CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Umrežena spremišta podataka

CCERT-PUBDOC-2009-07-271

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Razvojem različitih tehnologija pojavljuju se raznovrsni podaci koji se stalno razmjenjuju putem mreže. Kako bi takvi podaci bili svakodnevno dostupni raznim korisnicima sustava, dolazi do primjene raznovrsnih spremišta podataka. Postoje tri osnovna tipa tehnologija za pohranu podataka, a to su DAS (eng. Direct attached storage), NAS (eng. Network-attached storage) i SAN (eng. Storage area network) sustavi.

Kod DAS sustava tvrdi disk ili niz diskova priključuje se na osobno računalo te time donosi određena ograničenja u pristupu (npr. pristup preko računala koje je povezano na poslužitelj) i rukovanju podacima. NAS tehnologija podrazumijeva umreženo spremište podataka tj. omogućuje pristup sustavu za pohranu računalima s raznim operacijskim sustavima. Ovakav sustav karakterizira jednostavna implementacija i lakoća upravljanja. Posljednja – SAN tehnologija, omogućuje pristup spremištima za pohranu koja se nalaze odvojeno od LAN mreže. Predstavlja složeno i skupo rješenje pa se obično nalazi samo u velikim poslovnim sektorima.

Zahvaljujući svojim obilježjima NAS tehnologija prevladava u većini srednjih i manjih poslovnih okruženja (eng. small and medium enterprises). U nastavku dokumenta dan je opis implementacije i osobina spomenute tehnologije. Predstavljene su i osnovne implementacije otvorenog programskog koda. Zatim je napravljena usporedba s ostalim spomenutim tehnologijama te dan pregled sigurnosnih ranjivosti, kao i savjeta za zaštitu.

2. Umrežena spremišta podataka

Umrežena spremišta podataka ili NAS (eng. Network-attached storage) tehnologije su samostalna računala (ili drugi uređaji) priključena na mrežu, s osnovnom namjenom pružanja usluga pohrane podataka drugim uređajima na mreži. Slika 1 prikazuje mrežu koja sadrži računala s raznim operacijskim sustavima priključenim preko prespojnika (eng. switch) na umreženo spremište podataka. Budući da se radi o tehnologiji s mogućnosti jednostavnog upravljanja i povećanja kapaciteta, predstavljaju praktično rješenje za pohranu raznih vrsta podataka.

Slika 1 Arhitektura s umreženim spremištem podataka

2.1. Povijest

NAS tehnologije pojavile su se sa razvojem operacijskog sustava „NetWare“, za razmjenu podataka, tvrtke Novell te protokola NCP (eng. NetWare Core Protocol) 1983. godine. Riječ je o mrežnim protokolima koji omogućavaju pristup i pregled datoteka, razmjenu poruka, udaljeno pokretanje naredbi te druge mrežne funkcije. Godine 1984. tvrtka Sun Microsystems objavila je sustav NFS (eng. Network File System) koji je omogućavao mrežnim poslužiteljima dijeljenje prostora za pohranu s korisnicima. Novi napredak u razvoju tehnologije donose tvrtke 3Com i Microsoft koje razvijaju program „LAN Manager“, operacijski sustav koji sadrži komponente koje omogućuju obradu zahtjeva za pristupom resursima ili dohvat podataka. Programi „3Server“ i „3+Share“ tvrtke 3Com bili su prvi poslužitelji s uključenim odgovarajućim sklopovljem i programima, a radili su na više diskova za pohranu i bili prvenstveno namijenjeni umreženoj pohrani podataka.

Zahvaljujući uspjehu prethodnih uređaja, nekoliko tvrtki razvija namjenske datotečne poslužitelje. Tvrtka Auspex Systems bila je jedna od prvih organizacija koje su razvile NFS poslužitelje za operacijske sustave UNIX. Grupa inženjera spomenute firme odvojila se u zasebnu firmu u ranim 90-im godinama 20. stoljeća kako bi razvila integrirani filtar „NetApp“ s podrškom za sustave CIFS (eng. Common Internet File System) i NFS. Ovo je pokrenulo tržište NAS uređaja vođeno organizacijama NetApp i EMC Celerra.

Tvrtke poput NetApp, Exanet, IBRIX, Isilon, PolyServe i Panasas počinju razvoj alternativnih rješenja u obliku koji koriste distribuirani datotečni sustav pokrenut simultano na više poslužitelja (paralelni NAS). Primjer je sustav „Spinnaker Networks“ koji razvija tvrtka NetApp.

2.2. Opis

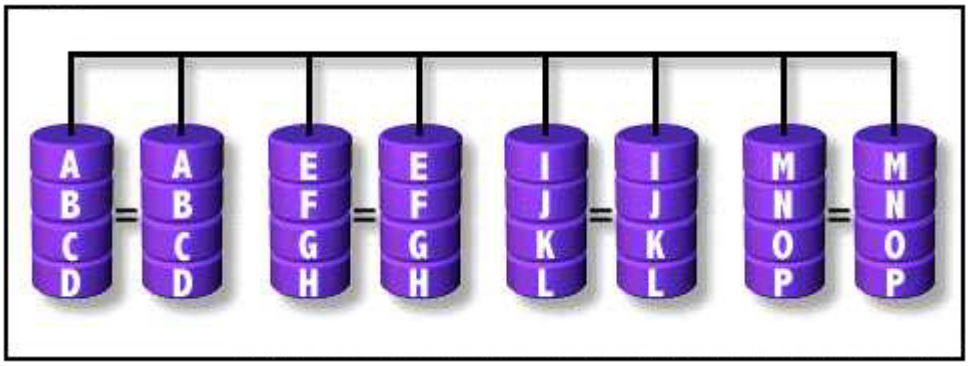
Operacijski sustav i programi NAS tehnologije pružaju funkcionalnosti pohrane podataka i pristupa datotekama. Najčešći način provođenja spomenutih radnji je spajanjem web preglednika na mrežnu adresu računala. NAS uređaji obično ne sadrže komponente poput tipkovnice i zaslona (Slika 2), a konfigurirani su i kontrolirani preko Internet ili Intranet mreže. Iako je tehnički moguće pokrenuti drugi program na takvom računalu, NAS uređaj inicijalno nije dizajniran za obavljanje općih zadataka računala. Osnovna namjena operacijskog sustava nije potrebna na NAS uređaju pa se obično koriste operacijski sustavi s minimalnom funkcionalnošću. Primjer je NAS tehnologija pod nazivom „FreeNAS" (detaljan opis dostupan u dijelu „Implementacije otvorenog koda") koja predstavlja inačicu operacijskog sustava FreeBSD sa funkcijama za pohranu.

Slika 2 Umreženo spremište podataka

Alternativa NAS tehnologijama na mrežama je uporaba računala kao poslužitelja datoteka. Radi se o računalu koje je priključeno na mrežu s namjenom pružanja usluga pohrane podataka, a može mu se pristupati preko radne postaje (eng. workstation) priključene na mrežu. U svojem najosnovnijem obliku, poslužitelj datoteka je upravo NAS sustav s tipkovnicom i zaslonom te operacijskim sustavom koji može obavljati dodatne operacije uz pohranu podataka.

NAS sustavi sadrže jedan ili više tvrdih diskova, obično uređenih u logične, redundantne spremnike za pohranu ili RAID (eng. redundant array of inexpensive disks) nizove. Radi se o tehnologiji koja omogućuje računalima da arhiviraju podatke na jeftinije diskovne komponente putem tehnologije nizanja uređaja u redundantne liste. Redundancija je postignuta stvaranjem kopija podataka (eng. mirroring), zapisivanjem dodatnih podataka preko liste za ispravljanje pogrešaka (eng. parity data) ili spremanjem podatka preko više diskova (eng. striped). Sve tehnologije pohranjuju podatke na način da uništenje jednog podatka na nekom od diskova ne rezultira trajnim gubitkom. Ako dođe do oštećenja nekog diska, njega je moguće zamijeniti novim i obnoviti izgubljene podatke s ostalih diskova. Više informacija o mogućnosti obnove podataka moguće je pronaći u dokumentu „Obnavljanje izgubljenih podataka" preko poveznice:

http://www.cert.hr/documents.php?id=377

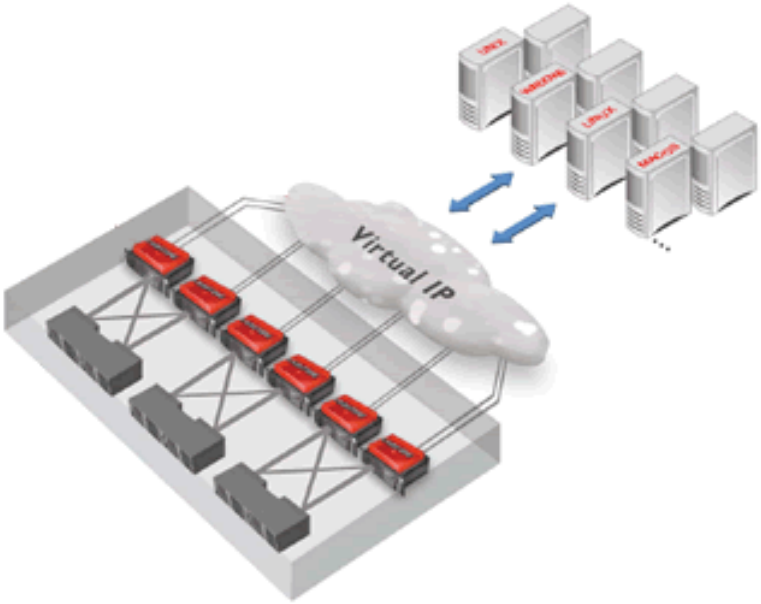


Slika 3 RAID tehnologija

Paralelni NAS je oblik umreženih spremišta podataka koji koristi distribuirane datotečne sustave koji su pokrenuti simultano na više čvorova ili poslužitelja (Slika 4). Osnovna razlika u odnosu na tradicionalne NAS tehnologije je mogućnost dijeljenja podatka i meta-podataka preko čvorova i NAS podsustava koji se krajnjem korisniku čine kao jedinstveni NAS sustav. Ovo omogućuje pristup mrežnom datotečnom sustavu s bilo kojeg čvora nepovezanog sa stvarnom lokacijom podataka.

Najveći nedostatak ovakvih mreža je dizajn namijenjen velikoj količini podataka i velikom broju korisnika što ga čini nepogodnim za većinu poslovnih okruženja. Postoje razne mogućnosti primjena ovakvih sustava u svim okruženjima gdje puno korisnika pristupa istim datotekama ili se očekuje veliki rast podataka koji se pohranjuju. Primjer su okruženja u kojim se odvija neko istraživanje ili statistička analiza. Više podataka o paralelnom NAS sustavu moguće je pronaći preko poveznice:

http://searchstoragechannel.techtarget.com/generic/0,295582,sid98_gci1343391,00.html.



