomocou príkazoveho riadku a správcu balíkov **apt**([15]). Program IET je v repozitároch Ubuntu uložený pod názvom „iscsitarget“. Jeho inštalácia bola realizovaná zadaním príkazu uvedeného nižšie.

```
apt-get install iscsitarget
```

Príkaz „apt-get install“ nariadi správcovi balíkov (apt) aby nainštaloval zvolený balík, čo v tomto prípade predstavuje balík iscsitarget.

Konfigurácia IET

Po nainštalovaní bolo potrebné IET správne nakonfigurovať a spustiť. Aby bolo možné IET spustiť, bolo potrebné upraviť konfiguračný súbor povoľujúci spustenie iscsitargetu v systéme. To sa vykonáva pomocou textového editora napr. „nano“, ktorý je obsiahnutý v základnej inštalácii Ubuntu.

Editovanie sa zahájuje príkazom:

```
nano /etc/default/iscsitarget
```

Obsah daného textového súboru bolo potrebné upraviť do požadovanej formy. Konkrétne bolo potrebné zmeniť hodnotu „false“ na „true“, takže v konečnom dôsledku vyzeral obsah súboru nasledovne.

```
ISCSITARGET_ENABLE = true
```

Stlačením Ctrl+x a následným zadaním znaku „y“ sa uložia zmeny v súbore a ukončí sa editor nano. Po tejto zmene je už možné IET spustiť. No zatiaľ ešte nieje nakonfigurovaný aby poskytoval logivké jednotky (LUNy) pre iscsi initiatory. Konfigurácia sa prevádza nastavením a zmenou parametrov obsiahnutých v konfiguračnom súbore programu. Program IET má svoj konfiguračný súbor v zložke „/etc/iet/“ a volá sa **ietd.conf**. Podobne ako v predchádzajúcom prípade tak aj teraz bol na editovanie použitý editor nano.

Editovanie bolo spustené nasledujúcim príkazom:

```
nano /etc/iet/ietd.conf
```

Pri editovaní konfiguračných súborov v linuxe obecne plati, že každý riadok začínajúci znakom „#“ je zakomentovaný, takže program ho neberie v úvahu. Konfiguračný súbor IET už obsahuje informácie ohľadom nastavenia jednotlivých logických jednotiek, potrebné a voliteľné parametre pri nastavovaní a ich vysvetlenia. Novú logickú jednotku je možné pridať dopísaním patričných záznamov a parametrov do ľubovoľnej časti konfiguračného súboru. Pre lepšiu prehľadnosť boli pridávané jednotlivé záznamy na koniec súboru.

Pri konfigurovaní nového targetu je nutné nastaviť niekoľko povinných parametrov, bez ktorých by target nebolo možné zdielať. Podľa potreby je potom možné pridávať jednotlivé voliteľné parametre. Zoznam všetkých voliteľných parametrov spolu s vysvetlením sú obsiahnuté v manuálových stránkach programu IET [6].

Medzi povinné parametre patrí názov targetu (Target <názov>), číslo logickej jednotky (Lun <číslo>) spolu s umiestnením disku alebo vytvorenej partície (Path=<umiestnenie>) a typ logickej jednotky (Type=(fileio|blockio)). Každý nový parameter sa zapisuje do nového riadku vždy k prislúchajúcemu targetu.

Pre potreby práce boli vytvorené 3 targety a ku každému pridelená jedna z partícií, vytvorených v bode 6.1.3. Okrem povinných parametrov boli použité aj voliteľný parameter nastavenia týkajúci sa zabezpečenia iSCSI targetu. Nasledujúci výpis 6.2 je výber z konfiguračného súboru programu IET, ktorý obsahuje všetky nezakomentované, čiže doplnené nastavenia.

Výpis kódu 6.2: Nezakomentovaná časť konfiguračného súboru programu IET

```
iSNSServer 147.229.204.50
iSNSAccessControl No

Target  iqn.2010-11.sk.testing:disk1
        Lun 0 Path=/dev/sdb1,Type=fileio

Target  iqn.2010-11.sk.testing:disk2
        Lun 1 Path=/dev/sdc1,Type=fileio
        IncomingUser san trinastznakov

Target  iqn.2010-11.sk.testing:disk3
        Lun 2 Path=/dev/sdd1,Type=fileio
        IncomingUser san trinastznakov
        OutgoingUser mas abcde12345abc
```

Aby bolo možné poznať, ktoré nastavenia patria ku ktorému targetu, musí každý nový target začínať slovom „Target“. Za týmto slovom nasleduje iqn názov 2.2. Do nového riadku je potrebné zadať ďalší povinný parameter a ten sa týka nastavenia LUN jednotky. To sa prevádza tak, že sa za slovom „Lun“ dá číslo (0-16384) logickej jednotky, za ním sa zadá cesta k disku alebo partícii (Path) a nakoniec sa nastaví typ (Type) logickej jednotky. V tomto nastavení bol ako typ zvolený „fileio“. Zvolený bol preto, lebo je vhodný pokiaľ sa za LUN používa priamo fyzický disk, čo je práve tento prípad.

Ostatné parametre, ktoré je možné vidieť vo výpise 6.2 sú voliteľné a slúžia na zabezpečenie iSCSI komunikácie. Parametre IncomingUser a OutgoingUser slúžia na overenie pomocou CHAP autentifikácie. IncomingUser predstavuje jednoduchú autentifikáciu a OutgoingUser predstavuje obojstrannú autentifikáciu. Zápis oboch parametrov je rovnaký, kde za IncomingUser alebo OutgoingUser nasleduje meno a tak heslo.

Parameter iSNSServer slúži na nastavenie IP adresy iSNS servera, ku ktorému sa má target registrovať. Tento parameter je globálny takže platí pre všetky vytvorené targety. Spolu s ním je parameter iSNSAccessControl, ktorý nám nastavuje či sa initiator môže pripojiť k targetu aj priamo alebo iba pomocou iSNS servera. Pokiaľ sa za iSNSAccessControl napíše „Yes“, tak pripojenie bude možné iba pomocou iSNS servera.

Po úspešnom nakonfigurovaní jednotlivých targetov je možné IET zapnúť. Zapínanie a taktiež vypínanie sa prevádza pomocou príkazu service zadaním do príkazového riadku

```
service iscsitarget start
```

pre štart a

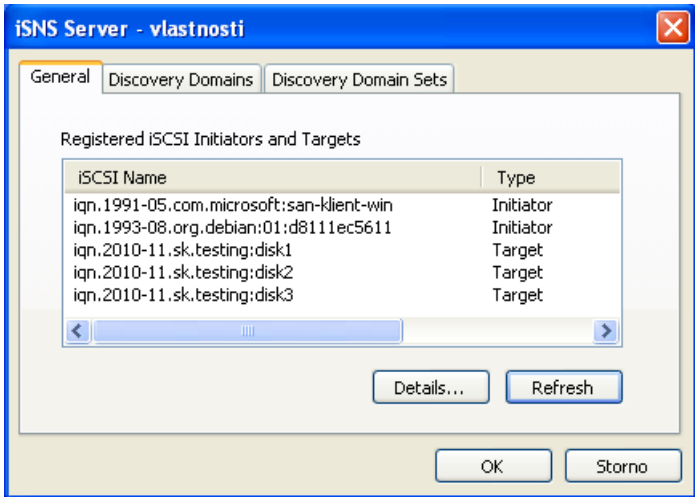
```
service iscsitarget stop
```

pre vypnutie IET programu.

6.3 Testovanie iSNS Servera

Pri konfigurácii zabezpečenia IET bolo prakticky odskúšané použitie iSNS servera na spojenie initiatora a targetu. K tomuto účelu bola do OS Microsoft Windows XP nainštalovaná aplikáciu **iSNS Server** od spoločnosti Microsoft. Použitý bol iSCSI target s tromi LUN jednotkami a 2 iSCSI initiatory.

Ako ukazuje obrázok 6.1 tak jednotlivé targety a initiatory sa registrovali u iSNS servera, pomocou ktorého ich bolo možné deliť do skupín.



Obr. 6.1: Zoznam registrovaných iSCSI zariadení na iSNS serveri

Program automaticky priradí všetky zariadenia do skupiny, ktorá je označená ako "Default DD", takže defaultne môže komunikovať initiator s hociktorým targetom. Používanie tejto skupiny je možné deaktivovať a navoliť si podľa potreby vlastnú skupinu pozostávajúcu iba z určitých iSCSI zariadení. Jednotlivé vytvorené skupiny je nutné ešte aktivovať pridaním do Domény a zaškrtnutím políčka „Enable“. V jednej doméne je možné mať viacero vytvorených skupín takže je možné spúšťať viacero skupín naraz.

ISNS server je veľmi vhodný pri správe veľkého počtu iSCSI targetov a initiatorov. Uľahčuje prácu initiatoru pri vyhľadávaní logických jednotiek ako aj správcom pri zlepšení bezpečnosti iSCSI komunikácie.

7 KONFIGURÁCIA ISCSI INITIATORA

Následne budú popísané návody ako pripojiť target k iSCSI initiatoru. Ako príkladný portál, na ktorom je prevádzkovaný iSCSI target bude slúžiť IET target nakonfigurovaný v bode 6.

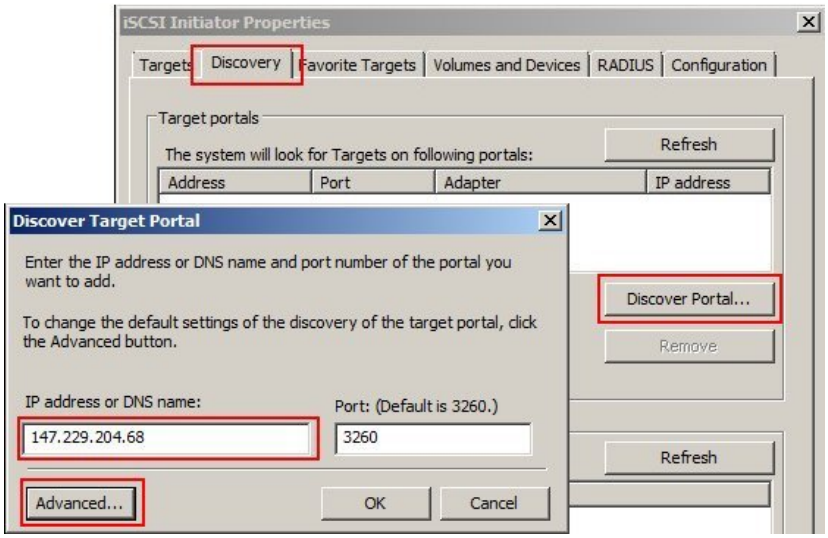
7.1 Konfigurácia iSCSI initiatora v prostredí OS Windows

Možnosť spravovať iscsi initiatory v OS windows je hneď po inštalácii prístupná od verzie systému Windows Vista a vyššie. Nasledujúci návod je vytváraný pre Windows Server 2008 RC2. Je ho však možné použiť aj pre iné systémy obsahujúce Microsoft iSCSI klienta pre protokol iscsi.

