LISA
Large Installation System Administration

AAU
15 Marts 2007

Karsten Thygesen
CTO, Partner, Netic A/S
karthy@netic.dk

Nature of Large Installations

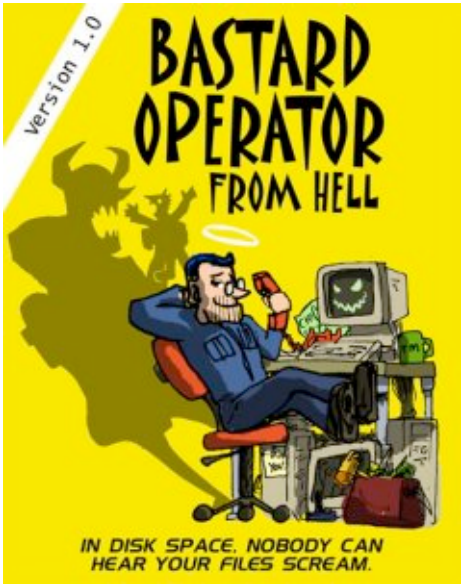
- Many servers
  - Multiple architectures
  - Complex setup
  - Many users/organizations
    - With different goals and privileges
- High requirements to
  - Security
  - Availability
  - Privacy
  - Manageability

Management Goal

- Low expenses
  - Few system administrators
  - Under skilled administrators
  - Low budget for administrative projects (make projects add to infrastructure)
- Low time-to-market
  - High workload
  - Pressure to cut corners (which means more work later on)
  - No focus on monitoring, maintenance, education
  - Preference for turn-key solutions

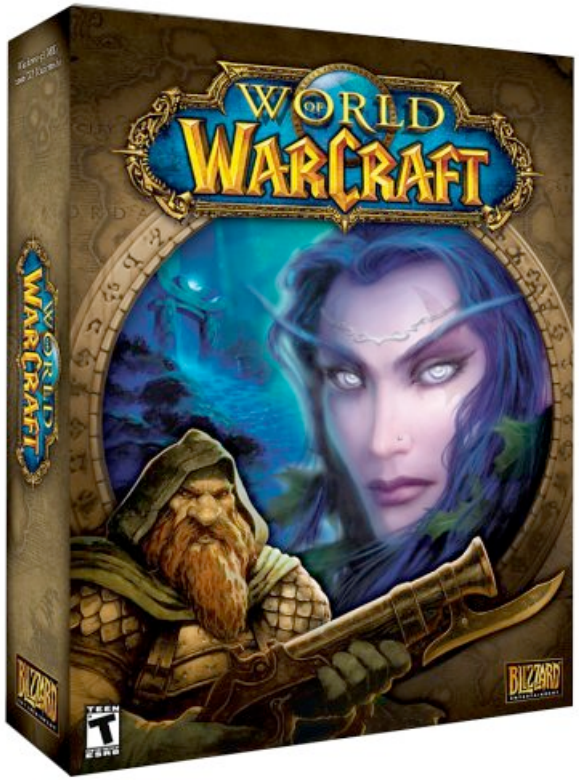
Organizations goals

- They are the center of the Universe
  - Nothing is more important than their current problem/needs
  - IT can't be that difficult – admin is just clueless - underestimate complexity
- 100% availability, 200% performance, no quotas
  - Even announced downtime is not acceptable
  - Central computers are always slow – mine at home is faster!



Administrators Goal

TO HAVE FUN



And do self-education by investigating different tools, languages etc.

Profile of an administrator

- Unquestionable technical skills in *all* aspects of computing
- Young with 25 years of experience
- Good communication skills (talk like an user)
- Good political skills (talk like management)
- Manager (both economy, strategy and staff)
- Projectleader, teamplayer, etc

- All done with too few staff, to low budget and too high workload – with no signs of stress!

