2009-08-12

KNA 8:15
KNA

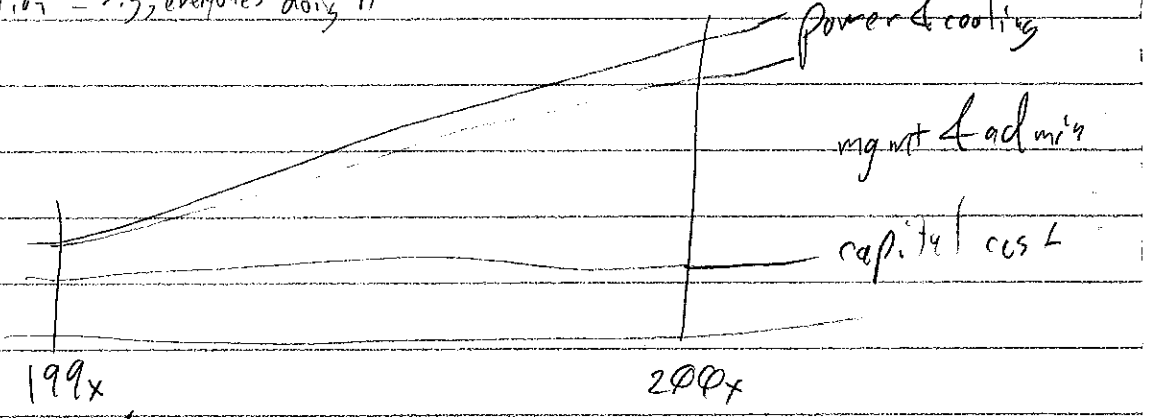
keynote KR

1/15

NF19:15

virtualization - big, everyones doing it

NF1 300s




Watts / Square Inch

Wolfe
Cooktop

x86 CPU

120

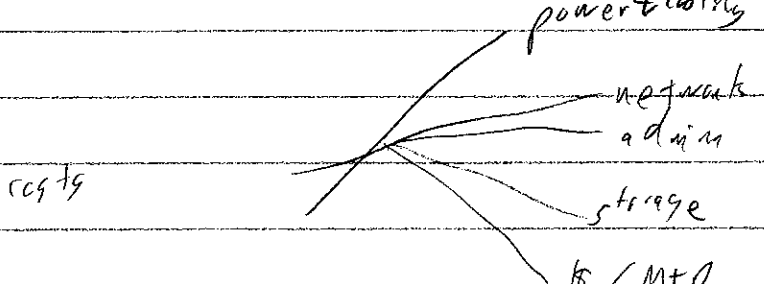
42

Legacy - Thermal management was an afterthought

PUE ~ 2.0 (1W to cool 1W of power used)

~~Alternator~~
~~33°~~

servers
AC conversion
cooling




Modular DC Design
enclosure power distribution
power supplies
CPU power

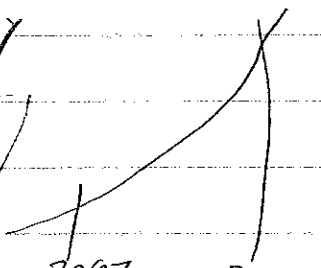
} complex chain in power efficiency

Net-Net changes PUE
from 2.0+ to 1.25 or less

and extreme scale-out
blades/racks are high growth areas

35/50/15 tower/rack/blade

Acquisition cost always important
Energy consumption has become a priority




Intelligent use of real estate (memory controllers on die, etc.) comm., crypto, ...
Si compaction 65nm ... 32nm ...

