goto; conference aarhus

Globally Distributed Cloud Applications

Adrian Cockcroft
@adrianco

Netflix Inc.

INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

gotocon.com

Abstract

- Netflix on Cloud – What, Why and When
- Globally Distributed Availability Model
- Open Source Components
- Build Your Own PaaS

What Netflix Did

- Moved to SaaS
  - Corporate IT – OneLogin, Workday, Box, Evernote…
  - Tools – Pagerduty, AppDynamics, Elastic MapReduce
- Built our own PaaS
  - Customized to make our developers productive
  - When we started, we had little choice
- Moved incremental capacity to IaaS
  - No new datacenter space since 2008 as we grew
  - Moved our streaming apps to the cloud

Why Use Cloud?

Get stuck with wrong config

Wait

Wait

File tickets

Ask permission

Wait

Wait

Wait

Things we don't do

Wait

Run out of space/power

Plan capacity in advance

Have meetings with IT

Wait

Keeping up with Developer Trends

	In production at Netflix
• Big Data/Hadoop	2009
• AWS Cloud	2009
• Application Performance Management	2010
• Integrated DevOps Practices	2010
• Continuous Integration/Delivery	2010
• NoSQL	2010
• Platform as a Service; Fine grain SOA	2010
• Social coding, open development/github	2011

AWS specific feature dependence….

Portability vs. Functionality

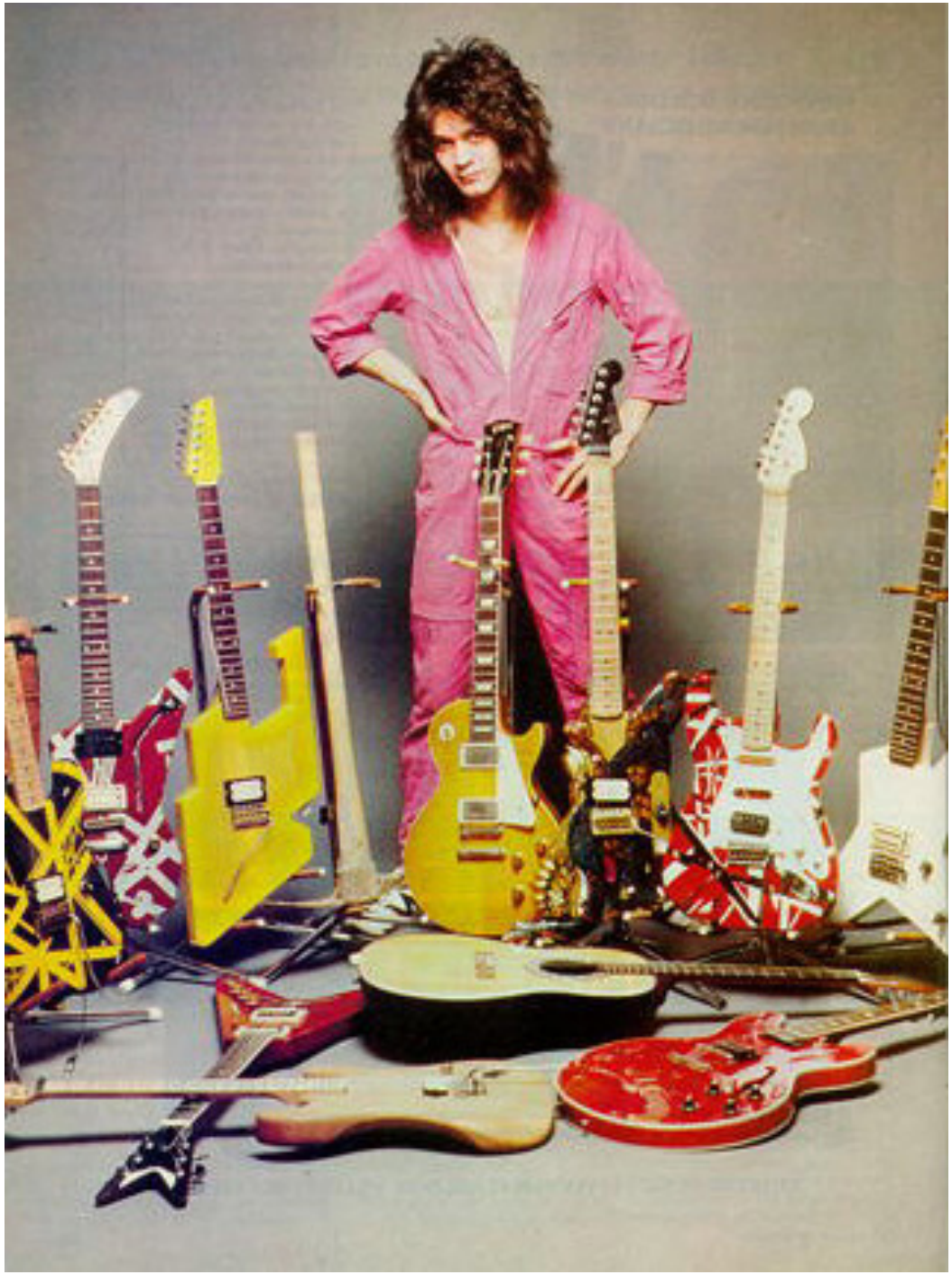
- Portability – the Operations focus
  - Avoid vendor lock-in
  - Support datacenter based use cases
  - Possible operations cost savings

- Functionality – the Developer focus
  - Less complex test and debug, one mature supplier
  - Faster time to market for your products
  - Possible developer cost savings

Functional PaaS

- IaaS base - all the features of AWS
  - Very large scale, mature, global, evolving rapidly
  - ELB, Autoscale, VPC, SQS, EIP, EMR, etc, etc.
  - Large files (TB) and multipart writes in S3

- Functional PaaS – Netflix added features
  - Very large scale, mature, flexible, customizable
  - Asgard console, Monkeys, Big data tools
  - Cassandra/Zookeeper data store automation



Don't let the roadie write the set list!

(yes you do need all those guitars on tour…)

Developers choose Functional over Portable

NETFLIX

Freedom and Responsibility

- Developers leverage cloud to get freedom
  - Agility of a single organization, no silos
- But now developers are responsible
  - For compliance, performance, availability etc.