The Solution

- Meta administration
- Micro Management -> Macro management
- Individual computers -> groups and clusters!
- Server virtualization
- Stateless clients
- Central
  - File/data store
  - access control
  - user id management
  - Backup
  - Monitoring
  - software deployment, configuration management

Central File/Data store

- Which storage architecture? JBOD, RAID, SAN, NAS, iSCSI
- Many protocols to choose from
  - NFS (version 2, 3 or 4? Windows support?)
  - CIFS (Unix support?)
  - AFS (complex but nice)
  - iSCSI - new
  - Many research projects still going on

Intransa IP 7500

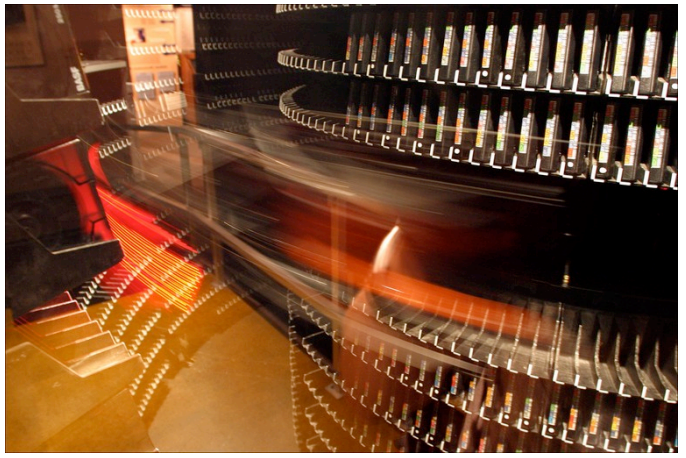
NFS, CIFS, AFS

	CIFS	NFS	AFS
Platform	Windows	Unix	Both
Internet ready	Partly	Partly v.4	Yes
Homogen view	No	No	Yes
Works on low bandwith	No	No	Yes
Scales	100's	100's	1000's
Security	AD	V3: trust, v4: gssapi	Kerberos
Non-trust clients	Yes	V3: no, V4: yes	Yes
Reliability	No	No	Replication
Caching	No	Inode	Yes
Complexity	Low	Low	High

Central Access-Control

- Central File/Data storage
- With many users
  - Impossible to keep track of all groups
  - Users must be able to define their own groups
    - NFS: v3: no, v4: partly, CIFS: partly, AFS: yes
- Central managed firewalls
- Central managed IDS (intrusion detection systems)
- Central identity management

- Which platform to choose?
  - Tivoli, Legato, HSM, Serverless SAN/NAS
  - Amanda, Bacula?
  - Platform support?



- What do we need to backup?
- How long retentiontime?
- NetApp Nearstorage as cache?
- Offsite tape storage and procedures?
- How do users get their lost files back?
- Backup verification?
- Backup of network configurations etc?

Central Monitoring

- *Really* aim at getting only one monitoring platform?
- Doing monitoring right can be as expensive as the monitored system it self!
- Monitoring is not red/green but statistics, trends and aggregation!
- What about staffing and escalations?
- Disaster plans?

Macro Management

- Automatic tools to:
  - configure systems and maintain that configuration
  - Deploy software and complex configuration files
  - Do simple, repeatable work
  - Self repairing Monitoring
  - Document (intended) state of system

Cfengine

- Central configuration/rule files
- Describes intended state – not how to change
- Adapts to current system
- Built-in secure configuration and file distribution, reporting, tripwire and more
- Works well across different (Unix)platforms
- Limited windows support
- Can be extended to almost anything
- Powerful but also potential dangerous.

Cfengine example - NTP

```
editfiles:
  solaris::
    { /etc/inet/ntp.conf
      AutoCreate
      AppendIfNoSuchLine "server ntp01.netic.dk"
      AppendIfNoSuchLine "server ntp02.netic.dk"
      AppendIfNoSuchLine "server ntp03.netic.dk"
      DefineClasses "startntp"
    }
  freebsd|linux::
    { /etc/ntp.conf
      AutoCreate
      AppendIfNoSuchLine "server ntp01.netic.dk"
      AppendIfNoSuchLine "server ntp02.netic.dk"
      AppendIfNoSuchLine "server ntp03.netic.dk"
      DefineClasses "startntp"
    }

shellcommands:
  startntp.solaris::
    "/etc/init.d/xntpd start"
  startntp.freebsd::
    "/usr/sbin/ntpd -p /var/run/ntpd.pid"
  startntp.redhat::
    "/etc/init.d/ntpd restart"
  startntp.debian::
    "/etc/init.d/ntp-simple restart"
```

