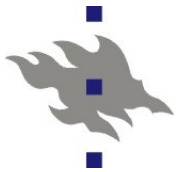
HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Linux-ylläpito: Verkkopalvelut

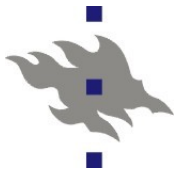
5. kalvosetti

Jani Jaakkola
jjaakkol@cs.helsinki.fi
http://www.cs.helsinki.fi/u/jjaakkol/lyp2010



Sähköposti

- Sähköpostin välitys internetissä on aidosti hankala asia
  - Historiallista painolastia on paljon
  - Näiden luentojen pohjalta ei pidä mennä pystyttämään ISP:n tai edes domainin sähköpostipalvelinta
- Postinvälitysprotokolla SMTP
  - SMTP – Simple Mail Transfer Protol
    - RFC821 vuodelta 1982
    - Tällä protokollalla meilit välitetään edelleen
  - ESMTP – Mekanismi uusien ominaisuuksien neuvotteluun SMTP-yhteydessä
    - RFC1896 vuodelta 1995
    - Mahdollistaa 8-bittiset merkistöt, TLS-yhteyden neuvottelun, yhteyksien autentikoinnin jne..



SMTP-postinvälityksen osapuolet

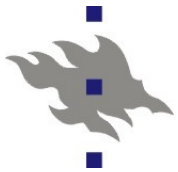
- MUA – Mail User Agent
  - Käyttäjän työpöydällä oleva sähköpostiohjelma
  - Thunderbird, mozilla, evolution, kmail, pine
- MSA – Mail Submission Agent
  - Palvelin, jolle MUA välittää viestin edelleen siirrettäväksi
  - Ei välttämättä käytä SMTP-protokollaa
    - Unixeissa MSA:na toimii */usr/sbin/sendmail* binääri (tai wräpperi)
    - MSA:n ei silti onneksi tarvitse olla sendmail
      - Muut MSA:t emuloivat sendmail:in /usr/sbin/sendmail komentoa (jonkin verran)
- MTA – Mail Transfer Agent
  - Välittää sähköpostit vastaanottajapalvelimelle tai välityspalvelimelle (relay)

SMTP-postinvälityksen osapuolet

- Välityspalvelin (SMTP-relay)
  - SMTP-protokollassa ei oleteta suoraa yhteyttä lähettävän ja varsinaisen vastaanottavan SMTP-palvelimen välillä
  - Välityspalvelimia käytetään:
    - Sähköpostien jonottamiseen varsinaisen palvelimen ollessa alhaalla
    - Kuorman tasoittamiseen
- MDA – Mail Delivery Agent
  - Toimittaa sähköpostit vastaanottajan MUA:n saataville
  - *procmail*
  - POP-protokolla
  - IMAP-protokolla

SMTP:n ominaisuudet

- Historiallisesti tavoitteena mahdollistaa viestinvälitys isojen keskuskoneiden välillä – eikä mitään muuta
  - Alkujaan ei minkäänlaista autentikointia
  - Ihmiset eivät kantaneet viestinvälitykseen pystyviä koneita povitaskuissaan
  - Kaikki SMTP-palvelimet suostuivat toimimaan välityspalvelimina kaikille muille palvelimille
  - Spam ja virukset olivat vielä keksimättä
  - Ei minkäänlaisia identiteettitarkistuksia
- Kirjekuoren käsite (envelope)
  - envelope sender ja envelope recipient
  - SMTP-protokollassa neuvotellaan erikseen vastaanottajan osoite ja osoite johon mahdolliset virheet palautetaan
  - Näillä osoitteilla ja välitetyn meilin sisällössä näkyvillä osoitteilla ei välttämättä ole mitään tekemistä keskenään!