Nastavenie adresy portálu

Konfigurácia iscsi initiatora spočíva vo viacerých krokoch. Ako prvý krok je nutné zadať adresu portálu, na ktorom je sputený iscsi target. Adresa môže mať podobu IP adresy alebo doménového mena (DNS).

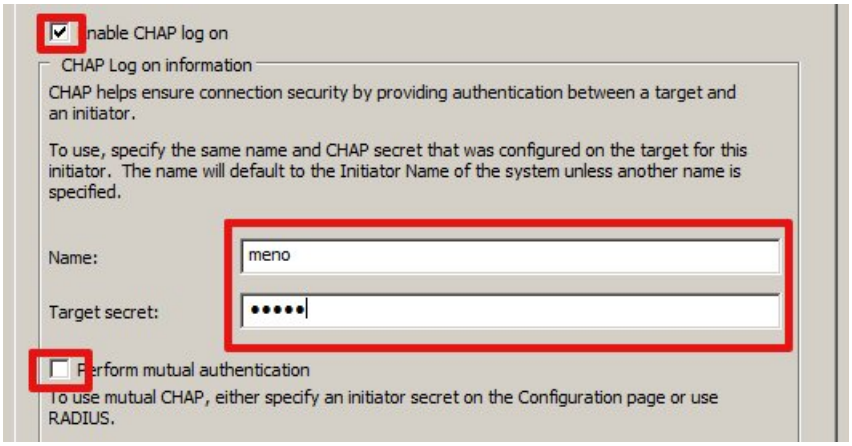
Toto nastavenie sa v Microsoft Initiatore prevádza na druhej záložke označenej ako „Discovery“. Na tejto záložke sa po stlačení tlačidla „Discover Portal“ zobrazí tabuľka 7.1, do ktorej je možné zadať adresu portálu a poprípade aj zmeniť port keď target vysiela na inom než je predvolený port 3260.



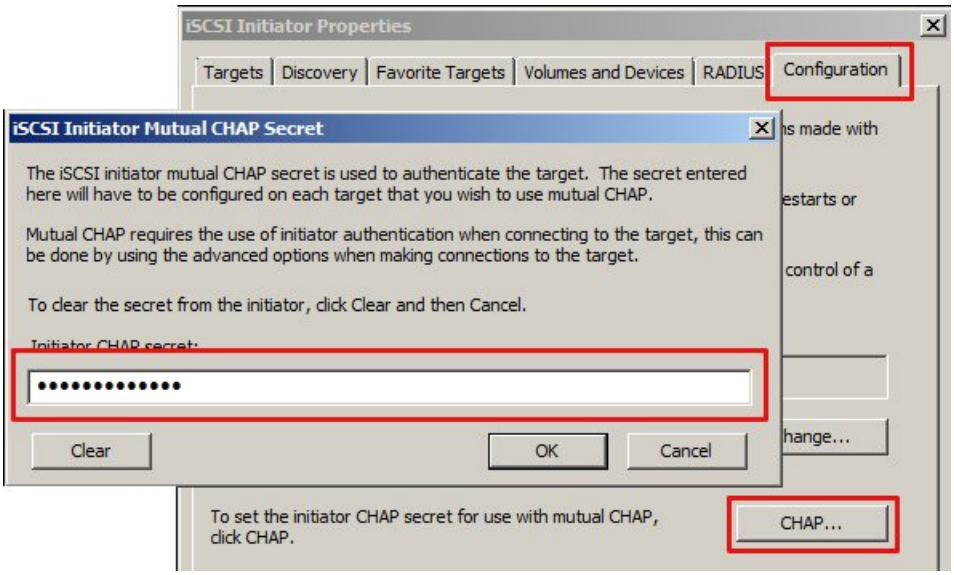
Obr. 7.1: Nastavenie IP adresy pre portál (iSCSI Target)

Nastavenie autentifikácie pre portál

V prípade že portál vyžaduje overenie pomocou CHAP autentifikácie, je nutné ju nastaviť kliknutím na tlačidlo „Advanced“. V zobrazenom okne 7.2 sa po zaškrtnutí voľby „Enable CHAP“ sprístupní možnosť zadať meno a heslo. Do príslušných políčok je nutné zadať meno a heslo nastavené v konfigurácii iscsi targetu. Pokiaľ sa jedná o jednoduchú autentifikáciu (v programe IET označovaná ako IncomingUser) stačí zadať meno, heslo a potvrdiť.



Obr. 7.2: Nastavenie autentifikácie pre portál



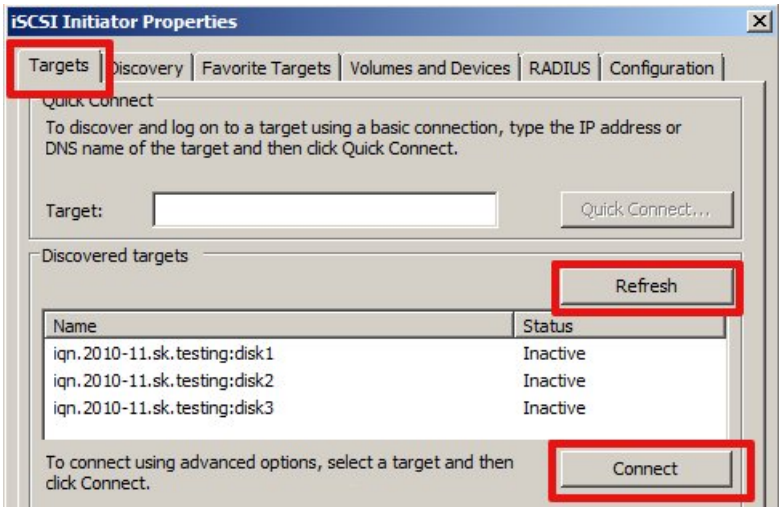
Obr. 7.3: Nastavenie mutual autentifikácie pre portál

V prípade použitia obojstrannej autentifikácie (v IET ako OutgoingUser) je nutné ešte zaškrtnúť voľbu „Perform mutual authentication“ a mať nastavené heslo

pre autentifikáciu initiatora. Táto možnosť sa nastavuje v poslednej záložke programu nazvanej „Configuration“, kde sa po stlačení tlačidla „CHAP“ objaví okno 7.3 pre zadanie hesla. Microsoft Initiator nezohľadňuje meno pri mutual autentifikácii takže ho nieje potrebné nastavovať.

Pripojenie targetov

Ako ďalší krok je pripojenie targetov. Po správnom nastavení adresy a autentifikácie portálu sa v prvej záložke programu nazvanej „Targets“ zobrazí zoznam targetov. Pokiaľ by tomu tak nebolo tak je nutné obnoviť zoznam stlačením tlačidla „Refresh“. Teraz už neostáva nič iné iba vybrať správny target, kliknúť na tlačidlo „Connect“ a potvrdiť pripojenie 7.4. Takýmto jednoduchým spôsobom je možné pripojiť viacero targetov, ktoré nie sú chránené autentifikáciou.



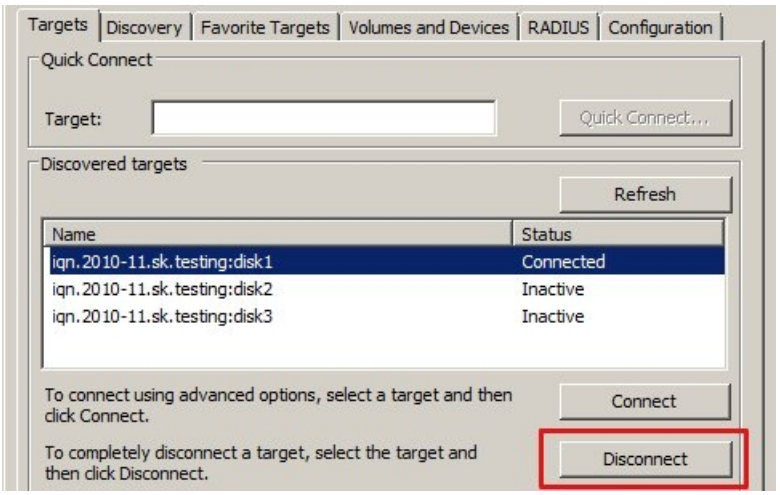
Obr. 7.4: Pripojenie targetu bez použitia autentifikácie

Nastavenie autentifikácie pre target

Pre pripojenie targetov, ktoré vyžadujú overenie pomocoou CHAP autentifikácie je nutné nastaviť potrebné údaje. Proces nastavovania je veľmi podobný ako pri nastavovaní autentifikácie pre portál. Po označení požadovaného targetu a stlačení tlačidla „Connect“ podľa predchádzajúceho návodu, je možné autentifikáciu nastaviť stlačením „Advanced“ tlačidla. Tým sa vyvolá okno kde rovnakým postupom ako v časti 7.1 možno nastaviť meno a heslo potrebné pre pripojenie targetu.