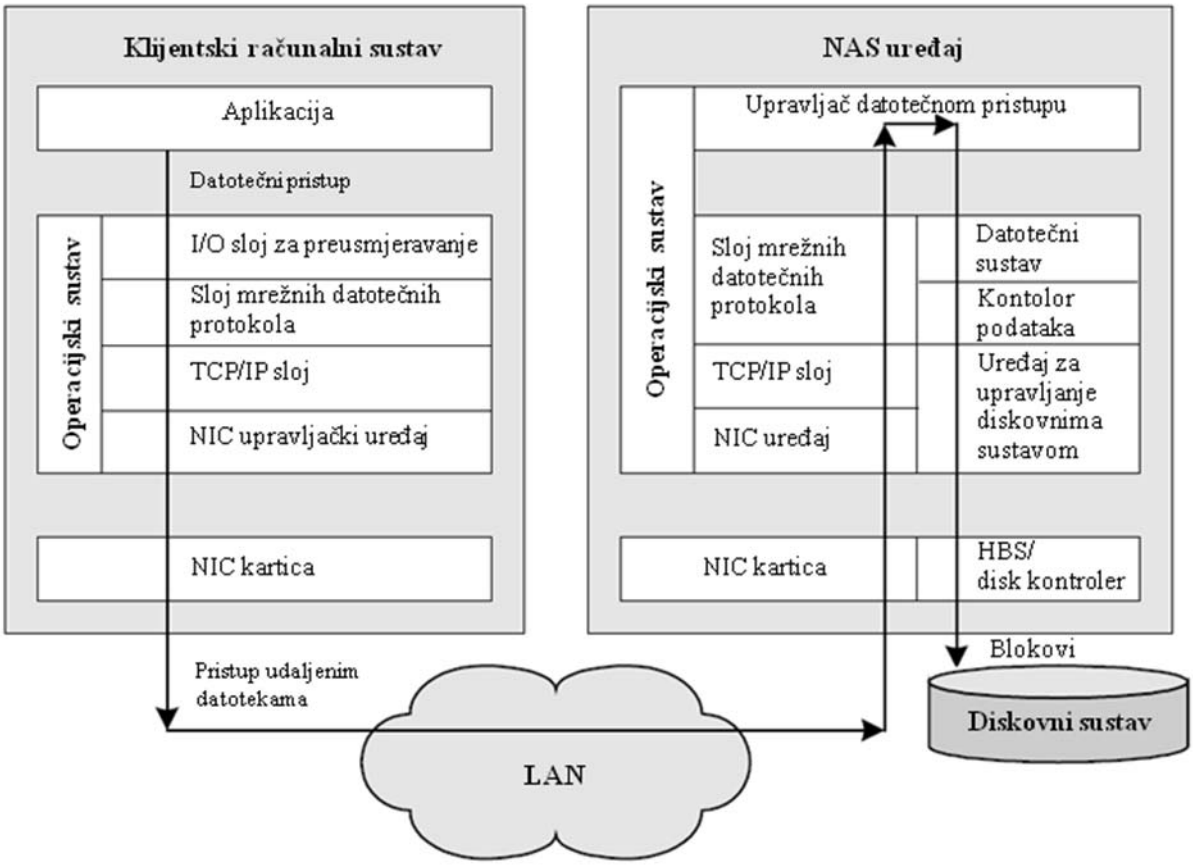
Slika 4 Paralelni NAS

2.3. Implementacija

NAS je jedno od rješenja koje omogućuje dijeljenje resursa za pohranu putem mreže, a odnosi se na spremište koje je izravno povezano na LAN (eng. local area network) mrežu putem protokola mrežnih datotečnih sustava (npr. NFS ili CIFS). Mrežni datotečni sustav oslanja se na diskovne blokove. Naredbe za pristup datotekama referencirane imenom datoteke prevode se u sekvence naredbi za blokovski pristup fizičkom disku. Prijenos podataka preko mreže odvija se u obliku niza podataka. Ovakav model je izgrađen na višoj razini apstrakcije pa zahtijeva dodatni sloj za obradu u poslužitelju i funkciji prevođenja između pristupa datoteci i blokovskog pristupa. Obrada zahtjeva u NAS sustavima može rezultirati dodatnim radom što utječe na procesorsku brzinu.

Osnovna arhitektura NAS spremišta dana je na slici 5. NAS tehnologija uvodi dvije vrste uređaja:

- **klijentski računalni sustav** – putem aplikacije pristupa virtualnim resursima za pohranu,
- **NAS uređaj** – predstavlja resurse za pohranu na LAN mreži koji su dijeljeni između klijentskih računalnih sustava priključenih na mrežu.



Slika 5 Arhitektura NAS sustava

U klijentskom sustavu, operacijski sustav rukuje sa zahtjevima aplikacije za pristup datotekama u obliku sustavnih poziva (eng. system call). Takvi sustavni pozivi interpretirani su preko I/O sloja za preusmjeravanje (najviši sloj operacijskog sustava) koji određuje jesu li traženi podaci dio udaljenog datotečnog sustava ili pridruženog lokanog sustava. Ako su podaci dio udaljenog datotečnog sustava, naredbe se prosljeđuju na NFS protokolni sloj koji omata pozive u naredbe za pristup udaljenom poslužitelju datoteka u obliku poruka NFS ili CIFS protokola. Takve poruke se predaju na TCP/IP (eng. Transmission Control Protocol/Internet Protocol) protokolni sloj, koji osigurava stvarni prijenos poruka preko mreže. NIC (eng. Network Interface Card) upravljački program pričvršćen je na TCP/IP sloj i na ENI

(eng. Ethernet Network Interface) karticu. Spomenuti uređaj pruža fizičko sučelje i kontrolne funkcije za pristup mediju (npr. LAN mreži).

U NAS uređaju, NIC prima Ethernet okvire koji nose naredbe za udaljeni pristup. NIC upravljački uređaj predaje datagrame TCP/IP sloju koji obnavlja izvornu NFS ili CIFS poruku. Zatim ovija naredbu u sustavni poziv za pristup datotečnom sustavu NAS uređaja. NAS datotečni sustav, kontrolor volumena i diskovni sustav uređaja upravljaju prevođenjem datotečnih naredbi u blokovske (podijeljene u logičke cjeline). Pretvorba se odvija između diskovnog kontrolora/HBA (eng. Host Bus Adapter) i diskovnog sustava koji je dio NAS uređaja ili je izvana spojen na NAS uređaj. Važno je napomenuti da diskovni sustav može biti jedan disk ili brojni diskovi povezani u jednu logičku cjelinu.

2.4. Uporaba

Općenito, NAS tehnologija može imati i više funkcionalnosti od samog pružanja centralizirane pohrane podataka korisničkim računalima u okruženjima s velikom količinom podataka. Moguće ju je koristiti za podršku jednostavnijih i jeftinijih sustava, poput poslužitelja poruka elektroničke pošte ili web stranica.

Potencijalno tržište NAS tehnologije su sustavi s potrebom pohrane velike količine multimedijskih podataka koji su danas široko dostupni. Primjer takve tehnologije prikazuje slika 6 koja donosi arhitekturu mreže s NAS tehnologijom za pohranu video zapisa, slikovnih datoteka i drugih podataka. Zahvaljujući širokom tržištu pojavile su se brojne tvrtke koje se bave izradom NAS uređaja. Njihov popis moguće je pronaći preko sljedeće poveznice:

http://en.wikipedia.org/wiki/List_of_NAS_manufacturers

Slika 6 Pohrana multimedijskog sadržaja

NAS tehnologije pružaju prilagodljivu umreženu pohranu podataka za malo višu cijenu od regularnih USB tehnologija ili vanjskih diskova koji koriste tehnologiju FireWire. Također, omogućuju stvaranje sigurnosnih kopija podataka koji su prethodno spremljeni na disk računala ili USB uređaj. Prilikom priključka uređaja, stvaranje kopija moguće je ostvariti automatski ili preko udaljene naredbe ovisno o implementaciji na uređaju. Slika 7 prikazuje prijenos podataka spremljenih na USB uređaju do NAS sustava preko odgovarajućeg priključka.

Slika 7 Stvaranje sigurnosnih kopija

Osim navedenih primjena, česta primjena NAS tehnologije je posluživanje SQL Server baza podataka. Koristi se u slučaju kada je poslužitelj baze podataka pokrenut na poslužitelju **A**, a podaci se nalaze na poslužitelju **B** kojim se upravlja preko mreže velike brzine s poslužitelja **A**. Budući da ovakvu konfiguraciju podržavaju sustavi tvrtke Microsoft, potrebno je samo stvoriti (Slika 8) i postaviti bazu podataka na UNC (eng. Uniform Naming Convention) lokaciju. Radi se o računalnom formatu koji specificira adresu resursa na LAN (eng. local area network) mreži, a ima sljedeći oblik: \\server-name\shared-resource-pathname. Pri tome, znakovi „\\“ označuju da se radi o mrežnom resursu, „server-name“ podrazumijeva DNS ime poslužitelja, dok „shared-resource-pathname“ predstavlja putanju do dijeljenog resursa kojem se želi pristupiti. Na primjer, kako bi se pristupilo datoteci „proba.txt“ u direktoriju „primjer“ na dijeljenom poslužitelju „test“ potrebno je zadati UNC u sljedećem obliku: \\test\primjer\proba.txt.

```
CREATE DATABASE SampleUNCDatabase ON
 ( NAME = Sample_dat,
  FILENAME = '\\\\mynas\\db\\sample.mdf',
  SIZE = 10MB,
  MAXSIZE = 2000MB,
  FILEGROWTH = 10MB)
 LOG ON
 ( NAME = Sample_log,
  FILENAME = '\\\\mynas\\db\\sample.ldf',
  SIZE = 5MB,
  MAXSIZE = 25MB,
 FILEGROWTH = 5MB)
```

Slika 8 Primjer naredbi za stvaranje baze podataka

2.5. Prednosti i nedostaci

Osnovna prednost koja dolazi s visokom apstrakcijom u NAS tehnologiji je jednostavnost uporabe, kao i jednostavnost realizacije u LAN okruženjima bez uvođenja nove mrežne infrastrukture ili novih uređaja. Osim navedenog, moguće je implementirati heterogenu mrežu s pristupom različitim operacijskim sustavima. Mnogi operacijski sustavi, poput sustava Linux i Unix, uključuju podršku za NAS protokole (npr. NFS). Također, u kasnijim inačicama operacijskog sustava Windows uvedena je podrška za CIFS protokol.