Memory trends ... core count ↑

communications radius effect
10Gbit 40 Gbit - 4 parallel cables

servers per rack continues to increase
≈ Petabyte storage/rack by 2010-11
packaging, fabric - will probably mostly be 10G Ethernet

thin provisioning & deduplication
PODular Data Center (containerized)
Virtualization - downsides - adds a layer of infrastructure/management
Need to have a strategy, metrics and a roadmap
need to add converged VM and physical management
Draconian standardization
Vendor Simplification
Almost always, fewer is better
once standardization has been in place for a full dev cycle, requests for variations become few and far between
Clouds - where are the applications? My data is where? standards?, cloud shared with competitor?, What about internal cloud?,

CA2 3000

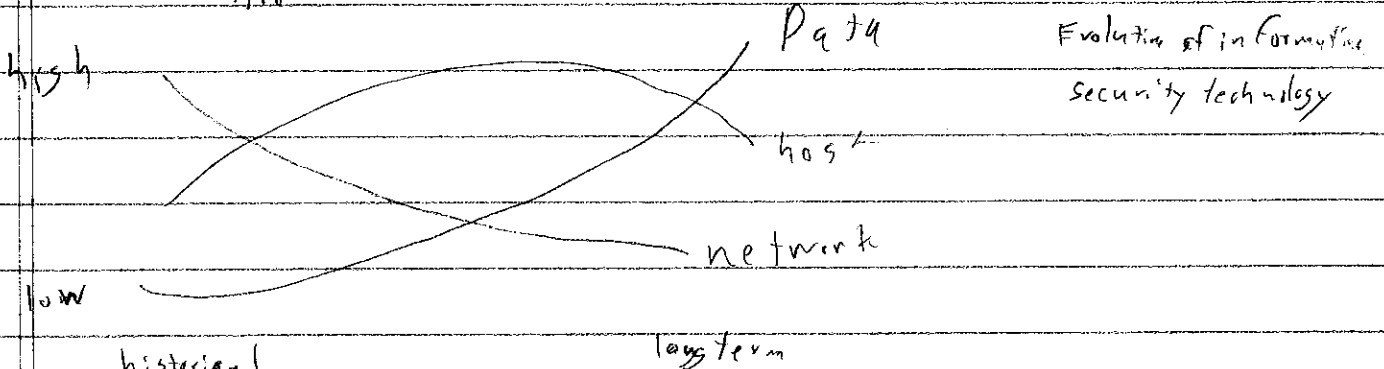
areas of most change - Firewall

- service/cloud provider
- overlay
- OS
- audit - prove firewall is/was there

Anti-Virus & network scanning/traffic analysis

Vulnerability Scanning ... permission, etc

Web Application Firewall




permission API for Cloud Vulnerability Scan

cloudsecurity.org

"A Security API for Cloud Stacks"

rational survivability.org

KN2 KR

$13,000 billed $6.00 refund vs. $800,000 server infrastructure election infrastructure; played for 13x, got 6x

SC6 3002

no PCI, SOX, etc. - not for business critical

Black Hat demonstrations on breaking cloud

Raging Wire - ~~Amazon~~ Strata Scale

NF3 3005

OPEX and CAPEX costs

space, power, cooling - when will you run out

utilization?

What is your datacenter energy bill

regulations that may apply, e.g. UK directive to consumers of electricity - top 20% must baseline...

in 2011 organizations will have to purchase $CO_2$ offsets

owning, operating, & disposing of IT - greening & costs data center and facilities

> 75% of IT shops have green IT plan in place or are considering it

for now green IT = efficient IT

despite down economy, outlook for green IT is positive

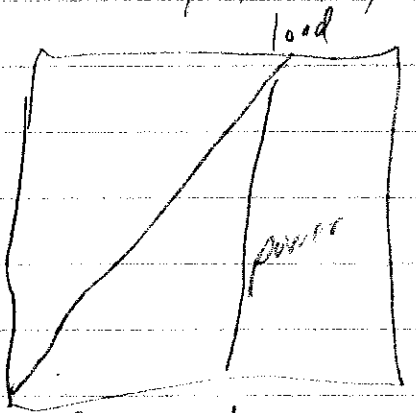
primary green motivator is cost reduction

60 Billion of US recovery into energy efficiency, etc,

2006 ≈ 2% of US energy consumption by data centers

2011 ≈ 7.5%

datacenters plagued by extremely low utilization




Standard Performance Evaluation Corporation

"Following the trail of toxic..."

