DKUUG nr. 167

Juli 2012

NYT

DKUUG - Unix Brugere, system administratorer
Dansk Forum for Åbne Systemer
Mødested for IT-specialister og IT-interesserede.

DKUUG

Brev fra formanden

Kære læser

I det forløbne halve år har DKUUG været aktiv for konferencen Open Source Days, hvor talrige aktivister har vist at der er interesse og entusiasme omkring Open Source.

For mig var det vigtigste at se, hvor fint det fungerede.

DKUUG har jo, fornuftige som vi er, skruet ned for udgifterne i forbindelse med at medlemsindtægterne er mindsket, men takket være salget i sin tid af DK-Hostmaster kan foreningen fortsætte med at give husly og støtte til foredrag og konferencer.

Vi er glade for at være i Symbion, en forskerpark, men vi kan måske udnytte kontakten til de andre virksomheder og foreninger noget bedre.

Vores kontorlokale er blevet ommøbleret så at der er plads til flere mødedeltagere, der er mere luft, ventilationen fungerer og nu vil man kunne holde mindre kurser og møder på kontoret uden at temperaturerne kommer op over de tropiske 28°C.

Kontoret markerer os udadtil med en lille skærm med dynamisk information om DKUUG.

Vi ønsker dig velkommen til et nyt DKUUG og håber vi ses efter sommerferien,

Venlig hilsen/Formanden

Symbion ligger på en stille vej og har gode parkeringsforhold

I dette nummer ...

DKUUG var først til at levere Internet til erhverv i Danmark, og vi har gennem tiderne på flere måder været involveret i åbne standarder, åben kommunikation og synliggørelse af bindinger til uhensigtsmæssige proprietære systemer. Det var til syvende og sidst dette at få generisk sunde systemer, som var drivkraften bag ophøjelse af Unix til en standard, POSIX og senere Single Unix Specification, http://www.unix.org/version4/overview.html

6.Juni var der World IPv6 Launch Day, hvor en række af de mest besøgte sites på verdensbasis gik på IPv6 nettet - og nu bliver de permanent på IPv6 nettet.

Vi fortsætter i dette nummer med omtale af IPv6, men i anledning af World-IPv6 day har vi koncentreret os om hvor galt det egentlig står til med den gamle IP protokol, IPv4. Herved stødte vi ind i en sand religionskrig, der var faktisk også nogen i bestyrelsen, som anså IPv6 for at være lidt overflødigt, en slags legeplads for viderekomne, om ikke ligefrem bloatware.

Desuden bringer vi en billedreportage fra Open Source Days 2012. Forsidebilledet er også fra OSD 2012 og siger meget om stemningen: det kan være sjovt athøre noget nyt og lære noget, især hvis man selv har en finger med i spillet, sådan tolker vi her på redaktionen det billede.

En gammel bekendt, Martin Skarbiniks, udfordrede DKUUG-Nyt til at fortælle om problemet med markedsføring og binding til leverandører ved hjælp af uddannelse. I Linux-miljøer, husker jeg at Martin sagde ved en hyggelig julemiddag, kan man ikke få et brush-up kursus i nyeste version af *postfix-mailserver,* eller et avanceret kursus i den udvidede udgave af PostgreSQL serveren. Det prøver Martin at råde bod på og vi håber at høre nyt fra den kant til næste sæson.

Imidlertid har LPI allerede i mange år arbejdet på certificering for Linux-specialister, og med de nyeste udspil fra LPI kan man nu blive certificeret som avanceret Linux sysadm eller engineer om man vil, med speciale indenfor et af de vigtige områder, hvor Linux gør sig stærkt gældende på serverside.

Certificering er en god ide - og er nødvendigt i visse markeds-segmenter for at understrege at Linux har anseelse og mange aktiviteter og mange professionelle brugere.

Linux berømt og berygtet for, at folk piller, eksperimenterer, laver nye løsninger, som kun *næsten* er flytbare. LPI certificering bør i fremtiden kunne garantere for, at folk har en grundlæggende forståelse af systemadministrations-principper og konventioner.

En video fra Linux Foundation fortæller, hvor meget Linux egentlig betyder indenfor high performance computing. Fx. ESO, NASA, CERN, Livermore, alle bruger de Linux. Det er tankevækkende, og man kan på billederne fra OSD se, at de nye opgaver til ESO observatoriet i Chile også har fanget opmærksomheden hos en foredragsholder, som har et billede på storskærmen af det planlagte mega-store observatorium.

Donald Axel

DKUUG-Nyt er medlemsblad for DKUUG, foreningen for Åbne Systemer og Internet

Udgiver:

DKUUG
Fruebjergvej 3
2100 København Ø
Tlf. 39 17 99 44
email: dkuugnyt@dkuug.dk

Redaktion:

Donald Axel (ansvarshavende)
og mange flere

Forsidefoto:

Kristian Vilmann
OSD på CBS marts 2012

Design og layout:

DKUUGs PR-gruppe

Annoncer:

pr@dkuug.dk

Tryk:

Digital-trykkeriet i Aarhus

Oplag:

500 eksemplarer

Medlem af Dansk Fagpresse
DKUUG-Nyt
ISSN-1395-1440

INDHOLD:

THE CAMP

I 2012 præsenteres for 11. gang en do-IT-yourself-sommerlejr for computernørder. TheCamp har rammerne - landlig idyl med internetforbindelse, strøm nok og en hel uge til at lave præcis hvad du har lyst til. Lejren foregår i uge 30 og varer fra lørdag d. 21 juli til lørdag d. 28. juli 2012. Billetterne er udsolgt - men følg med i hvad der foregår via internettet, **thecamp.dk**

Andre Arrangementer

Foredrag i Symbion:

Tirsdag d. 21. august kl. 18: Apache HADOOP er et bud på et storage system for distribueretde applikationer med mange dataset. Kenneth Geisshirt vil fortælle om dette og meget andet, Map/Reduce som generelt koncept og værktøjer som HBase, Pig, Hive og Mahout.

Tirsdag d. 4. september kl.19: Workshop om teknisk oversættelse.

Torsdag d. 20. september kl. 19: Basisviden om shellens systemkald, Donald Axel.

Torsdag d. 27. september kl. 18: Kan Apache OpenOffice bruges til layout? Donald m.fl.

Tirsdag d. 2. oktober kl. 19: IPv6, multihoming og mobile-devices - en akilleshæl?

Tirsdag d. 9. oktober kl. 18: Emner ikke fastlagt - Birds of Feather

Vores kontor er omstillet og ventilationen fungerer, så vi nu kan have gruppe-arbejde og afholde kurser eller workshops, både dag og aften. Skriv til pr@dkuug.dk eller til bestyrelsen i DKUUG, bestyr@dkuug.dk, og hør om du kan låne lokalet. Der er hurtig internetforbindelse.

Kom og få dine kompetencer plejet - hold et foredrag om det, der interesserer dig (og os).

IPv6 world launch day

6. juni permanent IPv6

De mest besøgte websites anbefaler IPv6

5. juni 2012 annoncerede Internet Society i Washington og Geneva (http://www.internetsociety.org/) at den 6. juni 2012 er *World-IPv6-Launch,* den dag, hvor tusinder af firmaer og websites nu permanent kan tilgås over IPv6.

I pressemeddelelsen (som kan læses på *World-IPv6-launch* websitet, http://www.worldipv6launch.org/press/world-ipv6-launch-unites-industry-leaders-to-redefine-the-global-internet/) forklares det, at IPv6 sikrer Internettets fortsatte expansion, og at tusinder af firmaer og millioner af websites nu har permanent IPv6 forbindelse.

IPv6 Launch omfatter de fire mest besøgte websites i verden, Google, Facebook, YouTube, og Yahoo! og mange flere. Det har stor betydning for branding af IPv6, at Cisco og andre router-firmaer er med i samarbejdet. Cisco forklarer at IPv6 er nødvendigt for at milliarder af mobile devices kan kommunikere hurtigt og effektivt og opnår rimelige hastigheder med videostreaming m.v.

Mere end 100 lande var med i lanceringen.

Sidste år var 8. juni en test dag, World IPv6 Day. De store websites var midlertidigt tilgængelige via IPv6 (Google fortsatte dog med at have ipv6.google.com til test af IPv6 connectivity). I år blev de samme websteders IPv6 service permanent d. 6. juni.

Det vejer tungt for den anseelse, IPv6 nyder, at så mange store websites er med til at lancere *permanent* IPv6 service.

Er IPv6 nu også nødvendigt?

Vi kender lancering af nye versioner, somme tider *oversolgt* som ny og bedre, men i realiteten med features, som kun ganske få brugere har glæde af. Man husker måske lancering af en *office-pakker* som noget nyt og banebrydende, store helsides-reklamer, men stadig essentielt det samme. Vi, der har været med fra begyndelsen af 80'erne, husker Wordstar. Så kom WordPerfect og det var lidt bedre. Der var også noget, der hed Word til DOS-2.1. Senere kom Windows og Word for Windows og nye versioner var ikke altid bedre. Derfor er det ikke så underligt, at mange brugere og iøvrigt også professionelle spørger om ikke IPv6 bare er en fidus for at sælge flere routere.

Nej, IPv6 er ikke en klam fidus, men forklaringerne stritter i alle retninger.

Deltagerne i *World-IPv6-Launch* siger først og fremmest, at IPv4 ikke kan rumme flere brugere og at der allerede er store problemer i Asien med at skaffe plads til flere, på trods af at man bruger Network Address Translation (NAT).

NAT i korthed

NAT gør, at brugere i et lokalnetværk med såkaldte private IP-numre kan tale med omverdenen. En anmodning om indhold fra typisk et website sendes fra brugeren på lokalnettet, klienten, til en server.

Men andre udefra kan ikke sende en request til klienten, med mindre klienten selv har lagt en "krog" på fx. en chat-server eller er gået på et website som *Facebook* og "lytter" på, hvad der sker dér. Det opfattes af de færreste som et problem, fordi vi ikke kender andet. Men det svarer til, at vi skal ringe til telefon-centralen og spørge, om der er nogen, der vil tale med os.

I praksis er NAT som regel NAPT, Network Address Port Translation. Det foregår på følgende måde: En lokal bruger, klienten, fx. 192.168.0.10, sender en pakke til en NAT-router, også kaldet en gateway; her får pakken gateway'ens, globalt unikke adresse plus et ledigt portnummer evt. et andet end det oprindelige. Portnummeret registreres i en tabel som hørende til klienten. Portnummeret er et tal, det er ikke en fysisk del af netværks-devicen, men svarer nærmest til et lokal-telefon-nummer. Når en datapakke kommer tilbage til gateway'en, vil den se hvilken lokal maskine, der har været knyttet til portnummeret, den del af netværks-adressen, som svarer til lokal-telefonnummeret.

Gateway'en har med andre ord registeret at der er en forbindelse mellem en lokal maskine og en extern maskine og bruger de ekstra bits, som udgør portnummeret, som en udvidelse af adresserummet.

Derved er IP numrenes dække-evne udvidet, og der er rigeligt til at dække verdens behov - siger NAT-tilhængerne.

Men det er nødvendigt at registrere en tilstand i gateway'en, og en statusløs kommunikation er nu blevet til statusbaseret, en session, som belaster gatewayen mere end nødvendigt.

Det er en gammel diskussion

I 2000 skrev T. Hain fra Microsoft en RFC-2993 med titelen *Architectural Implications of NAT*. En RFC, Request For Comment, er begyndelsen til en Internet specifikation eller, som her, en diskussion af et problem.

Hain skriver bl.a.:

Some people are proclaiming NAT as both the short and long term solution to some of the Internet's address availability issues and questioning the need to continue the development of IPv6. The claim is sometimes made that NAT 'just works' with no serious effects except on a few legacy applications. At the same time others see a myriad of difficulties caused by the increasing use of NAT.

[...] The arguments pro & con frequently take on religious tones, with each side passionate about its position.

- Proponents bring enthusiasm and frequently cite the most popular applications of Mail & Web services as shining examples of NAT transparency. They will also point out that NAT is the feature that finally breaks the semantic overload of the IP address as both a locator and the global endpoint identifier (EID).