Odpojenie targetu

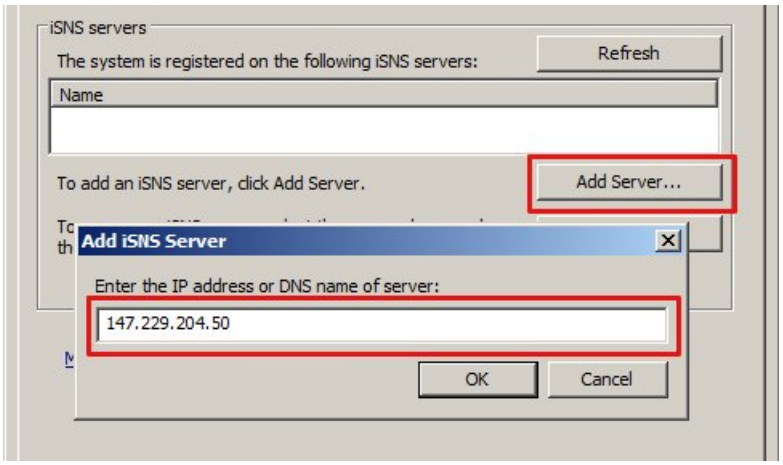
Odpájanie pripojeného targetu je možné jednoduchým kliknutí na tlačidlo „Disconnect“ v prvej záložke programu. Stačí označiť, ktorý target má byť odpojený a stlačiť Disconnect 7.5.



Obr. 7.5: Odpojenie pripojeného targetu

Nastavenie adresy pre iSNS Server

Adresa iSNS servera sa nastavuje v rovnakej záložke programu ako adresa portálu (záložka „Discovery“). Po stlačení tlačidla „Add Server“ 7.6 sa do zobrazeného okna zadá adresa iSNS Servera, u ktorého sa má initiator registrovať.



Obr. 7.6: Nastavenie adresy iSNS Servera

7.2 Konfigurácia iSCSI initiatora v prostredí OS Linux

Pripájanie targetu v prostredí OS Linux zabezpečuje v tomto prípade program Open-iSCSI [10]. Na rozdiel od klienta, ktorý je použitý v OS Windows neobsahuje grafické prostredie a je konfigurovaný iba za použitia príkazov poprípade editovaním textových súborov. Na inštaláciu programu a následné pripájanie targetov je nutné mať práva superužívateľa (roota). Preto je všetky nižšie spomínané príkazy nutné zadávať pod jeho právami. Nasledujúci postup je vytváraný pre linuxovú distribúciu Ubuntu.

Inštalácia Open-iSCSI

Program Open-iSCSI sa nachádza v repozitároch, takže jeho inštalácia je jednoduchá za použitia správcu balíkov „apt“. Inštalácia sa prevádza nasledujúcim príkazom.

```
apt-get install open-iscsi
```

Nastavenie autentifikácie pre portál

Program Open-iSCSI používa na správu pomocný program „iscsiadm“. Detailné info o jeho funkciách je obsiahnuté v manuálových stránkach [15].

Celý proces pripájania targetu sa skladá z viacerých krokov. Pokiaľ portál používa CHAP autentifikáciu na pripájanie sa k nemu, je dobré ju nastaviť hneď na začiatku. Vyžadované prihlasovacie meno a heslo sa nastavujú v konfiguračnom súbore programu. Ten sa nachádza v priečinku /etc/iscsi/ a má názov iscsid.conf. Vhodným textovým editorom je nutné upraviť jeho obsah na požadovaný tvar. Zadaním nasledujúceho prákazu sa otvorí konfiguračný súbor k editácii.

```
nano /etc/iscsi/iscsid.conf
```

V súbore je potrebné nájsť sekciu „CHAP Settings“ a upraviť vybrané riadky. Pokiaľ je pred riadkom znak „#“ znamená to, že je riadok zakomentovaný. Odstránením tohto znaku sa príkaz na danom riadku zohľadňuje v konfigurácii programu.

Pokiaľ portál vyžaduje iba jednoduchú autentifikáciu, je potrebné konfiguračný súbor upraviť podľa nasledujúceho výpisu 7.1 .

Výpis kódu 7.1: Skrátený výpis obsahu konfiguračného súboru iscsid.conf

```
# To enable CHAP authentication set node.session.auth.authmethod
# to CHAP. The default is None.
node.session.auth.authmethod = CHAP

# To set a CHAP username and password for initiator
# authentication by the target(s), uncomment the following lines:
node.session.auth.username = 'MENO'
node.session.auth.password = 'HESLO'
```

V prípade použitia obojstrannej autentifikácie je potrebné ešte dodať meno a heslo identifikujúce initiator. Ukážka je na výpise 7.2 .

Výpis kódu 7.2: Skrátený výpis obsahu konfiguračného súboru iscsid.conf

```
# To enable CHAP authentication set node.session.auth.authmethod
# to CHAP. The default is None.
node.session.auth.authmethod = CHAP

# To set a CHAP username and password for initiator
# authentication by the target(s), uncomment the following lines:
node.session.auth.username = 'MENO'
node.session.auth.password = 'HESLO'

# To set a CHAP username and password for target(s)
# authentication by the initiator, uncomment the following lines:
node.session.auth.username_in = 'MENO'
node.session.auth.password_in = 'HESLO'
```

Získavanie zoznamu targetov

Po správnom zeditovaní súboru a jeho následnom uložení je možné pristúpiť k zisťovaniu dostupných targetov na portáli. Táto voľba sa vykonáva nasledujúcim príkazom.

```
iscsiadm -m discovery -t st -p 147.229.204.68
```

Prepínačom „-m“ sa určuje mód v akom má iscsiadm pracovať. V tomto prípade je potrebné vyhľadať targety takže je zvolený mód „discovery“. Ďalší prepínač „-t“ určuje typ zariadenia ktoré sa má prehľadávať. Jeho parameter „st“ predstavuje protokol, ktorý umožní každému iSCSI targetu poslať svoj zoznam dostupných targetov. Posledný prepínač „-p“ označuje adresu a port portálu. Pokiaľ nieje zadaný port tak program uvažuje prednastavený port 3260.

Výpis zadaného príkazu by mal vyzerať obdobne ako nasledujúci výpis 7.3.

Výpis kódu 7.3: Výpis príkazu „iscsiadm -m discovery -t st -p 147.229.204.68“

```
147.229.204.68:3260,1 iqn.2010-11.sk.testing:disk2
147.229.204.68:3260,1 iqn.2010-11.sk.testing:disk1
147.229.204.68:3260,1 iqn.2010-11.sk.testing:disk3
```

Tento výpis sa skladá z adresy portálu spolu s portom (147.229.204.68:3260), čísla target skupiny (1) a názvu targetu (iqn.2010-11.sk.testing:disk2).

Pripojenie targetov

Target je možné pripojiť zadaním príkazu obsahujúceho názov targetu a adresu portálu. Tieto informácie sú obsiahnuté vo výpise z discovery módu (predchádzajúci krok). Syntax príkazu je zobrazená v nasledujúcom príkaze.

```
iscsiadm -m node -T iqn.2010-11.sk.testing:disk1 -p 147.229.204.68:3260 --login
```

Tentoraz je prepínačom „m“ nastavený mód „node“. Ďalší prepínač „-T“ značí názov targetu a „-p“ opäť adresu a port portálu. Na konci je parameter „--login“, ktorým sa zabezpečí pripojenie targetu.

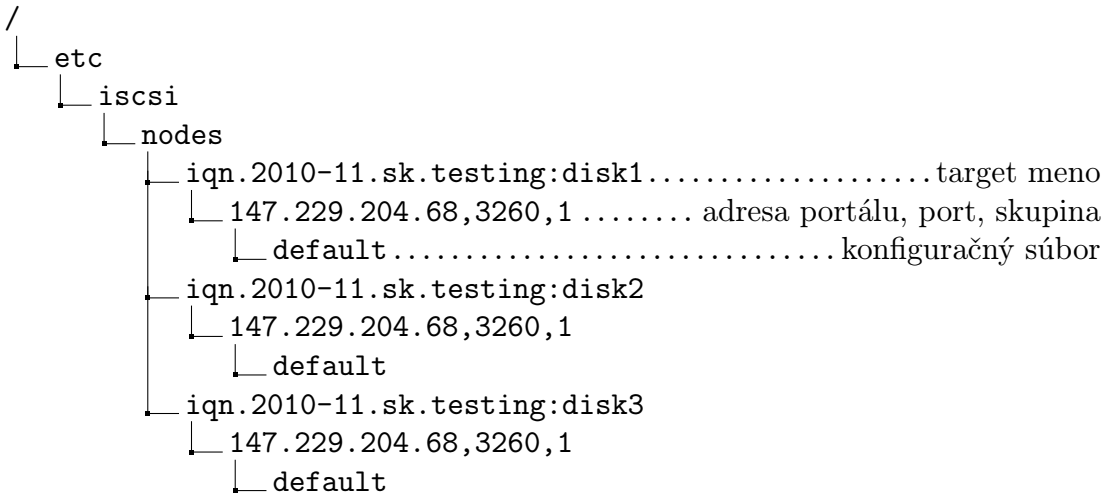
Po aplikovaní daného príkazu program iscsiadm vráti výpis ohľadom úspešnosti pripojenia. Pokiaľ je výpis ukončený slovom „successful“, pripojovanie prebehlo v poriadku. Skrátený výpis je zobrazený v rámčeku 7.4.

Výpis kódu 7.4: Skrátený výpis programu iscsiadm po úspešnom pripojení targetu

```
Logging in to [iface: ... portal: 147.229.204.68,3260]
Login to [iface: ... portal: 147.229.204.68,3260]: successful
```

Autentifikácia targetov

Každý pripájaný target môže mať podľa potreby iné prihlasovacie údaje. V programe Open-iSCSI má každý target nájdený cez discovery mód vytvorený priečinok nazvaný podľa jeho mena. Jednotlivé priečinky sú uložené v zložke „nodes“, ktorá sa nachádza v konfiguračnom priečinku programu, a to /etc/iscsi/. V každom priečinku sa nachádza konfiguračný súbor, v ktorom sa okrem iného nastavujú aj možnosti CHAP autentifikácie. Presné umiestnenie je zobrazené na nasledujúcej štruktúre.



Jednoduchá aj obojstranná autentifikácia sú nastavované v tom istom súbore. Ako prvý krok pri nastavovaní je zahájenie editácie konfiguračného súboru. Podobne ako v minulých krokoch tak aj teraz je použitý editor nano. Ako príklad bude slúžiť target iqn.2010-11.sk.testing:disk2 nachádzajúci sa na portáli 147.229.204.68. Editáciu je možné spustiť zadaním nasledujúceho príkazu.

```
nano /etc/iscsi/nodes/iqn.2010-11.sk.testing:disk2/192.168.1.109,3260,1/default
```

V obsahu konfiguračného súboru je najprv potrebné editovať parameter príkazu „node.session.auth.authmethod“ na hodnotu „CHAP“.