Scope of green datacenter is much more than IT systems

e-waste becoming widely publicized concern (eg_60 Minutes_)

space, power, cooling - data centers are running out

facility, architecture, power & cooling, applications, IT systems

Technology assets, services, best practices

70% MOOSE maintaining, upgrading... - maintaining what one already has

30% investment/new/improved capabilities

greening reduces MOOSE

CAPEX - capital expenditure

energy conservation ~~[illegible]~~

...

consolidation

check for energy efficiency incentives (e.g. PG&E government.) ↗ e.g. (NCIAPP 1.4 million dollar rebate)

justify, and prioritize - measure baseline; run the numbers

Google (has a datacenter in Belgium that uses no chillers! thermostat to 80°F

google.com/corporate/green/datacenters

greenest awarded and positive publicity (e.g. Blue Cross/Blue Shield)

Sprint (TM) example - saved tens of millions of dollars (energy, capital, HR, license fees, etc.)

when thinking about green data center - take all inclusive approach

measure, power audit, where's it going, when will we run out?

ASHRAE says 80°F is acceptable

localize cooling to where it's needed most

get rid of dead applications, dead servers (20 to 30% typical)

policy - virtualization first

go to 10G Ethernet to facilitate virtualization

i.e. improve operational processes

CA4 30000

look for:
- speed of deployment
- ease of use
- scales seamlessly
- accessible anywhere
- low total cost of ownership
- customer success driven
- interoperability
- self-service
- solve core business need
- quick return on investment
- low switching cost
- seamless updates
- ease of integration
- completeness of product vs. competition
- strength/viability of company

beware of:
- inflexible / avoid
- single tenant data architecture
- heavy customization
- ...
- security risks - match requirements
- performance issues
- complex products
- hard to use
- requires staff overhead to manage
- unplanned service downtime
- cost to scale
- islands - integration w. other systems
- required on-premises hardware/software

application performance?

requirements
monitor realistic transactions
multiple transaction types
multi-node monitoring
easy to set-up/maintain
easy to troubleshoot performance anomalies
historical trending
integrate to existing monitoring
do one's homework - reference checks, social networking

look for

ease of use
no/limited IT environment
quality track record
self provisioning
interoperability
single-instance, multi-tenant architecture

look out for

complex/costly setup & customization
extended time-to value
security
availability - SLA?
scale/performance
single-tenant architecture

what's the SLA?

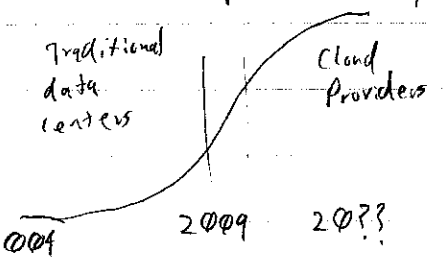
make sure purchase fits long-term company strategy
reference for track record
total cost of ownership
company viability
make sure company is customer success oriented

KN 3

KR
cloud, public, private, hybrid

KN 4

2008-08-13
"cloud computing" - way up in Google trends




Internet Growth
Massive Data
Moore's Law
— Perfect Storm fueling Cloud Computing

Natural evolution of web
websites
Applications SaaS
PaaS
IaaS

Internet scale demands have driven new application design patterns
Outgrowing traditional RDBS
"Wharehouse Scale" Machines - power & cooling major cost factors
Cloud - anyone can gain efficiencies
pay-as-you-go
scale up/down
Internal IT looks more like service providers
Service providers responding - vary to meet business needs regulatory requirements
diversity conflicts with standardization and automation
Separate applications from infrastructure
easily quantified cost model for resource allocation
Customers get resources from a nearly "infinite" pool of resources
Prediction: Specialization of Operating System
Application OS - just what's needed
more applications distributed as virtual machines
Hardening of VM containers: Immutable containers
built in tools and auditing
Sun Cloud - Virtual Data Center
Explosion of Apps (eg. 65,000 iphone apps, 1.5 billion downloads)
50,000 apps - Google app engine
Government turning to cloud - eg. GSA cloud portal
World Economic Forum - Project to study impact of cloud computing
some countries leap past building datacenters
Applications will increasingly be responsible for self-provisioning

51

IDS won't help if basic security isn't done
keep up on patches and IDS patches
scan and audit systems regularly
being proactive is better than reactive
IDS is
detects and logs scans, malicious activity