- An opposing view of NAT is that of a malicious technology, a weed which is destined to choke out continued Internet development. While recognizing there are perceived address shortages, the opponents of NAT view it as operationally inadequate at best, bordering on a sham as an Internet access solution.

Reality lies somewhere in between these extreme viewpoints.

[oversættelse ...] Argumenterne for og imod får ofte religiøse overtoner og hver side forsvarer lidenskabeligt sine meninger.

- Fortalerne (for NAT) nævner med entusiasme de mest populære applikationer, mail og web services, som skinnende eksempler på NAT transparens. De påpeger også at NAT er den feature, som endelig bryder det semantiske overbelastning af IP adressen som både locator (stedbestemmelse) og som global unik adresse.

- Et modsat syn på NAT er, at det er en ondartet teknologi, ukrudt, som vil kvæle fortsættelsen af Internet udviklingen. Mens de anerkender, at der er mangel på adresser, mener opponenterne at NAT i bedste fald er en midlertidig løsning, i værste fald på grænsen til en bedragerisk måde at få Internet adgang.

Virkeligheden ligger et sted midt imellem disse ekstreme synspunkter.

Statusløs kommunikation mellem to punkter

IPv6 fortalerne mener, at NAT var en nødvendig løsning, men at det ødelægger End-to-End princippet om at alt, hvad der sker mellem to IP-adresser er uden status. Al kommunikation på internettet bør være peer-to-peer, d.v.s. mellem ligestillede systemer, eller burde være det.

Folk er vant til at tænke i "TV-station" og "TV-modtager", klient-server - måske er det derfor, at man så gladeligt har accepteret NAT-systemet og er tilfredse med mail og web, som jo også kan strækkes til at fungere som bærer af fx. Skype og til dels også video-streaming.

Den generelle kritik af NAT er, at det indfører et ekstra lag af kompleksitet, som giver flere problemer og forårsager unødige tab af netværkspakker, og derved større belastning.

Et eksempel på status

Linux maskiner kan som bekendt bruges som routere. Linux kernemodulet ip_conntrack (Connection Tracking), som bruges i en NAT-router, er et eksempel på at det kan være nødvendigt for netværks-stakken at registrere status. Tidlige brugere af Linux vil kunne huske, at FTP gav problemer, hvis man sad bag en NAT-router eller en uintelligent firewall.

*** *** ***

IPv4 exhaustion

Vi må se lidt nærmere på det første argument om, at der ikke skulle være adresser nok. Herhjemme har TDC sagt, at der er rigeligt med IPv4 adresser og at man først regner med at få problemer med antallet om 5-10 år. For at forstå, hvorfor TDC og andre ISP'er kan sige dette, må vi se på hvordan Internet adresserne blev uddelt før og nu.

Fordelingen af Internet adresser

IP teknikken (Internet Protokollerne) blev opfundet i USA og i de første år var der langt flere amerikanske sites på Internettet. Tildelingen af IP-numre (adresser) var afslappet. Mere end halvdelen af globalt-unikke adresser er uddelt i USA. Nogle af de store amerikanske virksomheder fik flere IP adresser end alle lande i regionen Asien tilsammen.

Internettets administration er opdelt i regioner, hvor IP-adresserne administreres centralt og uddeles til de forskellige landes IP-autoritet, Regional Internet Registry (RIR).

Regionerne hedder:

ARIN American Registry for Internet Numbers, (Nordamerika og dele af Caribien).

LACNIC Latin American and Caribbean Network Information Centre (Sydamerika og Caribien).

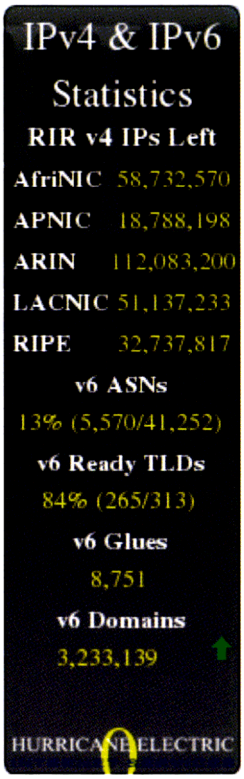
APNIC Asia-Pacific Network Information Centre (Asien, Australien, New Zealand).

AfriNIC African Network Information Centre.

RIPE-NCC Réseaux IP Européens Network Coordination Centre (Europa, Mellemøsten, Rusland og Central-Asien).

Det interessante her er, at *AfriNIC er kommet til i 2005,* og giver os en strømpil for eksplosion i antallet af devices. Afrikanere i de store afrikanske økonomier, bl.a. Sydafrika og Nigeria, bruger smartphones og har derved undgået en fase med fastnet telefoni; trådløs computernet er indenfor rækkevidde flere steder. Det er derfor, at antallet af brugere er ved at eksplodere.

Hurricane Electronics tunnelbroker (et sted hvor man kan få en tunnel hos til IPv6 nettet) har et barometer for Intnernet-adresser. Takket være at mange ISP'er har fulgt RIR - opfordringerne til at inddrage ubrugte IPv4 adresser, kan vi se at AfriNIC og APNIC stadig har lidt tid at løbe på. Men det spiller også ind, at der faktisk er et IPv6 backbone i Asiatiske lande, og at nye slut-brugere ikke får en IPv4 adresse; det gør kun store firmaer.



IPv4 adresser i 9maj 2012

Allokering i tal

Pakistan (under APNIC)

Antallet af IPv4 adresser pr. asiatisk land er forsvindende lille i forhold til befolkningernes størrelse.

Pakistan: i 2010 ca. 6900 /24 blokke (en /24 blok har som bekendt 253 slutbruger-adresser, fordi to går til hhv. net og broadcast) d.v.s 1.7mio IP-adresser; og i 2012 ca. 12000 /24 blokke eller ca. 3.5 mio. IPv4 adresser. (http://www.dailytimes.com.pk) Pakistans befolkning estimeres at være 177 mio. i 2011; seneste folketælling i 1998 viste 132 mio. Rundt regnet 1 IPv4 adresse pr. 55 indbyggere.

Philippinerne

Befolkningen på ca. 93 mio. har 5.3 mio. IPv4 adresser, rundt regnet 1 IPv4 adresse pr. 16

indbyggere.
http://blog.sploitlabs.com/post/3829918565/philippine-ipv4-address-space-allocation

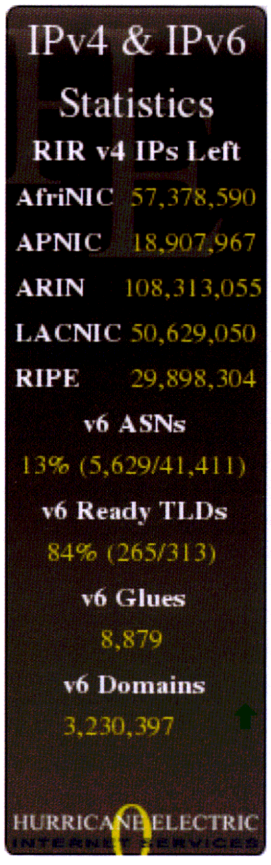
Kina

Med 1340 mio. mennesker det største land, men også mest atypiske land. APNIC skrev i 2004, at antallet af IPv4 adresser kunne dække behovet i 5 - 10 år. Dengang havde man ca. 102 mio IPv4 (mod 17 mio. i 2000) og Kina fik stadig tildelt flere.
http://www.apnic.net/community/about/internet-governance/articles/ip-addressing-in-china-2004

Antallet af Internet-brugere er mere interessant end antallet af allokerede IP-adresser, men det er også vanskeligere at tælle op - hvor mange brugere gemmer der sig fx. på et lokalt wireless-net. Antallet af solgte laptops og smartphones med Internet connectivity ville være interessant. I 2008 var antallet af Internet brugere større i Kina anslået 500 mio hvilket er flere Internet brugere end der er i USA.

De nøjagtige tal for hvor mange IPv4 adresser der er i Kina er lidt forskellige fra kilde til kilde, anslået er man i 2011-2012 oppe på at have 450 mio IPv4 adresser, men der som bekendt flere slutbrugere end IPv4 adresser p.g.a. NAT.

Men i de forløbne fire år er Kinas økonomi som bekendt expanderet, mens USA og EU har døjet med følgerne af boligboble og samvittighedsløse policies i finans-sektoren, og derfor har Kinas Internet organisationer haft større behov for expansion.



IPv4 12. Juni 2012

Iflg. http://www.ip2location.com-/reports/internet-ip-address-2012-report har Kina 11% af det totale antal IP adresser, nr.2 efter USA, som har 34% af IPv4 adresserne. Ved at genbruge og ved at indkræve ubrugte adresser kan levetiden for IPv4 udstrækkes i lang tid, anslået 4-5 år uden større problemer. Somme tider ses det på Hurricane Electric's optælling, at antallet af ledige IPv4 adresser er forøget i forhold til forrige måned.

Der har, så vidt jeg kan bedømme ud fra de forskellige artikler i IT-nyhedsmedier, også været modstand i Kina imod IPv6, blandt andet med påstand om, at IPv6 er mere usikkert. "Usikkert" betyder, i Kina, at folk kan gøre ting, som myndighederne ikke bryder sig om.

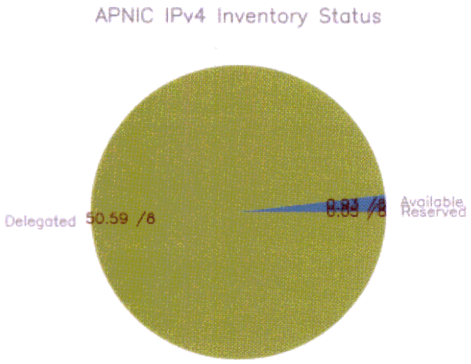
Derfor har det stor betydning, at Kinas Local Internet Registry (LIR), China Network Information Center (CNNIC), har advokeret for IPv6.

I 2012 er antallet af IPv6 adresser i Kina pludselig vokset med raketfart og Kina kører et IPv6 backbone.

En yderligere expansion af IPv6 backbone er planlagt, og ved store testkørsler i 2013 skal "sikkerheden" vurderes af de kinesiske civile myndigheder.

Asia and Pacific - APNIC

Der findes mange tabeller på forskellige websites, men APNIC har ikke en nemt tilgængelig tabel, kun antal delegerede (uddelte) adresser. APNIC har udleveret ca. 850 mio. IPv4 adresser.



APNIC har uddelegeret 50 x 17 mio IPv4 adresser, ca.850 mio, i Asien/Australien/Stillehavsregione. Kilde: APNIC

IANA uddeler IPv4 adresser i blokke og vil helst uddele såkaldte / 8 blokke. En /8 blok er en adresse-blok (fortløbende talrække) som fx. fra 123.0.0.0. til 123.255.255.255.

APNIC undersøgte, hvor meget panik der opstod sidste år, da de sidste /8 blokke blev uddelt. Der var pres på APNIC for at få de sidste, og derefter pres på de lokale Netværksadministrationer, men panikken, som kunne ses på øget pres for at få adresser, lagde sig hurtigt, og APNIC mener, at det skyldtes saglig og upartisk behandling af ansøgninger.

Europa

Som det ses af tallene fra Hurricane har RIPE (Europas Internet adm.) 29 mio. IPv4 adresser. Man skal nok lige have i tankerne at der er ca 800 mio mennesker i Europa, før man jubler over, hvor mange ledige adresser, der er tilbage. Selv om man bruger NAT, vil det være vanskeligt at tilfredsstille alle virksomheder, som ønsker selv at hoste et website.

Ind kommer hosting-løsninger. Apache serveren kan køre med såkaldt virtuelle hosts, derved kan mange websites deles om én IP-adresse.

Danmark

Vi har været på internettet i mange år, universiteterne først, og så - DKUUG tilbød som den første Internet-forbindelse til erhvervs-kunder i slutningen af 1980'erne. Måske derfor har vi rigeligt med IPv4 adresser herhjemme. TDC har dog set trenden og var med på *IPv6-Launch,* tdc.dk har en IPv6 adresse som kan pinges. TDC regner med, at der - med en forsigtig uddeling og inddragelse af ubrugte adresser - er adresser nok til ca. 10 år, og regner med at overgangen sker langsomt.