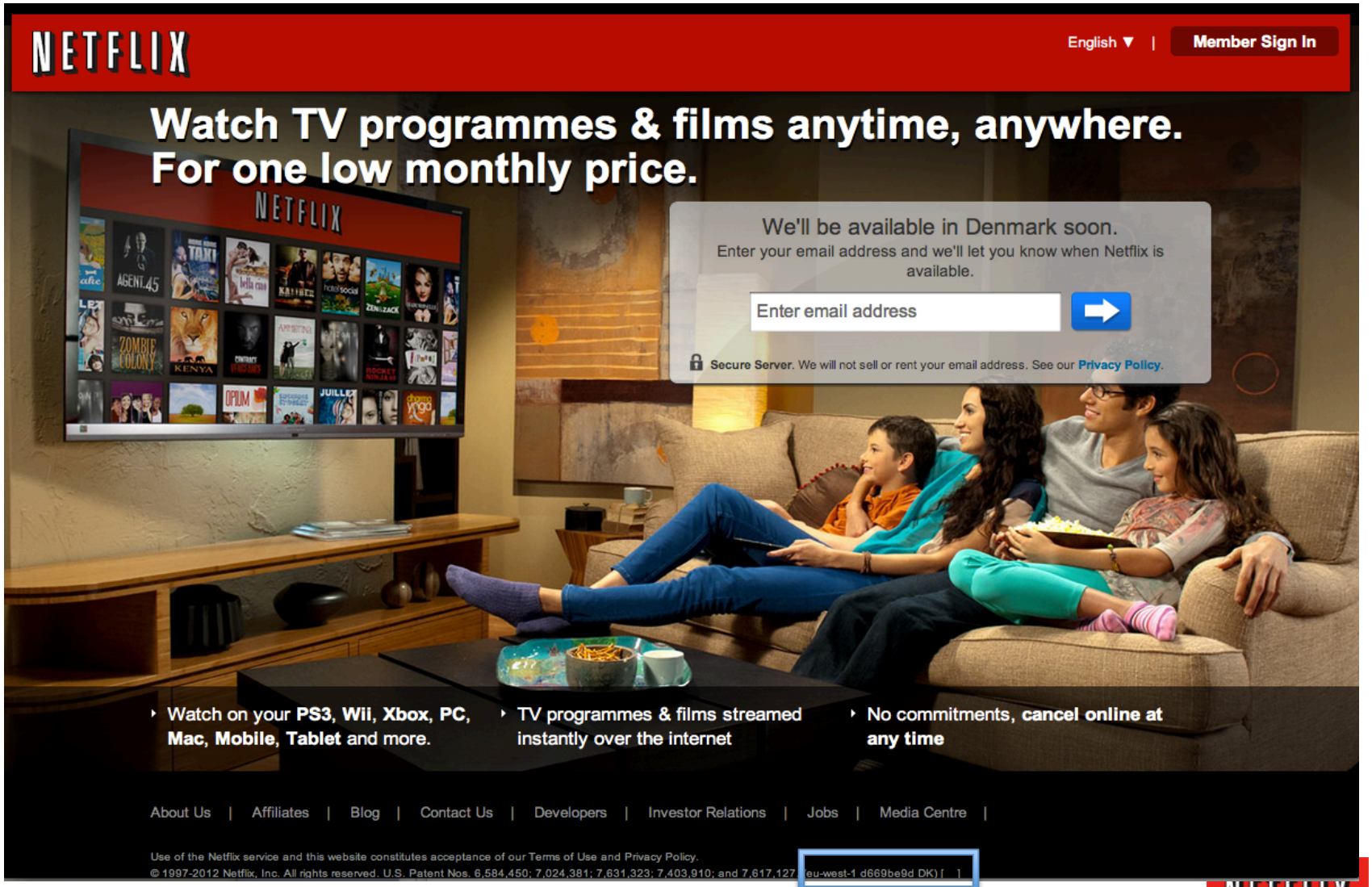
"As far as my rehab is concerned, it is within my ability to change and change for the better - Eddie Van Halen"

NETFLIX

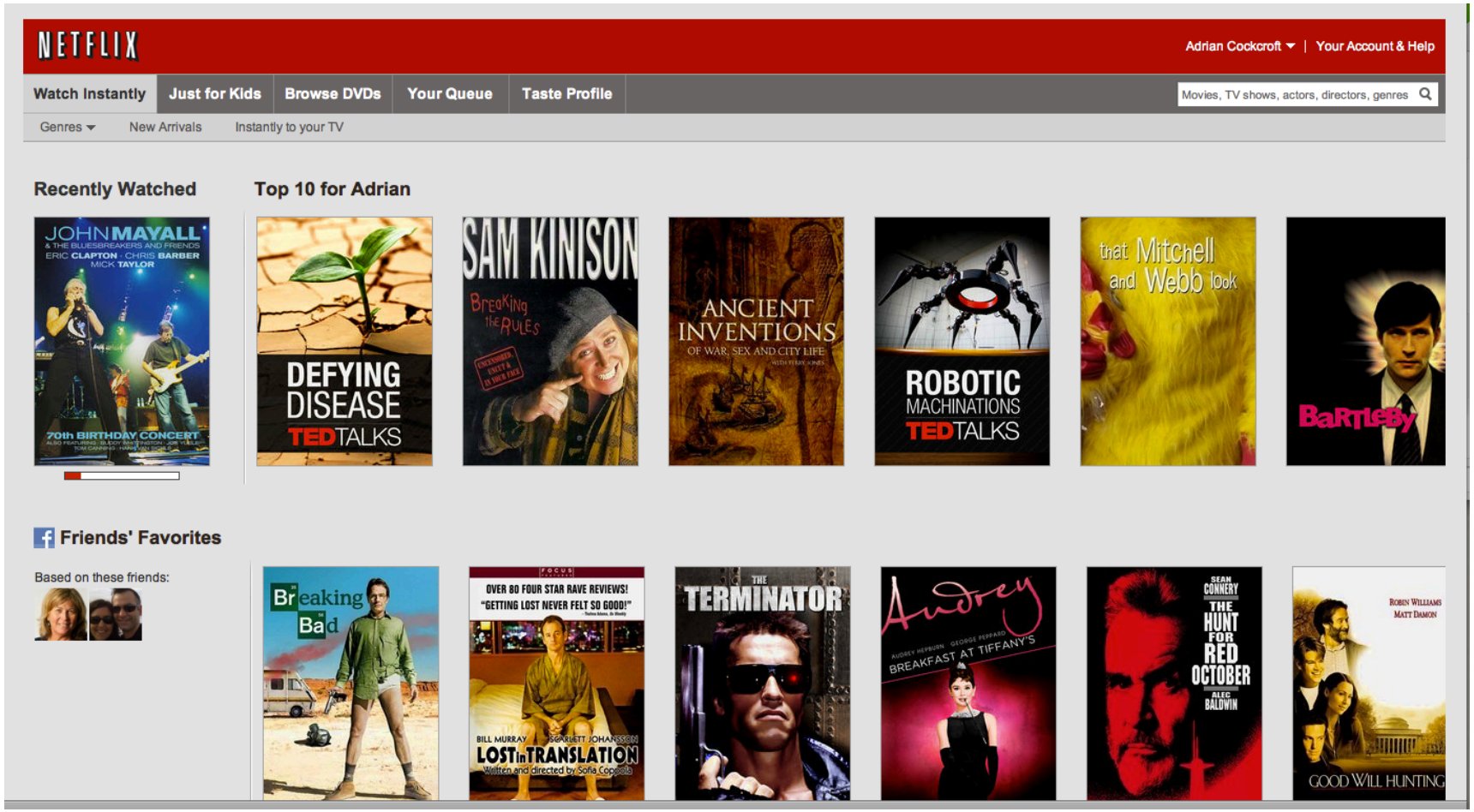
The Netflix Streaming Service

Coming soon to Denmark (and Norway, Sweden and Finland)

www.netflix.com in DK



Member Web Site



NETFLIX

Content Delivery Service

Distributed storage nodes controlled by Netflix cloud services

NETFLIX

Open Connect

- Overview
- FAQ
- Peering Information
- > Hardware Design
- Software Design
- Deployment Guide
- ISP Inquiry

Open Connect Appliance Hardware

Objectives

When designing the Open Connect Appliance Hardware, we focused on these fundamental design goals:

- Very high storage density without sacrificing space and power efficiency. Our target was fitting 100 terabytes into a 4u chassis that is less than 2' deep.
- High throughput: 10 Gbps throughput via an optical network connection.
- Very low field maintenance: the appliance must tolerate a variety of hardware failures including hard drives, network optics, and power supply units.
- Simple racking and installation. Front mounted power and network ports are the only things to connect at install time.

