

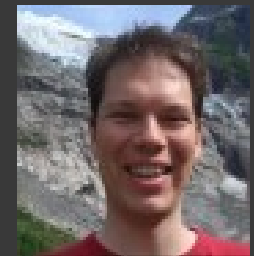
<http://www.cad-comic.com>

IT-forum 2011

# ITA og Mac ved UiB

<http://bit.ly/itamac>

Jan Ivar Beddari  
Faggruppe Unix



# #1

## Er drift av Mac vanskelig?



Nei, fordi ...



# ... det ligner mye på Linux\*

- TCP/IP
- DHCP
- TFTP
- LDAP og Kerberos
- Samba/Netatalk på Linux
- IMAP eller POP3
- Windows-filserver
- Active Directory
- Exchange

\* og andre Unix-lignende OS



Teknisk sett er det  
mange muligheter!



Ja, fordi ...

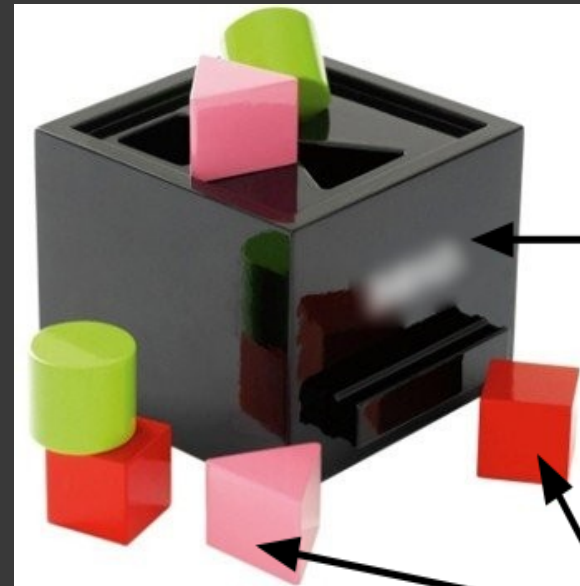


# ... det krever spesialiserte ressurser!

- Kursing
- Kompetansebygging
- Innkjøp
- Service på maskinvare
- Lisenser
- Installasjon av OS
- Fjernstyring
- Programvaresystem
- Tilpasninger i infrastruktur
- Ekstra testing
- Vedlikehold av programvare
- Oppfølging av **sikkerhet**
- Mac App Store?
- iPhone?
- iPad?



# Apple er også en stor utfordring



Typisk produkt  
(Veldig blankt!)

Byggeklosser

Ikke stol på  
Apple!



# #2

## Mål og teknologivalg



# Litt bakgrunnsinformasjon

- Arbeid startet i 2007
  - Lite ressurser tilgjengelig .. lagt dødt
  - Tatt opp igjen høsten 2010
- Organisert under Seksjon for infrastruktur, faggruppe for Unix
  - Samme infrastruktur som Linux
  - Drift av OSX som et "Unix-lignende" OS
  - Teknisk samarbeid i første rekke med UiO men også etterhvert andre Uninett-tilknyttede institusjoner



# Tekniske mål

- Ingen skal jobbe som administrator!
- Sentral konfigurasjon, sikring og oppdatering av OS
- Sentralisert programvareutrulling
  - Standard programvare skal ha en fornuftig konfigurasjon klar til bruk
  - Delegerte rettigheter til brukerstøtte
  - Jobbe mot å tilby en selvbetjeningsmodell



# Tekniske mål

- Robust i forhold til plassering og oppetid i nettverket
  - Synk-og-lagre metodikk, «atomiske» endringer
  - Endringer utføres på standardiserte tidspunkt
  - Også uten at maskinen er tilkoblet nett!
- Klientsystemene tilgjengelige også på eksterne nett
- SSL-sertifikat hovedmetode for sikker identifikasjon