IDS
host
network

Why IDS?
connected to Internet - subject to attacks
80 to 90% of attacks originate internally
IDS may be required for SOX or regulatory reasons

How IDS works
NIDS - network port or mirrored tap ("spanning" (Cisco))
↓ filter/preprocessor
↓ IDS engine
↓ log/report/monitor/alarm

HIPS → IDS engine
network
logs
system info. (ps, etc.) → IDS engine

rule based IDS
anomaly based IDS
IDS blades - eg. Cisco blades in Catalyst Switches
IDS issues/problems
switches - require port mirroring
encryption - NIDS cannot decode
busy networks - packets may be dropped
noise generators
false positives
false negatives
IDS requires care and feeding

Advanced intrusion detection

Intrusion Prevention
adherence to basic security
restrictive configurations
layered security

Intrusion Response
network node shunning/containment
TCP Reset packets - session sniping
the human factor

Snort NIDS
leading open source NIPS
stateful real-time traffic analysis and packet logging
mature, full-featured, extensible
rule based
some anomoly detection
packet sniffer, logger, NIDS mode
supports many plugins
can call external programs
log to any ODBC DB
Oinkmaster, IDScenter, Snort Center - management
Snort_Inline - IPS

Prelude
hybrid IDS
modular
can use Snort rulesets
...

HIDS - Tripwire AIDE Samhain
host/file based ? HIDS/FIDS

CVS based approach - http://

Linux IPS (LIDS), grsecurity, SELinux/LSM (IPS)

BASE Basic Analysis and Security Engine

Swatch and Logcheck - not really IDS, but useful related areas

PSAD port scan attack detector

OSSIM Open Source Security Info Management

Commercial IDS

- Cisco
- IBM (ISS)
- Symantec
- Sourcefire
- Siemens / Enterasys

Internet IDS Resources

- securityfocus.com
- linuxsecurity.com

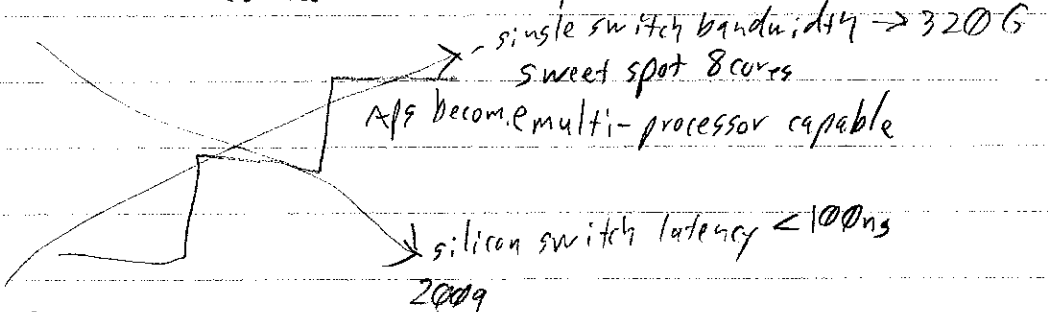
---

CI6

boot time agility
run time agility

- size of one's convenience
- # cores
- RAM
- ↓ performance

iterative testing to design optimal VM in cloud for given application
- fastest
- most cost effective




- generate cloud systems larger than single physical server

"Agility" firmware under OS, between OS and hardware resources

---

KN5

Implementing Lean Software Development

Smalltalk

"don't find out what the patents are" - re. IT policy

no IP in sandwich shop/deli

11/15

IT as dely
Personal Computing
Decision Support
End-User computing
Business Intelligence
End-User Development
The Gutenberg Galaxy (book)
"free" software ——— IT dept, server? - not free
"hit brick wall
cost
"we don't do that"
"they're going to get into trouble"
"it would become business critical" - then IT would have to support it
SOX?
cannot fight the beurocracy - must "embrace" it
Operating Model - Roles
Solution analysts - talk to users - understand problems
Infrastructure developers
Solution educators
Process Model
ticket system instead of project model
motivation - number of changes per person deployed to production IT KPI
Operating Model
tickets
customers write own documentation
library of screencasts
...
Enterprise Service Bus
TIBCO, Active MQ
Infrastructure
External hosted applications
...
Issues
Access to APIs
No dynamic SQL
Automated Deployments