Pri použití jednoduchej autentifikácie stačí už len dopísať ďalšie dva riadky obsahujúce údaje o prihlasovacom mene a hesle. Skrátený obsah konfiguračného súboru spolu s pridanými príkazmi je na nasledujúcom výpise 7.5 .

Výpis kódu 7.5: Skrátený výpis konfiguračného súboru s jednoduchou autentifikáciou

```
node.session.auth.authmethod = CHAP
node.session.auth.username = san
node.session.auth.password = trinastznakov
```

Pokiaľ target vyžaduje overenie pomocou obojstrannej autentifikácie, je nutné nastaviť ešte aj príkazy s menom a heslom pre autentifikáciu initiatora. Skrátený obsah už zeditovaného konfiguračného súboru je na výpise 7.6 .

Výpis kódu 7.6: Skrátený výpis konfiguračného súboru s obojstrannou autentifikáciou

```
node.session.auth.authmethod = CHAP
node.session.auth.username = san
node.session.auth.password = trinastznakov
node.session.auth.username_in = nas
node.session.auth.password_in = abcde12345abc
```

Odpojenie targetu

Keď už pripojený target nieje viac potrebný, je možné ho jednoducho odpojiť. Synntax zápisu je rovnaká ako pri pripájaní, akurát je potrebné zmeniť parameter „--login“ na parameter „--logout“. Príklad zápisu je v nasledujúcom rámčeku.

```
iscsiadm -m node -T iqn.2010-11.sk.testing:disk1 -p 147.229.204.68:3260 --logout
```

Nastavenie adresy pre iSNS Server

Nastavovanie iSNS servera sa prevádza v rovnakom konfiguračnom súbore ako nastavovanie autentifikácie pre portál, a to iscsid.conf. Po zadaní príkazu

```
nano /etc/iscsi/iscsid.conf
```

stačí iba nájsť sekciu o iSNS serveri a zeditovať hodnoty parametrov na požadované hodnoty. Príklad nastavenia parametrov je zobrazený na výpise 7.7.

Výpis kódu 7.7: Skrátený výpis konfiguračného súboru s iSNS konfigurácioou

```
################
# iSNS settings
################
# Address of iSNS server
isns.address = 147.229.204.50
isns.port = 3205
```

8 TVORBA WEBOVÉHO ROZHRANIA

Webové rozhranie vytvorené v nasledujúcej časti má slúžiť hlavne ako konfiguračný nástroj pre program IET, pomocou ktorého bude možné manipulovať s lun jednotkami a nastavovať jednotlivé targety. Okrem iného bude zobrazovať aj základné informácie o systéme a jeho vstupno/výstupných zariadeniach. Webové rozhranie je prispôsobené pre použitie v linuxovej distribúcii Ubuntu.

Aby stránka správne zobrazovala informácie, je potrebné ešte systém upravit. Ako prvé je potrebné nastaviť užívateľovi, ktorý spúšťa webový server potrebné práva. V systéme Ubuntu je týmto užívateľom **www-data**. Nastavenie práv sa vykonáva editovaním súboru „sudoers“ príkazom

```
visudo
```

ktorý je nutné zadať pod právami užívateľa root. V spustenom textovom editore stačí pridať nasledujúci riadok na koniec súboru.

```
%www-data ALL=(ALL) NOPASSWD:ALL
```

Ako ďalší krok je potrebné doinštalovať programy. Pre správu RAID polí je potrebný program **mdadm**, pre zobrazovanie teploty systému **lm-sensors** a na zobrazovanie S.M.A.R.T. informácií zase program **smartmontools**. Všetky tieto programy sú dostupné z repozitárov, takže k inštalácii môžno použiť správcu balíkov **apt**. Zadaním nasledujúceho príkazu opäť pod právami roota sa tieto programy nainštalujú do systému.

```
apt-get install mdadm lm-sensors smartmontools
```

Nakoniec je ešte potrebné nainštalovať iSCSI target podľa postupu v bode 6.2 .

8.1 Inštalácia webového servera

Aby bolo danú stránku vôbec možné prevádzkovať bolo potrebné najprv vytvoriť webový server, ktorý by dané rozhranie zobrazoval. Pre potreby tejto práce bol zvolený webový server Apache [1] kvôli jeho flexibilite a rozšírenosti.

V distribúcii Ubuntu bol tento webový server nainštalovaný spolu s programovacím jazykom PHP, ktorý bude vysvetlený neskôr v sekcii 8.2 . Ich inštalácia bola vykonaná podľa návodu v literatúre [16].

Nakoľko vytvorené rozhranie má byť prístupné cez internet, bolo nutné ho určitým spôsobom zabezpečiť. Pre tento účel bola zvolená možnosť zabezpečenia pomocou „.htaccess“ súboru. Soubor .htaccess je zvláštny textový súbor určený k tomu, aby si autor stránok mohol sám upravit niektoré vlastnosti servera bez toho, aby potreboval práva správcu. Je ho taktiež možné použiť na zabezpečenie určitého

adresára. Nastavovanie daného súboru spolu s konfiguráciou Apache serveru bolo prevádzané podľa návodu v literatúre [2]. Obsah .htaccess súboru je na výpise 8.1.

Výpis kódu 8.1: Obsah súboru .htaccess

```
AuthType Basic
AuthName "Accesss to page"
AuthUserFile /usr/share/apache2/passwd/passwords
AuthGroupFile /dev/null
Require valid-user
```

Pri nastavovaní niektorých parametrov programu IET sú posielané citlivé informácie, ktoré by nebolo dobré zverejňovať. Aby sa zabránilo nechceným stratám údajov bol server zabezpečený pomocou SSL šifrovania. Konfigurácia bola prevádzaná podľa návodu v literatúre [3]. Pri odvolávaní sa na „http“ server automaticky presmeruje na zabezpečené „https“.

Takto nastavený webový server je už možné použiť ako server pre vytvorené webové rozhranie.

8.2 Programovanie webového rozhrania

Naprogramované webové rozhranie je zo značnej miery tvorené programovacím jazykom PHP nainštalovaným v bode 8.1.

PHP je populárny, otvorený skriptovací programovací jazyk, ktorý sa používa najmä na programovanie klient-server aplikácií (na strane servera) a pre vývoj dynamických webových stránok. Je ho možné používať na všetkých známych operačných systémoch ako Windows, Linux či Mac OS X.

Spolu s PHP je použitý značkovací jazyk HTML a grafická časť je tvorená za pomoci kaskádových štýlov (CSS).

Zoznam všetkých požitých PHP skriptov spolu s formulármi a kaskádovými štýlmi je v prílohe B.

Zobrazovanie systémových informácií

Stránky **index.php** a **conf.php** nachádzajúce sa priamo v koreňovom adresári webového servera obsahujú okrem krátkych PHP skriptov aj HTML značky, pomocou ktorých sú zobrazované jednotlivé formuláre. Obe stránky obsahujú pomocou HTML zobrazené tabuľky, do ktorých su pomocou PHP pridávané informácie. Informácie sú získavané z výpisov linuxových príkazov alebo z obsahov súborov. Na spúšťanie príkazov je použitý PHP príkaz „exec“ alebo „passthru“. Výsledný text z príkazu je filtrovaný za použitia textovo filtračných programov ako grep, sed, cut či awk (informácie k týmto programom sú dostupné v manuálových stránkach [15]). Príklad krátkeho PHP skriptu obsiahnutého v súbore index.php je na výpise 8.2.

Výpis kódu 8.2: PHP skript na získavanie systémových informácií

```
<?php
echo exec("lsb_release -d | cut -d':' -f2");
?>
```

Daný skript spustí v systéme príkaz „lsb_release -d“ a pomocou rúry „|“ presmeruje výstup programu na vstup filtračného programu „cut“, ktorý vyfiltruje text podľa zadaných kritérií.

Ďalší súbor nachádzajúci sa v koreňovom adresári je HTML súbor **hlavicka.html**. Obsahuje základné informácie nutné pre vytvorenie html stránky spolu s informáciami o načítaní kaskádových štýlov a JavaScriptov [1]. Tento súbor je pomocou PHP príkazu „include“ pripojený na začiatok každého PHP súboru obsahujúceho určitý HTML formulár.

Skripty obsiahnuté v priečinku „info“ slúžia na vypisovanie informácií o systéme. Každý so skriptov **cpu_info.inc.php**, **disk_info.inc.php**, **ip_info.inc.php**, **memory_info.inc.php** obsahuje funkcie vypisujúce informácie buď o procesore, diskoch, pamäti alebo o sieťových nastaveniach. Jednotlivé informácie sú získavané zo systémových súborov umiestnených v priečinku „/proc“, poprípade z výpisov systémových príkazov.

Jedinou výnimkou tohto priečinku je skript **ssh_change.inc.php**. Tento skript slúži na zmenu stavu SSH protokolu. Pomocou php príkazu „exec“ sa vykoná systémový príkaz na zastavenie poprípade zapnutie SSH protokolu.

Skripty na konfiguráciu iSCSI

V koreňovom adresári webového servera sa nachádza zložka „iscsi“, ktorá obsahuje PHP skripty na nastavovanie iSCSI targetu. Priamo v priečinku iscsi sú obsiahnuté súbory, ktoré obsahujú okrem PHP aj HTML formuláre.

Súbor **add-target.php** obsahuje iba formulár spolu s vysvetlivkami ku jednotlivým nastaveniam. Vyplnené hodnoty údajov sú po potvrdení odoslané do PHP skriptu **add_target_inc.php** v zložke „scripts“.

Program IET je konfigurovaný pomocou obsahu jeho konfiguračné súboru. Ten súbor sa skladá z nastavení jednotlivých targetov spolu s globálnymi nastaveniami pre celý program. Úlohou **add_target_inc.php** skriptu je práve vytvoriť dielčí konfiguračný súbor konkrétne pre pridávaný target. Každý novo pridaný target má svoj vlastný konfiguračný súbor pomenovaný podľa jeho mena. Takto vytvorené súbory sú po aplikovaní status skriptu **apply.php** 8.13 prekopírované do hlavného konfiguračného súboru. Skrátený výpis **add_target_inc.php** skriptu je na výpise 8.3.