Cfengine features

- Copy files/directories ensure permissions, owner, checksum
- Check/create links, files, directories
- Run shell commands (and use output)
- Check/start/stop/signal processes
- Clean /tmp and similar directories
- Many commands to edit text files
- Check resolver, domainname, timezone etc
- Classes defined on OS, kernel, time, date, hostname, domain, user commands, other rules

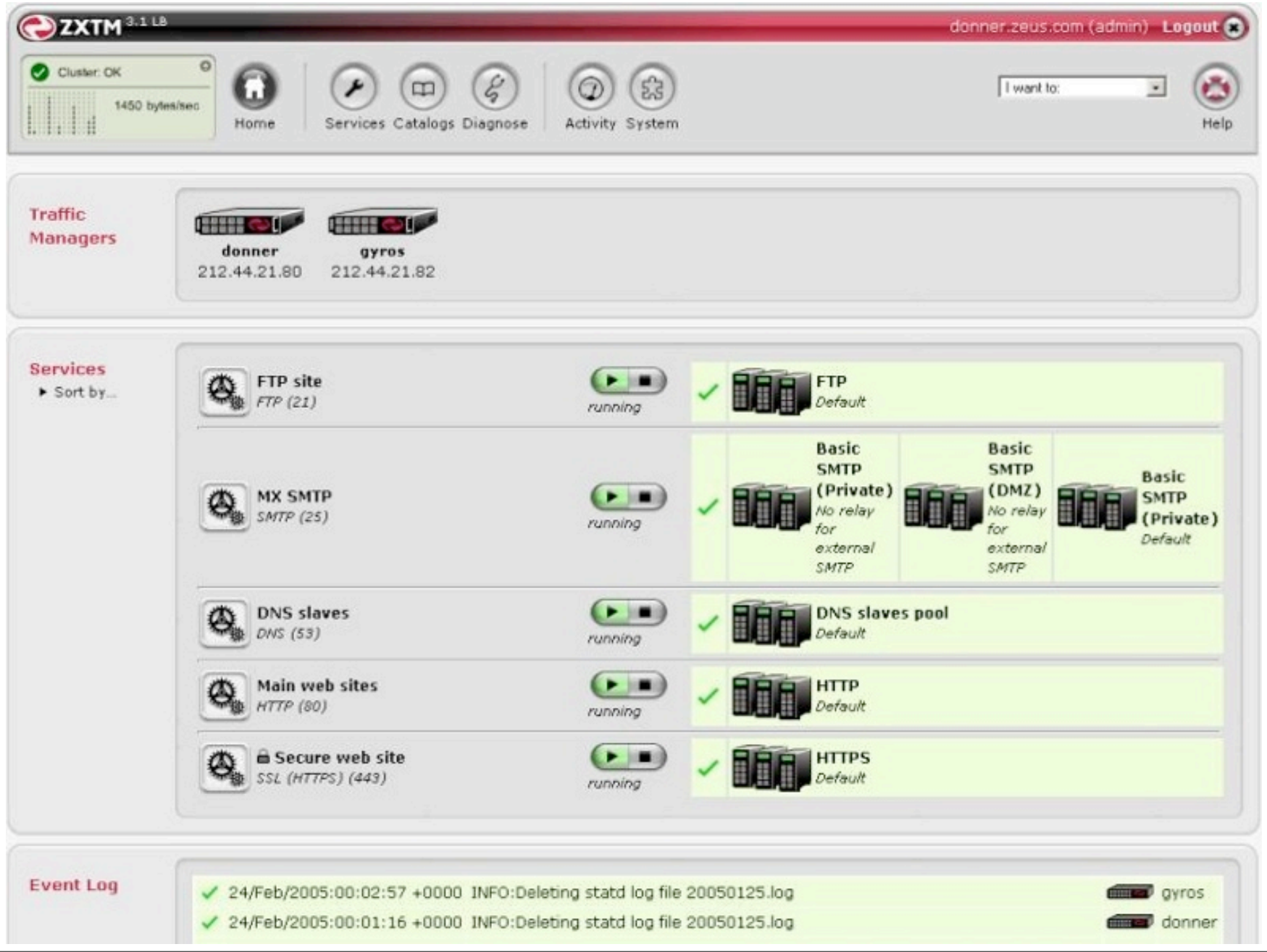
Is Cfengine the Silver Bullet?