Open Connect Appliances are servers based on commodity PC components (similar to the model used by all large scale content delivery networks). We were influenced by the excellent write-ups from the Backblaze team, and use a custom chassis due to a lack of ready made options for a compact unit.

To achieve over 100 TB of storage, spinning hard drives provide the highest affordable density, in particular 36 3TB SATA units. The hard drives are not hot swappable, as we wish to avoid the operational burden of field service. For lower power utilization and simpler sourcing we select commodity units from two vendors and use software to manage failure modes and avoid field replacement. Dead drives reduce the total storage available for the system, but don't take it offline. We also add 1 TB of flash storage (2 solid state drives) for system files, logs and popular content. To augment the motherboard attached controller, we use two 16 port LSI SAS controller cards that connect directly to the SATA drives. This avoids I/O bottlenecks of SATA multipliers or SAS expanders, and also reduces system complexity.

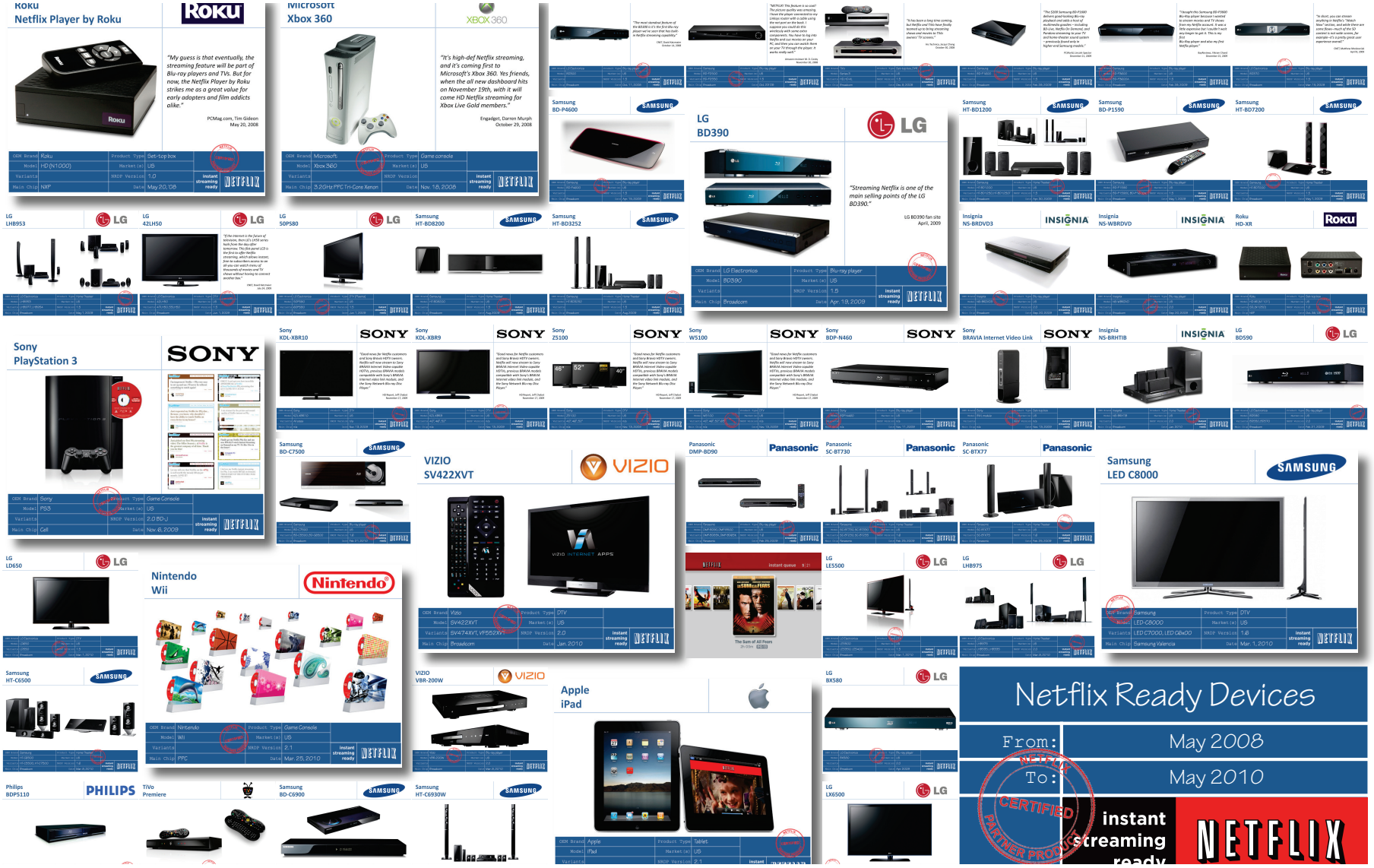
From a compute point of view, the system has modest requirements moving bits from the storage to network packets on the interface. To reduce the power usage and hence also cooling requirement (which in turn reduces vibration from case fans) we use a single low power 4 core Intel Sandy Bridge CPU on a small form factor Supermicro mATX board with the full 32 GB of RAM installed.

We use redundant, hot swappable power supply units that have interchangeable AC and DC options for maximum installation flexibility. Zippy reversed the fan rotation of the units to allow mounting at the front of the case, and thus allow network and power connects to be positioned here.

The network card has two 10 Gbps modules, which can power a variety of SR and LR optic modules, for installation flexibility and scalable interconnection.