Lisää SMTP:n ominaisuuksia

- Välityspalvelimet
  - Viestin ei tarvitse kulkea suorinta mahdollista reittiä
  - Lähettävän MTA:n ja vastaanottavan MTA:n välissä voi olla mielivaltaisen monta välityspalvelinta
  - Redundanssia ja kuorman tasausta
- Viestijonot
  - MTA:t varautuvat tietoliikennekatkoksiin, kuormitustilanteisiin ja palvelinten kaatuiluun viestijonoilla
- Vaihtoehtoiset vastaanottaja MTA:t
  - Domain voi listata DNS-tietueissaan useita viestejä vastaanottavia palvelimia ja niiden väliset prioriteetit

SMTP autentikointi

- Nykyään kaikki tulevat SMTP-yhteydet joudutaan jotenkin autentikoimaan
  - Ammattimaiset spammerit löytävät nopeasti avoimet välityspalvelimet
  - Siksi MTA:t konfiguroidaan välittämään eteenpäin ainoastaan omasta domainista tulevat viestit
    - mail.cs.helsinki.fi -palvelin suostuu välittämään kaikki cs.helsinki.fi-domainin IP-osoitteista tulevat viestit
    - Vastaavasti ISP:iden meilipalvelimet suostuvat välittämään eteenpäin vain ISP:n omista IP-osoitteista tulevat viestit
    - Ficora on komentanut ISP:t oletusarvoisesti blokkaamaan SMTP:n kokonaan asiakasliittymistä (27.8.2004)
  - Oman domainin ulkopuolelta tuleville viesteille
    - Vaaditaan ennen viestin välitystä SMTP-autentikointi, salasanalla tai muulla menetelmällä (POP-before-SMTP)
    - MSA-portti, jossa vaaditaan aina autentikointi

MTA välinen autentikointi

- Viestit joiden recipient -osoite on MTA:n vastaanottamassa domainissa täytyy perinteisesti päästää läpi ilman autentikointia
  - Ja spam ja virukset leviävät
  - Ratkaisu #1: mustat listat
    - Ei vastaanoteta tunnettujen spämmiä lähettäviä palvelinten viestejä
    - Ei vastaanoteta tunnettujen kuluttajaliittymien IP-osoitteista lähetettyjä meilejä (ts. Vaaditaan jokin ISP:n MTA väliin)
    - ISP:t blokkaavat myös itse kuluttajaliittymien SMTP-liikennettä
  - Ratkaisu #2: jonain kauniina päivänä globaali MTA-palvelinten välinen autentikointi:
    - SPF
    - MS:n Sender-ID

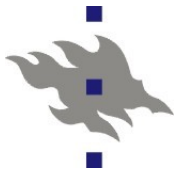
SPF – Sender Policy Framework

- Menetelmä jolla viestin domainista X vastaanottava MTA voi varmistua siitä että viestin lähettävällä MTA:lla on oikeus lähettää viestejä domainista X
  - Domainin X DNS-tietueisiin on lisätty lista domainin X MTA-palvelimista
  - SPF suojaa SMTP:n envelope-sender kentän väärennöksiltä
  - viestin sisäisessä From: -kentässä voi edelleen lukea mitä tahansa
  - SPF voi aiheuttaa ongelmia viestien edelleenlähetykselle
  - Kyseenalaista auttaako spam-ongelmaan lainkaan

```
x40-4:~$ host -t TXT cs.helsinki.fi
cs.helsinki.fi text "v=spf1 ip4:128.214.9.1 ip4:128.214.9.2 ~all"
```

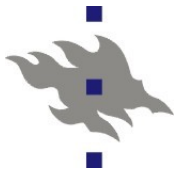
Miksi MSA työasemassa?

- MUA:n voi konfiguroida lähettämään viestit suoraan keskitetylle MTA:lle
  - MSA työasemassa ei ole lainkaan välttämätön
- Työasemassa olevan MSA:n edut
  - Mahdollistaa paikalliset postilaatikot
  - Keskitetty paikka konfiguroida tunnelointi organisaation varsinaiselle MTA:lle
  - Postien paikallinen jonotus verkkokatkosten vuoksi
    - Ei pelkästään hyvä asia: käyttäjät eivät välttämättä huomaa postin jääneen jonoon
  - Mahdollistaa viestien lähetys daemoneilla ja skripteille jotka eivät osaa puhua SMTP:ta



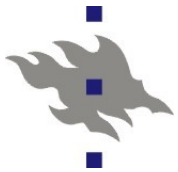
Erilaiset meilikonfiguraatiot

- Kiinteä työasema intranetissä, ei paikallisia postilaatikoita
  - Helppo tapaus
  - Paikallinen MSA yksinkertaisesti toimittaa kaikki viestit eteenpäin domainin MTA:lle
  - Ei kuuntele ulkoista SMTP-porttia lainkaan
- Työasema, jolla on joitain paikallisia postilaatikoita
  - Tyypillinen distron asennuksen jälkeinen oletuskonfiguraatio
  - Daemonien generoimat viestit toimitetaan paikallisiin postilaatikoihin
  - Loput toimitetaan edelleen eteenpäin domainin MTA:lle
  - Ei kuuntele ulkoista SMTP-porttia lainkaan