Z výpisu je možné si všimnúť, že skript ukladá pomocou „exec“ príkazu jednotlivé konfigurácie do súboru v zložke „/etc/iet/targets“. Danú zložku si pri prvotnom spustení skript vytvorí a nastaví jej vlastníka na užívateľa spúšťajúceho PHP skripty („www-data“). Pomocou znaku > sa prepíše obsah cieľového súboru zdrojovým a

[1] JavaScript je skriptovací programovací jazyk používaný najmä pri tvorbe webových stránok.

pokiaľ cieľový súbor neexistuje tak sa vytvorí. Za pomoci znaku >> sa už iba dopisujú jednotlivé ďalšie nastavenia do súboru.

Výpis kódu 8.3: Skrátený PHP skript na vytváranie konfigurácie nového targetu

```
<?php
if(isset($_POST['add_target'])) { //keď je stlačené tlačidlo
 $dire_exist=exec("[ -d /etc/iet/targets ] && echo '1' || echo '0'");
                //testuje či existuje zložka
 if($dir_exist==0) { //keď neexistuje
  exec("sudo mkdir /etc/iet/targets");  //vytvorí zložku
  exec("sudo chown -R www-data:www-data /etc/iet/targets");
                //nastaví jej práva
  }
   $target=$_POST['target_name']; //uloží názov targetu z formulára
   exec("echo Target $_POST[target_name] > /etc/iet/targets/$arget");
   exec("echo Wthreads $_POST[Wthreads] >> /etc/iet/targets/$target");
                //ukladá jednotlivé nastavenia pre target
}
?>
```

Pmocou súboru **add-lun.php** sú pridávané logické jednotky (LUNy) k vytvoreným targetom. Jeho obsah spočíva v zobrazení formulára spolu s vysvetleniami jednotlivých zadávaných nastavení. Vyplnený a potvrdený formulár sa odvoláva na skript **add_lun_inc.php** v zložke „scripts“. Jeho úlohou je iba doplniť záznam ohľadom LUN jednotky do konfiguračného súboru konkrétneho targetu pomocou príkazu na výpise 8.4.

Výpis kódu 8.4: Skrátený PHP príkaz na pridanie LUN jednotky do konfigurácie

```
$target=$_POST['target']; //uloží názov targetu z formulára
exec("echo Lun $_POST[lun2] ... ,Type=$_POST[type2] >> /etc/iet/targets/$target");
                //pridá záznam o LUN jednotke do konfigurácie
```

Aby bolo možné meniť nastavenia vytvorených targetov je potrebné editovať ich konfiguračné súbory. K tomu slúži súbor **edit-target.php**. Jeho obsah je skoro rovnaký ako obsah **add-target.php** akurát sú už editačné polia prednastavené na hodnoty uložené v súbore vytvoreného pomocou skriptu **add_target_inc.php**. Údaje sú načítavané pomocou PHP skriptov jednoduchým načítavaním konkrétnych riadkov v súbore.

Po potvrdení editácie sa formulár odvolá na skript **edit_target_inc.php**. Tento skript už musí zohľadňovať možnosť pridaných LUN jednotiek. Preto ešte pred prepisovaním jednotlivých nastavení vyexportuje všetky existujúce LUN záznamy do dočasného súboru. Až potom uloží nastavenia rovnakým spôsobom ako skript **add-target.php** 8.3. Ako posledný krok vykoná to, že pridá na koniec upraveného konfiguračného súboru obsah dočasného súboru obsahujúceho LUN záznamy.

V súbore **edit-target.php** je taktiež možnosť zrušiť aktívny target. Stačí vybrať potrebný target z vytvoreného zoznamu a potvrdiť zmazanie. Daný formulár sa odvolá na skript **delete_target_inc.php** v zložke „scripts“, ktorý sa postará o zmazanie targetu. Mazanie sa prevádza jednoduchým odstránením konfiguračného súboru zvoleného targetu podľa príkazu 8.5.

Výpis kódu 8.5: Príkaz na odstránenie konfiguračného súboru zvoleného targetu

```
exec("rm /etc/iet/targets/$_GET[target]");
```

Rovnako ako je potrebné editovať nastavenia targetu je potrebné editovať aj nastavenia LUN jednotiek. K tomuto účelu slúži PHP stránka **edit-lun.php**, ktorá zobrazuje formulár spolu s prednastavenými hodnotami editačných polí. Rovnako ako pri **edit-target.php** tak aj tu sú hodnoty získavané z konfiguračného súboru targetu. Riadok obsahujúci LUN záznam je vhodne odfiltrovaný pomocou programov grep, cut alebo sed a výsledná hodnota sa zobrazuje ako prednastavená hodnota editačného poľa vo formulári.

Po potvrdení zeditovanej konfigurácie sú vyplnené hodnoty poslané do skriptu **edit_lun_inc.php**. V tomto skripte sa vykonáva úprava nastavení. Konfiguračný súbor targetu, ktorý je nutné editovať obsahuje okrem LUN záznamov aj konfiguráciu targetu, a preto je potrebné ju skopírovať do dočasného súboru príkazom 8.6.

Výpis kódu 8.6: Príkaz na skopírovanie konfigurácie targetu do dočasného súboru

```
exec("head /etc/iet/targets/$_POST[selected_disk] -n15>/etc/iet/targets/temp.txt");
```

Príkaz 8.6 skopíruje pomocou príkazu „head“ [15] a parametru „-n15“ prvých 15 riadkov konfiguračného súboru do dočasného súboru „/etc/iet/targets/temp.txt“. Prvých 15 riadkov preto, lebo práve tie obsahujú konfiguráciu targetu. Riadky s číslom 16 a vyššie obsahujú už LUN záznamy. Následne sa do dočasného súboru doplnia editované LUN záznamy podľa príkazu 8.4 a premenuje sa dočasný súbor „temp.txt“ na názov targetu. Spôsob premenovania je na výpise 8.7.

Výpis kódu 8.7: Príkaz na premenovanie dočasného súboru na konfiguračný súbor

```
exec("mv /etc/iet/targets/temp.txt /etc/iet/targets/$_POST[selected_disk]");
```

Všetky doteraz vysvetlené skripty slúžia iba na editovanie nastavení jednotlivých targetov. Súbor **edit-global.php** poskytuje oproti tomu zmenu nastavení pre celý program IET. Slúži na vypisovanie editačného formulára spolu so zobrazovaním už nastavených jednotlivých hodnôt. Prednastavené informácie sú zisťované pomocou PHP skriptov, ktoré čítajú konfiguračný súbor pre globálne nastavenia.

Po nastavení správnych hodnôt a následnom potvrdení sa formulár odvolá na skript **edit_global_inc.php**, ktorý sa postará o vytvorenie alebo zmenu konfiguračného súboru. Tak ako má každý target vlastný konfiguračný súbor, takisto aj

globálne nastavenia sú ukladané do vlastného konfiguračného súboru. Ukladanie hodnôt do súboru prebieha pobobne ako pri editovaní targetu 8.3.

Takto vytvorený globálny konfiguračný súbor je spolu s jednotlivými konfiguračnými súbormi targetov spojený do hlavného konfiguračného súboru programu podľa postupu 8.13.

Súbor **iscsi.php** slúži ako informačná stránka zobrazujúca aktuálne nastavenia targetov a informácie o programe IET. Informácie sú pomocou PHP skriptov získavané z konfiguračných súborov vytvorených skriptami **add_target_inc.php** alebo **edit_global_inc.php**.

Skript **show_targets_inc.php** nachádzajúci sa v zložke functions slúži na výpis aktívnych targetov. Pomocou linuxového programu „ls“ zistí počet súborov, ktoré majú iqn meno a z ich názvov vytvorí zoznam. Výpis funkcie na zisťovanie názvov vytvorených targetov je na výpise 8.8.

Výpis kódu 8.8: Funkcia na načítavanie názvov vytvorených targetov

```
$target=exec("ls /etc/iet/targets/ | grep -c iqn"); //zistí počet targetov
 for($i=1;$i<=$pocet_target;$i++) {
        $nazov_iscsi[$i]=exec("ls /etc/iet/targets/ | grep iqn | sed -n '$i p'");
        } //uloží jendotlivé názvy do poľa $nazov_iscsi[$i]
```

Skripty použité pri práci s RAID poľom

Všetky skripty, ktoré sú pri manipulácii s poľom potrebné sú uložené v priečinku „raid“. Súbory **sw-raid.php** a **remove-raid.php** obsahujú HTML kódy na zobrazenie formulára s editačnými poľami pre vloženie údajov.

Pomocou formulára na stránke **sw-raid.php** sa vyplnia údaje potrebné k vytvoreniu RAID poľa. Následne sa formulár odvolá na skript umiestnený v priečinku „scripts“, a to na **create_raid_inc.php**. Úlohou tohto skriptu je naformátovať vybrané disky na typ potrebný pre RAID pole a následne dané pole vytvoriť. Formátovanie sa opäť vykonáva pomocou programu „fdisk“, takže je nutné vytvoriť spustiteľný BASH skript. V tomto prípade skript vytvorí **format_disk_bash.sh**, ktorý následne cez PHP príkaz „exec“ spustí.

BASH skript je vytváraný jednoduchým ukladaním potrebných hodnôt do súboru. Následne mu je cez PHP príkaz „exec“ a systémový príkaz „chmod“[15] pridelený príznak „x“, čo v linuxvých systémoch znamená spustiteľnosť daného súboru. Takýto BASH skript je už možné v systéme spustiť.

Pre vytvorenie RAID poľa sa využíva systémový príkaz „mdadm“[15]. Jeho použitie je tiež vykonávané pomocou BASH skriptu. Skript **create_raid_inc.php** si k tomuto účelu vytvára BASH skript **create_raid_bash.sh**, ktorý následne spúšťa.

Stránka **remove-raid.php** obsahuje okrem HTML formulára aj PHP skript na zrušenie aktívneho RAID poľa. Daný formulár sa odvoláva na vlastnú stránku, kde sa vykonáva skript na zrušenie. Jeho obsah je na výpise 8.9.