Još jedno važno pozitivno obilježje NAS tehnologije je sigurnost podataka u slučaju gubitka zahvaljujući RAID listama. Također, odvajanje spremišta podataka s računala na posebno mjesto povećava performanse klijentskog i poslužiteljskog sustava. Ipak, korisnost NAS sustava ovisi o dobroj implementaciji svih komponenti.

NAS sustav ima ograničena sredstva što znači da može posluživati ograničen broj korisnika i zahtjeva što ovisi o tipu poslužitelja i korištenoj implementaciji NAS sustava. Budući da je NAS uređaj ograničen na vlastito sklopovlje, u većini slučajeva nije ga moguće nadograditi.

Ponekad NAS uređaji ne mogu pružiti usluge koje su svojstvene datotečnom sustavu ili omogućiti takve usluge na učinkovit način. Primjeri uključuju: mogućnost procjena iskorištenosti diska odvojenih direktorija, mogućnost brzog pronalaženja datoteka, mogućnost učinkovitog preslikavanja diskova na druge diskove kroz aplikacije za sinkronizaciju podataka (npr. rsync).

2.6. Korišteni protokoli i tehnologije

NAS sustavi podržavaju razne tehnologije za prijenos podataka i implementaciju sučelja. Neki od važnijih dani su u nastavku dokumenta zajedno s poveznicama na dodatnu literaturu.

- ATA (eng. AT Attachment) – Osnovno vanjsko sučelje za pohranu kod osobnih računala koje povezuje poslužiteljski sustav s tvrdim diskovima, optičkim diskovima, CD-ROM uređajima i sl. Ultra ATA je proširenje izvornog ATA sučelja za veće brzine prijenosa.

  http://en.wikipedia.org/wiki/Parallel_ATA

- SATA (eng. Serial ATA) – Nova generacija sučelja dizajnirana je za zamjenu Ultra ATA sučelja, a predstavlja evoluciju ATA sučelja sa paralelne na serijsku arhitekturu.

  http://en.wikipedia.org/wiki/Serial_ATA

- SCSI (eng. Small Computer System Interface) – Standard koji definira univerzalno, paralelno sustavno sučelje za spajanje do devet uređaja preko jednog kabela.

  http://en.wikipedia.org/wiki/SCSI

- SAS (eng. Serial Attached SCSI) – Standard je definiran kao zamjena za fizički sloj SCSI sučelja sa serijskom tehnologijom. Osnovni cilj je povećanje brzina prijenosa podataka.

  http://en.wikipedia.org/wiki/Serial_Attached_SCSI

- FC (eng. Fibre Channel) – Tehnologija korištena za povezivanje mrežnih spremišta, a omogućuje brzine prijenosa reda gigabita.

http://en.wikipedia.org/wiki/Fibre_Channel

Kod NAS tehnologija, koje rijetko ograničavaju korisnike na jedan protokol, koriste se protokoli poput:

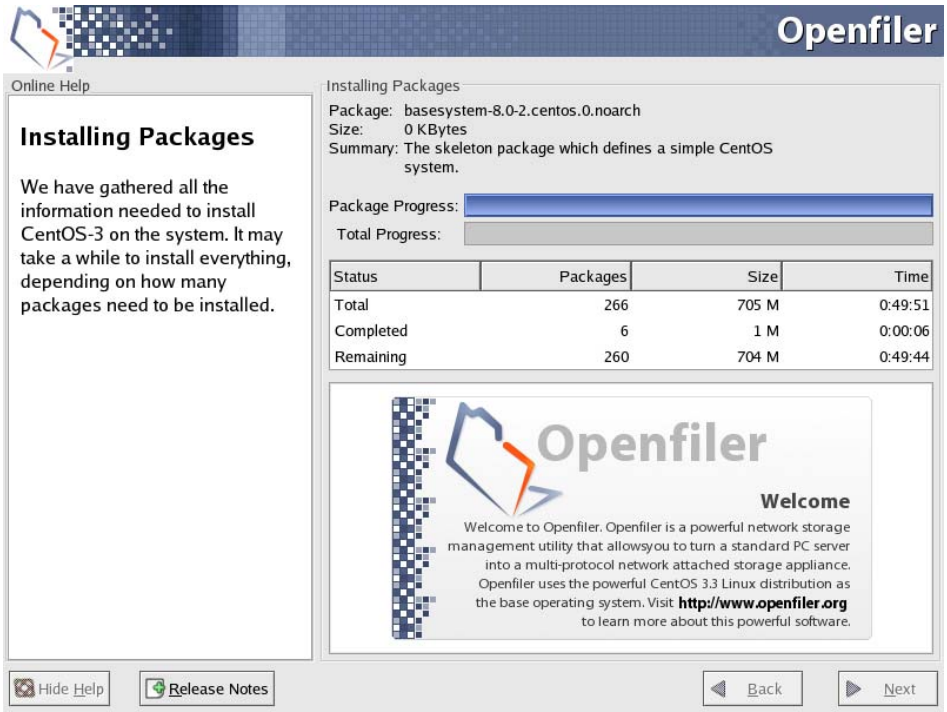
- NFS (eng. Network File System) – protokol koji je izvorno razvila tvrtka Sun Microsystems za omogućavanje pristupa datotekama na korisničkim računalima preko mreže. Radi se o otvorenom standardu izgrađenom na sustavu ONC RPC (eng. Open Network Computing Remote Procedure Call). Obično se upotrebljava na operacijskim sustavima Unix, ali moguće ga je koristiti i na platformama Mac OS, OpenVMS, Microsoft Windows, Novell NetWare i IBM AS/400.
- SMB/CIFS (eng. Server Message Block/Common Internet File System) – protokol aplikacijskog sloja koji se koristi za pružanje dijeljenog pristupa datotekama, pisačima te raznovrsne komunikacije (prijenos podataka, razmjena poruka i sl.) između mrežnih čvorova. Obično se koristi između računala koja koriste operacijski sustav Microsoft Windows. Koristi se i u raznim implementacijama umreženih spremišta podataka (poput FreeBSD i FreeNAS).
- AFP (eng. Apple Filing Protocol) – mrežni protokol koji pruža usluge razmjene datoteka kod operacijskih sustava Mac OS X i Mac OS. Trenutno podržava standarde Unicode i POSIX te ACL (eng. Access control list) liste, kao i napredno zaključavanje datoteka. Postoji nekoliko NAS tehnologija koje podržavaju spomenuti protokol, a primjeri su ReadyNAS, ExaStore i FreeNAS.
- FTP (File Transfer Protocol) – mrežni protokol za izmjenu i upravljanje datotekama preko mreže zasnovane na IP (eng. Internet Protocol) protokolu. Koristi se za dijeljenje i prijenos datoteka, uporabu udaljenog pristupa i sl., a podršku mu pruža TCP (eng. Transmission Control Protocol) protokol.
- HTTP (eng. Hypertext Transfer Protocol) – protokol aplikacijskog sloja za distribuirane informatičke sustave sa svrhom dohvaćanja resursa za sustave WWW (eng. World Wide Web). Zasniva se na sustavu upit/odgovor gdje korisnik postavlja upit te dohvaća željene resurse.
- UPnP (eng. Universal Plug and Play) – skupina mrežnih protokola koje održava UPnP Forum s ciljem omogućavanja lakog povezivanja uređaja te jednostavne implementacije mreža. Forum definira i objavljuje kontrolne protokole za UPnP uređaje koji prilikom priključivanja na mrežu automatski objavljuju svoju mrežnu adresu omogućujući korisnicima njihovo trenutno korištenje.
- SSH (eng. Secure Shell) protokol – mrežni protokol koji omogućuje razmjenu podataka korištenjem sigurnog kanala između dva uređaja. Obično se koristi na platformama Linux i Unix, a razvijen je kao zamjena za nesigurne udaljene pristupe. Koristi kriptiranje informacija koje osigurava povjerljivost i integritet podataka preko nesigurne mreže.
- iSCSI (eng. Internet Small Computer System Interface) – standard temeljen na IP protokolu za povezivanje objekata za pohranu podataka. Služi za prijenos SCSI naredbi preko IP mreže te upravljanje spremištima na velikoj udaljenosti.
- AOE (eng. ATA over Ethernet) – mrežni protokol koji omogućuje jednostavan pristup SATA uređajima (uređajima koji podržavaju SATA sučelja) za pohranu preko Ethernet mreže. Ne oslanja se na mrežne protokole iznad Ethernet sloja (poput protokola IP i TCP). Iako ne omogućuje pristup preko Interneta ili drugih IP mreža, jednostavan je za implementaciju i pruža visoke performanse i sigurnost pa se koristi se za prijenos poruka ATA protokola preko mreža Ethernet.
- FCOE (eng. Fibre Channel over Ethernet) – standard koji definira ovijanje FC okvira za prijenos u Ethernet mrežama.
- Rsync – Aplikacija za sustave Unix koja omogućuje sinkronizaciju datoteka i direktorija s jedne mrežne lokacije na drugu uz minimiziranje prijenosa podataka.

3. Implementacije otvorenog koda

Trenutno postoje četiri aktivne i popularne implementacije otvorenog koda koje pružaju usluge NAS tehnologije. Razvoj takvih programa doživio je veliki rast nakon javljanja potrebe za pohranom većih količina podataka. Zahvaljujući jednostavnosti i stalnom razvoju ovakve tehnologije postaju sve popularnije, posebno u srednjim i manjim tvrtkama.

3.1. Openfiler

Openfiler (Slika 9) je operacijski sustav koji pruža umreženo spremište podataka, a temeljen je na Linux distribuciji rPath. Riječ je o besplatnom paketu koji je licenciran GNU GPL (eng. General Public License) licencom. Trenutno valjana inačica je inačica 2.3, a omogućuje rad na platformama i386/AMD64.