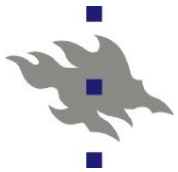
Lisää meilikonfiguraatioita

- Liikkuva työasema vaihtuvalla IP-osoitteella
  - Kannettavat, joiden verkko vaihtuu sen mukaan missä ne kulloinkin sattuvat sijaitsemaan
  - Liikkuvan työaseman MSA:n pitää tällöin
    - Osata vaihtaa käytössä oleva MTA aina IP-osoitteen vaihtuessa
    - Tai autentikoida itsensä jollekin kiinteällä MTA:lle
    - Tai unohtaa paikallinen MSA ja jättää ongelma kokonaan käyttäjälle ja MUA:lle
- Varsinainen keskitetty meilipalvelin
  - Toimii domainin työasemien välityspalvelimena
  - Vastaanottaa domainiin tulevat viestit
  - Sisältää domainin käyttäjien postilaatikot
  - Suodattaa viestejä



Postilaatikot

- Tiedostojärjestelmässä:
  - Perinteinen mbox-formaatti
    - Meilit peräkkäin yhdessä tekstitiedostossa From-riveillä eroteltuna
    - Tehoton, ainakin ilman erillistä indeksointia
  - Maildir-formaatti
    - Meilit yksittäisinä tiedostoina hakemistossa
  - Kumpaakin voi jakaa NFS yli
- Erilaiset tietokannat
- POP-etäpostilaatikko
  - Käyttäjän MUA hakee säännöllisesti serverille saapuneet viestit ja säilöö ne käyttäjän työasemalle
- IMAP
  - Viestit ja arkistot pysyvät palvelimella
  - Postilaatikoita voi olla useita ja ne voivat olla jaettuja

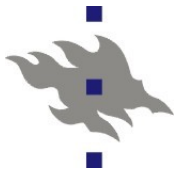


SMTP-ongelmien debuggaus

- Viestin kaikki otsakkeet
  - Kun käyttäjää pyytää forwardoimaan ongelmatapauksen eteenpäin otsakkeet lähes aina hukkuvat matkalla
- MTA:n lisäämät Received: -otsakkeet ovat ainoa keino selvittää viestistä mitä sille oikein matkalla tapahtui
- Envelope-Sender ja Return-Path voivat olla hyödyllisiä
  - Kuten todettua From: ja To: kentät eivät välttämättä kerro mitään
- MTA:n loki

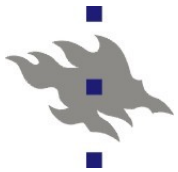
Linux MTA:t

- Sendmail
  - Ikivanhaa softaa – Yhtä vanha kuin SMTP
  - Monimutkainen, hankarasti konfiguroitava historiallinen jäänne
  - Muut MTA-softat tyypillisesti ovat jonkin verran komentoriviyhteensopivia sendmail:in kanssa
- Exim
- Qmail
  - Dan Bernstein - ”Threat or Menace”
- Postfix
  - Helppo, ei asenneongelmia
- Courier
  - Integroitu SMTP, IMAP, POP, LDAP, SSL ja HTTP
  - Käytössä laitoksella



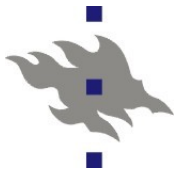
Sendmail

- Näistä ei varmaan koskaan pääse eroon
  - Siksi hyvä ymmärtää jonkin verran sendmailin toiminnasta
- Konfiguraatiotiedosto */etc/mail/sendmail.cf*
  - Hillitön makrohässäkkä jossa itse asiassa on suuri osa meilien käsittelyn toteutuksesta
  - Nykyään kyseinen konfiguraatiotiedosto itse asiassa generoidaan m4-makroilla */etc/mail/sendmail.mc* tiedostosta
- Jonkinlainen tuki kaikelle mahdolliselle
  - Jos vain osaa konfiguroida
  - Myös meilinvälitykselle ilman SMTP:tä
- Paikalliset aliakset */etc/aliases* tiedostossa
- Nykyään MSA ja MTA toiminto eriytetty eri käyttäjätunnuksille