- No! – but sure helps
- Cfengine also have limitations
- Bootstrapping is hard
- Unix centric, but with some Windows support
- Other projects aims at the same goal but with different methods
  - Radmind (Mac OS-X focused)
  - LCFG (Linux/Solaris focused)
  - Many windows (only) solutions (SMS)

Availability

- No single point of failure
- Loadbalancing
- Clustering
- Redundant Net, firewall, switches, routers
- Multiple ISP's (BGP, AS-numbers etc)
- Replicated storage
- UPS and generators
- Redundant cooling
- Multiple server rooms with redundant setup

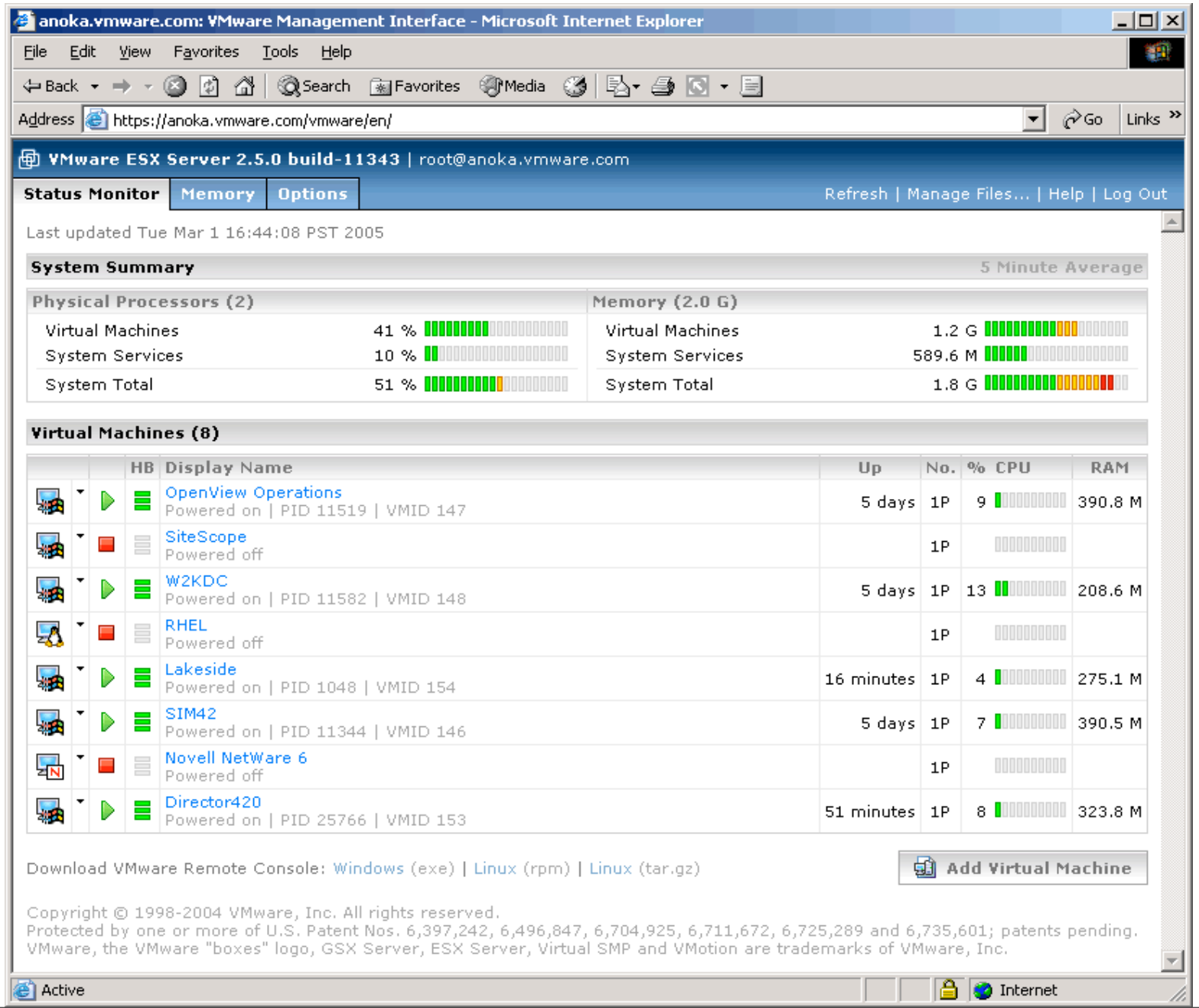
Zeus ZXTM Screenshot



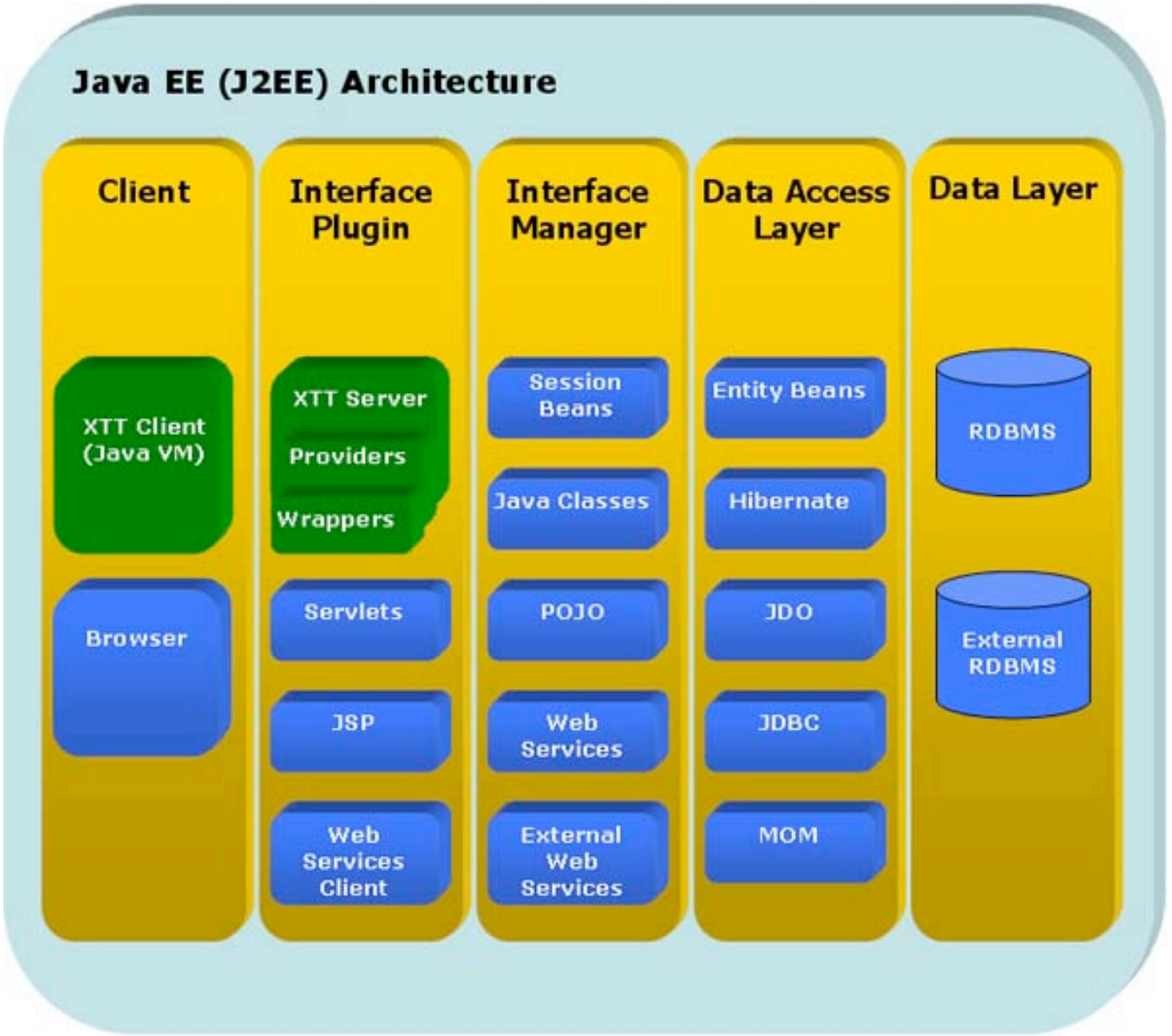
Virtualization

- VMWare ESX and Virtual Center
- Hardware is just a pool of resources
- Built-in intelligence on hardware utilization
- Finally a common (virtual) hardware platform?
- Create new servers by cloning
- Virtual network components
- VMWare Marketplace for standard components