TDC er gået i gang med såkaldt 'refarming'. IPv4-adresser, som ikke bliver brugt lægges tilbage i TDC's pulje. På den måde kan man udsætte det tidspunkt, hvor man bliver nødt til at gå et skridt videre.

Det næste skridt vil for mange internetudbydere være såkaldt 'carrier grade NAT', som fungerer ligesom NAT til almindelige netværksroutere, men hvor udbyderen placerer eksempelvis en stor mængde ADSL-kunder bag en særlig NAT-router, så hver ADSL-kunde ikke behøver en unik IPv4-adresser, som er synlig for resten af internettet.

Et af problemerne med den type løsninger er, at gatewayen kan komme i underskud af porte, idet brugere med mange aktive sessions og forbindelser bruger flere portnumre. Men der skal mange kunder til før det bliver et alvorligt problem. Til gengæld er videresendelse af fx. tunnelprotokoller, VPN og lign. ikke altid lige vellykket med carrier grade NAT.

Andre grunde til IPv6

IPv4 address exhaustion er og bliver den væsentligste grund til at gå over til IPv6. Men der er andre grunde:

Bedre *Statusløs Automatisk Adresse Configuration* **(SLAAC),**

mindre belastning af routere,

bedre multicast og streaming,

bedre håndtering af mobile devices,

bedre fordeling af PI og PA adresser, hvorved man kan mindske størrelsen af router-tabeller, som er meget store på IPv4 backbone,

IPsec - sikkerhed på transport-niveauet.

De vil blive omtalt i senere artikler, her skal kun omtales aflastning af routere.

Mindre belastning af routere

IPv6 headeren er mindre kompliceret end IPv4 headeren, selv om adressefelterne er 4 gange så store. Sjældent anvendte felter er flyttet til optional extensions delen af headeren.

IPv6 routere skal ikke foretage fragmentering.Det kræves at en maskine på nettet spørger om Max. Transmit Unit, *path MTU discovery*. En host skal selv fragmentere applikationernes pakker hvis de er større end ruten tillader. I stedet for *path MTU discovery* kan systemet vælge at sende pakker, der er maximum 1280 byte, hvilket er minimum for IPv6 routere.

IPv6 headeren er ikke checksum-beskyttet, integriteten skal sikres af både link-layer (netkort-lag, typisk Ethernet) og de højere lag (TCP, UDP). Derfor behøver routere ikke at beregne ny checksum, når header felter ændres, fx. *Hop-tal (Hop-Limit).* De store rutere brugere dedikeret hardware til at genberegne checksummer, men for software-rutere kan det være af betydning.

Hop-Limit erstatter *TTL, Time to Live.* Routere skal ikke længere holde styr på ventetid, queue-time, hvilket afspejles i at TTL er omdøbt til *Hop Limit.* I praksis var der ikke mange routere, som holdt styr på pakkers levetid, så det er i realiteten ikke en ændring.

Det vigtigste er imidlertid formindskelse af router-tabller. IPv6 har et enormt antal adresser, men det var ikke designernes hensigt at hver kvadratcentimeter skulle have sin egen adresse, derimod muliggøres allokering i et hierarki af det store antal adresser, og det muliggør aggregering af ruter, d.v.s. at routere kan se på de første få bits og ud fra dem afgøre, hvor pakken skal sendes hen. Med den aktuelle IPv6 adresse specifikation, vil vi kun se 8192 ruter i Default Free Zone (DFZ), den del af Internet Backbone, hvor routere vedligeholder fuld routing tables; lokale routere har kun explicitte ruter for de nærmeste netværk og en default rute for alt andet.

IPv6 skal - og kan - være nem for slutbrugerne

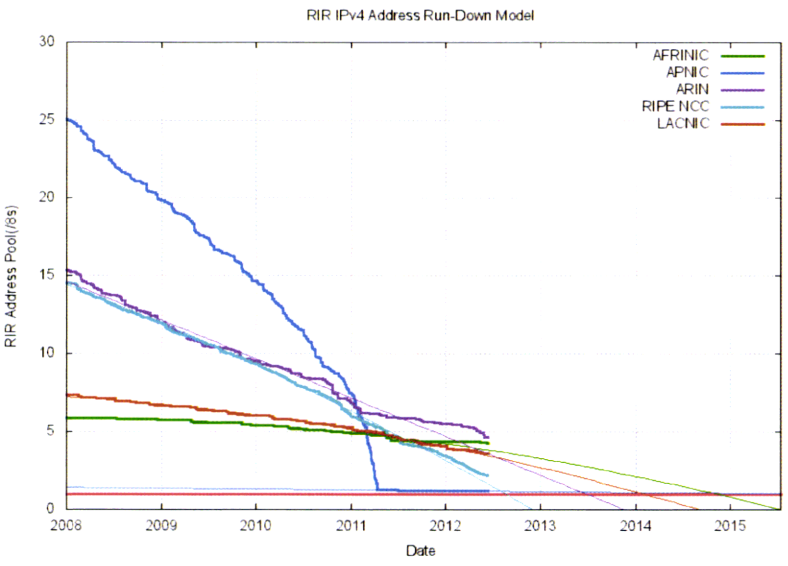
En maskine, som går på IPv6 nettet, behøver ikke at vide ret meget om sin IP-adresse, den kan opfatte sin adresse som 128 bit uden struktur. Kompleksiteten i bruger-devices bliver ikke forøget ved anvendelse af IPv6; en bruger behøver ikke at vide noget om nettets transport.

Men viden om IPv6 er tilgængelig for alle, der vil vide mere, og det er en spændende proces, der er igang, opbygning af et verdensomspændende netværk, som skal fungere så effektivt og så hurtigt som overhovedet muligt.

Vi sidder midt i en udvikling af en ny teknologi, og det er svært at vurdere hvad der er nødvendigt. Der er nogle usikkerheder omkring IPv6, bl.a. har det været fremhævet, at der ikke var router-hardware, som kunne opfylde kravene til fx. mobile-devices. I næste artikel skal vi se på *multicast* som et eksempel på en del af IPv6, der er på forkant, men som også rummer problemer, hvor løsningerne er udefinerede.

Der er med andre ord hist og her tvivl om, hvorvidt IPv6 nu er så god og færdig, som den gerne skulle være. Den utrolige expansion af det nuværende Internet fra 1980 til nu - 32 år, fra et par hundrede til et par milliarder brugere, har medført en tilbageholdenhed, et ønske om at fortsætte med IPv4: If it works, don't fix it. Men der er ingen, som kan argumentere imod at IPv4 adresse-rummet er for lille.

Ved at fastholde IPv6 som den nye normale netværksprotokol, gør de virksomheder, som deltog i *World-IPv6-Launch* det muligt for millioner af slutbrugere at nyde fordelene ved Internettet.



Regionale Internet Registries har fået de sidste /8 grupper fra IANA; skemaet viser prognosen for, hvornår de forskellige regioner løber tør for IPv4 adresser

Privilegeret kommando begrænsning – SSH vs. sudo

Af Jon Bendtsen jon.bendtsen@jonix.dk

Af sikkerhedsgrunde er det smart kun at have så få privilegier som absolut nødvendigt - så er der mindre som kan gå galt. Derfor kører de fleste daemoner ikke længere som *root*, og mange af dem også med chroot.

Men nogle gange har man behov for at køre en specifik kommando med en anden brugers privilegier, ofte *roots*. Det kan fx være Nagios som skal overvåge noget som kræver root-adgang. Eller Apache som skal bruge mod_authnz_external og checkpassword-pam (se side 10 i DKUUG-Nyt nummer 163). I denne artikel vil vi tage udgangspunkt i at Nagios regelmæssigt uden menneskelig interaktion skal køre kommandoen check_md_raid som *root*.

På localhost kan man sætte programmet *setuid* eller bruge *sudo*. SSH kan både starte programmet på localhost og via netværket. Man kan med fordel bruge kombinationen af sudo og SSH, så SSH-login ikke behøver at have root-adgang og det dermed er bedre sikret. Alternativt kan man bruge Nagios NRPE (se s.11), men SSH+sudo er en **generel** teknik og kan bruges til meget andet.

Denne artikel vil kort gennemgå sudo, SSH og kombinationen af de to. Alternativet NRPE nævnes sidst i artiklen.

Sudo

Sudo er den gamle løsning, opfundet ca. 1980, og den fungerer godt. Sudo kan både bruges til interaktivt og scriptet. Sudo er et specielt program, fordi det er setuid[1], læser en konfigurations fil, og ud fra den kan give den kaldende bruger privilegier som en anden bruger. Ofte er den anden bruger root.

Sudos konfigurationsfil ligger i /etc/sudoers , og med den kan man en hel masse, læs evt. man siden, sudo(8) som du finder i *Læs mere boksen* til sidst. /etc/sudoers består af linier som enten er alias definitioner eller specifikationer af hvem der må køre hvilke programmer som hvilke brugere. Specifikationerne kan bruge nogle af de tidligere alias definitioner så man ikke kan have mange similære linier.

I vores eksempel er det dog nok med en enkelt linie, som tillader at brugeren *nagios* kører check_md_raid som brugeren *root*, og dette uden at *nagios* brugeren skal angive sit password, for Nagios-systemet skal jo køre automatisk uden interaktion. Der findes en -S option som tillader at *sudo* læser password fra stdin - derved ville det kunne scriptes, men det vil klart være en sikkerhedsrisiko at lade nagios brugeren opbevare sit eget password i klar tekst. Uden klartekst kan scriptet jo ikke sende sit password til *sudo*.

Den linie, vi tilføjer til /etc/sudoers (brug kommandoen *visudo)* ser ud som denne linie:

```
nagios mesters = (root) NOPASSWD: /usr/local/sbin/check_md_raid
```

Det betyder, at bruger *nagios* fra system (maskine) *mesters* må udføre kommandoen *check_md_raid* som *root* uden at skulle give password.

Hvis du ikke har en bruger som hedder *nagios* eller et program som hedder */usr/local/sbin/check_md_raid* så vil jeg anbefale at du med dit eget login prøver dig frem med kommandoerne *id* og *touch*, så du får en praktisk erfaring med hvordan sudo virker.

SSH

SSH (Secure SHell) er opfundet i 1995, dog med et andet formål end sudo, nemlig at erstatte rsh, remote shell, som (stadig) kører ukrypterede kommandoer over netværk. Rsh er en smule hurtigere fordi den ikke har krypteringsoverhead og kan med fordel bruges på aflåste parallel-computing systemer.

[1] http://en.wikipedia.org/wiki/Setuid

Men SSH kan også lidt af det samme som sudo kan, nemlig at tillade at køre administrator-kommandoer, og i dette eksempel, hvor vi ønsker at nagios brugeren kan køre en kommando som root, så kan det let lade sig gøre.