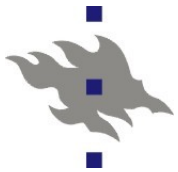
Postfix

- Luennoijan suositus uuteen työasema-asennukseen
- Helpohko konfiguroida
- Ei pahoja asenneongelmia
- Ei liikaa historiallista painolastia
- Hyvä dokumentointi
- Tärkeimmät ”uudet” ominaisuudet tuettu
  - STARTTLS TLS-yhteyden neuvottelu
  - SASL SMTP-autentikointi



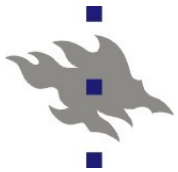
POP – Post Office Protocol

- RFC1725
- Postilaatikon tyhjentämiseen käytettävä protokolla
- Ei hienouksia
  - Ei useampia postilaatikoita
  - Ei arkistointia palvelimelle
- ISP:iden suosiossa
  - Käyttäjille tuttu
  - Käyttäjille ei tule kiusausta arkistoida postejaan palvelimelle
- Linux POP-ohjelmistoja
  - Dovecot
  - Cyrus IMAP
  - Courier
  - Qpopper



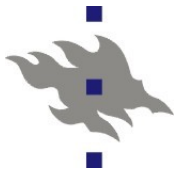
IMAP

- Internet Message Access Protocol
- Useita eri postilaatikoita
  - Arkistointi liikkuvalle käyttäjälle
    - Laitoksella tilaa on hankittu sitä mukaa lisää kun käyttäjille on tullut lisää postia
  - Palvelinpäässä tapahtuva lajittelu ja suodatus
  - Jaetut postilaatikot
- Useita eri autentikointimenetelmiä (starttls, sasl)
- Dovecot
- Cyrus IMAP
  - Tietotekniikkaosastolla
- Courier
  - Laitoksella
- UW-IMAPD
  - Ensimmäinen, mutta unohtakaa tämä



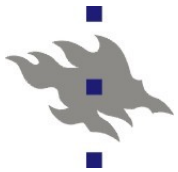
Courier

- Kaikki meilipalvelimen osat yhdessä paketissa
  - Unix-filosofian vastaisesti
- ESMTP, POP, IMAP
- MDA:na maildrop
- Sähköpostilistat
- Webmail
  - Sqwebmail
- Selainkäyttöliittymä konfigurointiin
  - Edelleenohjaus (forward)
  - Lajittelu
  - Suodatus
  - Sähköpostilistat



Procmail

- Procmail on tähän asti esitellyistä ohjelmista ainoa, joka on suunniteltu hoitamaan pelkästään MDA:n tehtävät
- Kun MTA on todennut viestin olevan tarkoitettu paikalliselle koneella, se voi antaa sen procmailin käsiteltäväksi
- Procmail toimittaa viestin käyttäjän postilaatikkoon
- Käyttäjät voivat lisätä sopivaksi katsomansa mielivaltaiset suodattimet omalla *.procmailrc* -tiedostolla
- Procmail:in käyttö edellyttää politiikkapäätöstä käyttäjien omien ohjelmien suorittamisen sallimisesta sähköpostipalvelimella

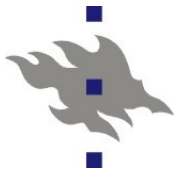


Fetchmail

- Työkalu viestien hakemiseen POP- tai IMAP-protokollan ylitse ja edelleen lähettämiseen
- Mahdollistaa etäpostilaatikoiden automaattisen tyhjentämisen
  - Arkistointiin
  - Paikalliseen uudelleenlähettämiseen

Roskaposti laitoksella

- Petri Kutvosen tilastot 6.4 klo 16.00
  - Alkuvuosi 2006
  - Rajalla torjuttuja: 20303160
  - Bogofiltterin mielestä spämmiä: 1633681
  - Bofilter epävarma: 71941
  - Kelvollisia: 1471072
    - Näissä on jälkikäteen torjuttuja ja vääriä negatiivisia joukossa
  - 94% kaikesta meilistä spämmiä