VMWare ESX Console



SOA - Service Oriented Architecture

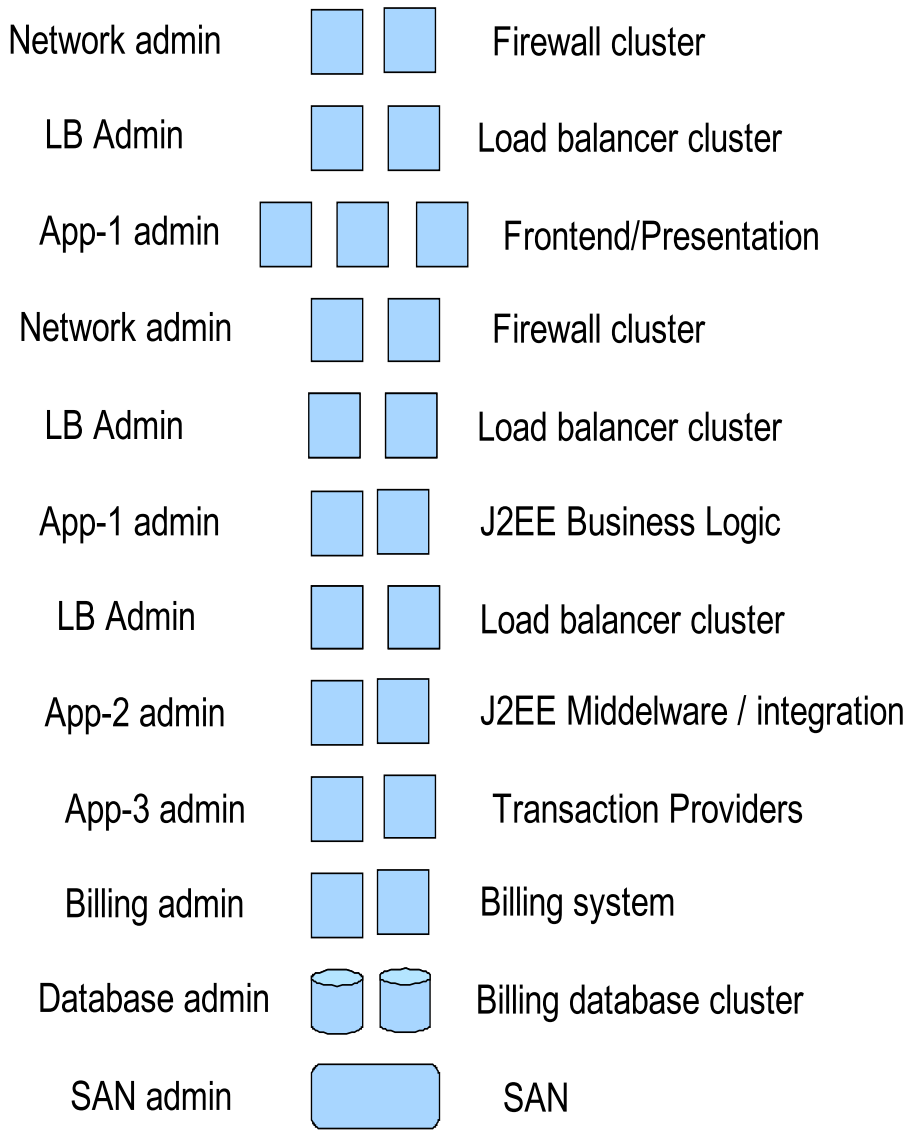


The Future?

- Hardware just a farm of resources
- Heavily virtualization
- SOA – Service Oriented Architecture
- Simpler to write frontend apps, but more complex backend layers
- System administrators needs to have some programming skills and knowledge of SOAP
- Diversion between “system administration” and “application administration”
- Increased need for infrastructure architects

Typical Telco Selfservice platform

- Many roles
- Many people
- Many layers
- Many servers
- Many data
- Many level of knowledge
- Debugging difficult



Questions?

Links

- http://vmware.com
- http://usenix.org (And LISA)
- http://cfengine.org

Exercises

- Study cfengine documentation – perhaps deploy on your own computer
- Study VMWare Server - free download!