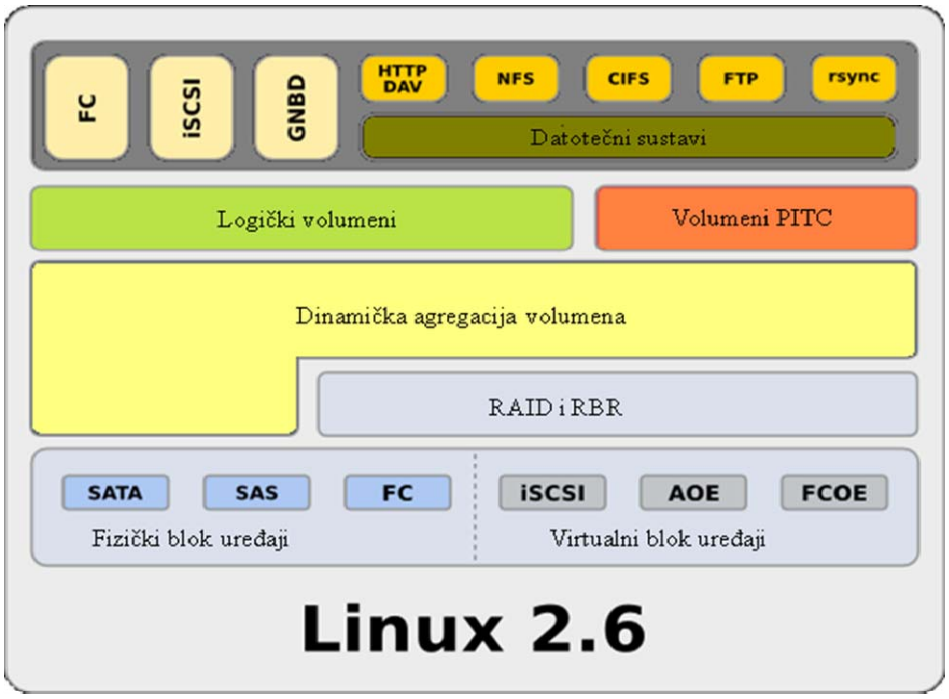
Slika 9 Openfiler

Izvor: http://en.wikipedia.org/wiki/Openfiler.

Na slici 10 prikazana je struktura paketa Openfiler koja uključuje sve komponente i funkcije sadržane u njemu. Svaki disk ili volumen smatra se blok uređajem, a mogu postojati fizički (SATA, SAS, SCSI i FC) i virtualni (iSCSI, AOE i FCOE) blok uređaji. Podržano je spajanje blok uređaja putem upravljačkog sloja RAID, kao i umnožavanje blokova ili RBR (eng. Remote Block Replication) tehnologije.

Prije predstavljanja pohrane vanjskom sloju, potrebno je povezati blokove pohrane, virtualne blok uređaje, RAID volumene i umnožene volumene u jedinstvenu skupinu putem dinamičke agregacije volumena. Logičke i PITC (eng. Point In Time Copy) particije označavaju dijelove DVA (eng. Dinamic Volume Agregation) instance koju je moguće predstaviti korisnicima preko raznih protokola. Također, podržani su razni datotečni sustavi poput XFS i ext3 te ReiserFS v3 i JFS.

Posljednju komponentu na vrhu strukture čine razni protokoli koji zajedno pružaju usluge korisnicima. Protokolima CIFS, NFS, HTTP, FTP ili rsync pristupa se datotečnim sustavima, dok protokoli Fibre Channel, iSCSI i GNBD (eng. Global Network Block Device) služe za pristup blokovskoj razini. Protokol GNBD omogućuje pristup blokovima pohrane preko Ethernet LAN mreže.



Slika 10 Struktura Openfiler-a

Izvor: http://www.openfiler.com/products/openfiler-architecture.

3.2. NASLite

Paket NASLite je besplatna Linux distribucija dizajnirana s ciljem pretvorbe računala temeljenih na x86 okruženju u jednostavno umreženo spremište podataka. Dostupan je za uporabu na operacijskim sustavima Windows, Linux, Mac OS X te drugima. Prva inačica ovog paketa distribuirana je pod GPL licencom, dok je druga izdana kao vlasnički proizvod pod nazivom NanoNAS (obje i dalje dostupne za preuzimanje i uporabu).

Postoje tri vrste paketa ovisno o podršci protokolima Samba (re-implementacija protokola SMB/CIFS), NFT ili FTP. Također, omogućuje udaljenu administraciju preko protokola Telnet (mrežnog protokola za pružanje dvosmjerne interaktivne komunikacije) te uključuje web poslužitelj za prikaz zapisa o pogreškama.

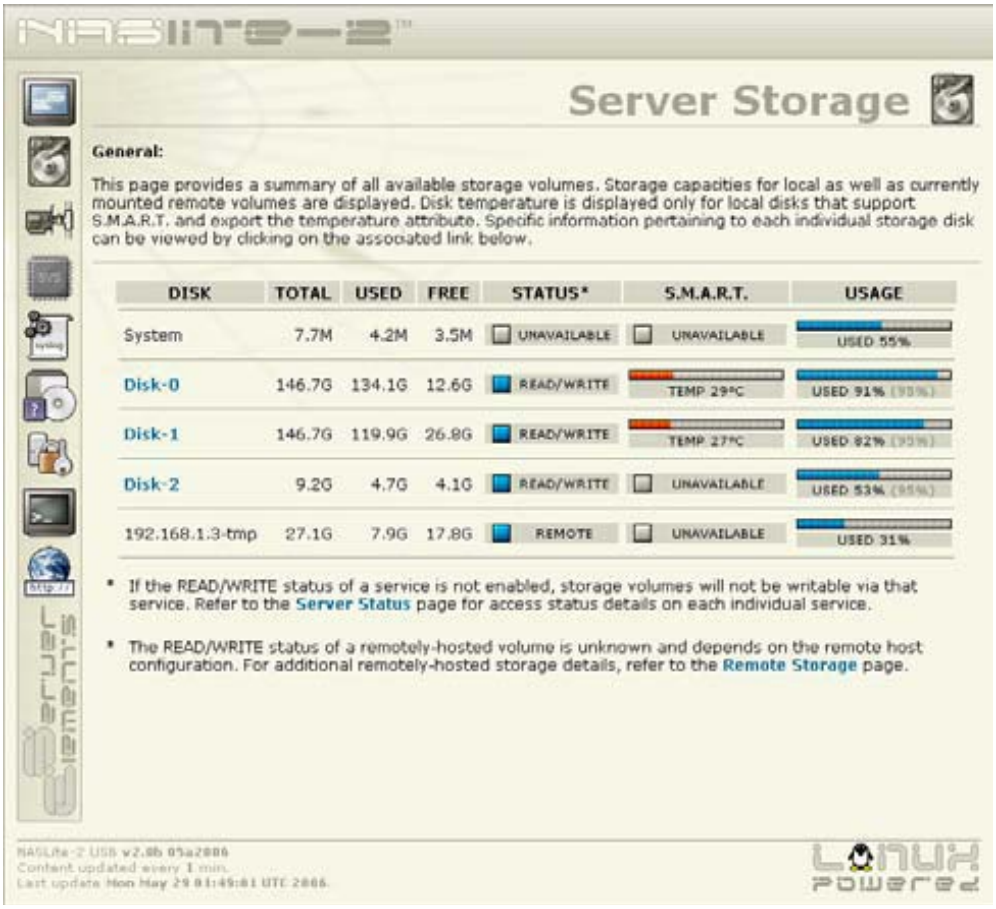
Glavne osobine paketa NASLite:

- jednostavno rukovanje i administracija,
- podrška za protokole SMB/CIFS, NFS, AFP, FTP, HTTP i RSYNC,
- mogućnost spajanja preko priključaka SATA, SCSI, USB i FireWire,
- podrška za ACPI (eng. Advanced Configuration and Power Interface), tj. sustav za upravljanje koji kontrolira napajanje svakog uređaja priključenog na računalo,
- podrška za S.M.A.R.T. (eng. Self-Monitoring, Analysis, and Reporting Technology) sustav koji omogućuje „predviđanje pogrešaka“ na tvrdom disku računala.

NanoNAS, novija inačica paketa koja uz sva navedena obilježja sadrži podršku za pokretanje sa prijenosnih medija (poput CD-ROM uređaja), dolazi u dvije inačice:

1. NanoNAS SMB – pokreće se sa diskete, gdje sprema i konfiguracijske postavke , a dizajnirana je za uporabu sa sustavima WindowsTM. U ovoj se inačici koriste protokoli SMB/CIFS i HTTP.
2. NanoNAS AFP – također se pokreće sa diskete (uz spremanje konfiguracijskih postavki), a namijenjena je za uporabu s sustavima Apple OS X uz protokole AFP i HTTP.

Slika 11 prikazuje izgled izvješća o statusu spremišta na poslužitelju.



Slika 11 NASLite2

Izvor: http://www.serverelements.com/nanonas.php.

3.3. Sun Open Storage

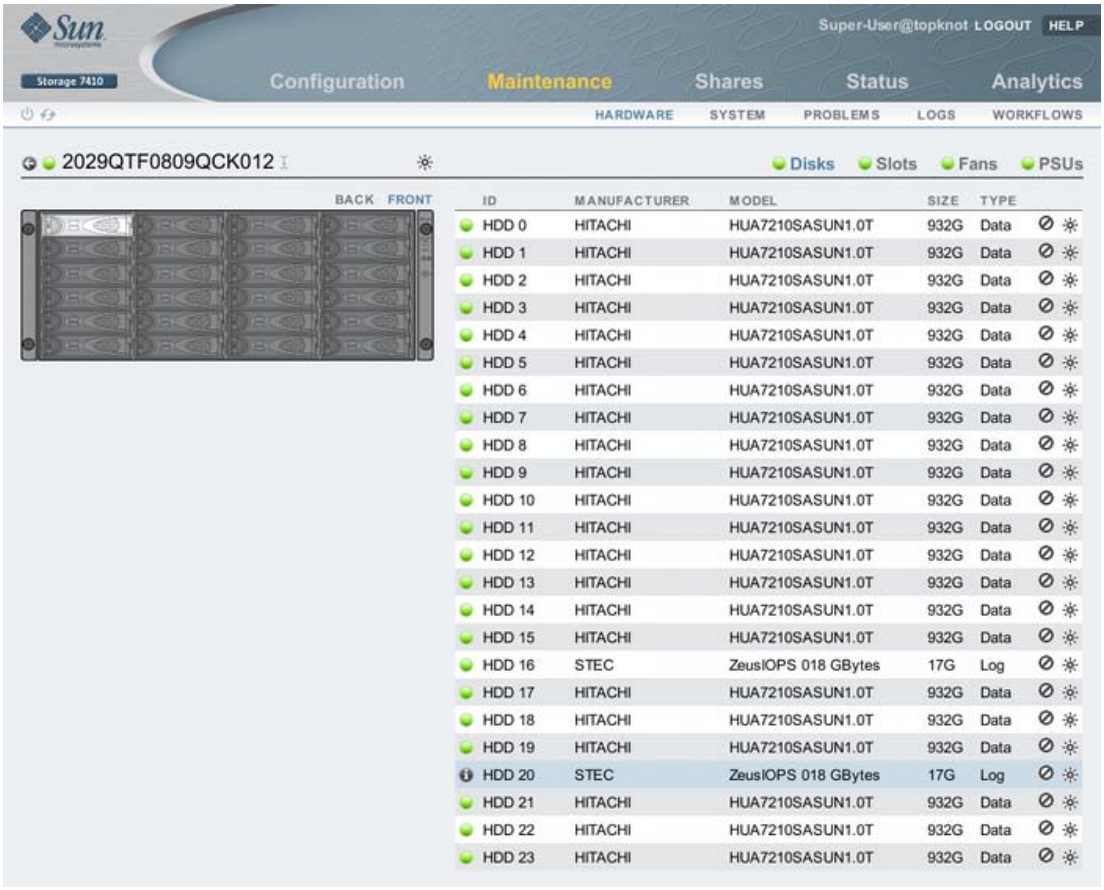
Paket Sun Open Storage je platforma otvorenog koda za pohranu podataka koju je razvila organizacija Sun Microsystems. Dostupan je za platforme Sun Fire X4500 i Sun StorageTek 5800 System. Sučelje spomenutog paketa prikazuje slika 12.