NETFLIX

Streaming Device API

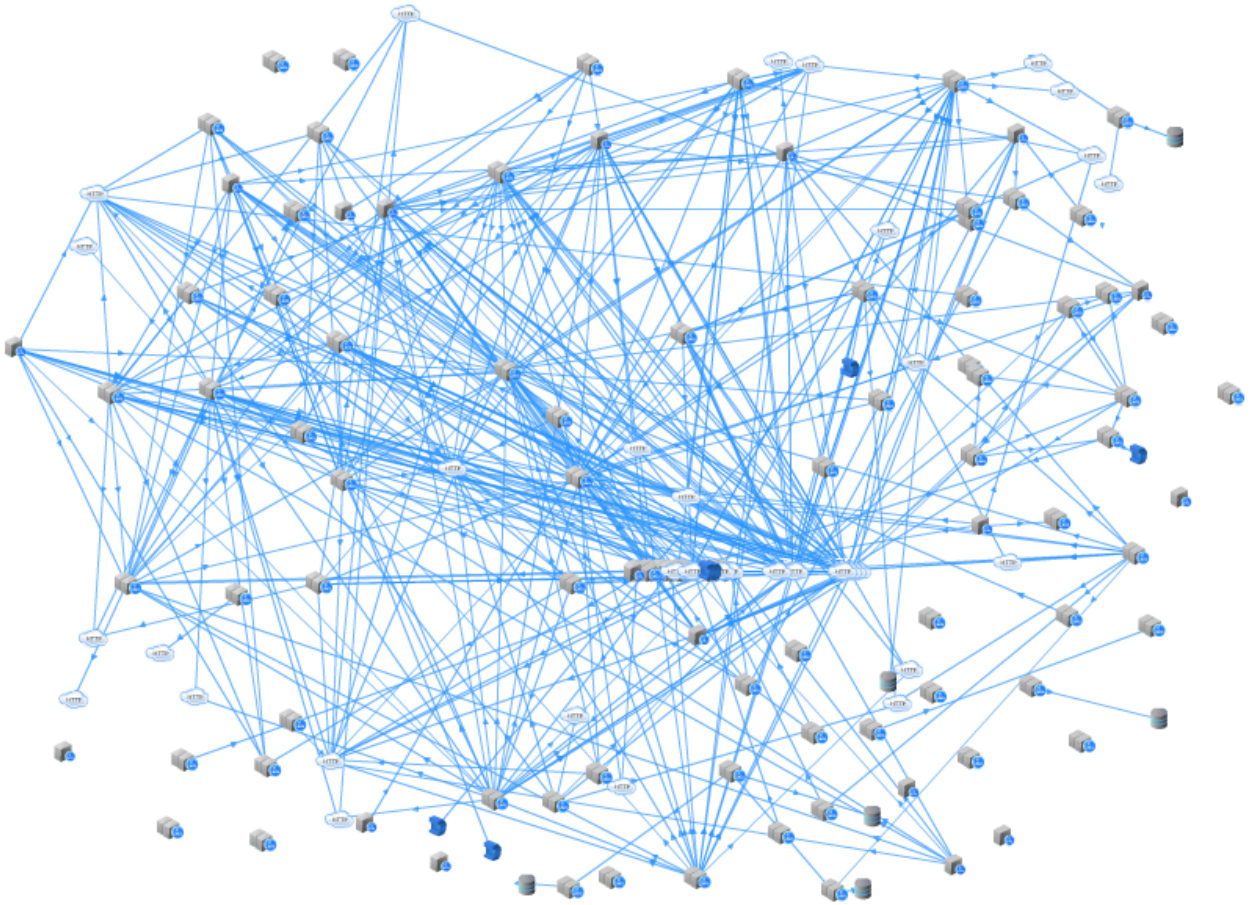


Major Front End Services

- Non-member Web Site www.netflix.com
  - Marketing driven, sign up flow, SOX/PCI scope
- Member Web Site movies.netflix.com
  - Personalization driven
- CDNs for delivering bulk video/audio
  - Netflix CDN: openconnect.netflix.com
- API for external and device user interfaces
  - Mostly private APIs, limited public API docs at developer.netflix.com
- API for controlling video playback
  - DRM, QoS management, Bookmarks

Component Services

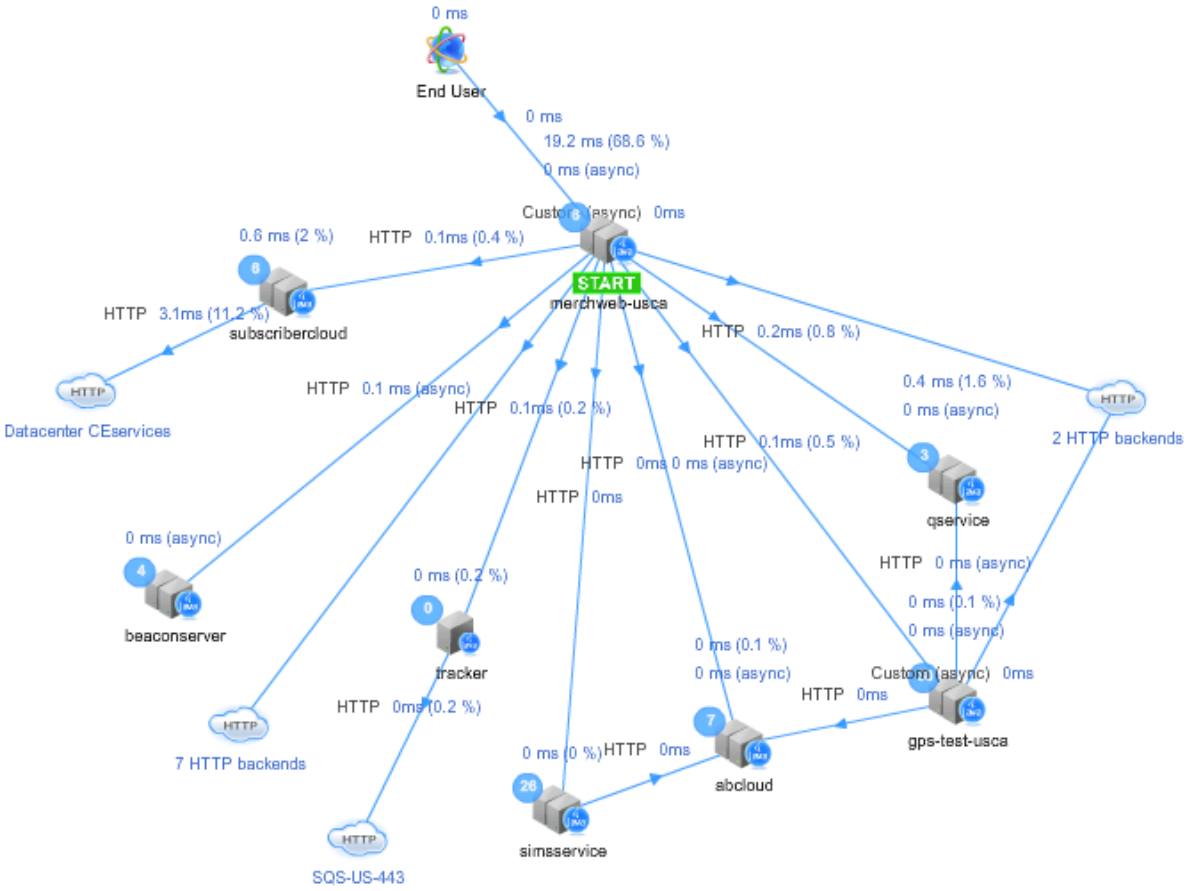
(Simplified view using AppDynamics)