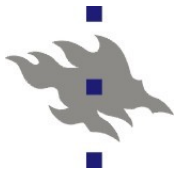


Roskapostin suodatus

- Mustat listat
  - DNS-protokollalla reaaliaikaisesti ylläpidettyjä
  - Useita erilaisia listoja eri tarkoituksiin
  - Tavallisesti reagoivat liian myöhään: spammaus tapahtui jo
  - Osuvat usein syyttömiin tahoihin
  - Listat kuolevat pois yllättäen ja nopeasti
- Bogofilter
  - Suodatus tilastollisella analyysillä
- Spamassasin: suodatuksen linkkuveitsi
  - Viestin sisällön järkevyys
  - Mustat listat
  - Tilastollinen analyysi
- Virustorjunta Linuxilla
  - Clamav
  - F-Secure

Varmistuskopiointi

- Hajoavat laitteet vain yksi ongelma
  - Ihmisten ja ylläpitäjien sähläys
  - Katastrofit: tulipalot, varkaudet, tulvat, heinäsirkat
- Varmistuskopioinnin vaatimuksia
  - Automatisoitua, mutta valvottua
    - Myös palautuksia pitää testata
  - Useita vanhoja versioita
    - Inkrementaalivarmistukset
- Media
  - Nauha on edelleen halvempaa kuin kovalevytila
    - marginaalisesti
    - Ainakin jos nauhurin hintaa ei lasketa..
  - Hotplug-levyt: USB2, firewire, E-SATA
  - Optinen media:
    - Kallista, hidasta, medialla kovin vähän tilaa
  - Verkon yli kopiointi!



Medioiden hinnat

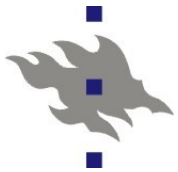
- Nämä ovat alv-hintoja!
- HP Ultrium LTO4 800G nauha 20kpl: 1089e
  - 0.07e/G
- 1.5TB Drivestation Turbo ulkoinen kovalevy: 155e
  - 0.11 e/G
- DVD-R 4.7GB 50kpl: 58e
  - 0.25 e/G
- Blu Ray 25GB 5kpl: 58e
  - 0.464 e/G

Varmistuskopiointipolitiikkaa

- Mitä varmistetaan?
  - 500:n työaseman verkossa tarvittaisiin ~50T tilaa täydellisiin varmistuskopioihin (ja vastaava määrä verkkoliikennettä)
  - Työasema-asennuksien (ja usein palvelintenkin) varmistus tavallisesti turhaa
  - Kotihakemistot verkkolevyllä tekevät keskitetystä varmistuksesta helpomman
  - Skriptatut kotihakemistojen poltot optiselle medialla tai kopiointi hotplug-levylle
- Useamman kovalevyn kikat
  - RAID ei suojaa käyttäjän virheiltä, mutta yölliset tai viikottaiset varmistuskopiot suojaavat
  - Käytetään toinen kovalevy RAID:in sijasta varmistuskopioihin

Varmistuskopiointi Linuxissa

- Punnitaan ylläpitäjän shelliskriptien kirjoitustaito
- Työkaluja
  - Tar – tiedostojen paketointi
  - Cpio – vaihtoehtoinen paketointi
  - Dump – paketointi suoraan tiedostojärjestelmästä
    - Vaarallinen ja nykyaikana lähinnä turhana
  - Gzip, bzip2 – pakkaus
  - Rsync – Tiedostojen synkronointi verkon yli
    - Ssh-kryptattuna, ssh-avaimilla autentikoituna
  - Cdrecord, dvdrecord
    - Poltto optiselle medialle
  - Crond
    - Automaattinen ajastaminen

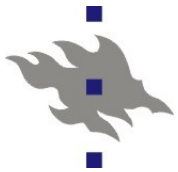


Amanda

- The Advanced Maryland Automatic Network Disk Archiver
  - Käyttäjille jotka haluavat valmiiksi mietityt ja testatut skriptit
  - Kopioi ensin levylle, vasta sitten nauhalle
  - Varsinaiset varmistuskopiot: tar, smbtar, dump
  - Oma protokolla: Ei käytä rsh:ta tai ssh:ta
    - Tietoturvariski. Uusin versio osaa openssh:n
  - Ymmärtää erilaisten nauhalaitteiden päälle (mm. Nauharobottien)
  - Osaa itse skeduloida täydet ja inkrementaaliset varmistukset
  - Pitää yllä indeksejä tiedostojen sijainnista nauhalla
  - Suunniteltu toimimaan cron:ista käsin
  - Verkon yli toimiva palautustyökalu
  - Ei GUI:ta