Pruža podršku za:

- tehnologije SCSI i protokole iSCSI te iSNS (eng. Internet Storage Name Service) koji omogućuje automatsko otkrivanje i konfiguriranje iSCSI uređaja,
- mrežne tehnologije Fibre Channel i FCoE (omogućuju najviše brzine od nekoliko Gb),
- topologiju InfiniBand u kojoj računala komuniciraju preko jednog ili više FC (eng. Fibre Channel) prespojnika,
- RDMA (eng. Remote Direct Memory Access) izravan pristup memoriji jednog računala iz memorije drugog bez uključivanja operacijskog sustava,
- uređaje OSD (eng. Object-based Storage Device) koji omogućuju stvaranje dijeljenih i sigurnih umreženih spremišta podataka te
- tehnologiju prijenosa podataka SAS.

Detaljnu usporedbu performansi različitih inačica paketa Sun Open Storage moguće je pronaći preko poveznice:

http://blogs.sun.com/brendan/category/Performance.



Slika 12 Sun Open Storage

Izvor: http://www.sun.com/storage/openstorage/.

3.4. FreeNAS

Paket FreeNAS je besplatni NAS poslužitelj koji ima podršku za protokole CIFS, FTP, NFS, AFP i druge, a izdan je pod BSD (eng. Berkeley Software Distribution) licencom. Osim navedenih protokola podržava i tehnologiju S.M.A.R.T., tj. sustav koji omogućuje „predviđanje pogrešaka" na tvrdom disku računala.

Trenutno dostupna inačica je inačica 0.69.2, a sadrži podršku za platforme Intel 80386/IA-32. Dostupan je u mnogim jezicima, a do sada je dobio nekoliko nagrada od kojih je najznačajnija organizacije „InfoWorld" za najbolji projekt otvorenog koda za pohranu podataka.

NA slici 13 dano je sučelje paketa FreeNAS.

Slika 13 Sučelje FreeNAS alata

Izvor: FreeNAS

Neke osnovne osobine uključuju:

1. Dodatke za tehnologije SlimServer (audio poslužitelj), XBMSP (protokol za prijenos niza podataka raznih vrsta) i iTunes (aplikacija za pokretanje digitalnih medija).
2. Poslužitelj rsync prikazan na slici 14.
3. Podršku za program Unision koji omogućuje sinkronizaciju datoteka.
4. Protokol iSCSI, tj. tehnike za prijenos datoteka u intranetu i upravljanje spremištima podataka.
5. Dinamički DNS (eng. Domain Name System) klijenta koji omogućuje otkrivanje i registraciju korisničkih javnih IP adresa kako bi se sve promjene adresa brzo odrazile u DNS sustavu.
6. Datotečne sustave: UFS, ext2/ext3, NIFS i FAT32.
7. Tehnologije: P-ATA/S-ATA, SCSI, USB i FireWire.
8. Particioniranje diskova putem standarda GPT/EFI (eng. GUID Partition Table/Extensible Firmware Interface) koji omogućuje smještanje jedne ili više particija na isti fizički tvrdi disk.
9. Podrška za veliki skup različitih mrežnih kartica.
10. Mogućnost pokretanja s tvrdog diska, USB uređaja te CD uređaja.
11. Kriptiranje diskova.
12. Upravljanje grupama i korisnicima.

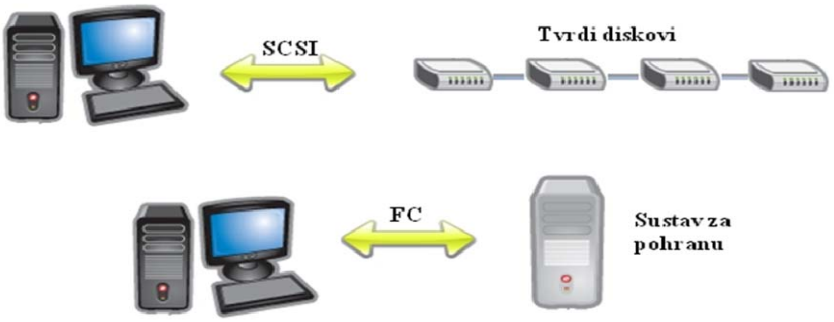
Slika 14 rsync paketa FreeNAS

Izvor:FreeNAS (http://www.freenas.org/)

4. Usporedba s drugim tehnologijama za pohranu

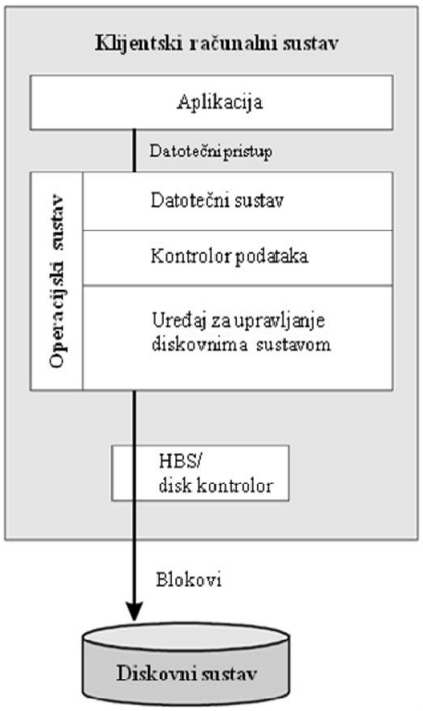
4.1. DAS sustavi

DAS (eng. Direct attached storage) sustavi su najjednostavniji i najčešće korišteni model za pohranu koji se može pronaći u većini računala. Tipična DAS konfiguracija sadrži računalo koje je izravno povezano na jedan ili nekoliko tvrdih diskova ili diskovnu listu. Slika 15 daje primjer povezivanja računala na niz tvrdih diskova, kao i na sustav za pohranu. Između diskova i računala koriste se standardi poput SCSI, ATA, SATA ili FC.



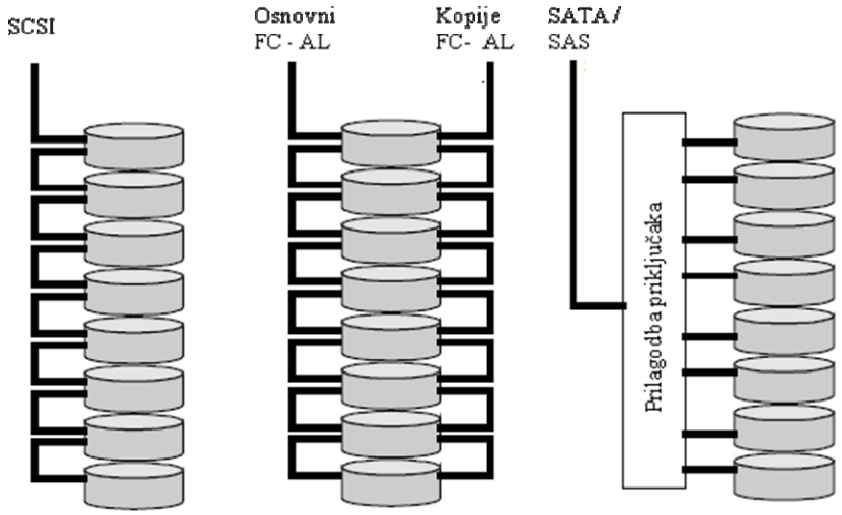
Slika 15 DAS sustavi

Arhitektura DAS sustava dana je na slici 16. Diskovnim sustavom upravlja klijentski operacijski sustav, a aplikacija pristupa podacima preko sustavnih poziva. Takvim pozivima rukuje datotečni sustav koji obavija datoteke u diskovne blokove. Kontrolor podataka (eng. Volume Manager) upravlja blokovskim resursima koju su smješteni u jedan ili više fizičkih diskova u diskovnom sustavu. Uređaj za upravljanje diskovnim sustavom povezuje operacijski sustav s diskovnim kontrolorom ili HBA adapterom koji su odgovorni za prijenos naredbi između računala i diskova. Datotečni pristup koji inicira klijentska aplikacija omotan je u blokove koji se prenose između sučelja računala i diskovnog sustava.



Slika 16 Arhitektura DAS sustava

U slučaju uporabe sustava za pohranu umjesto diskova, oni najčešće sadrže RAID liste ili sustave JBOID (eng. Just a Bunch Of Disks). Radi se o skupini tvrdih diskova kojima se pristupa kao odvojenim uređajima. Postoje brojni načini povezivanja diskova u JBOID sustav, i ovise o tipu tvrdog diska. Osnovni načini povezivanja su putem standarda SCSI, FC te SATA/SAS kako je prikazano na slici 17.



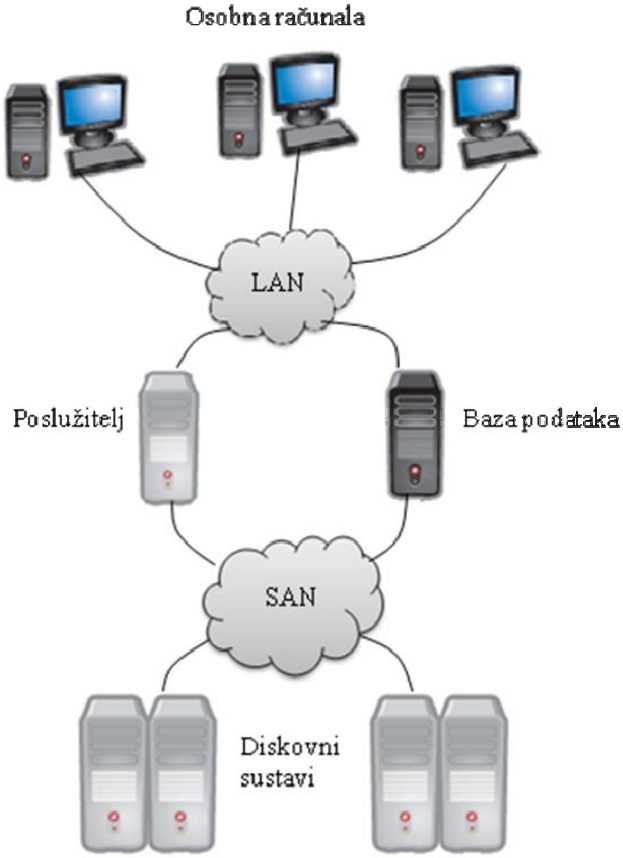
Slika 17 JBOID sustav

Jedno od ključnih obilježja DAS sustava je povezivanje resursa za pohranu s individualnim računalom ili poslužiteljem. Međutim, djelotvornost resursa za pohranu je niska zato što je kapacitet vezan uz jedno računalo. Kapacitet DAS sustava ograničen je na broj diskova, a dodavanje ili uklanjanje diska može narušiti pristup svim diskovima. Osim toga, performanse DAS sustava ograničene su na brzinu obrade individualnog računala. Dostupnost sadržaja DAS sustava je također ograničena jer svaka pogreška na računalu dovodi do nemogućnosti pristupa podacima. Kako bi se osigurali podaci na DAS sustavu, potrebno je napraviti sigurnosne kopije.