NETFLIX

Web Server Dependencies Flow

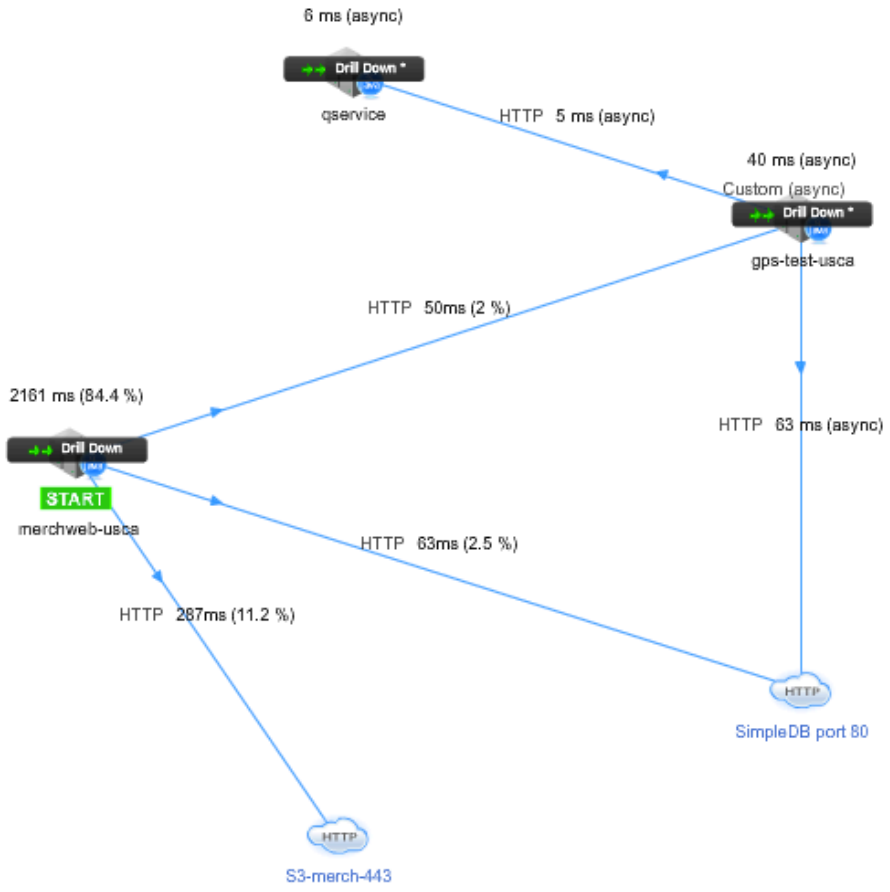
(zooming in to one business transaction in test account)



NETFLIX

One Request Snapshot

(captured because it was unusually slow)



NETFLIX

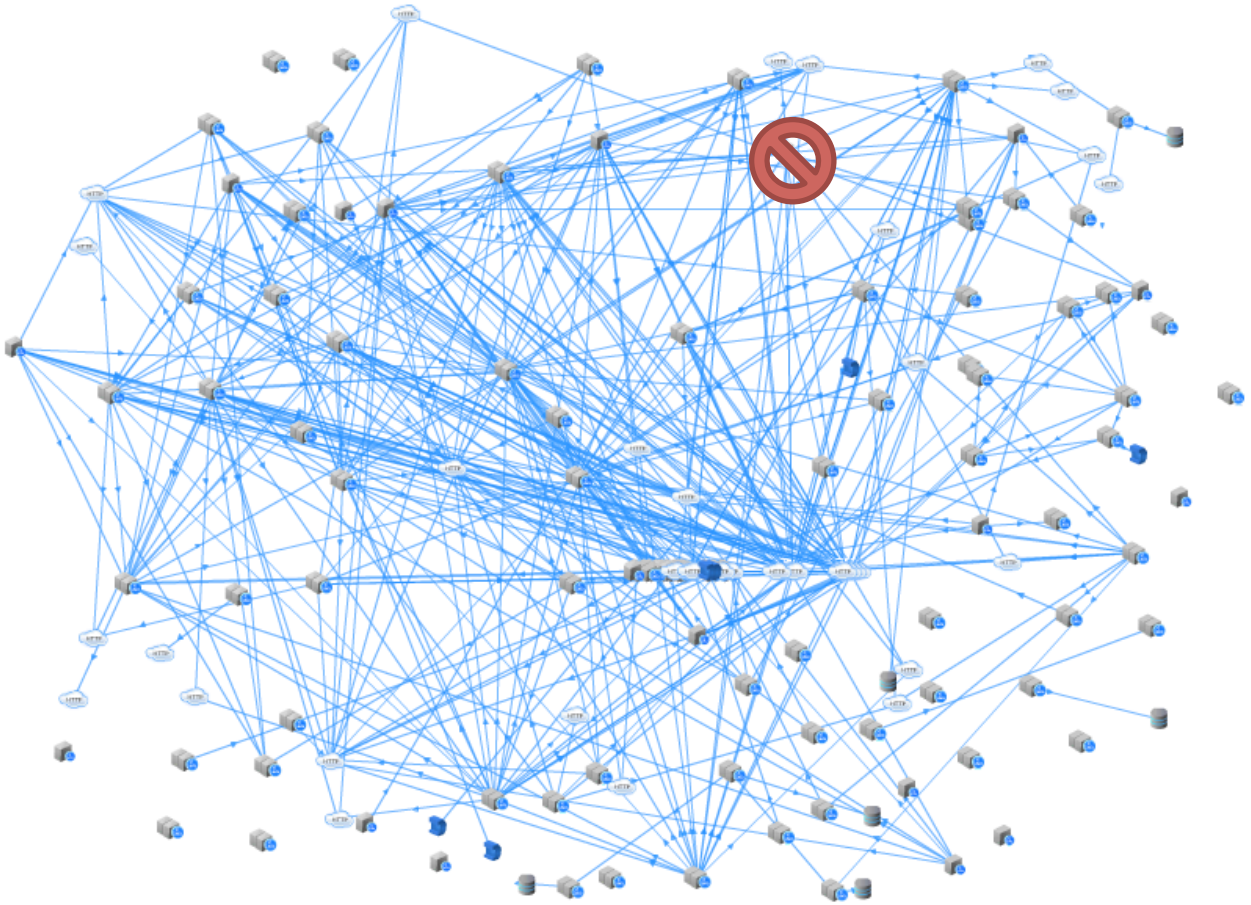
Current Architectural Patterns for Availability

- Isolated Services
  - Resilient Business logic
- Three Balanced Availability Zones
  - Resilient to Infrastructure outage
- Triple Replicated Persistence
  - Durable distributed Storage
- Isolated Regions
  - US and EU don't take each other down