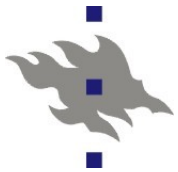
Virtualisointi

- Yhdellä laitteella ajetaan samanaikaisesti useampaa käyttöjärjestelmäinstanssia
  - Instanssin käyttöjärjestelmä (KJ) on riippumaton virtuaalikoneen käyttöjärjestelmästä
  - Instanssit näkevät virtuaalisen laitteiston
    - Esim. vain osan fyysisestä laitteistosta. Instanssille on varattu vain osa koneen muistista tai CPU:ista
    - Laitteisto voi olla emuloitua. esim. Yksi fyysinen verkkokortti jaettu kaikkien instanssien kesken
    - Instanssin KJ:lta ei tarvita erityistä tukea virtuaalilaitteistolle
      - Virtuaalilaitteisto tavallisesti emuloi jotain tunnettua oikeaa laitteistoa (VGA-näytönohjaimet, verkkokortit, SCSI-ohjaimet)
  - Instansseja voidaan luoda ja sulkea lennossa
  - Tarvitaan ohjelmisto, joka toteuttaa virtuaalilaitteiston: hypervisor
  - Instanssi voi siirtyä fyysiseltä raudalta toiseen
    - Live Migration, jos hypervisor vain tukee



Miksi virtualisoida?

- Tehostetaan fyysisten laitteiden käyttöastetta
  - Asennetaan useita virtuaalipalvelimia yhdelle fyysiselle laitteelle
  - Hypervisor jakaa prosessoritehoa ja muistia tarpeen mukaan
- Luotettavuus
  - Riippumattomuus fyysisestä laitteesta: instansseja voi siirtää laitteelta toiselle
    - ”live migration” -tuen avulla myös ilman palvelukatkoksia
  - Virtuaalikoneen voi replikoida verkon yli toiselle laitteistoille
  - Virtuaalikoneen snapshotteja voi käyttää varmistuskopiointiin ja ongelmatilanteista toipumiseen
- Yhteensopivuussyyt
  - Tarvitaan käyttöjärjestelmää X, mutta ei haluta ostaa pelkästään sitä varten erillistä rautaa
- Tietoturvasyyt
  - Erotetaan ohjelmistot ja käyttäjät omille hiekkalaatikoilleen
- Ylläpidon ja asennuksien helppous
  - Etähallinta, etäasennukset ja monitorointi hypervisorin kautta

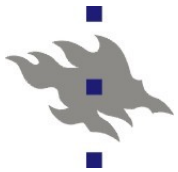


Virtualisoinnin huonot puolet?

- Virtuaalilaitteen kaatuminen vie mukanaan kaikki laitteessa asustaneet virtuaalikoneet
  - Virtuaalikoneiden replikoinnilla pyritään välttämään juuri tämä tilanne
- Virtuaalikoneet ovat aina jonkin verran hitaampia kuin fyysiset koneet
- Virtuaalikoneella voi olla odottamatonta latenssia, jos muistia tai CPU-aikaa ei olekaan saatavilla juuri silloin, kun sitä tarvittaisiin
- Aivan kaikki oikean laitteiston ominaisuudet eivät toimi kunnolla virtuaalikoneissa
  - Multimedia
  - 3D-kiihdytys

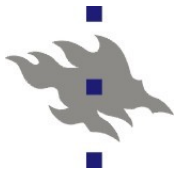
Virtuaalikonesovellukset

- Virtual Appliance
- Kokonaisia valmiita palvelinasennuksia voidaan jakaa virtuaalikoneimageina
- Palvelinohjelmiston mukana tulee kylkiäisenä käyttöjärjestelmä, joka on valmiiksi konfiguroitu yhteensopivaksi palvelinohjelmiston kanssa
- Virtuaalikonesovelluksina on myös helppo monistaa itse koottuja virtuaalikoneasennuksia klusterikäytössä