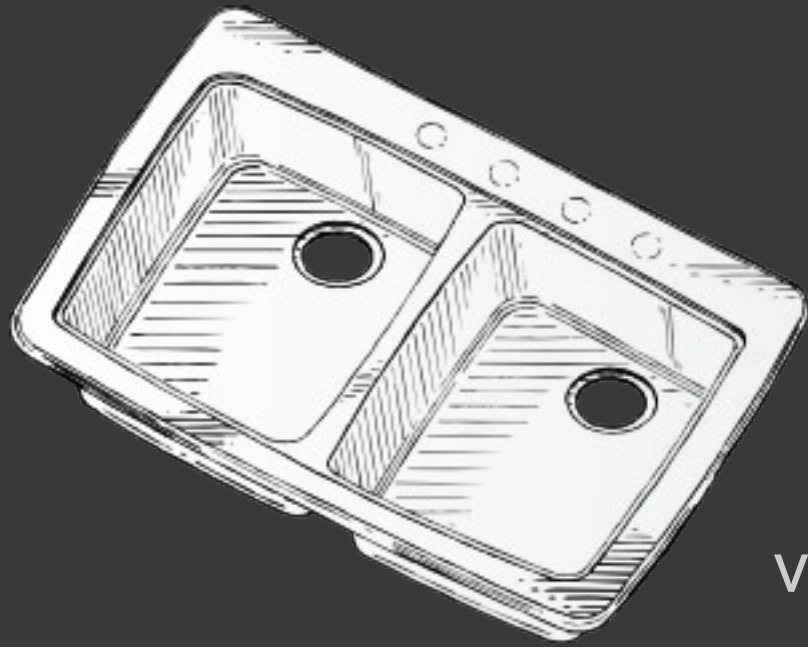
Problem ..

alt unntatt kjøkkenvasken

eller plukke

kirsebær?





versus







versus



# Divide and conquer

- ✓ Installasjon
- ✓ Systemkonfigurasjon
  - ✓ Maskinkonfig
  - ✓ Brukerkonfig
  - ✓ Tidspunkt for tilordning
- ✓ Programvare
  - ✓ Utrulling
  - ✓ Vedlikehold
- ✓ Support og rapportering
  - ✓ Fjernsupport
  - ✓ Maskinwaresupport
- ✓ Avvikling

Felles begrepsapparat



# Divide and conquer

- ✓ Systemkonfigurasjon
  - ✓ Tidspunkt for tilordning

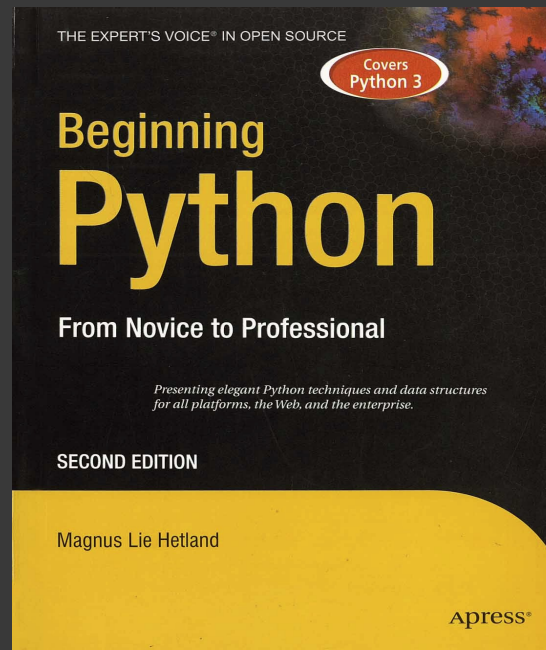
Tidspunkt	Maskinkonfig		Brukerkonfig	
	Policy	Standardverdi	Policy	Standardverdi
Ved første oppstart av OS	✓	✓		
Ved oppstart av OS	✓	✓		
Når bruker logger inn eller ut			✓	✓
Når brukeren ønsker det				✓
Daglig/ukentlig/månedlig	✓	✓	✓	✓
På et gitt tidspunkt	✓	✓	✓	✓

# Valg av system

- Installasjon DeployStudio
- Systemkonfigurasjon Puppet
- Programvare Munki  
*Selvbetjening*
- Support og rapportering Teamviewer  
Apple Remote Desktop  
*Ny rapporteringsløsning*

# Valg av system

- Unix klientdrift har tradisjonelt benyttet Bash som skriptspråk
- For Mac er målet at så mye som mulig av det vi trenger av «lim» skal skrives i Python
- Unixgruppen leser for tiden en Pythonbok :-)



# Høye krav til oss selv

- Vi har valgt løsninger som krever en høy grad av egenkompetanse
  - Er *ikke* alene og det er mulig å få kjøpt kompetanse
- Vi er avhengig av en sterk evne til analyse og feilsøking – på flere systemer
- Svært viktig å dokumentere systemene slik de henger sammen



En slurk kaffe? :-)



# #3

Mer tekniske detaljer, takk!