SC12 Unified Communications over IP

- web
- mail
- IM
- VoIP

UC o IP support

- DNS
- LDAP
- ENUM

communication addresses in UC o IP

- mail
- Voice / video
- IM
- Web

→ email address

DNS is essential for UC o IP

internal DNS (private)

external DNS (public)

How are communications handled?

synchronous (real-time related)

separate clients – loosely coupled (needn't be concurrent/synchronous)

Steps

calling (email)

find domain SIP

deliver call to (email) on SIP

no SIP device, but alias, convert/follow

---

CI7

NIST's cloud definition

NaaS – Network as a Service – original "cloud"

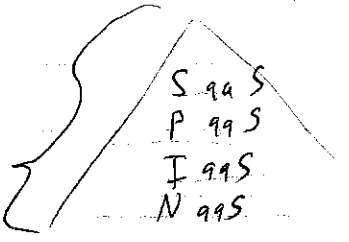
IaaS Infrastructure

PaaS Platform

SaaS Software

Cloud Stack_ higher layers built on lower layers

higher abstractions include lower ones



# Moving Target

dynamic marketplace
semantics matter

players are making moves – adding offerings, coalescing offerings

direction is flexibility and standardization

Cloud Security is... technology + process + due diligence – core issue is trust

Technology: Defense in Depth

similar to security in outsourcing

many of the issues that apply to non-cloud apply to cloud

some unique to cloud: administration and shared resources

Trust

reputation matters

approach: ~~trust~~ but verify

weaknesses don't have to be fatal

IAAS

challenges

virtualization issues: VM "breakout", hypervisor, log flooding, etc.

shared infrastructure issues: storage, CPU, RAM: clean it before de-allocating it

depend on outsourced datacenter practices ~~don't overallocate resources~~

benefits

Virtualization

machine-level instrumentation

simplified incident response, forensics, recovery

shared infrastructure benefits

~~shared industrial strength instrumentation~~

correlate security information across customers

relatively simple to understand

~~IaaS is much like any other outsourced data center~~

case study: Enterprise Cloud: Terremark's offering

...

PaaS challenges

Complex, powerful APIs

Security mechanisms are "secret sauce"

Applications might still be insecure

PaaS security benefits
centrally managed platform
more and better expertese about the platform
many non-cloud measures translate directly
PaaS: case study: Google Apps
...

SaaS: security challenges
even more sharn with PaaS - trust is key
vendors are tight lipped
no opportunity to work around weaknesses (by customer - controlled by vendor)
SaaS advantages
Centrally managed
attention to the application
original concept is simple
SaaS: case study: Salesforce.com

---

S4

Vulnerability databases - zero regulation
post unverified reports
no attempt to contact vendor
very slow to correct
rely on scare tactics
reports share too little, or too much info
Govt. is involved, and is an offender
no self regulation in the industry
who keeps them honest

Secunia
security focus
National Vulnerability database
researchers may contact vendor
vendors want to be first to publish, despite...
Joomla 1.5.5 Password Reset vulnerability
↘ disclosed 0 day
15 minutes to fix, about 3 hours to release, 100K sites compromised before release

Don't play fair
don't validate, can damage reputations
little PB contact info provided
when they do remove it's a private retraction
Security Focus
SQL injection attack - listed but no vulnerability
contacted, haven't ~~fixed~~ fixed posting
Not just security companies
Media companies
Content posted with little or no verification
e.g. Computer Weekly published "vulnerability" that doesn't exist
media
"Will say anything for Publicity
Information Week - e.g. false "vulnerability" report
- article still on Information Week
Disclosures ~~have~~ have too much or too little
- need working exploit?
- need enough info to identify, etc.
how does volunteer project defend itself
not condoning, but some do...
imageshack - eliminate vulnerability disclosures
to succeed - fight back
Publicly disclose
reported: there are sites that report on accuracy & hoaxes
of reports on various DB sites