4.2. SAN mreže

SAN (eng. Storage area network) mreža omogućuje povezivanje udaljenih uređaja za pohranu na poslužiteljima (ili drugim računalima) u takvom obliku da izgledaju kao da su lokalno spojeni na operacijski sustav. Slika 18 prikazuje tipičnu SAN mrežu koja je često izgrađena na odvojenoj mreži od LAN mreže kako ne bi utjecala na promet LAN mreže. U primjeru se vidi povezivanje brojnih poslužitelja, baza podataka te brojnih diskovnih sustava. Svi spomenuti elementi spojeni su kao čvorovi (eng. peers).

Iako je moguće implementirati zajedničku infrastrukturu između LAN i SAN mreža u iSCSI okruženju, postoji više razloga zašto je bolje napraviti podjelu. Prvo, mreže obično postoje u različitim segmentima cjelokupne mreže (često različitih osobina) jer je SAN mreža obično ograničena na povezivanje poslužitelja s uređajima za pohranu. Za razliku od toga, LAN mreža obično uključuje povezivanje između poslužitelja i osobnih računala. Drugo, promet i zahtjevi za kvalitetom usluga su različiti. Također, SAN mreža može zatražiti veliki prijenosni kapacitet za stvaranje sigurnosnih kopija na određeni vremenski period što LAN mreža ne može osigurati. I na kraju, SAN mreža zasniva se na drugačijem protokolu od LAN mreža (obično se radi o FC standardu).

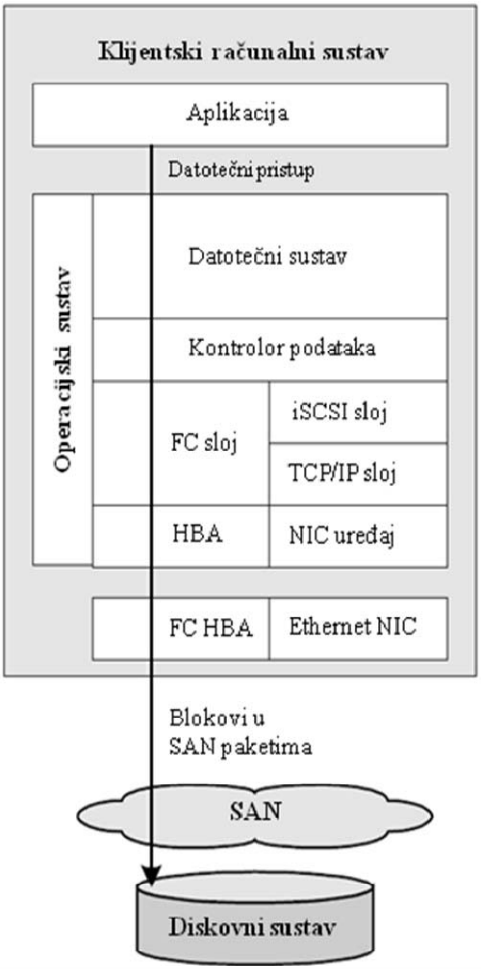


Slika 18 SAN mreža

Arhitektura za podršku SAN mreže potrebna na poslužiteljima (prikazana na slici 19) vrlo je slična arhitekturi DAS sustava. Sastoji se od aplikacije, operacijskog sustava te uređaja za prijenos. Operacijski sustav sadrži više podslojeva: datotečni podsustav, kontrolor podataka, FC ili iSCSI/TCP/IP sloj te sloj za prijenos podatkovnih okvira. Osnovna razlika u odnosu na DAS sustave je u tome što je diskovni kontrolor zamijenjen sa FC slojem ili iSCSI/TCP/IP slojem koji osiguravaju funkcije transporta za blokovske naredbe do udaljenog diskovnog sustava preko SAN mreže.

Na primjer, ako se koristi FC standard (definira četiri podsloja koji se podudaraju sa prva četiri sloja OSI referentnog modela - http://www.cert.hr/documents.php?id=369), blokovske SCSI naredbe su ovijene u FC okvire na četvrtom podsloju FC arhitekture. Na prvom i drugom podsloju provodi se signalizacija i fizički prijenos okvira preko HBA uređaja. Budući da je apstrakcija resursa za pohranu provedena na razini blokova, aplikacije koje pristupaju podacima mogu raditi u SAN okruženju na isti način kao i u DAS.

Jedna od prednosti SAN mreža je mogućnost brze i jednostavne zamjene poslužitelja jer SAN mreža „vidi" resurse za pohranu kao SCSI uređaje. Općenito SAN mreže teže prema omogućavanju efektivnog procesa oporavka od pogrešaka.



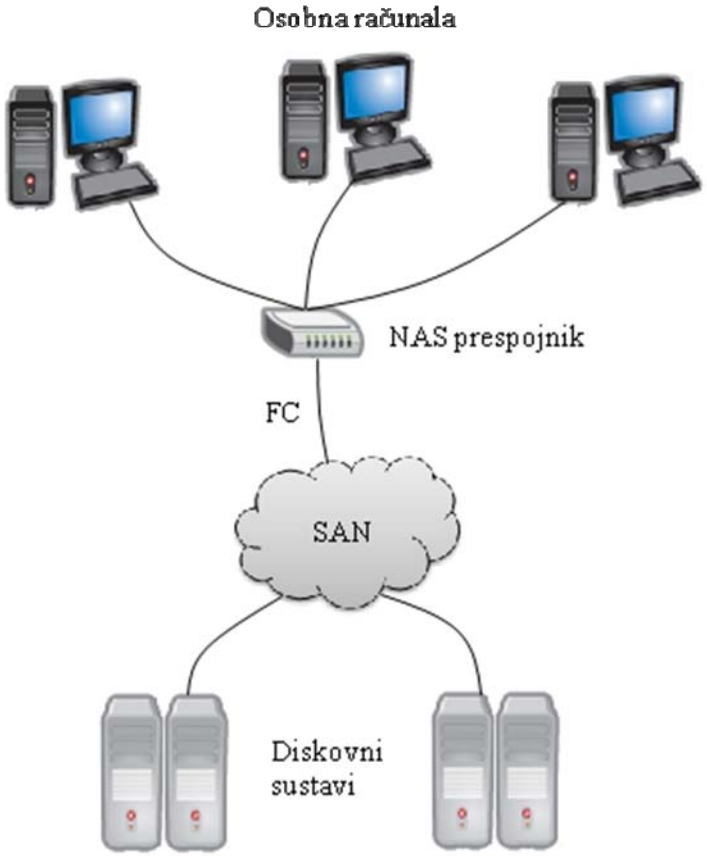
Slika 19 SAN arhitektura

4.3. SAN-NAS hibridni sustav

Povezano rješenje tehnologija NAS i SAN omogućuje odličnu prilagodljivost i napredak performansa za većinu organizacija. NAS sustav vrlo je važan za heterogena okruženja, a SAN za okruženja u kojima se razmjenjuje puno podataka (kako bi se osigurala efektivnost rada). Povezivanjem SAN i NAS tehnologija nastaje SAN-NAS hibridni sustav poput onoga prikazanog na slici 20.

Posjedovanje NAS sustava omogućuje jednostavniji pristup SAN mreži. Zapravo, NAS sustav je idealan prespojnik (eng. gateway) prema SAN mreži, koji usmjerava blokove podataka iz SAN mreže do odgovarajućih poslužitelja u obliku datoteka. U isto vrijeme, posjedovanje SAN mreže omogućuje učinkovitiji rad NAS tehnologije jer uklanja opterećenje koje donosi pohrana manje kritičnih podataka (manje važnih podataka za korisnika). Važne datoteke moguće je pohraniti lokalno na NAS uređaju dok se manje važne podatke mogu isporučiti SAN mreži.

NAS prespojnik se sastoji od NAS uređaja sa FC HBA adapterom, što omogućuje povezivanje s SAN mrežom. Takav uređaj zadržava jednake mogućnosti razmjene datoteka, ali s većom razinom prilagodljivosti. Administratorima omogućuje preraspodjelu pohrane između SAN i NAS sustava. Osim toga, olakšana je izrada sigurnosnih kopija podataka na NAS uređaju preko SAN mreže. Ipak, NAS prespojnik ne spaja u potpunosti SAN i NAS sustave pa je potrebno pohranjivati blokovske i datotečne podatke na različitim uređajima. Također dolazi i do određenog kašnjenja u prijenosu podataka, što je uz složenost implementacije, jedan od osnovnih nedostataka sustava.



Slika 20 SAN-NAS hibridni sustav

4.4. Usporedba tehnologija

DAS sustav čini najosnovniju razinu pohrane podataka u kojoj je uređaj za pohranu dio poslužiteljskog računala. Mrežna računala moraju biti izravno povezana s poslužiteljem kako bi se povezale s uređajem za pohranu. Za razliku od toga, u SAN i NAS sustavu razni korisnici mogu pristupati podacima povezivanjem s NAS uređajem ili SAN mrežom. Ovo je i osnovna razlika u odnosu na NAS i SAN tehnologije koje se povezuju s računalima preko mreže. Budući da je DAS sustav izravno povezan na računalo, mogućnost i brzina pohrane ovise o performansama i aktivnim procesima na računalu. Ovakva arhitektura pogodna je za lokalizirano dijeljenje datoteka u okruženjima s jednim ili nekoliko poslužitelja. Odlikuje se jednostavnošću upravljanja uporabom mrežnog operacijskog sustava priključenog na poslužitelj. Ipak, složenost upravljanja može se povećati dodavanjem novih poslužitelja (jer se svakim prostorom za pohranu upravlja zasebno.)