SSH bygger på brugen af public-key encryption til både at sikre imod aflytning og replay foruden til at autentikere og autorisere brugerens adgang. Du laver din egen SSH nøgle-par bestående af 1 privat nøgle og 1 offentlig nøgle ved at køre kommandoerne i figur 1.

```
jon@apache:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/jon/.ssh/id_rsa):
Created directory '/home/jon/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/jon/.ssh/id_rsa.
Your public key has been saved in /home/jon/.ssh/id_rsa.pub.
The key fingerprint is:
ec:3a:94:e6:3e:de:2e:2e:bc:5d:b7:bf:6c:bf:77:d0 jon@apache
The key's randomart image is:
+--[ RSA 2048]----+
|                 |
|                 |
|                 |
|      .          |
|     .S     . |
|     +.      . E|
|  . + o .    . |
|   o.=+ . o.   o|
|   .**=o .o+ooo.|
+-----------------+
jon@apache:~$ cd .ssh/
jon@apache:~/.ssh$ cat *.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCsHxmFRuEAVe4
QEo9LJt+l3WlBSssSiTMcojkc7E3SV0cQv4dAcqabMjNH0tHtE
pDiO/kHKQa3pbqrz8BdBCWrqyc/7EeloKtfvlnOLdeWoPFlEcL
4mpNmgrCZyixSNEfoxwXb1AYOgwb39aomOQPHieEyZWsT
4fqhucZBWxi4PeGEHq/ggvVrC49uMPHu1wWhVi2o+/OcLRG
2N0gXvJwUjMnOx/7KEFvX41jiy8dwxpC9lsryfTClZs7pg/2L8kS
cl8YjKM+eUnjQKk+rh/ybSLSlpK24pzv82Tx/8fJZvGRhuRNMrn
qHlyyx/RAhUp4/BcyQZZoNlwWUcqFIHIk3 jon@apache
```

Figur 1. Key oprettelse, generation of key

Da dette nøgle-par er din identifikation, så bør du angive en passphrase når den beder om det. Men en passphrase virker selvfølgelig ikke hvis du skal bruge det automatisk og uden menneskelig interaktion. Derfor kan man heldigvis også undlade at vælge en passphrase til at beskytte den private nøglen. Ulempen er at alle som får fat på denne private nøgle kan udgive sig for at være dig over for en SSH server.

Heldigvis kan du ikke bare sådan få adgang til en vilkårlig anden SSH server med din private nøgle. 2 ting skal være opfyldt.

1. Du skal kende en gyldig bruger konto på den maskine du forsøger at logge ind på.
2. Din offentlige nøgle skal være indsat i filen ~/.ssh/authorized_keys i homediret for den bruger du forsøge at logge ind som på den maskine du forsøger at logge ind på.

Hvis disse 2 krav ikke er opfyldt vil SSH som regel bede dig om et kodeord til dit brugernavn. Man kan dog i SSH serverens konfigurationsfil, /etc/ssh/sshd_config, slå brugen af kodeord til

eller fra PasswordAuthentication [yes|no]. Det anses for mest sikkert at slå det fra fordi det er nemmere at brute force et kodeord end en public key.

Prøv at indsætte din offentlige ssh nøgle i en anden brugers, benny, authorized_keys file så du kan se hvordan det virker, lige som i eksemplet i figur 2. Hver linie er en specifik nøgle + evt. lidt andre oplysninger.

```
benny@apache:~/.ssh# cat ../jon.id_rsa.pub >> authorized_keys
benny@apache:~/.ssh# cat authorized_keys
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCsHxmFRuEAVe4QEo9
LJt+I3WlBSssSiTMcojkc7E3SV0cQv4dAcqabMjNH0tHtEpDiO/kHKQ
a3pbqrz8BdBCWrqyc/7EeloKtfvlnOLdeWoPFIEcL4mpNmgrCZyixSN
EfoxwXb1AYOgwb39aomOQPHieEyZWsT4fqhucZBWxi4PeGEHq/g
gvVrC49uMPHu1wWhVi2o+/OcLRG2N0gXvJwUjMnOx/7KEFvX41jiy
8dwxpC9lsryfTClZs7pg/2L8kScl8YjKM+eUnjQKk+rh/ybSLSIpK24pzv
82Tx/8fJZvGRhuRNMrnqHlyyx/RAhUp4/BcyQZZoNlwWUcqFIHIk3
jon@apache
```

Figur 2. Keyfil indsættes i authorized_keys filen

Du burde nu fra din normale brugerkonto kunne logge ind som benny via denne kommando: ssh benny@localhost. Ulempen er selvfølgelig at du nu kan køre en vilkårlig kommando som benny. Men det løser vi ved at specificere den eneste kommando som er tilladt at køre når der forbindes med den nøgle. Dette gøres ved at indsætte command="$command_allowed_to_execute", se figur 3. Kommandoen ***id*** tillades i eksemplet:

```
command="id" ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCsHxmFRuEAVe4
QEo9LJt+I3WlBSssSiTMcojkc7E3SV0cQv4dAcqabMjNH0tHtE
pDiO/kHKQa3pbqrz8BdBCWrqyc/7EeloKtfvlnOLdeWoPFIEcL4
mpNmgrCZyixSNEfoxwXb1AYOgwb39aomOQPHieEyZWsT4f
qhucZBWxi4PeGEHq/ggvVrC49uMPHu1wWhVi2o+/OcLRG2N
0gXvJwUjMnOx/7KEFvX41jiy8dwxpC9lsryfTClZs7pg/2L8kScl8
YjKM+eUnjQKk+rh/ybSLSIpK24pzv82Tx/8fJZvGRhuRNMrnqHl
yyx/RAhUp4/BcyQZZoNlwWUcqFIHIk3 jon@apache
```

Figur 3. En enkelt kommando tillades

Når du nu prøver at logge ind, så vil du se teksten fra figur 4, uanset hvilken kommando du prøver at bede SSH om at udføre.

Naturligvis kan hvem som helst, der får fat på din private nøgle, logge ind og køre den kommando, med mindre din private nøgle er beskyttet af et kodeord, derfor bør du beskytte nøglen så ingen får fat på den, og det bør ikke være en potentielt farlig kommando der udføres. Så længe du tilgår din egen localhost er sikkerheden præcis lige som sudo. Hvis du har behov for at forbinde dig hen over netværket, så kan du i SSH serverens konfigurationsfil og i authorized_keys specificere yderligere restrictioner på hvem, hvordan og hvorfra der må logges ind. Se *man* siderne for SSH.

SSH ind som root

Hvis SSH serverens konfigurationsfil tillader root login, så kan man også SSH'e ind som root, men det er en dårlig ide at tillade direkte root login fra generelt alle IP adresser. Ofte kan en kombination af SSH og sudo klare det.

Hvis man absolut skal logge ind som root, så kan man begrænse det i konfigurationsfilen ved specifikt tillade root login fra en (eller flere) bestemte adresser:

```
# Allow ak and ve to login in as root on each other
Match address 10.239.23.0/24
        PermitRootLogin without-password
```

Konfigurationsfilen er normalt som **/etc/ssh/sshd_config** og den kan editeres med en hvilken som helst tekst editor.

Når man har rettet i **sshd_config** skal man genstarte eller give sshd et signal:

pkill -HUP sshd

```
jon@apache# ps -fC sshd
UID   PID  PPID  C STIME TTY  TIME     CMD
root  978     1  0 May16 ?    00:00:06 /sbin/sshd -D
root 2345   978  0 May16 ?    00:02:33 sshd: root@pts/4
jon@apache# kill -HUP 978
```

Skal du køre flere kommandoer?

SSH authorized_keys filen tillader kun 1 kommando pr. nøgle, så hvis du vil kunne udføre flere kommandoer har du behov for flere nøgler. Det er dog ikke noget problem, bare kør ssh-keygen det nødvendige antal gange og brug **ssh -i id_file**. Se figur 5 på næste side.

I figur 5b kan du se et eksempel på brug af **ssh -i id_file**. Forud for figur 5b er roots authorized_keys blevet ændret med SSH nøglen vi genererede i figur 5 og ***command="echo $PATH"*** (eller den kommando, man vil prøve) står forrest på key-linien.

```
jon@apache:~/.ssh$ ssh -i echo-id_rsa root@localhost
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/bin/X11
Connection to localhost closed.
jon@apache:~/.ssh$ ssh root@localhost
uid=0(root) gid=0(root) grupper=0(root)
Connection to localhost closed.
```

Figur 5b. Afprøvning af ny nøgle til echo-kommando

Figur 6 i bunden af næste side viser indholdet af ovenstående authorized_keys fil. Først med RSA nøglen fra figur 3, bemærk at linien er meget lang og derfor ombrudt som fx. vi-editoren gør det, og derefter ses (på næste linie) RSA nøglen fra figur 5.

SSH og sudo Kombineret

Af sikkerhedsgrunde vil man ofte blokere for SSH root login i SSH serverens konfigurationsfil, derfor bliver man ofte nødt til at kombinere SSH og sudo hvis man ønsker automatisk at udføre en specifik kommando som root på en anden computer uden menneskelig interaktion. Dette kræver lige som ovenstående eksempler at man har en konto som tillader login med SSH nøgler, og at denne konto kan få lov til at udføre en kommando som root uden at angive password. Dette kræver en tilføjelse i både /etc/sudoers og i ~/.ssh/authorized_keys. Jeg foreslår du laver en speciel brugerkonto til dette login, i mit eksempel hedder den nagios. Du indsætter den enkelte linie fra den gule box lige under i din sudoers fil med visudo.

```
jon@apache:~/.ssh$ ssh benny@localhost
uid=1000(benny) gid=1000(benny) grupper=1000(benny)
Connection to localhost closed.
jon@apache:~/.ssh$ ssh benny@localhost bash
uid=1000(benny) gid=1000(benny) grupper=1000(benny)
Connection to localhost closed.
jon@apache:~/.ssh$ ssh benny@localhost echo hej
uid=1000(benny) gid=1000(benny) grupper=1000(benny)
Connection to localhost closed.
```

Figur 4. Kun en enkelt kommando udføres - trods kommandolinie som anmoder om shell eller andet

```
jon@apache:~/.ssh$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/jon/.ssh/id_rsa): echo-id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in echo-id_rsa.
Your public key has been saved in echo-id_rsa.pub.
The key fingerprint is:
44:fd:e0:91:d2:fc:f2:12:1e:63:0a:ea:49:f3:5f:68 jon@apache
The key's randomart image is:
+--[ RSA 2048]----+
|       .+ .      |
|      .. B       |
|       .o =      |
|     .. B o      |
|    . .S+ *      |
|   +   ..o .     |
|  o +  E ..      |
|   o .. .        |
|      ..         |
+-----------------+
jon@apache:~/.ssh$ ls -loa
totalt 28
drwx------ 2 jon 4096 27 nov 19:39 .
drwxr-xr-x 3 jon 4096 27 nov 13:46 ..
-rw------- 1 jon 1675 27 nov 19:39 echo-id_rsa
-rw-r--r-- 1 jon  392 27 nov 19:39 echo-id_rsa.pub
-rw------- 1 jon 1675 27 nov 13:46 id_rsa
-rw-r--r-- 1 jon  392 27 nov 13:46 id_rsa.pub
-rw-r--r-- 1 jon  442 27 nov 14:08 known_hosts
jon@apache:~/.ssh$ cat echo-id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQChCdR3wt-
UoKZhWXiBkDIz75QvD4XR2pHq3/76RUUi36+oxWnJV9ZYbwGMm0K6iNQiEBf4KMqRIZvH0OL9Cpasy6K9hUV0TDqeyftuBdJiY
D7MVBkDXGdEAjJNRjnn63tR/oBaQORxPC8o9ia0nqelvEyJcpd3YNDbZFnFD0uc7ozXwnTIjbuQojKcel0T/9AjxkdiQ3/mILzMgNW
VRmqv4H5LdNpppru0hlDH3RO6okNk2XHncPC90Z+7Dh3jDPBl/J0QMWryJgpm2jjqzEwz6aLKlFplFqhIT0aeqLcYJgPzwQqkDlLk
hCn0QMgqZiqT89v9RoBthVDjlKf2t7AUN jon@apache
```

Fig 5. Generering af ny nøgle til echo-kommando, der er endnu ikke indsat kommando-specifikation

Derefter tilføjer du en SSH nøgle på samme måde som før, i nagios brugerens homedir/.ssh/authorized_keys, og specificerer den kommando, nemlig sudo, der skal udføres som i eksemplet i figur 7 på næste side.

Opsummering

Med disse teknikker er du nu klar til at lave dine egne ændringer i konfigurationen af sudo og SSH, således at du kan udføre overvågningskommandoer (og andre kommandoer) automatisk via scripts.