NETFLIX

Isolated Services

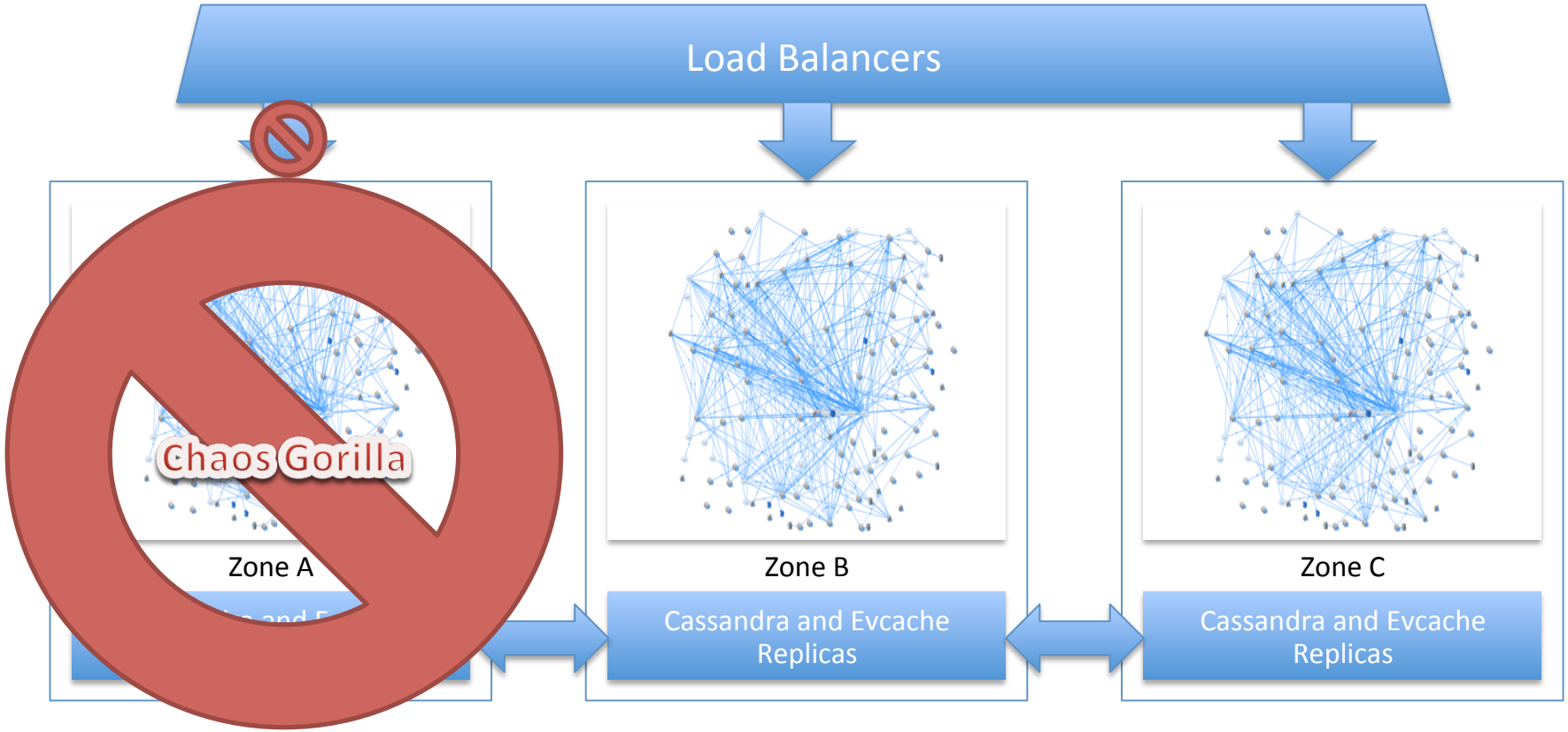
Test With Chaos Monkey, Latency Monkey



NETFLIX

Three Balanced Availability Zones

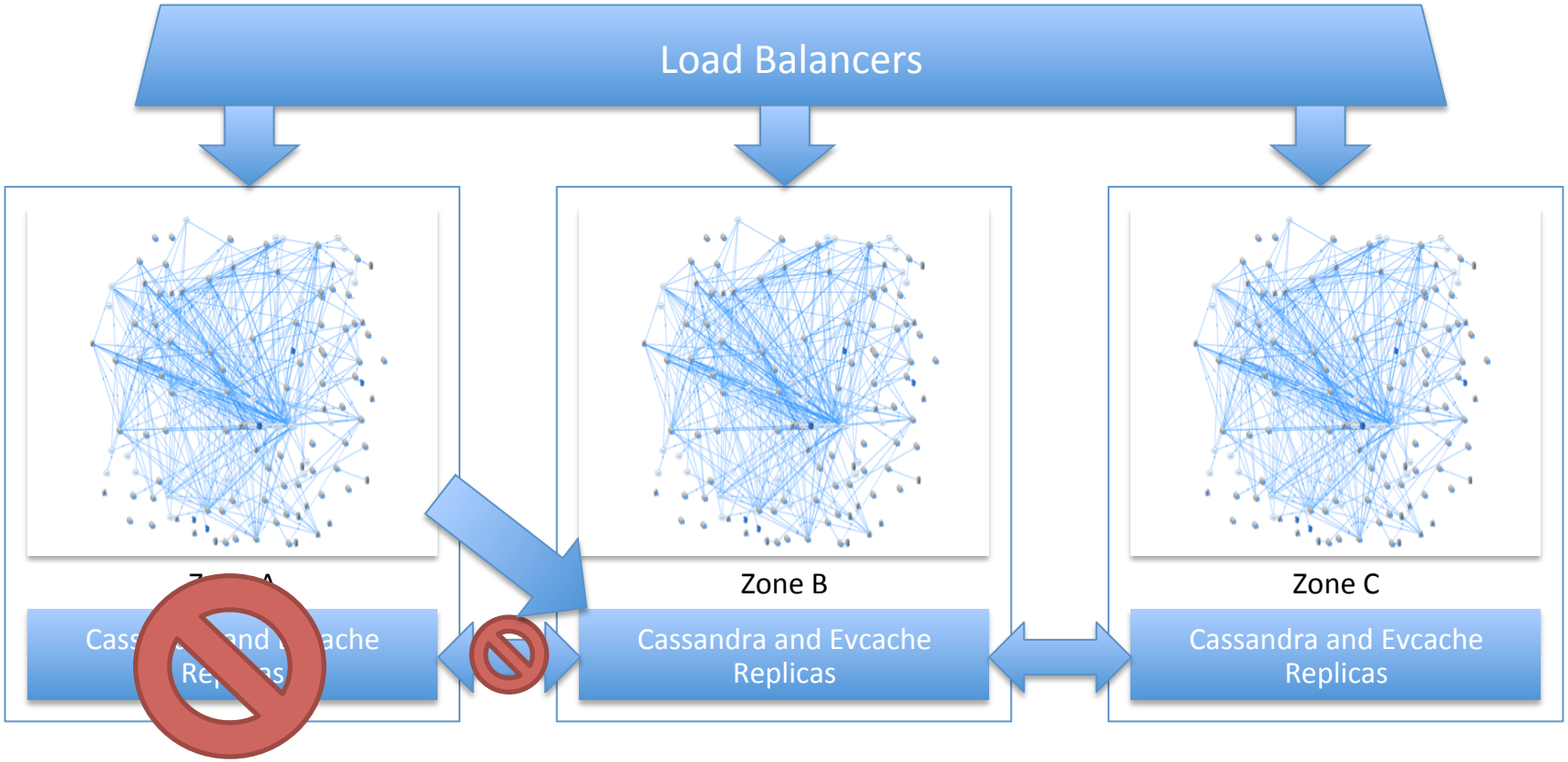
Test with Chaos Gorilla



NETFLIX

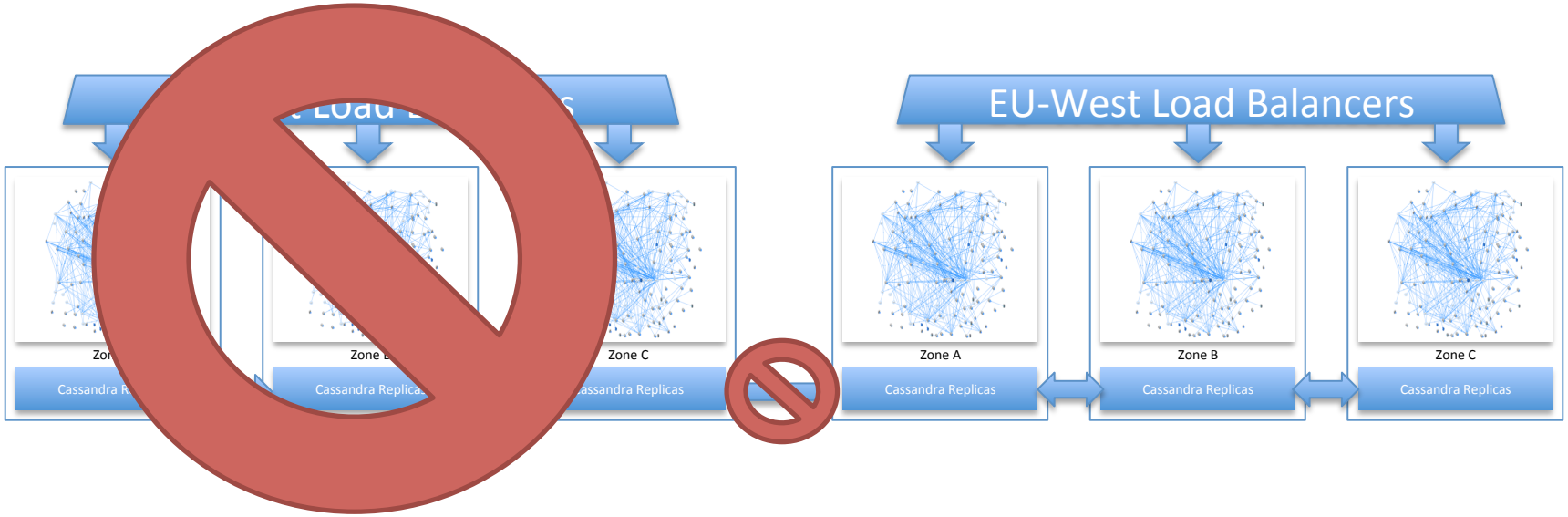
Triple Replicated Persistence

Cassandra maintenance drops individual replicas



NETFLIX

Isolated Regions



NETFLIX

Failure Modes and Effects

Failure Mode	Probability	Mitigation Plan
Application Failure	High	Automatic degraded response
AWS Region Failure	Low	Wait for region to recover
AWS Zone Failure	Medium	Continue to run on 2 out of 3 zones
Datacenter Failure	Medium	Migrate more functions to cloud
Data store failure	Low	Restore from S3 backups
S3 failure	Low	Restore from remote archive

NETFLIX

Netflix Deployed on AWS

2009	2009	2010	2010	2010	2011
Content	Logs	Play	WWW	API	CS
Content Management	S3 Terabytes	DRM	Sign-Up	Metadata	International CS lookup
EC2 Encoding	EMR	CDN routing	Search	Device Config	Diagnostics & Actions
S3 Petabytes	Hive & Pig	Bookmarks	Movie Choosing	TV Movie Choosing	Customer Call Log
	Business Intelligence	Logging	Ratings	Social Facebook	CS Analytics
	hadoop	Cassandra	MySQL	Cassandra	Cassandra

CDNs
ISPs
Terabits
Customers

NETFLIX

Cloud Architecture Patterns

Where do we start?

Datacenter to Cloud Transition Goals

- Faster
  - **Lower latency** than the equivalent datacenter web pages and API calls
  - Measured as mean and 99th percentile
  - For both first hit (e.g. home page) and in-session hits for the same user