Výpis kódu 8.9: PHP skript na zrušenie RAID poľa

```
if(isset($_GET['raid_sw_select_delete'])) { //keď je stlačené tlačidlo
        echo "<tr><td><textarea>"; //vytvorí písacie pole
        exec("sudo mdadm -S /dev/$_GET[raid_sw]"); //zruší RAID pole
        exec("sudo mdadm --detail --scan > /etc/mdadm/mdadm.conf");
        $temp_time=exec("date +%H:%M"); //zistí systémový čas
        passthru("sudo tail -50 /var/log/messages | grep $temp_time");
                                //vypíše log zo systému
        echo "</textarea></td></tr>";
        }
```

Skript **raid_show_inc.php** má za úlohu vypísať zoznam aktívnych RAID polí do rolovacieho zoznamu. Informácie o tom, aké polia sú aktívne získava z obsahu súboru „/proc/mdstat“ podľa príkladu 8.10.

Výpis kódu 8.10: PHP skript na výpis aktívnych RAID polí

```
<?php
function raid_sw_select($selected = NULL ) {
$raid_number=exec("cat /proc/mdstat | grep -c '\<md[0-9]*\>'");
        //zistí počet aktívnych polí
echo "<select name=\"raid_sw\">";
for($i=1;$i<=$raid_number;$i++) {       //pre každé pole
$rd=exec("cat /proc/mdstat | grep -o '\<md[0-9]*\>' | sed -n '$i p'");
        //do rd uloží názov poľa
echo "<option value=\"$rd\">$rd</option>";
        //vypíše záznam do rolovacieho zoznamu
        }
echo "</select>";
        }
?>
```

Pomocou BASH skriptu **mdadm_scan.sh** sú ukladané informácie o aktívnych RAID poliach do konfiguračného súboru „mdadm.conf“. Uložením patričných údajov sa zabezpečí prístupnosť RAID polí aj po reštarte systému. Tento BASH skript je používaný v PHP skripte **create_raid_inc.php** a **remove-raid.php**.

Posledný skript **lun_show_checkbox_inc.php** vytvára a vypisuje zaklikávací zoznam aktívnych systémových partícií. Zoznam je vytváraný z výpisu programu „fdisk“ obdobným spôsobom ako výpis 8.10.

Skripty pre vytváranie a mazanie partícií

Stránky **create-lun.php** a **delete-lun.php** nachádzajúce sa priamo v adresári „lun“ obsahujú okrem krátkych PHP skriptov aj HTML formuláre odvolávajúce sa na skripty v priečinku „scripts“.

Pomocou skriptu **delete_lun_inc.php** sa vykonáva mazanie logických partícií. Zdrojový kód je na nasledujúcom výpise 8.11.

Výpis kódu 8.11: PHP skript na mazanie logických partícií

```
<?php
$partitions=$_GET['disk_partitions']; //ukladanie dát z formulára
$active_disk=$_GET['active_disk']; //ukladanie dát z formulára
for ($i=0;$i<count($partitions);$i++) {
        exec("sudo parted -s /dev/$active_disk rm $partitions[$i]");
        } //spustenie príkazu parted pre každú zvolenú partíciu
header('Location: ../delete-lun.php'); //vráti na stránku
?>
```

Z výpisu je možné vyčítať, že mazanie sa prevádza spustením systémového príkazu „parted“[15] spolu s príslušnými parametrami, ktoré sú doplnené v závislosti na vyplnenom formulári na stránke **delete-lun.php**.

Skript **create_lun.inc.php** naopak slúži na vytváranie nových partícií. Je volaný stánkou **create-lun.php**. Na vytváranie partícií sa využíva systémový program „fdisk“. Vytvoriť novú partíciu pomocou tohto programu nieje možné za pomoci jedného príkazu ako pri programe „parted“, a preto je potrebné najprv vytvoriť spustiteľný bash skript. Najprv skript **create_lun.inc.php** uloží potrebné informácie spolu s prevzatými hodnotami z formulára do bash skriptu **create_part_bash.sh**, ktorý následne cez exec príkaz spustí. Výsledkom je vytvorená nová logická partícia o zvolenej veľkosti. Vytvorený bash skript môže mať napríklad takýto obsah 8.12.

Výpis kódu 8.12: Obsah BASH skriptu na vytvorenie partície

```
#!/bin/bash     #deklarácia interpréta

fdisk /dev/sdh << EOF   #príkaz na vytvorenie partície
n       #vytvorenie novej partície
p       #nastavenie ako primárna
2       #číslo partície

+29MB   #veľkosť partície
w       #aplikovať zmeny
EOF     #označenie konca príkazu
```

Zvyšné dva skripty v tomto priečinku slúžia na vytváranie zoznamov dostupných diskov alebo partícií. Skript **partitions_checkbox.inc.php** má za úlohu vytvoriť zaškrtávací zoznam dostupných logických partícií v systéme. Zoznam je získavaný z výpisu systémového príkazu „fdisk“, ktorý je následne odfiltrovaný cez programy gred, sed a cut do požadovaného tvaru.

Na rovnakom princípe funguje aj skript **disk_list_inc.php**, ktorý ale zase vytvorí rolovací zoznam dostupných diskov a partícií v systéme.

JavaScript skripty

V zložke „skripty“ sa nachádzajú skripty jazyka JavaScript, ktoré majú za úlohu upozorňovať na nevyplnené alebo zle vyplnené editačné polia, doplňovať prednastavené hodnoty do editačných polí alebo zablokovať určité polia pred editovaním. Tieto skripty slúžia iba ako pomôcka pri vytváraní konfigurácie, poprípade ako kontrola vyplnených editačných polí.

Skript **add_info.js** slúži na doplnenie prednastavených hodnôt do editačných polí pri nastavovaní nového targetu. Je dobré ho použiť pokiaľ je potrebné nastaviť target do základnej konfigurácie. Tento skript je volaný po stlačení tlačidla „Default“ na stránke **add-target.php** alebo **edit-target.php**.

Pomocou skriptu **empty_alert.js** je zabezpečované vyplnenie všetkých potrebných editačných polí vo formulári. V prípade nevyplnenia potrebných informácií skript nedovolí potvrdenie formulára a upozorní na konkrétne editačné pole, ktorého hodnotu je nutné nastaviť.

Ďalší upozorňovací skript je skript **alert.js**. Je volaný pri vytváraní RAID poľa a pri mazaní targetu. Jeho úlohou je upozorniť na vážnosť danej operácie a poskytnúť možnosť stornovať danú operáciu.

Skripty **onclick_change.js** a **onload_disable.js** slúžia na blokovanie editačných polí pred editáciou. Sú volané buď automaticky hneď po načítaní stránky alebo po označení daného poľa za „disabled“.

Jquery-1.5.1.min.js [7] je rýchlá a stručná JavaScript knižnica, ktorá zjednodušuje prácu s HTML dokumentami.

Status skripty

Skripty nachádzajúce sa v zložke „status“ slúžia na zmenu stavu programu IET. Pomocou skriptu **start.php** je možné IET zapnúť, pomocou **stop.php** vypnúť a pomocou **reload.php** zase program reštartovať. Skripty su opäť riešené pomocou „exec“ príkazu, kde je ako jeho parameter zadaný systémový príkaz „service iscsitarget“ so zvoleným parametrom start, stop alebo restart.

Skript **apply.php** sa stará o aplikovanie prevedených zmien v nastavení. Jeho úlohou je spustiť BASH skript **apply.sh** 8.13 a následne presmerovať na informačnú stránku iSCSI čo je **iscsi.php**.

Výpis kódu 8.13: BASH skript na vytvorenie konfigurácie programu IET

```
#!/bin/bash

sudo cat /var/www/status/komenty > /etc/iet/ietd.conf
sudo echo >> /etc/iet/ietd.conf #vloží prázdny riadok
sudo cat /etc/iet/targets/ietd_global >> /etc/iet/ietd.conf
sudo echo >> /etc/iet/ietd.conf #vloží prázdny riadok
sudo cat /etc/iet/targets/iqn* >> /etc/iet/ietd.conf
sudo service iscsitarget restart #reštartuje IET
```

Systémovým príkazom „cat“ sa pomocou > alebo >> vypisuje obsah jednotlivých dielčích súborov do hlavného konfiguračného súboru programu. Jednotlivé dielčie súbory obsahujú konfigurácie vytvorené pomocou iných skriptov z časti 8.2. Po vykonaní reštartu programu programu sa odvolá späť na informačnú stránku „iscsi.php“.

Kaskádové štýly

Kaskádové štýly sú uložené v priečinku „CSS“. Priečinok obsahuje hlavný css súbor **main.css**, ktorý obsahuje všetky nastavenia okrem natavení jednotlivých menu. Tie sa nachádzajú v súbore **menu_style.css**.

9 ZÁVER

Cieľom tejto bakalárskej práce bolo zoznámiť sa s problematikou SAN úložísk a popísať ich implementáciu do sietí. Ako ďalšie mal byť popísaný protokol iSCSI spolu so zameraním na jeho bezpečnosť a implementáciu v OS Linux a OS Windows. V praktickej časti mala byť realizovaná inštalácia a následná konfigurácia iSCSI target v OS Linux, inštalácia iSCSI initiator do prostredia OS Linux a OS Windows a vytvorenie webového rozhrania na konfiguráciu iSCSI target.

V práci je rozoberaná problematika ohľadom SAN úložísk. Sú popísané základné prvky týchto úložísk spolu s protokolmi, ktoré sa v SAN sietiach používajú. Hlavný dôraz je kladený na protokol iSCSI, ktorý sa v značnej miere používa v Ethernetových SAN sietiach.

Sú popísané hlavné výhody protokolu iSCSI spolu s vysvetlením jednotlivých pojmov. V ďalšej časti sú rozobrané možnosti zabezpečenia tohto protokolu a je vysvetlená jeho implementácia v OS Linux a OS Windows.

Časť tejto práce venovaná praktickej časti obsahuje detailný postup inštalácie a konfigurácie iSCSI target do prostredia OS Linux. Postup je vytváraný pre program IET (ISCSI Enterprise Target) v Linuxovej distribúcii Ubuntu. Inštalácia a konfigurácia iSCSI target je v ukážke prevádzaná vo virtuálnom prostredí programu VirtualBox. V tomto prostredí sú taktiež simulované fyzické diskové zariadenia používané v konfigurácii. Pomocou programu iSNS Server od spoločnosti Microsoft je v prostredí OS Windows overená funkčnosť zabezpečenia pomocou iSNS servera.