SSH man-page

Manual siden for ssh klienten er spækket med oplysninger; der er to ssh-protokoller,men den første er forældet. *Beskrivelsen (Description)* lyder: ssh (SSH client) er et program til at logge ind på en remote maskine. Dets formål er at erstatte rlogin og remote-shell, rsh, og at give en sikker krypteret kommunikation mellem to systemer, som ikke kan anses for sikre (fare for aflytning) henover et usikkert netværk. X11 (grafik) forbindelser og arbitrære TCP porte kan også forwardes over den sikre krypterede tunnel.

ssh forbinder sig og logger ind på det specificerede host-navn (valgfrit med bruger-login angivet). Brugeren må bevise sin identitet på en af flere måder, afhængig af protokol-versionen. Hvis en kommando angives, udføres denne i stedet for en login shell.

```
root@apache:~/.ssh# cat authorized_keys
command="id" ssh-rsa AAAAB3NzaC1yc2EAAAADAQAB-
AAABAQCsHxmFRuEAVe4QEo9LJt+I3WlBSssSiTMcojkc7E3SV0cQv4dAcqabMjNH0tHtEpDiO/kHKQa3pbqrz8BdBCWrqyc/7Eel
oKtfvlnOLdeWoPFIEcL4mpNmgrCZyixSNEfoxwXb1AYOgwb39aomOQPHieEyZWsT4fqhucZBWxi4PeGEHq/ggvVrC49uMPHu1w
WhVi2o+/OcLRG2N0gXvJwUjMnOx/7KEFvX41jiy8dwxpC9lsryfTClZs7pg/2L8kScl8YjKM+eUnjQKk+rh/ybSLSIpK24pzv82Tx/8fJZv
GRhuRNMrnqHlyyx/RAhUp4/BcyQZZoNlwWUcqFIHIk3 jon@apache
command="echo $PATH" ssh-rsa AAAAB3NzaC1yc2EAAA-
ADAQABAAABAQChCdR3wtUoKZhWXiBkDIz75QvD4XR2pHq3/76RUUi36+oxWnJV9ZYbwGMm0K6iNQiEBf4KMqRIZvH0OL9C
pasy6K9hUV0TDqeyftuBdJiYD7MVBkDXGdEAjJNRjnn63tR/oBaQORxPC8o9ia0nqelvEyJcpd3YNDbZFnFD0uc7ozXwnTIjbuQojK
cel0T/9AjxkdiQ3/mILzMgNWVRmqv4H5LdNpppru0hlDH3RO6okNk2XHncPC90Z+7Dh3jDPBl/J0QMWryJgpm2jjqzEwz6aLKlFplF
qhIT0aeqLcYJgPzwQqkDlLkhCn0QMgqZiqT89v9RoBthVDjlKf2t7AUN jon@apache
```

Figur 6. Indholdet af authorized_keys efter tilføjelse af nydannet ssh-key med kommando-specifikation forrest, command="echo $PATH" - det er altid nødvendigt med citationstegn

```
command="/usr/bin/sudo /usr/local/sbin/check_md_raid" ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAs9wQ89ph9ThiDW4KQyGsLOoq1Ce2DUDRVwyONAzzC+DeDASisjzfdv1hme4E+N/cdi+j
aL45qPfslSdrmBMBYudjUcBH2e1QAW/bNJ5hGJQJU1yXPo/t7xnk+F+0nPI0QT0VRAA/B7iMJpDNChpncfwars7EJKz2oUJPG3fn
BZraZN5YzBR3UCZluX2NE8I9F4Pe1nVuZkkSyhHo4bor6d6jA9Xk0UJMJLX0xwdLkfpj4W5FR7Kv2Md+gDSNRTeHN8UKYAROf
HGQpo1jPfS8fHGtrlJhg0B20MWyy7tWnMzqHwh/XenxY/T7hS3pQUa/QI9RUloQjeREWd+qPKFvxQ== nagios@apache
```

Fig 7. En ssh-keyfil med kommando begrænset til sudo etc.

Nagios

Nagios er et kendt overvågningssystem der kan indsamle, opdage, alarmere og reagere på uforventede unormaliteter før disse bliver til drift forstyrelser. Desuden kan Nagios også genere forskellige rapporter.

Nagios er Open Source, og blev frigivet i 1999. Siden dengang har der været et aktivt miljø omkring Nagios der har udviklet plugins til stort set alle services, netværk og servere. Og skulle du mangle noget så er det let at skrive dine egne udvidelser.

Nagios kan være omstændelig at komme i gang med, og derfor har vi i DKUUG også et ønske om et introduktionsforedrag og/eller artikel. Kontakt arr@dkuug.dk for et foredrag, og blad@dkuug.dk hvis du vil skrive en artikel.

Læs mere:

- http://www.sudo.ws/sudo/man.html
- http://www.eng.cam.ac.uk/help/jpmg/ssh/authorized_keys_howto.html
- http://www.nagios.org/
- http://nagios.sourceforge.net/docs/3_0/addons.html

NRPE

I stedet for at bruge SSH og sudo til at løse overvågnings problemet der blev brugt som et eksempel i denne artikel, så kunne man have brugt NRPE.

Nagios Remote Program Execution, NRPE er et Nagios system til sikker afvikling af et program fra en monitoreriende maskine (Nagios-master) på klienter der skal overvåges. NRPE har sine egne konfigurationsfiler. NRPE er et plugin til Nagios systemet og kan hentes på exchange.nagios.org - NRPE kan bruges uafhængigt af Nagios.

NCSA

Endnu et "rigtigt" Nagios alternativ kunne være NCSA, der står for Nagios Service Check Acceptor.

NSCA er en passivt lyttende daemon der afventer at modtage rapporteringen fra et program installeret på det system der skal overvåges.

En af fordelene ved denne passivitet er fx hvis der er en firewall imellem det system der skal overvåges og så Nagios server(ne).

NSCA er også et plugin til Nagios systemet og kan også hentes på exchange.nagios.org.

Om Jon Bendtsen – artiklens forfatter:

Jon har brugt Linux siden midten af 90'erne og har arbejdet professionelt med IT fra nogle år senere. Jon er sidenhen blevet kandidat i datalog fra DIKU.

Jon arbejder pt. som freelance IT konsulent der kan hyres til stort og småt.

I fritiden er Jon kasserer i både DKUUG og Open Source Days. Desuden er han aktiv med at arrangere foredrag og konferencer. Endelig er han også ofte i gang med at skrive artikler til DKUUG-nyt, fx denne artikel som er blevet til fordi Jon ønskede at udbrede kendskabet til dette emne. En sjælden gang imellem afholder Jon også foredrag om forskellige Open Source værktøjer.

Extra SSH sikkerhed

Det er muligt, og en god ide, at lave yderligere restriktioner på ovenstående SSH command i authorized_keys filen så chancen for misbrug af SSH forbindelsen sænkes. Dette kan bla. gøres ved at indsætte yderligere konfigurationsoplysninger imellem " og ssh-rsa direkte efter ".

I eksemplet forneden har vi indsat 4 extra restriktioner i forhold til figur 7.

1. Forbindelsen skal ske fra en maskine med ip adressen 10.20.30.40
2. Vi tillader ingen user rc files bliver læst
3. ingen port forwarding
4. ingen X11 forwarding

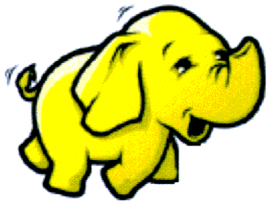
```
command="/usr/bin/sudo /usr/local/sbin/check_md_raid",from="10.20.30.40",no-user-rc,no-port-forwarding,no-X11-forwarding ssh-
rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAs9wQ89ph9ThiDW4KQyGsLOoq1Ce2DUDRVwyONAzzC+DeDASisjzfdv1hme4E+N/cdi+j
aL45qPfslSdrmBMBYudjUcBH2e1QAW/bNJ5hGJQJU1yXPo/t7xnk+F+0nPI0QT0VRAA/B7iMJpDNChpncfwars7EJKz2oUJPG3fn
BZraZN5YzBR3UCZluX2NE8I9F4Pe1nVuZkkSyhHo4bor6d6jA9Xk0UJMJLX0xwdLkfpj4W5FR7Kv2Md+gDSNRTeHN8UKYAROf
HGQpo1jPfS8fHGtrlJhg0B20MWyy7tWnMzqHwh/XenxY/T7hS3pQUa/QI9RUloQjeREWd+qPKFvxQ== nagios@apache
```

Fig 8. ssh-keyfilen fra Figur 7 med extra sikkerhed.

Apache Hadoop

Et Open Source framework til data-intensiv distribueret computing

Hadoop er udviklet af Doug Cutting, og navnet stammer fra hans søns tøjelefant! Sådan.



Når man hører at projektet oprindeligt var udviklet til et søgemaskine-projekt og at det er afledt af MapReduce og Google File System (GFS) så forstår man måske bedre, at vi her på redaktionen blev glade for at Kenneth Geisshirt vil fortælle om de ting efter sommerferien (21. august i Symbion, kl.18-21).

Hadoop (udtales hadup) består af Hadoop Common, (den almindelige del, grundlæggende del) og Hadoop Distribueret Fil System (HDFS) og MapReduce, et framework for fordeling af jobs m.v.

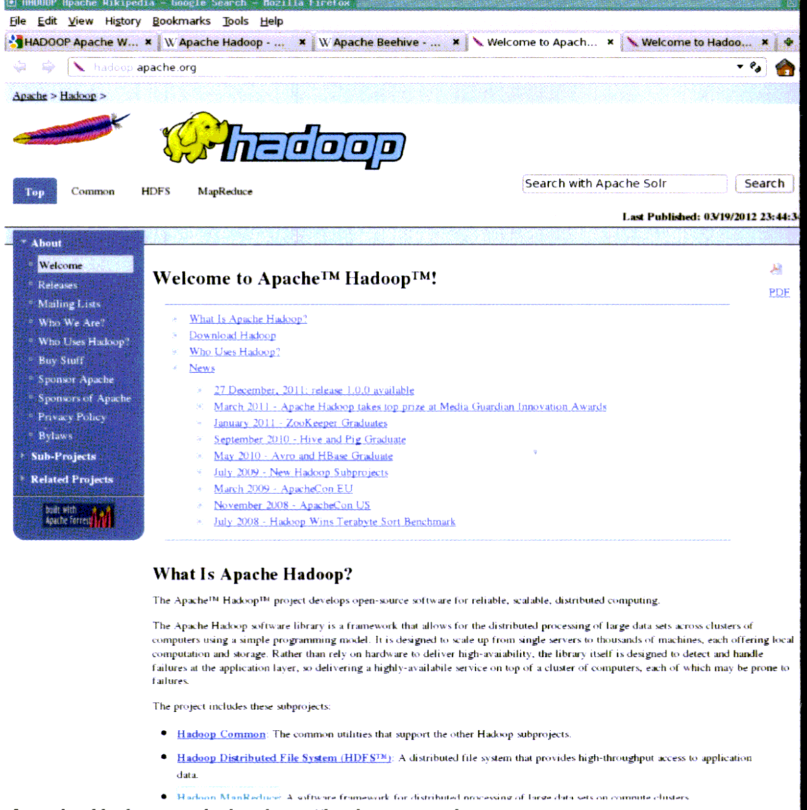
Når man hører, at filsystemer, som skal deltage i Hadoop skal levere information over hvor de befinder sig - eller rettere hvilken netværksswitch/router/site, maskinen hører under, og samtidig lige kommer i tanke om at det oprindeligt kommer fra Google og søgemaskineprojekt, så kan man begynde at danne sig en ide om, hvad opgaven er, og hvilke metoder Hadoop kontstruktionen benytter sig af for at få effektiv udnyttelse af et distribueret system.

I et lille system vil der være en enkelt master og mange arbejds-maskiner, noder (knudepunkter). Master-systemet består af en job-administration, opgave-administration, navne-node og data-node. Job-administrationen er proces-administration. I en opgave kan indgå flere job.

Navne-noden holder styr på filers navne (og hvor de er, hvor langt væk, hvor hurtigt man kan få fat på dem og den slags) og i større installationer holder en sekundær navne-node øje med den primære og kan tage et dump af den primære navne-nodes hukommelses-struktur, så man ikke får korrumperet data-filnavne og minimerer tab af data. Hver arbejdsmaskine har typisk en enkelt data-node, og alle datanoderne udgør tilsammen et HDFS, et filsystem spredt over flere enheder.

Man kan anvende Hadoop core imod alternative filsystemer, i så fald erstattes navne-node og sekundær navne-node af de filsystem-specifikke tilsvarende elementer.