- Scalable
  - **Avoid needing any more datacenter capacity** as subscriber count increases
  - No central vertically scaled databases
  - Leverage AWS elastic capacity effectively
- Available
  - Substantially **higher robustness and availability** than datacenter services
  - Leverage multiple AWS availability zones
  - No scheduled down time, no central database schema to change
- Productive
  - Optimize **agility** of a large development team with automation and tools
  - Leave behind complex tangled datacenter code base (~8 year old architecture)
  - Enforce clean layered interfaces and re-usable components

Netflix Datacenter vs. Cloud Arch

Anti-Architecture

Central SQL Database	Distributed Key/Value NoSQL
Sticky In-Memory Session	Shared Memcached Session
Chatty Protocols	Latency Tolerant Protocols
Tangled Service Interfaces	Layered Service Interfaces
Instrumented Code	Instrumented Service Patterns
Fat Complex Objects	Lightweight Serializable Objects
Components as Jar Files	Components as Services

NETFLIX

Availability and Resilience

Chaos Monkey

http://techblog.netflix.com/2012/07/chaos-monkey-released-into-wild.html

- Computers (Datacenter or AWS) randomly die
  - Fact of life, but too infrequent to test resiliency
- Test to make sure systems are resilient
  - Allow any instance to fail without customer impact
- Chaos Monkey hours
  - Monday-Friday 9am-3pm random instance kill
- Application configuration option
  - Apps now have to opt-out from Chaos Monkey