Hypervisor

- **Hypervisor** on ohjelmisto joka jakaa oikeita fyysisiä resursseja virtuaalikoneiden käyttöön ja toteuttaa virtuaalikonerajapinnan
  - Tyypin 1 bare bone hypervisor on itse samalla käyttöjärjestelmä
    - MS:n Hyper-V
  - Tyypin 2 hypervisor toimii **isäntäkäyttöjärjestelmän** (Host OS) alla
    - Isäntäkäyttöjärjestelmä toimii kuten normaali KJ, mutta jakaa osan resursseista hypervisorin käyttöön
    - Tyypillisesti hypervisor tarvitsee KJ:lta lisäpalveluita, joita tavalliset sovellukset eivät tarvitse
      - Linuxissa KVM tai erilliset kernelin modulit
  - Hypervisorin toteuttamaan virtuaalikoneeseen asennettua käyttöjärjestelmää **vieraskäyttöjärjestelmäksi** (guest OS)
    - Vieraskäyttöjärjestelmään voidaan tehokkuussyistä haluta asentaa erillisiä virtuaalilaiteajureita, jotka toimivat tehokkaammin kuin aidon raudan emulointi



Hypervisorin käyttö

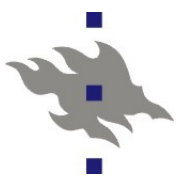
- Hypervisor tarjoaa:
  - Mahdollisuuden uusien virtuaalikoneiden luomiseen
    - Varataan levytila, CPU:t ja virtuaaliset verkkolaitteet
    - Virtuaalikone voi myös nähdä oikeita fyysisiä laitteita
      - Esim. Levypartitioita tai USB-väyliä
  - Virtuaalikoneen käynnistyksen virtuaaliselta medialta
    - Cdrom, dvd, verkkobuutti, kovalevy
  - Virtuaalikoneiden suspendointi
  - Snapshotit virtuaalikoneista
  - Virtuaalikoneiden exporttaus ja importtaus
    - Eri hypervisoreilla on omat epäyhteensopivat formaatit instanssien talletukseen
  - Konsolin luoduille virtuaalikoneille
    - Näytönohjaimen, näppäimistön ja hiiren emulointi
  - Resurssien käytön monitoroinnin

Virtuaalikonetyypit: Emulointi

- Virtuaalilaitteisto on toteutettu ohjelmistolla
  - Emuloidun laitteiston ei tarvitse olla sama kuin fyysisen koneen
  - Toisaalta emulointi on ainoa vaihtoehto, jos fyysinen rauta ei ole yhteensopivaa
- Usein kertaluokan verran hitaampaa kuin koodin natiivi suoritus
  - Tämä ei ole kuitenkaan kiveen kirjoitettu sääntö: Just In Time kääntäjät voivat olla hyvin tehokkaita
- Turvallinen ja helppo tapa
  - ei tarvitse tukea isäntäkäyttöjärjestelmältä
  - Kaatuva vieraskäyttöjärjestelmä ei vie isäntää mukanaan
- Esim. Qemu

Virtuaalikonetyypit: paravirtualisointi

- Paravirtualisoinnissa vieraskäyttöjärjestelmä toimii yhteistyössä hypervisorin kanssa
  - Intelin käskykannassa oli aina joitain käskyjä, joiden suoritus virtuaalikoneessa järjestelmävalvojatilassa aiheutti poikkeuksen ja jotka oli emuloitava
  - Paravirtualisoinnissa vieraskj ei suorita näitä komentoja ollenkaan, vaan käyttää hypervisorin tarjoamia palveluja
  - Vieraskäyttöjärjestelmä ei oleta, että fyysiset prosessorit ja muistit ovat aina välittömästi sen käytettävissä
  - Edellyttää että vieraskj on muokattu käyttämään hypervisorin palveluita
- Paravirtualisointi on potentiaalisesti tehokkaampaa
  - Ei turhaa emulointia
  - Ei tuhlata laitteistoresursseja, jotka eivät oikeasti ole käytössä
- Vieraskäyttöjärjestelmän hypervisorin rajapintoja ymmärtävät ajurit ovat tavallaan paravirtualisointia
- Esim. Xen