JobTracker og *TaskTracker* er ideen bag Map/Reduce: Klient applikationer (distributed computing/parallel computing jobs) sender *MapReduce* anmodninger til JobTracker'en. Denne skubber opgaven ud til de ledige *TaskTrackere* i clusteret. Med et filsystem, der forstår rack-positioner, kan TaskTrackeren se hvilken node (maskine/gruppe af CPU'er) der har data og hvilke beregnings-noder der ligger tæt på.



Apache Hadoop website, http://hadoop.apache.org

Hadoop er et Apache top-level projekt. Apache Software Foundation (ASF) er et community af programmører og brugere. ASF støtter Open Source software projekter, som er til gavn for almenheden. ASF udgøres af over 100 top-level projekter, og Hadoop er et af disse; Apache webserveren er et andet og nok det mest kendte.

Hadoop er skrevet i programmeringssproget Java. Yahoo har været den største bidragsyder til projektet, og bruger Hadoop i hele virksomheden.

Alternative parallel-computing systemet

OpenMP og MPI, Message Passing Interface, er alternativer, der har været brugt igennem mange år, ideerne begyndte at tage form for 20 år siden. MPI er sprog-uafhængigt og er blevet en de-facto standard, som findes i flere implementeringer. De største computer-clusters kører OpenMPI.

En af forskellene mellem Hadoop og OpenMPI er, at Hadoop er fejltolerant. I en mail-liste (stackoverflow.com, why-isnt-hadoop-implemented-using-mpi og open-mpi.org/faq) opdager jeg, at udviklerne bag OpenMPI overvejer at implementere fault-tolerance i OpenMPI, bl.a. data reliability and network fault tolerance, noget, der også findes i LA-MPI.

Generelt kan man konkludere, at mens Hadoop er for data-intensive parallel computing opgaver, er MPI og OpenMP m.fl. mere tænkt til CPU intensive opgaver.

Call for patches to the *at job queue system* – proper email subject wanted.

By Jon Bendtsen jon.bendtsen@jonix.dk

During my years as a system-administrator I have repeatedly used the *at job queue system (at)* to restart my scripts at a later time if right now was a bad time. This bad time could be because of high load, network trouble or just that the script from last run was not finished yet.

at is good for starting a "one time" job at a later time, where as the *cron job system (cron)* is good for regularly starting the same job over and over, like the daily backup.

cron is pretty good at sending email reports, also if something goes wrong:

```
From            Subject
Cron Daemon     Cron <root@srv155> /usr/local/sbin/double_restart_for_all_vserver_guests_rsync.sh
root            Cron <root@backup>    /usr/local/sbin/backup/update_latest_backup.sh (failed)
root            Cron <root@vpn1> apt-get -q -q update && apt-get --dry-run upgrade
root            Cron <root@dk2> clamscan -i --exclude-dir="/sys" -r / (failed)
```

but *at* is very bad at sending email reports telling about job type and result, and that means we have to solve that by adding to scripts, over and over again in our scripts:

```
From            Subject
root            Output from your job      3237
root            Output from your job      3216
root            Output from your job      3201
root            Output from your job      3029
root            Output from your job      2987
root            Output from your job      2561
root            Output from your job      1900
```

This output from *at* gives no clue as to which server the email is coming from, which script was executed, when it was executed, or what the result was.

Call for patches

Therefore I would like to send out a call to all those that have yet to submit a patch to any open source project to submit patches to *at* such that it gets better email reporting.

Starting point: http://packages.debian.org/changelogs/pool/main/a/at/at_3.1.12-1+squeeze1/at.copyright

> This package was debianized by its author Thomas Koenig <ig25@rz.uni-karlsruhe.de>, taken over and re-packaged first by Martin Schulze <joey@debian.org> and then by Siggy Brentrup <bsb@winnegan.de>, and then taken over by Ryan Murray <rmurray@debian.org>.
>
> In August 2009 the upstream development and Debian packaging were taken over by Ansgar Burchardt <ansgar@43-1.org> and Cyril Brulebois <kibi@debian.org>.
>
> This may be considered the experimental upstream source, and since there doesn't seem to be any other upstream source, the only upstream source.

So you probably have to submit the patches to the Debian project, but if you send them to your distribution one could hope that it would be spread among the other distributions.

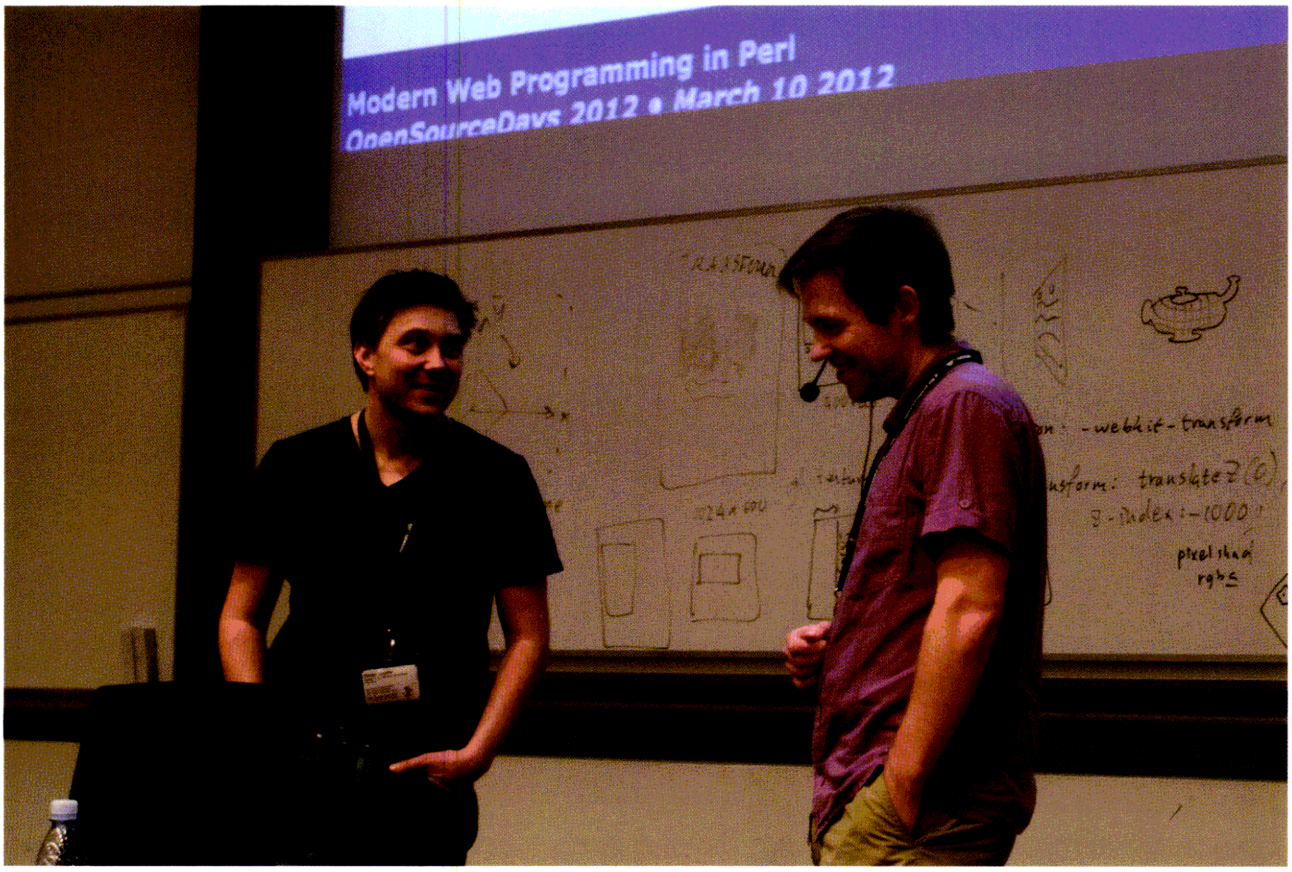
Read more:

http://unixhelp.ed.ac.uk/CGI/man-cgi?at
http://unixhelp.ed.ac.uk/CGI/man-cgi?cron
http://packages.qa.debian.org/a/at.html

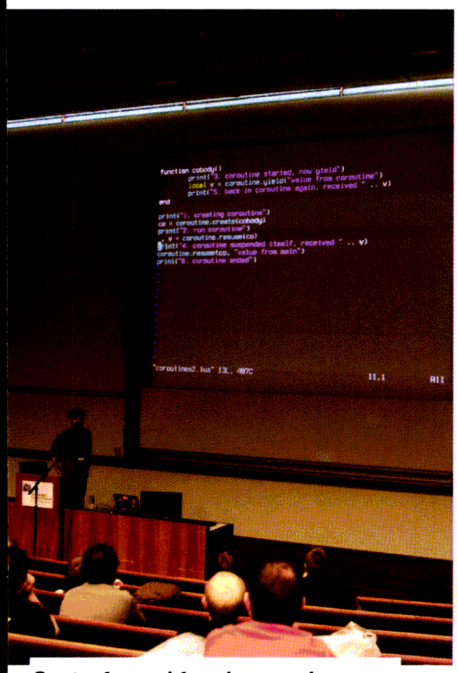
Billeder fra Open Source Days 2012

Tre fotografer viser indtryk fra konferencen i CBS 10 marts.

På Open Source Days (OSD) var der repræsentanter fra kursushuse, fra hosting-services og fra foreninger (foto: Kristian Vilmann)



Kenneth Geisshirt og Peter Makholm foran den magiske lampe (tegnet på tavlen)(foto: Andreas Plesner Jacobsen)

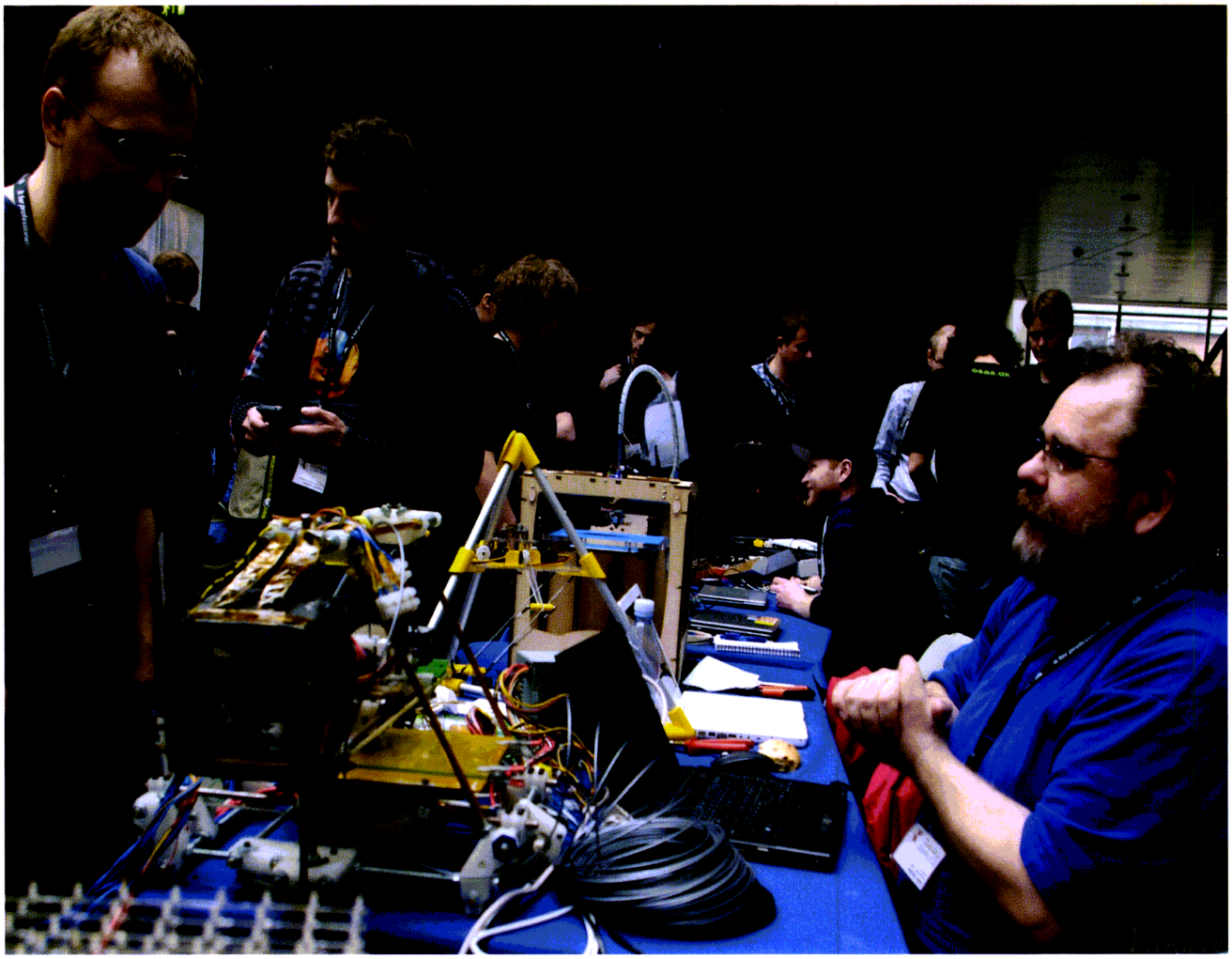


Syntaxfarver i foredrag om Lua
(foto: Morten Siebuhr)