V ďalšej časti sú podrobne popísané návody ako nakonfigurovať iSCSI initiator pre pripojenie targetu. Návody sú písané ako pre OS Windows tak aj pre OS Linux. V OS Windows je použitý program Microsoft iSCSI Initiator a v prostredí OS Linux je to program Open-iSCSI.

Ďalšia praktická časť obsiahnutá v práci sa venuje webovému rozhraniu. Je popísaný postup ako nainštalovať a nakonfigurovať použitý webový server Apache, ako nainštalovať potrebné programy pre funkčnosť rozhrania a ako prispôsobiť OS pre použitie webového rozhrania. Pre prístup k rozhraniu je použité zabezpečenie pomocou .htaccess súboru a rozhranie je prístupné cez https. V prílohe B je obsiahnutá stromová štruktúra všetkých súborov použitých pri tvorbe rozhrania. Webové rozhranie je tvorené z veľkej miery pomocou skriptovacieho jazyka PHP a v texte je popísaná funkčnosť každého použitého PHP skriptu.

Webové rozhranie slúži hlavne ako rozhranie pre správu a konfiguráciu iSCSI targetu, konkrétne programu IET. Medzi jeho ďalšie možnosti patrí aj zobrazovanie systémových informácií. Pomocou rozhrania je možné sledovať stav zaplnenia diskových jednotiek, RAM pamäte, informácie o procesore, sieťových nastaveniach alebo o pripojených vstupno/výstupných zariadeniach. Pre bližšie informácie ohľadom diskových jednotiek je v rozhraní možnosť zobrazovať S.M.A.R.T. informácie poprípade spúšťať nové testy na diskoch. Pre lepšiu správu diskového priestoru je pridaná aj možnosť vytvárať a mazať RAID polia a taktiež vytvárať a mazať jednotlivé logické partície.

V prílohe je taktiež vytvorený návod na obsluhu webového rozhrania spolu s grafickými ukážkami rozhrania.

Možnosti vylepšenia vytvoreného webového rozhrania by mohli spočívať hlavne v zautomatizovaní jeho inštalácie. To by bolo možné buď vytvorením určitého BASH skriptu, ktorý by vykonal potrebné systémové zmeny automaticky alebo vo vytvorení .deb balíčka ktorý by bolo možné jednoducho nainštalovať pomocou správcu balíkov.

Ďalšie vylepšenie by mohlo spočívať v obmedzení práv pre rozhranie iba na spúšťanie konkrétnych príkazov v súbore sudoers. Tým by sa zvýšila bezpečnosť systému.

Pri písaní tejto práce som sa dozvedel veľa nových vecí. Oboznámil som sa s protokolom iSCSI, o ktorom som pred písaním nemal vôbec žiadne vedomosti. Ďalším prínosom bolo pre mňa naučenie sa aspoň základov skriptovacieho jazyka PHP spolu s HTML a CSS.

LITERATÚRA

[1] Apache [online]. c2011 [cit. 2011-05-27]. Dostupné z WWW: <http://www.apache.org>.

[2] *Apache HTTP Server Version 2.2* [online]. c2011 [cit. 2011-05-27]. Apache Tutorial: .htaccess files. Dostupné z WWW: <http://httpd.apache.org/docs/current/howto/htaccess.html>.

[3] *Apache HTTP Server Version 2.2* [online]. c2011 [cit. 2011-05-27]. SSL/TLS Strong Encryption. Dostupné z WWW: <http://httpd.apache.org/docs/2.2/ssl/ssl_faq.html>.

[4] BAKKE, M., et al.. *RFC 3721 : Internet Small Computer Systems Interface (iSCSI) : Naming and Discovery* [online]. 2004 [cit. 2010-12-11]. Dostupný z WWW: <http://tools.ietf.org/html/rfc3721>.

[5] HUFFERD, John. *ISCSI : The Universal Storage Connection.* [s.l.] : Addison Wesley, 2002. 368 s. ISBN 0-201-78419-X.

[6] LEHMANN, A.; ZHANG, M.; REDLI, A. *Manpages.ubuntu.com* [online]. 2005-07-27 [cit. 2010-12-10]. Manuálová stránka ietd.conf. Dostupné z WWW: <http://manpages.ubuntu.com/manpages/maverick/en/man5/ietd.conf.5.html>.

[7] *JQuery* [online]. c2010 [cit. 2011-05-29]. Dostupné z WWW: <http://docs.jquery.com/Main_Page>.

[8] NEMETH, Evi; SNYDER, Garth; HEIN, Trent. *Linux : Kompletní příručka administrátora.* 2. aktualizované vydání. Brno : Computer Press, 2008. 984 s. ISBN 978-80-251-2410-9.

[9] *Microsoft* [online]. c2010 [cit. 2010-12-17]. Dostupné z WWW: <http://www.microsoft.com/windowsserver2003/technologies/storage/iscsi/default.mspx>.

[10] Open-ISCSI [online]. c2010 [cit. 2010-12-17]. Dostupné z WWW: <http://www.open-iscsi.org/docs/open-iscsi-0.jpg >.

[11] Qlogic [online]. c2010 [cit. 2010-12-14]. Dostupné z WWW: <http://www.qlogic.com/Products/adapters/>.

[12] POELKER, Christopher; NIKITIN, Alex. *Storage Area Networks For Dummies.* 2nd edition. Hoboken : Wiley Publishing, 2009. 438 s. ISBN 978-0-470-38513-5.

[13] SATRAN, J., et al.. *RFC 3720 : Internet Small Computer Systems Interface (iSCSI)* [online]. 2004 [cit. 2010-12-11]. Dostupný z WWW: <http://tools.ietf.org/html/rfc3720>.

[14] SIMPSON, W. *RFC 1994 : PPP Challenge Handshake Authentication Protocol (CHAP)* [online]. 1996 [cit. 2010-12-11]. Dostupný z WWW: <http://tools.ietf.org/html/rfc1994>.

[15] *Ubuntu Manpage* [online]. c2010 [cit. 2010-12-12]. Dostupné z WWW: <http://manpages.ubuntu.com/manpages/maverick/en/>.

[16] *Ubuntu Wiki* [online]. c2010 [cit. 2011-05-27]. Apache a PHP. Dostupné z WWW: <http://wiki.ubuntu.cz/Apache%20s%20MySQL%20a%20PHP>.

[17] *VirtualBox* [online]. 2010 [cit. 2010-12-11]. Dostupné z WWW: <http://www.virtualbox.org/manual/UserManual.html>.

ZOZNAM SYMBOLOV, VELIČÍN A SKRATIEK

ASCII American Standard Code for Information Interchange - kódovací systém znakov abecedy, číslic, iných znakov a riadiacich kódov

GBIC Gigabit Interface Converter - gigabitový konvertor rozhrania

HBA Host Bus Adapter - hosťovský adatér

HW Hardware - hardvér (fyzické vybavenie počítača)

IET iSCSI Enterprise Target

IP Internet Protocol - internetový protokol

iSCSI Internet Small Computer System Interface - protokol na prenos dát

iSNS Internet Storage Name Service - služba zabezpečujúca správu úložísk

LAN Local area network - lokálna sieť

MAC Media Access Control - riadenie prístupu k médiu

NIC Network Interface Card - sieťová karta

OS Operating System - operačný systém

PDU Protocol data unit - protokolová dátová jednotka

RAID Redundant Array of Independent Disks - redudantné pole nezávislých diskov

SAN Storage Area Network - sieť skladovacích priestorov

SCSI Small Computer System Interface - rozhranie na výmenu dát

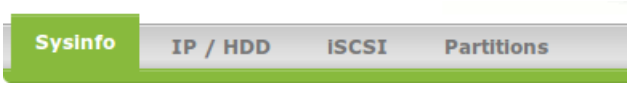
S.M.A.R.T. Self-Monitoring, Analysis, and Reporting Technology

SW Software - softvér (programové vybavenie počítača)

SSH Secure shell - bezpečný prístup

A NÁVOD K WEBOVÉMU ROZHRANIU

Hlavná ponuka webového rozrhrania je celkovo tvorené zo štyroch hlavných záložiek A.1. Prvé dve majú iba informačný charakter a zobrazujú informáce o systéme a pripojených zariadeniach. Ďalšie dve záložky označené ako „iSCSI“ a „Partitions“ obsahujú ako informácie tak aj možnosti editácie príslušného programu.



Obr. A.1: Hlavné menu rozhrania

A.1 Sysinfo

Prvá záložka označená ako „Sysinfo“ zobrazuje informácie o systéme. Je z nej možné vyčítať napr. informácie o úrovni zaplnenia systémovej pamäti, verziu OS, zoznam vstupno/výstupných zariadení či informácie o procesore.

V tabuľke „System info“ je okrem prezerania informácií možno zmeniť stav SSH protokolu. Nastavením danej voľby na Enabled bude povolené vzdialené pripájanie sa k systému pomocou SSH protokolu. Naopak nastavením na Disabled sa dané pripájanie zablokuje.

A.2 IP / HDD

Ďalšia záložka informačného charakteru je označená ako „IP / HDD“. Ako už názov naznačuje je z nej možné vyčítať informácie ohľadom nastavených IP adresách na daných rozhraniach či informácie o stave zaplnenia jednotlivých diskových zariadení.

Posledná tabuľka na stránke sa týka S.M.A.R.T. informácií o jednotlivých diskoch. S.M.A.R.T. je monitorovací systém pevných diskov, ktorý detekuje a posiela správy o rôznych ukazovateľoch spoľahlivosti v snahe predvídať zlyhaniam. V sekcii „View info“ je možnosť vybrať si z troch rôznych typov informácie.

Basic - zobrazuje iba základné informácie ako je typ zariadenia, jeho sériové číslo alebo to či podporuje SMART.

All SMART - pokiaľ disk podporuje SMART tak použitím tejto voľby sa dajú vypísať všetky jeho SMART informácie.

Smart+nonSMART - použitím tejto voľby sa zobrazia všetky informácie ako pri použití predchádzajúcej voľby ale ešte naviac sú pridané ďalšie dodatočné informácie.