Iako implementacije NAS sustava rastu velikom brzinom, DAS sustavi još su uvijek jeftiniji u usporedbi sa SAN i NAS sustavima. S ekonomske perspektive, inicijalno ulaganje u DAS je malo što pogoduje organizacijama koje moraju implementirati sustav za pohranu bez planiranja. Ipak, potrebno je voditi računa o ograničenjima u mogućnosti pohrane podataka. Za okoline u kojima se očekuje velik rast podataka pogodnije je koristiti NAS sustave.

NAS sustav čini uređaj koji je sastavljen od tvrdih diskova i programa za upravljanje. Za razliku od DAS sustava, gdje jedan poslužitelj obavlja funkciju dijeljenja datoteka i posluživanja aplikacija, NAS razdvaja spomenute funkcionalnosti.

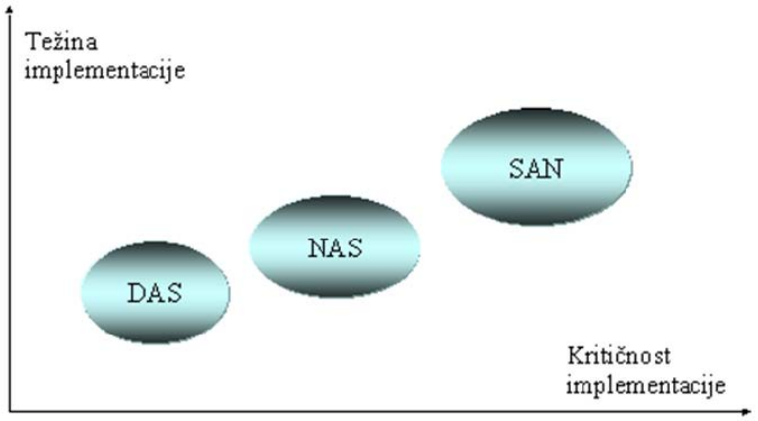
NAS je idealan izbor organizacijama koje traže jednostavno i jeftino rješenja za ostvarivanje brzog pristupa datotekama za više korisnika na razini datoteka. Najčešće se koristi u malim i srednjim poslovnim sektorima. Također je vrlo jednostavno proširiti sustav za pohranu zasnovan na NAS tehnologiji (za razliku od DAS sustava). Još jedna važna prednost NAS tehnologije nad DAS sustavom je mogućnost implementacije u heterogenim okolinama (razni operacijski sustavi). U posljednje vrijeme, NAS se sve češće pojavljuje u kombinaciji s SAN mrežama tvoreći SAN-NAS hibridni sustav. Tablica 1 prikazuje usporedbu značajki svih spomenutih tehnologija za pohranu podataka.

Tehnologija	Mreža	Medij	Protokol	Brzina prijenosa	Dijeljeni kapacitet	Dijeljenje podataka
DAS	Ne	SCSI,FC ili SSA	SCSI	40 MBps – 160 MBps	Ručno ili ne	Ne
SAN	Da	FC	SCSI	100 MBps – 200 MBps	Da	Zahtjeva posebni program
NAS	Da	Ethernet	NFS, CIFS	10 MBps – 1 GBps	Da	Da
NAS prespojnik	Da	Ethernet	NFS, CIFS	10 MBps – 1 GBps	Da	Da

Tablica 1 Usporedba značajki tehnologija za pohranu

SAN mreža je mreža visokih performansi koja prenosi podatke između poslužitelja i uređaja za pohranu odvojeno od LAN mreže. Zbog njihove složenosti i visoke cijene najčešće se primjenjuju u kritičnim poslovnim aplikacijama. SAN mreža može uključivati NAS spremišta i DAS sustave priključene preko standarda FC. Za razliku od njih, snaga SAN mreže je u njenoj mogućnosti za prijenos velikih blokova podataka (važno za baze podataka).

SAN mreža je pogodna za okruženja koja zahtijevaju svakodnevnu dostupnost podataka za više korisnika. Iako SAN mreža ima razne prednosti, poput visokih performansi, nedostatak standarda za SAN mreže i cijena odrazila se na njihov razvoj. Razlika u težini i kritičnosti implementacije prikazana je na slici 21.



Slika 21 Usporedba implementacije tehnologija za pohranu

5. Sigurnosne ranjivosti

5.1. XSS ranjivosti

XSS (eng. Cross-site scripting) ranjivost je tip sigurnosnog problema koji se obično pojavljuje u web aplikacijama. Zlonamjernim korisnicima omogućuje umetanje skriptnog ili HTML koda u web stranicu što često može dovesti do zaobilaženja kontrole pristupa, povećanja ovlasti te izvođenja raznih drugih napada. Upravo zbog takvih posljedica, ovakve ranjivosti predstavljaju velike problema za očuvanje sigurnosti informacija u umreženim spremištima podataka.

Postoje tri inačice XSS napada:

1. **XSS ranjivost temeljena na DOM objektima** (eng. Document Object Model) – XSS napad pokreće se zahvaljujući propustu u pregledniku koji omogućuje prikaz lažne web stranice umjesto legitimne. Takve lažne web stranice obično sadrže i zlonamjerni kod.

2. **Neustrajni XSS napad** – XSS napad se pokreće kada korisnici posjećuju zlonamjerno oblikovane poveznice koje sadrže proizvoljni kod. Najčešći primjer ovakvih napada javlja se prilikom pretraživanja sadržaja putem niza koji uključuje posebne HTML oznake. Ova vrsta napada ujedno čini i najčešći oblik XSS ranjivosti.

3. **Ustrajni XSS napad** – XSS napad zahtjeva pohanu zlonamjernog programskog koda u samu aplikaciju. Primjer je umetanje posebno oblikovanog koda u HTML forme za unos korisničkih podataka. Ova vrsta napada predstavlja najopasniji oblik jer je moguće ugroziti više korisnika u jednom trenutku.

U veljači 2009. godine otkrivena je XSS ranjivost kod paketa Openfiler inačice 2.x. Uzrok problema bilo je nepravilno rukovanje ulaznim vrijednostima „redirect“ parametra u datoteci index.html. Zahvaljujući neispravnoj provjeri vrijednosti prije povratnog slanja korisnicima, napadač je mogao pokrenuti proizvoljni skriptni ili HTML kod u korisničkom pregledniku. Detaljniji opis problema dostupan je preko sljedeće poveznice:

http://secunia.com/advisories/33681/.

5.2. Otkrivanje osjetljivih podataka

Pojam osjetljivi podaci označava sve informacije koje za korisnika imaju određenu vrijednost. Mogu uključivati neke povjerljive informacije (poput autentifikacijskih podataka), poslovne informacije ili korisničke podatke. Zajedničko svojstvo svih navedenih oblika je potreba za odgovarajućom zaštitom pristupa i pregleda takvih podataka neovlaštenim korisnicima. Iako osnovna zaštita osjetljivih podataka uključuje njihovo kriptiranje, napadači razvijaju metode za dekriptiranje poruka ukradenih prisluškivanjem mreže ili probojem u sustav.

Budući da je uloga sustava za pohranu podataka upravo očuvanje sigurnosti, konzistentnosti, cjelovitosti i dostupnosti podataka, vrlo je važno ugraditi zaštitu od pokušaja njihovog pregleda, izmjene ili uništenja.

Ranjivost koja omogućuje otkrivanje osjetljivih podataka pronađena je u siječnju 2009. godine kod programskog paketa FreeNAS. Spomenuti sigurnosti problem uzrokovan je pogreškom u implementaciji protokola Samba. Za opisani problem objavljene su ispravljene inačice paketa, a više informacija moguće je pronaći preko poveznice:

http://www.vupen.com/english/advisories/2009/0018.

5.3. Zaobilaženje sigurnosnih ograničenja

Sigurnosna ograničenja definiraju osnovnu zaštitu podataka definiranjem prava svakog korisnika. Legitimnim korisnicima potrebno je omogućiti pristup podacima te odgovarajuća prava pregleda, izmjene ili uklanjanja podataka. Za razliku od toga, neautentificiranim korisnicima potrebno je ograničiti pristup, kao i pregled i izmjenu podataka.

Kod paketa Openfiler pronađen je, u travnju 2009. godine, nedostatak koji može dovesti do povećanja prava pristupa na sustavu. Problem se javlja u funkcionalnosti za promjenu lozinki. Napadač ga može iskoristiti za postavljanje globalne varijable „userauthenticated" preko zahtjeva POST skripti „account/password.html". Slanjem takvih zahtjeva napadač može zaobići sigurnosna ograničenja te dobiti administratorski pristup. Proizvođač je izdao potrebne programske ispravke za opisane probleme, a za detaljniji opis savjetuje se pregled poveznica u nastavku:

http://www.securityfocus.com/bid/33605/info,
https://project.openfiler.com/tracker/ticket/888.

6. Zaštita

U nastavku dokumenta opisane su neke od metoda koje mogu podići razinu sigurnosti umreženih skladišta podataka. Ipak, primjena samo jedne od ovih metoda često nije dovoljna za osiguravanje zaštite NAS sustava pa se korisnicima preporuča primjena njihovih kombinacija.

6.1. Obnovljene inačice paketa i sigurnosne kopije

Osnovna sigurnosna mjera za zaštitu od svih poznatih ranjivosti je u prvom redu obnavljanje inačica programskog paketa koji se koristi na nekom sustavu. Proizvođači računalnih programa svakodnevno izdaju programska rješenja za otkrivene ranjivosti kako bi povećali sigurnost proizvoda. Primjena takvih programskih rješenja je vrlo jednostavna te ne zahtjeva puno vremena, a često predstavlja jedno od važnijih metoda zaštite sustava. Napadači često koriste ranjivosti čije je otkriće javno objavljeno upravo zbog činjenice da veliki broj krajnjih korisnika ne primjenjuje nadogradnju sustava programskim zakrpama pravovremeno.

Drugu važnu komponentu u zaštiti podataka pohranjenih na nekom od umreženih spremišta podataka čini izrada sigurnosnih kopija. Sigurnosne kopije predstavljaju umnožavanje sadržaja radi njegove pohrane na drugom mjestu kako bi se sadržaj mogao obnoviti nakon uništenja. NAS tehnologija obično se zasniva na RAID listama koje donose redundanciju podataka. Ovo svojstvo omogućuje obnavljanje izgubljenih podataka s jednog ili više mjesta u listama te samim tim donosi određeni stupanj sigurnosti od gubitka podataka. Ipak, gubitkom cijelog sustava nije moguće povratiti podatke pa je u takvim slučajevima jedino rješenje postojanje sigurnosnih kopija podataka koji su bili pohranjeni na ugroženom umreženom spremištu podataka.