Korridor-konference
(foto: Morten Siebuhr)

(foto: Morten Siebuhr)

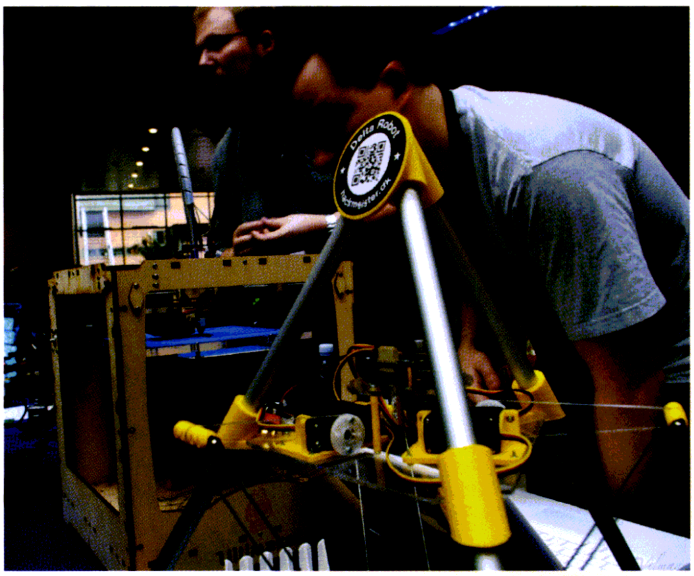
(foto: Kristian Vilmann)



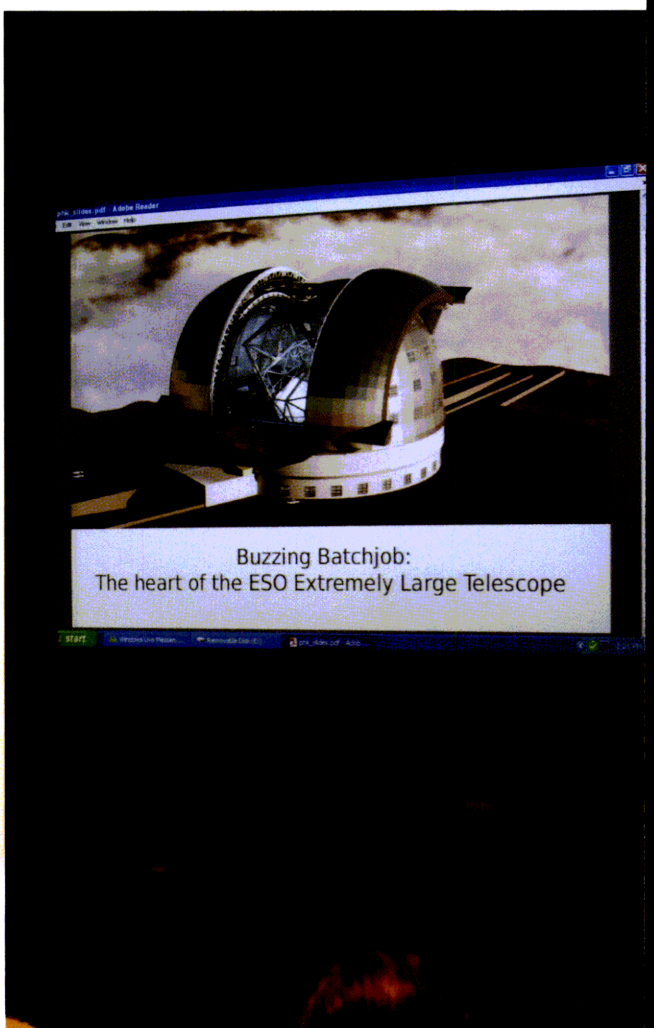
Hackmeister!

Hardware er ikke så mystisk, når man først får fat i den og bøjer den til egne formål.

En ny R2D2 i støbeskeen (foto: Kristian Vilmann)



ESO observatoriet styres af Linux-systemer og er egentlig heller ikke så mystisk, men bare kæmpestort. (Foto: Morten Siebuhr)



Linux Professional Institute Certification

Kompetence-pleje bliver vigtigere

Certificering kan være med til at overbevise en arbejdsgiver om, at man kan sit stof. Indenfor især systemadministration er det vanskeligt for en arbejdsgiver - selv på professionelle, store virksomheder - at bedømme om opgaverne bliver udført effektivt, om vidensniveauet er højt nok til at medarbejderne finder de bedste løsninger.

Der er meget markedsføring af videnstunge produkter forbundet med kurser - det gælder indenfor alle områder, både vores IT-område og andre fag med videnstunge opgaver, special-udstyr som scannere og laserapparatur i sundhedssektoren, flytyper med tilhørende pilotuddannelse til luftfartssektoren, og meget andet.

LPI er et tilbud om certificering indenfor Unix/Linux uden skelen til hvilken distribution, der bruges.Et af de problemer, som har gjort Linux svag i markedssammenhæng er, at der simpelthen er for mange distributioner. I praksis skelnes mellem RedHat eller RPM baserede distributioner og Debian baserede.

Nu er der sikkert mange, der tænker "hvad med Suse" eller Slackware, eller Gentoo, eller ... men pointen her er, at man gør sig selv og arbejdet en tjeneste ved at anse de andre som specialiserede varianter. Jovist, der er nok nogle distributioner, som har forsøgt at gøre livet lettere for folk ved at lave deres egen "peg-og-klik"-løsning, (fx. den Ubuntu-baserede Mint-Linux) men grundlæggende set er det en Debian; og ser man det i den vinkel, er det lettere at huske undtagelser og afvigelser. Man burde lige nævne Linux Standard Base (LSB) som Debian og RedHat tager hensyn til; men det er alligevel ikke nok til at gøre systemerne ensartede. Man kan konvertere en RPM til en Debian pakke med *alien* programmet.Det fungerer fint.

Det er ellers ikke så let at installere noget fra den ene leverandør på et andet system. Man kan selv kompilere en softwarepakke, hvis det virkelig gælder, men det er desværre for vanskeligt for de fleste.

LPI blev grundlagt allerede 1999, med ønsket om at tilbyde en uddannelse, som fungerer på tværs af leverandører og distributioner. Det fungerer fint for folk som er lidt eksamensvante; men det er jo ikke en gratis uddannelse. Microsoft har et program med lettelser for studerende på datalogiske uddannelser, og derfor vil mange studerende, som i forvejen er vante til Microsoft produkter og som er job-bevidste, benytte de muligheder, der byder sig for gratis eller billig certificering indenfor Microsoft produkter. Det gør til syvende og sidst situationen tungere for Linux. Derfor er det måske ekstra meget bemærkelsesværdigt, at Linux på flere forskellige markeder har en pæn andel; i en video fra Linux Foundation (link på DKUUGs webside, eller søg på *How Linux is built* på YouTube og se en pragtfuld video, som viser hvor mange steder Linux bruges; fx. som embedded system i TV-boxe, Android telefoner og routere, og i servere og websites over hele verden.

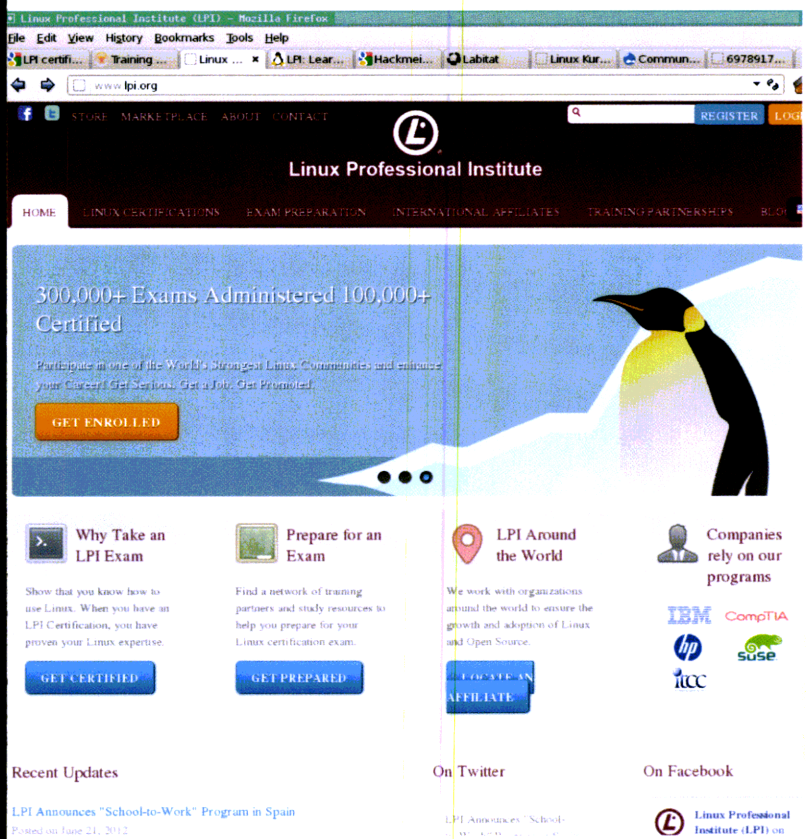
What is LPI ?

LPI (Linux Professionel Institut) is a **non-profit organization** registered in Canada, October, 1999.

Focusing solely on setting certification standards.

Training-vendor independent: encouraging a variety of methods and approaches to test preparation

Distribution-neutral: verifying knowledge on any standard Linux system



LPI.org - Linux Professional Institute har kun det formål at standardisere certificering af Linux-experter

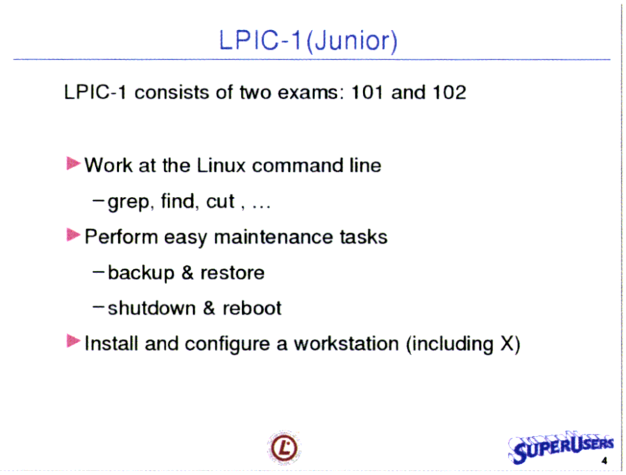
For at imødegå behovet for støtte til unge under uddannelse er LPI igang med at beta-teste et Linux essentials program.