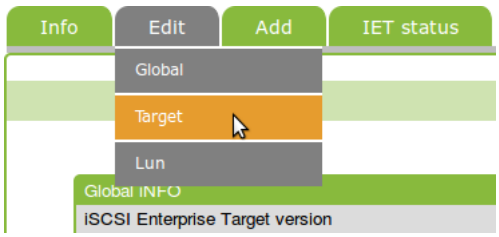
Sekcia „Run test“ slúži na výber druhu testu aký sa má na disku spustiť. Výsledkom daného testu je správa o stave disku. Sú dva druhy testov.

Short - predstavuje krátky test v časovom rozmedzí asi 10 minút. Má za úlohu otestovať jednotlivé mechanické a elektrické súčasti disku. Výsledok testu sa dá zobraziť pomocou voľby All SMART v sekcii View info.

Long - long predstavuje dlhšiu verziu testu ako short. Trvá niekoľko desiatok minút ale testuje disk dôkladnejšie. Výsledok testu je tiež možné zobraziť pomocou voľby All SMART.

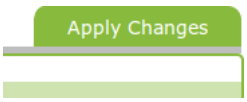
A.3 iSCSI

Záložka iSCSI obsahuje informácie o programe IET spolu s možnosťami jeho editácie. Hlavná záložka obsahuje niekoľko podzáložiek pre lepšiu orientáciu A.2.



Obr. A.2: Menu pre záložku iSCSI

Všetky informácie upravené v záložke „iSCSI“ sú ukladané iba v dočasných súboroch. Aby boli zmeny aplikované je nutné kliknúť na tlačidlo „Apply Changes“A.3 nachádzajúce sa v pravej časti menu.



Obr. A.3: tlačidlo na aplikovanie zmien

Info

V prvej záložke označenej „Info“ sú ako prvé základné informácie o nainštalovanej verzii programu IET a o jeho aktuálnom stave. Ďalej sú zobrazené globálne nastavenia pre program IET. Ide o Adresu iSNS servera a nastavenie autentifikácie pre portál. Pokiaľ sa pri zadanej informácii nenachádza žiadna hodnota znamená to, že nieje nastavená resp. že je vypnutá.

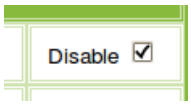
Ako posledná možnosť je zobrazovanie jednotlivých aktívnych targetov. Ich nastavenia spolu so zoznamom pridelených lun jednotiek.

Edit

Záložka „Edit“ obsahuje ďalšie tri podzáložky obsahujúce formuláre na editáciu globálnych informácií, jednotlivých targetov a lun jednotiek.

Edit Global

Podzáložka „Edit Global“ obsahuje formulár na nastavenie adresy iSNS servera spolu s možnosťami nastavenia mena a hesla pre autentifikáciu. Pokiaľ je žiadúce nejakú z volieb vypnúť je potrebné zaškrtnúť voľbu „disable“ A.4 a následne potvrdiť tlačidlom „Edit“.



Obr. A.4: Vypnutie/zapnutie danej voľby

Edit Target

V tejto podzáložke je hneď po načítaní k výberu možnosť editovať alebo vymazať nejaký z aktívnych targetov.

Po vybratí targetu pre zmazanie a následnom potvrdení sa vyvolá potvrdzujúce okno, ktorým je ešte možné operáciu mazania prerušiť alebo pokračovať v zmazaní.

V sekcii pre editovanie targetu je potrebné najprv zvoliť target, ktorý má byť editovaný a následne potvrdiť výber. Zobrazí sa formulár na editovanie jednotlivých nastavení. Autentifikáciu je možné vypnúť zaškrtnutím voľby „Disable“. Pokiaľ je vhodné nastaviť hodnoty do prednastavených hodnôt, stačí stlačiť tlačidlo „Default“, ktoré automaticky doplní prednastavené hodnoty do editačných polí. Po upravení všetkých potrebných nastavení sa hodnoty uložia tlačidlom „Edit“.

Edit Lun

Pri editovaní lun jednotiek sa najprv musí zvoliť target, ktorého lun jednotky sa budú editovať. Po výbere sa vypíše zoznam aktívnych jendotiek obsahujúci editačné polia. Podľa potreby je potom možné upraviť parametre nastavenia poprípade vymazať jednotku zaškrtnutím „Disable“ možnosti a uložením nastavení tlačidlom „Edit“.

Add

Záložka „Add“ slúži na pridávanie nových targetov alebo lun jednotiek.

Add Target

Táto podzáložka obsahuje formulár s editačnými poľami na nastavenie jednotlivých nastavení. Rovnako ako u predchádzajúcich formulároch tak aj tu je možnosť vypnúť autentifikáciu pomocou voľby „Disable“. Pomocou tlačidla „Default“ je tiež možné vyplniť editačné polia prednastavenými hodnotami. Pri vypĺňovaní mena je potrebné zachovať tvar rovnaký ako je uvedený v príklade. Inak systém ohlási chybu. Po nastavení všetkých hodnôt sa konfigurácia ukladá tlačidlom „Add“.

Add Lun

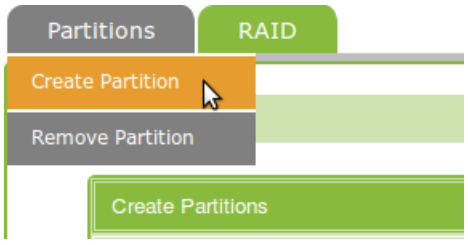
Pridávanie lun jednotky spočíva vo vyplnení predpripravených polí. Význam jednotlivých položiek je vysvetlený hneď v príslušnej tabuľke. Po ich úspešnom vyplnení stačí uložit konfiguráciu tlačidlom „Add“.

IET status

Záložka „IET status“ obsahuje podzáložky Start, Stop a Restart pomocou ktorých je možné spustiť, zastaviť alebo reštartovať IET. Ako už bolo spomínané vyššie, tak reštartovaním sa nedosiahne aplikovanie vykonaných zmien ohľadom IET. K tomu je nutné použiť tlačidlo A.3.

A.4 Partitions

Hlavným cieľom tejto záložky je informovať o aktuálnych logických diskoch (partíciach) a poskytnuť možnosť vytvoriť nové. Ako ďalšia voľba, ktorú je možné využiť je vytváranie poprípade mazanie RAID poľa. Táto záložka obsahuje taktiž vlastné menu A.5 pre lepšiu orientáciu po stránke.



Obr. A.5: Menu pre hlavnú záložku Partitions

Create Partition

Sekcia tejto stránky s názvom Disk Info slúži na informovanie o dostupných diskoch a ich stave voľného miesta. Získané informácie v tejto časti by mali slúžiť ako odrazový mostík pri vytváraní partície v sekcii Create Disk Partitions.

Pri vytváraní je nutné zadať veľkosť partície a jej číslo. Každá vytvorená partícia má mať iné číslo. Maximálne množstvo partícií na disk je obmedzená na čtyri.

Remove Partition

Tak ako je možné vytvárať partície je ich možné aj mazať. Mazanie spočíva vo vybratí potrebného disku a zobrazení jeho partícii. Až po stlačení tlačidla „Show partitions“ sa zobrazí klikací zoznam s názvami diskov a tlačidlom na mazanie. Pre zmazanie vybraných partícií ich stačí zaškrtnúť v zobrazenom zozname a zmazať tlačidlom „Remove partitions“.

Create RAID

Pre lepšiu manipuláciu s diskovým priestorom je v rozhraní obsiahnutá možnosť vytvárať RAID pole. Stránka obsahuje sekciu Disk Info kde sa dajú zistiť potrebné informácie o jednotlivých diskoch a vybrať tie, ktoré vyhovujúce pre tvorbu RAIDu.

Vytváranie RAIDu spočíva v zvolení jeho mena, levelu, počtu pridaných zariadení a následne z akých diskov bude zložený. Pokiaľ je vytvorených viacero RAID polí, tak je potrebné aby bolo každé pomenované inak. Vytvorenie poľa sa potvrdzuje tlačidlom „Create“.

Remove RAID

Už nepotrebné RAID polia je možné mazať v tejto záložke označenej ako „Remove RAID“. Stačí vybrať patričné RAID pole a podľa potreby buď zobraziť jeho informácie alebo ho hneď odstrániť pomocou tlačidla „Delete“.

B STROMOVÁ ŠTRUKTÚRA SÚBOROV WEBOVÉHO ROZHRANIA

```
/
├── index.php
├── conf.php
├── hlavicka.html
├── css
│   ├── main.css
│   └── menu_style.css
├── images
│   ├── black.jpg
│   ├── blue.jpg
│   ├── ciara.gif
│   ├── ciara.jpg
│   ├── current-bg.gif
│   ├── favicon.ico
│   ├── logo.gif
│   └── menu-bg.gif
├── info
│   ├── cpu_info.inc.php
│   ├── disk_info.inc.php
│   ├── ip_info.inc.php
│   ├── memory_info.inc.php
│   └── ssh_change.inc.php
├── iscsi
│   ├── add-lun.php
│   ├── add-target.php
│   ├── edit-global.php
│   ├── edit-lun.php
│   ├── edit-target.php
│   ├── scripts
│   │   ├── add_lun_inc.php
│   │   ├── add_target_inc.php
│   │   ├── delete_target_inc.php
│   │   ├── edit_global_inc.php
│   │   ├── edit_lun_inc.php
│   │   └── edit_target_inc.php
│   └── functions
│       └── show_targets_inc.php
└── lun
    ├── create-lun.php
    ├── delete-lun.php
    └── scripts
        └── create_lun.inc.php
```

```
        ├── create_part_bash.sh
        ├── delete_lun_inc.php
        ├── disk_list_inc.php
        └── partitions_checkbox.inc.php
    ├── raid
    │   ├── sw-raid.php
    │   ├── remove-raid.php
    │   └── scripts
    │       ├── create_raid_bash.sh
    │       ├── create_raid_inc.php
    │       ├── format_disk_bash.sh
    │       ├── lun_show_checkbox_inc.php
    │       ├── mdadm_scan.sh
    │       └── raid_show_inc.php
    ├── skripty
    │   ├── add_info.js
    │   ├── alert.js
    │   ├── empty_alert.js
    │   ├── jquery-1.5.1.min.js
    │   ├── onclick_change.js
    │   └── onload_disable.js
    └── status
        ├── apply.sh
        ├── apply.php
        ├── komenty
        ├── reload.php
        ├── start.php
        └── stop.php
```