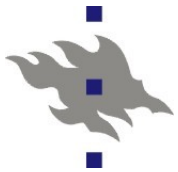


Virtuaalikonetyypit: Laitteistotason virtualisointi

- Vieraskäyttöjärjestelmään ei tehdä muutoksia
  - Vieraskäyttöjärjestelmää pyöritetään sellaisenaan oikealla laitteistolla
  - Tämä voi edellyttää joidenkin konekäskyjen emulointia poikkeuksien kautta hypervisorilla
- Intel ja AMD tukevat laitteistovirtualisointia
  - AMD:n AMD-V laajennos kaikissa uusissa AMD CPU:issa
  - Intelin VT-x laajennos suuressa osissa CPU:ita
- Vieraskäyttöjärjestelmä voi kuitenkin tarvita erillisiä ajureita virtuaalilaitteistolle
  - Usein kuitenkin virtuaalilaitteet näyttävät joltain yleisesti käytetyltä vanhalta laitteelta ja voidaan käyttää olemassa olevia vanhoja ajureita
    - Esim. Vmwaren virtuaaliverkkokortit ja SCSI-ohjaimet
- VMWare ja KVM tukevat laitteistotason virtualisointia

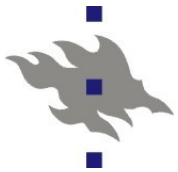
Ohjelmistoja ja yrityksiä

- Virtualisoinnista on tullut bisnestä (ja jopa hypeä)
- Sun: Solaris Zones
  - Virtualisointi sisäänrakennettuna Solarikseen
- MS: Hyper V
  - MS:n oma hypervisor
- Citrixin XEN
  - Alunperin OS-softaa Cambridgen yliopistolta
- KVM – Kernel Virtual Machine
  - Linuxin kernelistä löytyvät tuki virtuaalikoneiden toteutukselle käyttäjätason prosesseina
- Qemu
  - Prosessoriemulaattori
- VMWare
  - Monta eri tuotetta eri markkinasegmenteille
  - Ensimmäinen tuotteistettu käyttökelpoinen virtuaalikone vuodelta 1999



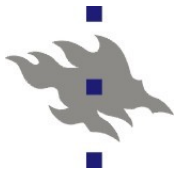
XEN

- Käynnistyslataaja lataa ylemmän tason XEN-hypervisor minikäyttöjärjestelmän
  - Toimii Intel-prosessorien suojaustasolla 0
  - Virtuaalikoneissa tasolla 1 pyörivät käyttöjärjestelmät pyytävät hypervisorilta resursseja käyttöönsä: muistia, laitteistoa, keskeytyksiä
    - Hypervisor siis tarjoaa paravirtualisointirajapinnan
- Domain0 instanssi:
  - Modifioitu isäntäkäyttöjärjestelmä (Linux, NetBSD tai Solaris), jonka xen-hypervisor käynnistää automaattisesti
  - Isäntäkäyttöjärjestelmä toteuttaa fyysiset laiteajurit ja tarjoaa ne hypervisorin käyttöön
  - Ylläpitäjä kirjautuu sisään domain0 instanssiin ja sieltä käsin ylläpitää vieraskäyttöjärjestelmiä



KVM

- Kernel-based Virtual Machine
  - KVM on kernelin moduli, joka tarjoaa käyttäjätason ohjelmistolle rajapinnan (*/dev/kvm*), jonka avulla käyttäjätasolta voidaan toteuttaa virtuaalikoneita
    - Tarvitaan AMD:n tai Intelin virtualisointilaajennokset
  - Mahdollistaa laitteistopohjaisen virtualisoinnin
- Qemu ja Virtualbox ovat KVM-rajapintaa käyttäviä virtualisointiohjelmistoja
- *Virtual-manager* ohjelmalla ylläpidetään virtuaalikoneita



VMWare

- VMWare
  - Pitkä lista vaihtoehtoisia virtualisointituotteita eri käyttötarpeisiin (ja lompakon paksuuksiin)
  - VMWare Infrastructure
    - Maksullinen useista fyysisistä koneista koostuvan virtuaalikoneverkon hallintajärjestelmä
  - VMWare ESX
    - Bare Bone-tyyppinen Linux-pohjainen käyttöjärjestelmäasennus, jossa isäntäkäyttöjärjestelmä tarjoaa vain verkkopalvelut virtuaalikoneiden ylläpitoon
  - VMWare Workstation
    - Työasemalle asennettava virtuaalikoneohjelmisto
  - VMWare Player
    - Virtuaalikonesovelluksia suorittava ilmainen ohjelmisto
    - Ei tue virtuaalikoneiden luontia