Linux Essentials Heroes Complete Beta Tests

(Sacramento, CA, USA: June 19, 2012) The Linux Professional Institute (LPI), the world's premier Linux certification organization, announced that volunteers from throughout Europe, the Middle East and Africa completed the beta testing of LPI's new Linux Essentials exam--an innovative program measuring foundational knowledge in Linux and Open Source Software. Targeted at new technology users, the Linux Essentials program is set to be adopted by schools, educational authorities, training centers and others commencing in June 2012.

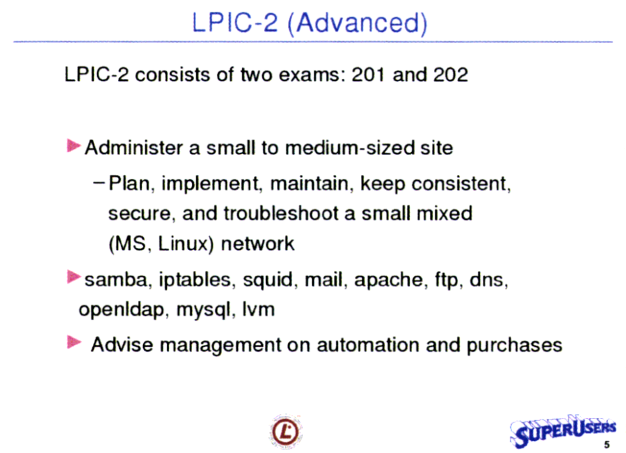
Ved Linux-Tag i Berlin blev det første frie (og gratis) studiemateriale for Linux Essentials præsenteret af Linup Front, som har udviklet kursusmaterialer gennem længere tid. Studiematerialet er en 250 siders e-bog, som kan downloades, både på engelsk og tysk - gratis, frit download. Det er et materiale, som begynder med at forklare login - efter lige at have nævnt de store operativsystemer, Microsoft, OSX, herunder BSD, og Linux, på 10 sider. Efter 244 sider slutter den med grundlæggende netværk og Linux som net-klient og giver eksempler på eksamens-spørgsmål og svar.

Det er som sagt for begyndere. De professionelle Linux certificeringer går lidt hurtigere frem, men har faktisk også grundlæggende emner omkring elementær brug af et Linux-system.



Grundlæggende Linuxviden er en forudsætning

Det næste niveau er langt mere krævende og ender med at certificere, at man kan administrere et blandet miljø af Microsoft, OSX og Linux-systemer, inclusive server-programmer som Apache, Samba og Openldap m.v.

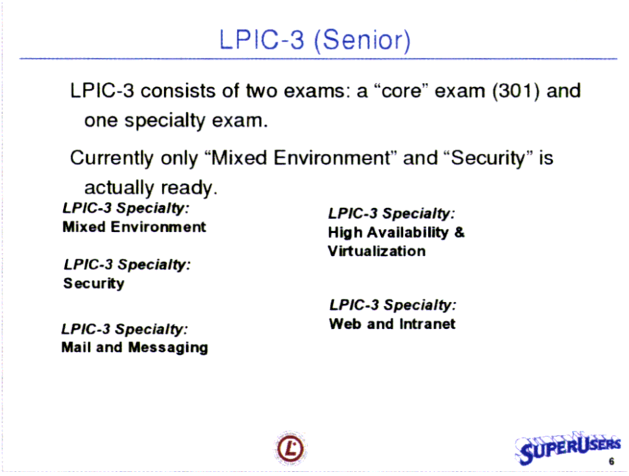


Det omfattende stof her kræver nogle måneders erfaring eller 2 ugers intens bootcamp.

Det forventes imidlertid ikke, at man efter LPIC-2 er dybt inde i stoffet omkring fx. mailsystemer.

LPIC-3

Niveau 3 består af flere kurser og flere separate certificeringer. Derved bliver certificerings-forløbet bragt i overensstemmelse med den virkelige verden, hvor en sysadm ved lidt om alt og meget om et eller flere specielle områder.



Efter en generel core eksamen tages en speciale-eksamen

Rosinen i pølseenden er LPIC-3 specialerne, hvor Mixed Environment (med alle typer lap-toppe, mobile devices og workstations ude blandt brugerne) nok vil være den, der er mest relevant for en supporter i et større firma med en afslappet IT-politik.

I fremtiden vil det være netværks-administratoren, som udgør den væsentligste kompetence i en IT-afdeling, men det er underforstået, at en netværks-specialist skal kende de grundlæggende egenskaber ved brugersystemerne.

Det er et somme tider tungt fuldtidsarbejde.

Eksempler på spørgsmål - og svar

De mere fornuftige spørgsmål er selvfølgelig generiske, som fx. shell syntax for at føre output fra ét program ind som input i et andet program. Svaret er selvfølgelig

```
program1 | program2
```

De efterfølgende spørgsmål er selvfølgelig mere krævende, og man kan med en vis ret hævde at det er omsonst at lære fx. option-bogstavkoder udenad, men de vigtigste forekommer som spørgsmål i LPI. I Speciale-området Mixed environment spørges fx. hvordan, i et Microsoft-brugersystem, NTuser.dat gøres til en mandatory brugerprofil, og svaret er at **man renamer til NTuser.man**

Certificering i Danmark

Man kan få kurser og certificeringer hos bl.a. Firebrand og hos vores sponsor, SuperUsers.

Tak til Martin M.S. Pedersen for brug af slides vedrørende LPI.

Ny direktør i DK-Hostmaster

Velkommen til John Schweitzer

DK-hostmaster står for accept og registrering af domænenavne under .dk domænet - Lande-kode Top Level Domain (engelsk: Country Code Top Level Domain, **ccTLD**).

https://www.dk-hostmaster.dk/

Bestyrelsesformanden var meget tilfreds med at dette valg af formand og skrev bl.a. at *den nye direktion med John Schweitzer og Lise Fuhr er den helt rigtige til fortsat at udvikle DIFO og DK-Hostmaster og sikre, at administrationen af .dk-domænet til stadighed er på det høje niveau, som det danske internetsamfund har krav på.*

Antal registrerede domæner - årsoversigt

Ultimo	Antal registrerede	Total	Tilgang
1997		41.259	n/a
1998		75.488	34.229
1999		141.308	65.820
2000		248.727	107.419
2001		351.792	103.065
2002		395.674	43.882
2003		468.210	72.536
2004		560.896	92.686
2005		651.558	90.662
2006		754.738	103.180
2007		864.845	110.107
2008		965.910	101.065
2009		1.035.480	69.570
2010		1.095.384	59.904
2011		1.156.327	60.943

Ultimo - Tal er opgjort ved slutningen af periode.
Antal registerede - Det totale antal registerede .dk domæner.
Tilgang - Stigning i antal registerede den pågældende periode.

John Schweitzer er 57 år og har gennem det meste af sin karriere varetaget lederjob i IT-branchen, de seneste år som nordisk direktør for forskellige funktioner i CSC.

Besøg på administrations-web hos DK-Hostmaster er pænt stort. Antallet af registrerede domænenavne var pr.16.Juni i år 1.190.340.

I oversigten her ses udviklingen fra 1997. Allerede i begyndelsen af 1990'erne var der mange uddannelsesinstitutioner og en del virksomheder, som havde Internetforbindelse.

Apache OpenOffice

OpenOffice.org er blevet til Apache OpenOffice, AOO - men er ikke top-level projekt endnu (sådan som Hadoop er det).

Projekter i ASF kører først som inkubator projekter. Det er et krav til alle nyligt accepterede projekter indtil et nærmere eftersyn viser, at infrastruktur, kommunikation og beslutningstagning er stabiliseret på en måde, som er konsistent med andre ASF projekter. At køre i en inkubator er en typisk management betegnelse for opstartsfirmaer, og her altså for nystartede projekter eller projekter, som er blevet "herreløse". Open Office, der stammer fra tyske Star Office, blev herreløst da Sun blev købt af Oracle, som lukkede flere Sun projekter. Inkubation er ikke nødvendigvis relateret til programmernes kvalitet og stabilitet, men er blot et tegn på at ASF endnu ikke fuldud støtter projektet.

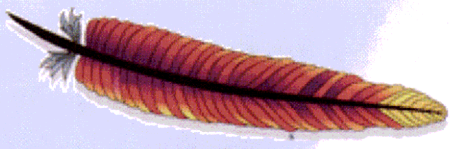
Smid ikke penge væk

Ud over at AOO er nr.13 på Huffington Post's liste over sparetips, er AOO også et Open Source projekt med en lang og interessant historie. Sun overtog et tungt og langsomt Star-Office fra et tysk firma, og bragte det i løbet af kort tid på en form, så det kørte hurtigt og med færre crash. Man skal lige huske at computerne gennem årene også blev hurtigere og fik mere hukommelse, men vi, der er længe om at skifte workstation har konstateret at Sun's erfaring med modulopdeling gav en mirakuløs performance forbedring af Office,som gjorde det til en fornøjelse at bruge programmet.

Den 19. juni i år passerede AOO 5 mio. downloads. 5 mio på 6 uger. Men udviklerne laver andet end at tælle downloads: Man har includeret en del bug-fixes fra IBM Symphony og har desuden arbejdet på at planlægge et længere forløb med merge af features fra Symphony.

AOO et stykke software mange komponenter, og kan det, man skal bruge til daglig. Denne tryksag er hovedsageligt lavet med OpenOffice - endda i en lidt ældre version 3.1

If it works, don't fix it.



SUPERUSERS

Du kan finde mere information her:
www.superusers.dk/linux.htm

Linux Professional Institute

Linux-kurser rettet mod certificeringer fra Linux Professional Institute (LPI)

Nr.	Titel	Dage	Kort beskrivelse
LX-099	Linux Introduktion	1	Hvis man ikke har arbejdet med andre operativsystemer, er dette et godt kursus til at komme i gang med Linux og netværk.
LX-100	Linux Grundkursus	5	En grundlæggende og praktisk orienteret indføring i brug af Linux. Efter kurset kan du bruge Linux og det tilhørende netværk

LPIC-1: Linux Professional Institute level 1 — I alt 2 tests

LPIC-1 er en grundlæggende certificering (Junior Level Administration). Fokus er på arbejde fra kommandolinie, udføre simple administrative opgaver og kunne opsætte og forbinde en arbejdsstation.

LPIC-1 certificering kræver at 2 tests bestås.

Bestå 2 obligatoriske tests:	Kvalificerende kursus eller kursusrække:
117-101: LPI level 1 Exam 101	**LX-101 (4 dg)** Linux Install and Use + evt. **BX-101 (1 dg)** Linux LPIC-1 101 Bootcamp Basic Level Administration
117-102: LPI level 1 Exam 102	**LX-102 (4 dg)** Linux Administration and Networking + evt. **BX-102 (1 dg)** Linux LPIC-1 102 Bootcamp Basic Level Administration

LPIC-2: Linux Professional Institute level 2 — I alt 4 tests

LPIC-2 (Intermediate Level Administration) er en overbygning på LPIC-1. Administration af mellemstore installationer, med fokus på implementering, sikring, fejlsøgning og stabilisering af installationen.

LPIC-2 certificering kræver 4 tests (opnås ved først at blive LPIC-1 og dernæst tage de 2 nedenstående tests).

Bestå 2 obligatoriske tests:	Kvalificerende kursus eller kursusrække:
117-201: LPI level 2 Exam 201	**LX-201 (3 dg)** Linux Administration Advanced + evt. **BX-201 (1 dg)** Linux LPIC-2 201 Bootcamp Advanced Level Administration
117-202: LPI level 2 Exam 202	**LX-202 (3 dg)** Linux Networking Advanced + evt. **BX-202 (1 dg)** Linux LPIC-2 202 Bootcamp Advanced Level Administration

BX (Boot camp) er 1 dag hos SuperUsers med effektiv gennemgang af emnerne i det tilhørende LX kursus. Dagen afsluttes med den specifikke test (undervisning samt test er inkluderet i prisen for BX kurserne)

Karlebogaard: Karlebovej 91 • 3400 Hillerød & **Kampehøjgaard**: Krajbjergvej 3, Vorre • 8541 Skødstrup
Tlf.: 48 28 07 06 • **Mail**: super@superusers.dk • **Web**: www.superusers.dk