# Eksisterende tjenester

- Sentralisert DHCP for alle subnet
  - Gir mulighet for netboot på hele UiB
  - Vi bruker ISC dhcpd – og vi kan sortere ut Mac
  - Intel-baserte Mac støtter tftp og next-server
- Autentisering og autorisering
  - LDAP-katalog med studenter og ansatte
  - Kerberos-realm UNIX.UIB.NO (mulig trust mot AD)
  - Oppsett for pålogging og tjenestetilgang ved hjelp av LDAP og Kerberos



# Installasjon

- Installasjon med DeployStudio
  - Gratis programvare, mye funksjonalitet
  - Netbooter et redusert image av OSX
    - Leser image fra nett med NFS
    - God støtte for automatisering av oppgaver før og etter image er skrevet til lokal disk
    - Alle maskiner vil bli tatt backup av ...



<http://www.deploystudio.com>

<http://web.me.com/driley/web/deploystudio.html>



# Installasjon

1. Netboot til DS Runtime
2. Autentisering
3. Valg av arbeidsflyt
4. Backup
5. Imaget kopieres til lokal disk over NFS
6. Puppet-pakken installeres til lokal disk
7. DS Runtime-miljøet kobler til Puppetmaster (Puppet CA server) og genererer et SSL-sertifikat som lagres til disk inn i det nye filsystemet vi nettopp har kopiert inn
8. Ved første oppstart av maskinen tar Puppet over. SSL-sertifikatet sikrer authN/authZ og kommunikasjon

# Systemkonfigurasjon

- Systemkonfigurasjon med Puppet
  - Filbasert konfigurasjonsstyringsverktøy
  - Åpen kildekode
  - Integreres med versjonskontroll for høy grad av sporbarhet ved endringer
  - Mange brukere på OSX - direkte støtte for plist-filer
  - **Hele unixgruppen vil ta verktøyet i bruk**



<http://www.puppetlabs.com>

<http://link.uib.no/?50pzr>



# Systemkonfigurasjon

- Puppet er ikke noe «magisk», man definerer konfigen i et eget, enkelt språk (Puppet DSL)
  - Uttrykker konfigurasjon som en avhengighetsgraf eller enn å følge prosedyrer i en gitt rekkefølge (som i konfigurasjonsscript)
  - Filene som utgjør denne avhengighetsgrafene kan man versjonskontrollere med f.eks Git eller Subversion



Dette skal vi utnytte så godt vi kan!



# Systemkonfigurasjon

- Lagringsløsning for hjemmekatalog
  - NetApp skal redde oss!
  - Samba fra NetApp skal fungere g med OSX
  - Stasjonære vs bærbare maskiner
  - Mulige løsningsscenario avhengig av testing
    - Auto-synkronisering av alt
    - Auto-synkronisering av noe (Documents)
    - Manuell synkronisering
    - Vi har et uløst problem..
      - » Synk er ikke for store datamengder
      - » Kan vi få til en løsning med «delt» lagring?