6.2. Kriptografija

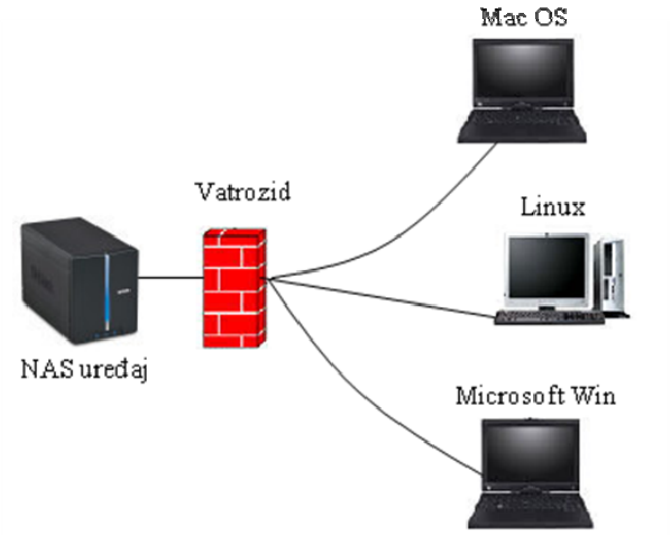
Kriptografija označava predstavljanje podataka u nekom obliku koji nije poznat korisnicima kojima nije namijenjen. Obično se obavlja preko nekog kriptografskog algoritma primjenom tajnih ključeva. Spomenuti tajni ključevi su zapravo vrijednosti korištene u postupku kriptiranja, a poznate su samo korisnicima sustava.

Umrežena spremišta podataka mogu sadržavati raznovrsne informacije koje za korisnike mogu imati različitu razinu važnosti i vrijednosti. Kako bi se osigurala sigurnost od otkrivanja takvih informacija zlonamjernim korisnicima, moguće je provesti neki od postupaka kriptiranja podataka prije njihove pohrane na sustav. U slučaju kada napadač otkrije pohranjene podatke ili informacije potrebne za postizanje pristupa sustavu, podaci su i dalje zaštićeni zbog nemogućnosti njihovog dekriptiranja bez posjedovanja tajnih ključeva.

6.3. Vatrozid

Vatrozid (eng. firewall) je jedan od osnovnih alata za zaštitu računalnog sustava ili mreže. Predstavlja uređaj ili skupinu uređaja koji su dizajnirani za blokiranje neovlaštenog pristupa. Njegov rad se temelji na skupu pravila i kriterija koji služe za prosljeđivanje prometa između sigurnosnih domena.

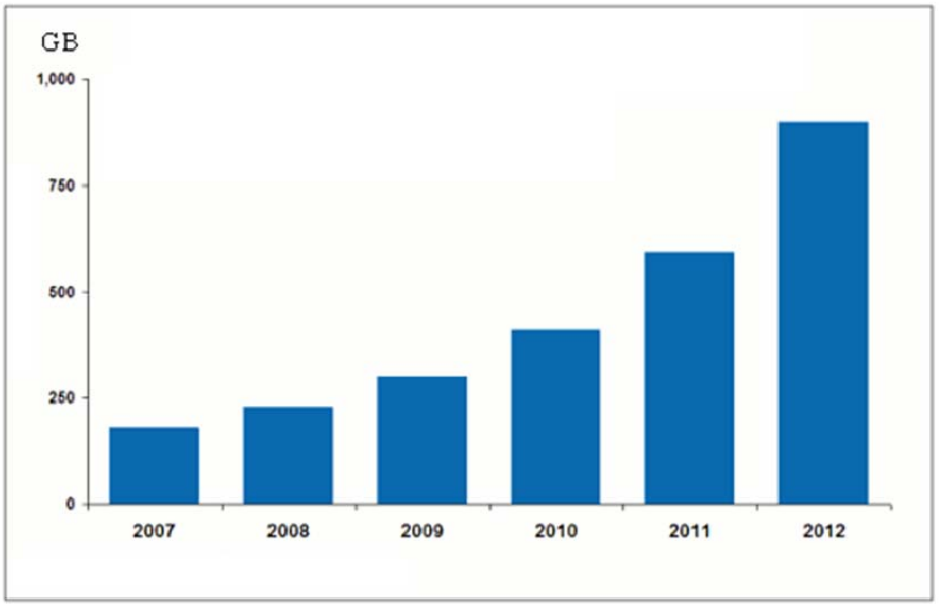
Ugradnjom vatrozida u sustave za pohranu podataka moguće je spriječiti pokušaje neovlaštenog pristupa sustavu. Potrebno ga je smjestiti ispred NAS uređaja (slika 22) kako bi se filtrirao sav promet prije dolaska do pohrane. Ako su lokalna računala sadrže spomenuti alat, moguće je samo postaviti dodatna pravila za filtriranje sadržaja te na taj način izbjeći potrebu za ugradnjom novog vatrozida.



Slika 22 Ugradnja vatrozida

7. Očekivanja u budućnosti

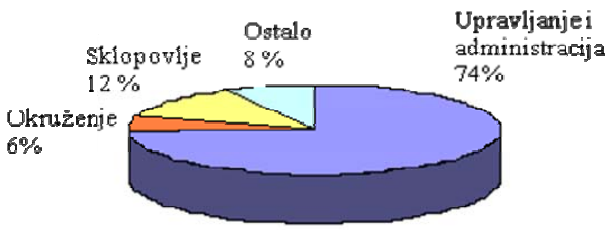
Razvoj multimedijskih sadržaja, poput video zapisa, donosi veće zahtjeve na prostor potreban za pohranu podataka. Korisnici sve češće imaju zahtjeve za prostorom za pohranu video zapisa, slika ili sličnih podataka. Do 2012. godine predviđa se vrlo veliki rast potreba za prostorom za pohranu podataka po korisničkom računalu kako je prikazano na slici 22. U razdoblju od 2007. do 2012. godine predviđa se porast od gotovo 0,7 GB po osobnom računalu. Prema istraživanju „Home Servers and Consumer Storage: Analysis and Forecasts" (http://parksassociates.ecnext.com/coms2/summary_0256-10184_ITM) predviđa se uporaba gotovo 13 milijuna NAS uređaja do 2012. godine.



Slika 23 Povećanje potrebnog prostora za pohranu

Kako bi se zadovoljile potrebe korisnika očekuje se razvoj rješenja za jednostavniju alokaciju datoteka, pretragu i dijeljenje podataka. Proizvođači uređaja za pohranu moraju pažljivo razvijati značajke koje tržište zahtjeva (poput jednostavnosti stvaranja sigurnosnih kopija, dijeljena datoteka i spajanja novih uređaja). Na taj način NAS uređaji će proširiti svoju ulogu u okruženjima gdje su potrebni poslužitelji podataka.

S druge strane, korisnici zahtijevaju sustave kojima je jednostavno upravljati. Podjela troškova na pohranu podataka pokazuje da najviše troškova dolazi zbog složenosti upravljanja i administriranja sustava. Ostali troškovi pohrane podataka, prikazani na slici 23, ukazuju na puno veću ulogu postupka upravljanja podacima u odnosu na sklopovlje i okruženje. Prema ovim podacima, očekuje se da budući razvoj NAS uređaja uključi još jednostavnije postupke upravljanja podacima.



Slika 24 Troškovi pohrane podataka

8. Zaključak

Umrežena spremišta podataka u osnovi predstavljaju tvrde diskove kojima je moguće pristupiti putem Ethernet mreže. Osnovna funkcija ovakvog spremišta je distribucija podataka svim korisnicima koji su fizički povezani na mrežu te imaju pravo pristupa. Osim funkcija pohrane podataka, ovakvi sustavi imaju razna obilježja poslužitelja (pa se čak i na najjeftinijim uređajima može omogućiti podrška za poruke elektroničke pošte). Naprednije inačice NAS uređaja sadrže RAID liste te osiguravaju mogućnost obnove izgubljenih podataka. NAS uređaji uklanjanju potrebu pohrane podataka na drugim poslužiteljima u mreži pa se često susreću u raznim poslovnim okruženjima.

Kombiniranjem ove tehnologije s ostalim tehnologijama za pohranu podataka (SAN i DAS) moguće je povećati performanse sustava. U budućnosti se očekuje povećanje korištenja NAS tehnologija zbog povedene potrebe za prostorom za pohranu podataka.

9. Reference

[1] Umrežena spremišta podataka, http://en.wikipedia.org/wiki/Network-attached_storage, srpanj, 2009.

[2] Heng Liao, Storage Area Network Architectures, http://www.pmc-sierra.com/cgi-bin/document.pl?docnum=2022178, travanj, 2003

[3] NFS protokol, http://en.wikipedia.org/wiki/Network_File_System_(protocol), srpanj, 2009.

[4] SMB protokol, http://en.wikipedia.org/wiki/Server_Message_Block, srpanj, 2009.

[5] AFP protokol, http://en.wikipedia.org/wiki/Apple_Filing_Protocol, srpanj, 2009.

[6] FTP protokol, http://en.wikipedia.org/wiki/FTP, srpanj, 2009.

[7] HTTP protokol, http://en.wikipedia.org/wiki/HTTP, srpanj, 2009.

[8] UPnP protokoli, http://en.wikipedia.org/wiki/UPnP, srpanj, 2009.

[9] SSH protokol, http://en.wikipedia.org/wiki/Secure_Shell, srpanj, 2009.

[10] FreeNAS, http://en.wikipedia.org/wiki/FreeNAS, srpanj, 2009.

[11] FreeNAS, http://www.freenas.org/, srpanj, 2009.

[12] Openfiler, http://en.wikipedia.org/wiki/Openfiler, srpanj, 2009.

[13] Openfiler, http://www.openfiler.com/, srpanj, 2009.

[14] NASLite, http://en.wikipedia.org/wiki/NASLite, srpanj, 2009.

[15] NanoNAS, http://en.wikipedia.org/wiki/Nanonas, srpanj, 2009.

[16] NASLite/NanoNAS, http://www.serverelements.com/index.php, srpanj, 2009.

[17] Sun Open Stogare, http://en.wikipedia.org/wiki/Sun_Open_Storage, srpanj, 2009.

[18] DAS, http://en.wikipedia.org/wiki/Direct-attached_storage, srpanj, 2009.

[19] SAN, http://en.wikipedia.org/wiki/Storage_area_network, srpanj, 2009.

[20] NAS, DAS or SAN?, http://www.storagesearch.com/xtore-art1.html, srpanj, 2009.

[21] David Sacks, Demystifying Storage Networking, http://www-03.ibm.com/industries/ca/en/education/k12/technical/whitepapers/storagenetworking.pdf, lipanj, 2001.

[22] Usporedba tehnologija, http://www.michcomp.com/storage.html, srpanj, 2009.