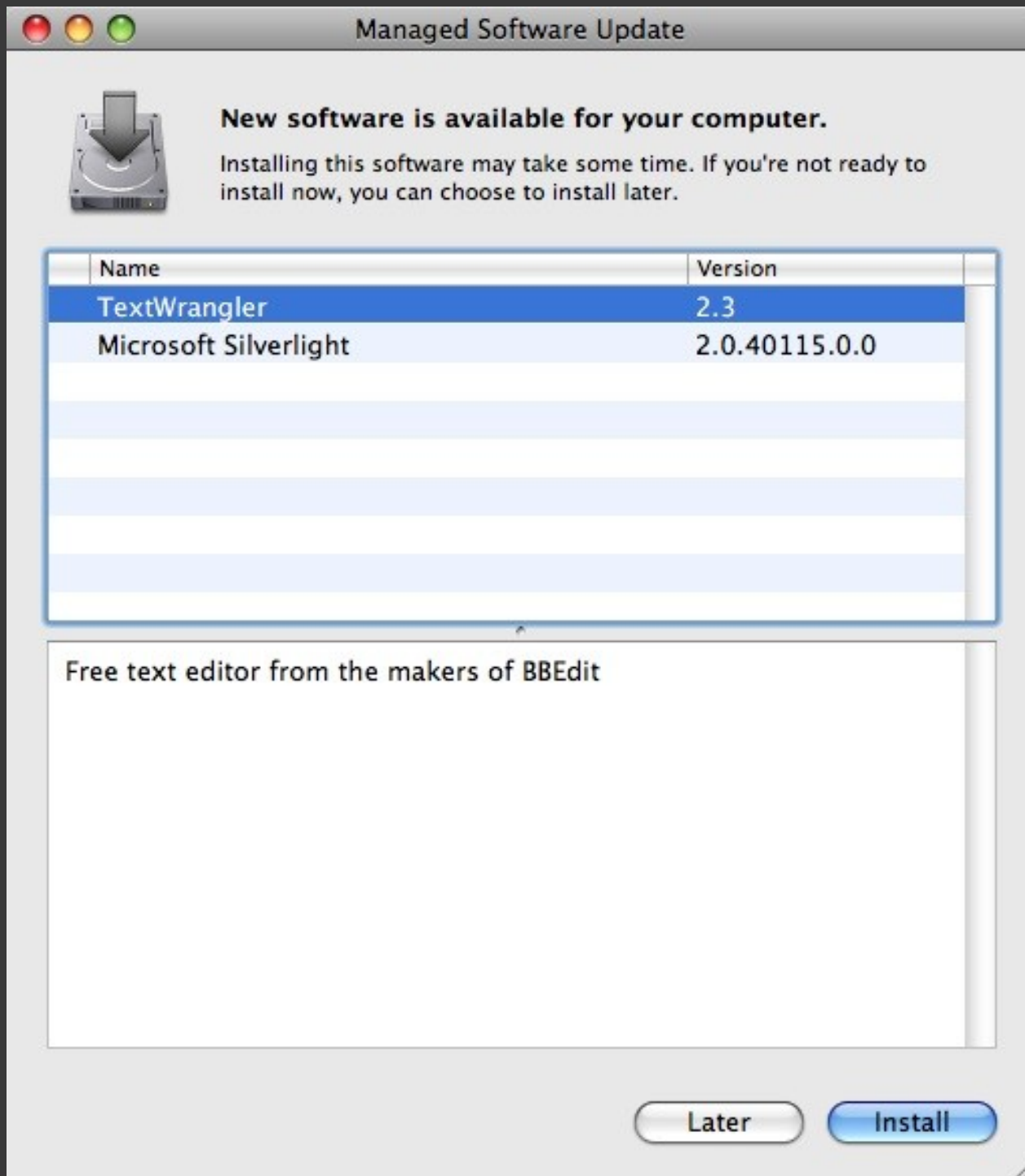
# Programvare

- Munki for programvareutrulling
  - Programvarerepositorie med klient over HTTPS
  - Åpen kildekode, skrevet i Python
  - Baserer seg på pkg, Apple sin standard for programvarepakker - dokumentert format
  - Avhengigheter mellom pakkene ligger på serversiden, klienten er "dum"
  - Integreres med versjonskontroll for høy grad av sporbarhet ved endringer



<http://code.google.com/p/munki/>







# Programvare

- The Luggage
  - Et Makefile-basert verktøy for å kunne pakke programvare som pkg-filer
  - Utviklet av en tidligere Google-ansatt etter modell av Google sitt eget interne verktøy
  - Gir høy synbarhet og muligheter for versjonskontroll

<https://github.com/unixorn/luggage>



# Support og rapportering

- Apple Remote Desktop for rapportering
  - Klientene kobler til og rapporterer egen konfig til en rapporteringsserver
  - Vi kan gjøre detaljerte spørringer mot databasen
  - Dette er selvfølgelig et OS-spesifikt produkt

<http://www.macenterprise.org/macworld-2010-slides>



# Support og rapportering

- Teamviewer for fjernsupport
  - Tilgjengelig på alle OS
  - Unixgruppen har ansvaret for Mac og Linux-klientene og har bestemt å ta det i bruk for Mac og har det til vurdering for neste Linux-klient
  - Er basert på VNC
  - Fungerer i praksis overalt og bedre enn mange andre løsninger på dårlig linje



# Support og rapportering



# #3

## Brukerperspektivet



Hva får jeg som bruker?



# Sikkerhet

## Økt tjenestetilbud

## Support



Hva skjer hvis jeg ikke vil?





# Vet ikke?

Det er ikke utformet noen  
policy for håndtering av  
migrasjon enda



.. men vi lover å være flinke!



# IT-forum 2011:

Jan Ivar fra Unix klientdrift  
lover at leveringstid på  
*standard* programvare skal  
være under fem arbeidsdager

\* standard defineres av oss .. lisenser, maskinvare, etc

# IT-forum 2012:

?

Vi skal stille med statistikk