NETFLIX

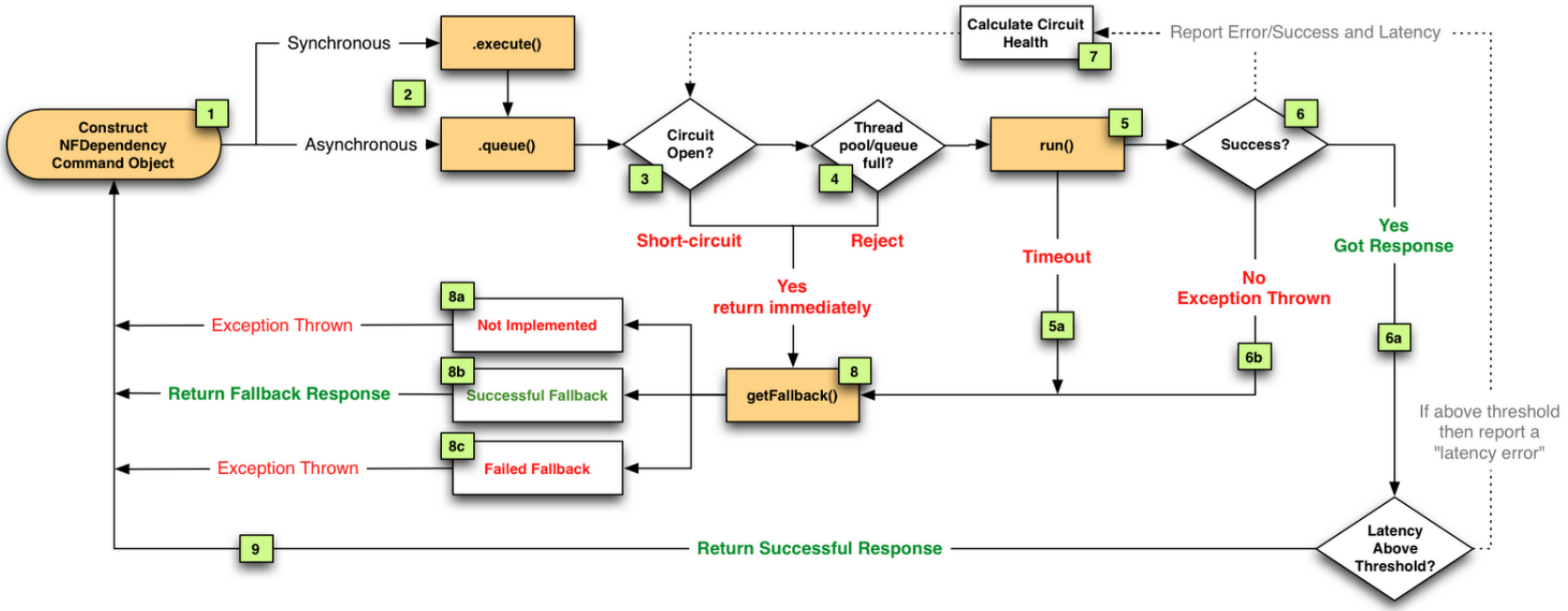
Responsibility and Experience

- Make developers responsible for failures
  - Then they learn and write code that doesn't fail
- Use Incident Reviews to find gaps to fix
  - Make sure its not about finding "who to blame"
- Keep timeouts short, fail fast
  - Don't let cascading timeouts stack up
- Make configuration options dynamic
  - You don't want to push code to tweak an option

NETFLIX

Resilient Design – Circuit Breakers

http://techblog.netflix.com/2012/02/fault-tolerance-in-high-volume.html



NETFLIX

Build Your Own PaaS

NETFLIX

Components

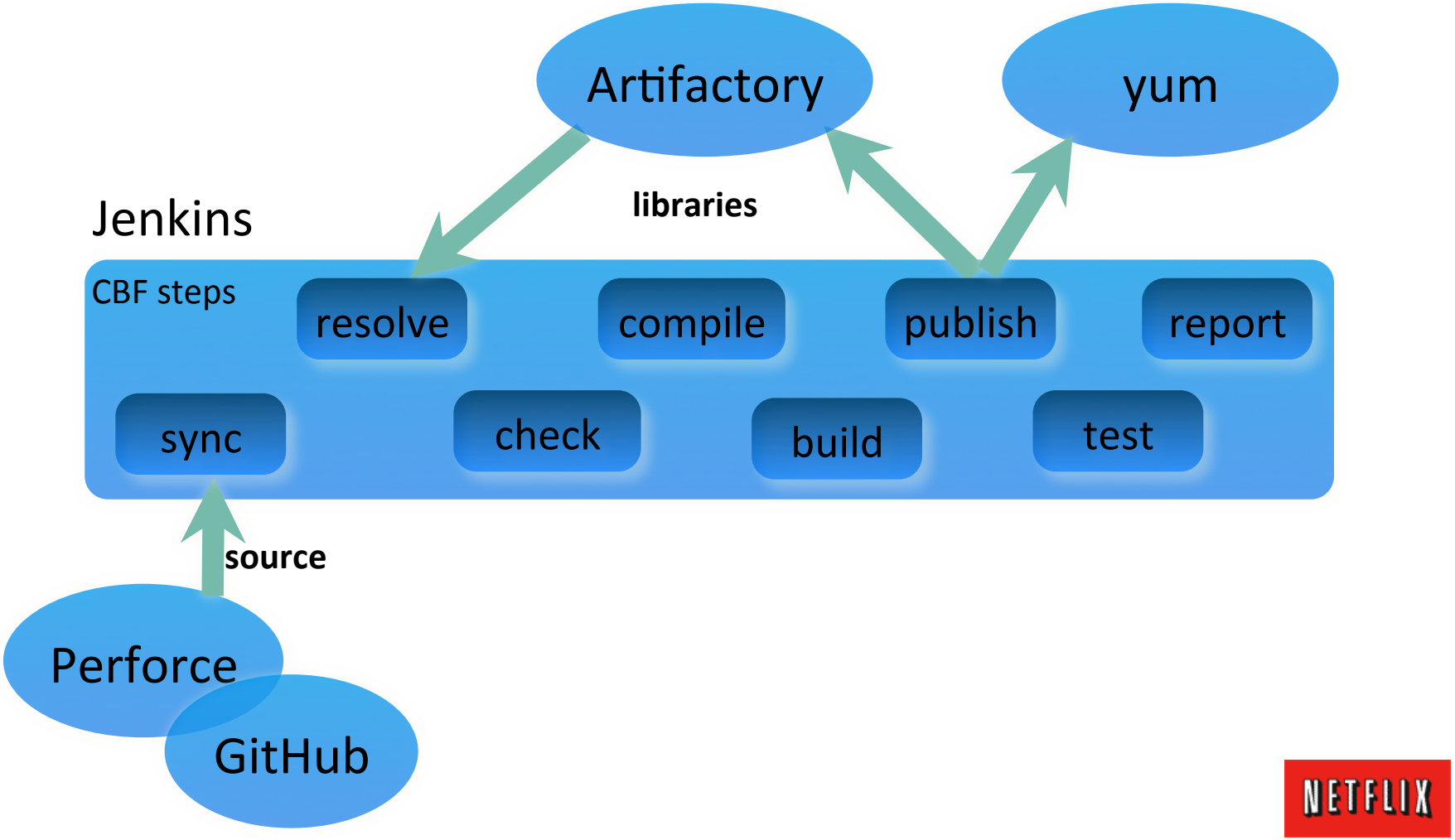
- Continuous build framework turns code into AMIs
- AWS accounts for test, production, etc.
- Cloud access gateway
- Service registry
- Configuration properties service
- Persistence services
- Monitoring, alert forwarding
- Backups, archives

NETFLIX

Common Build Framework

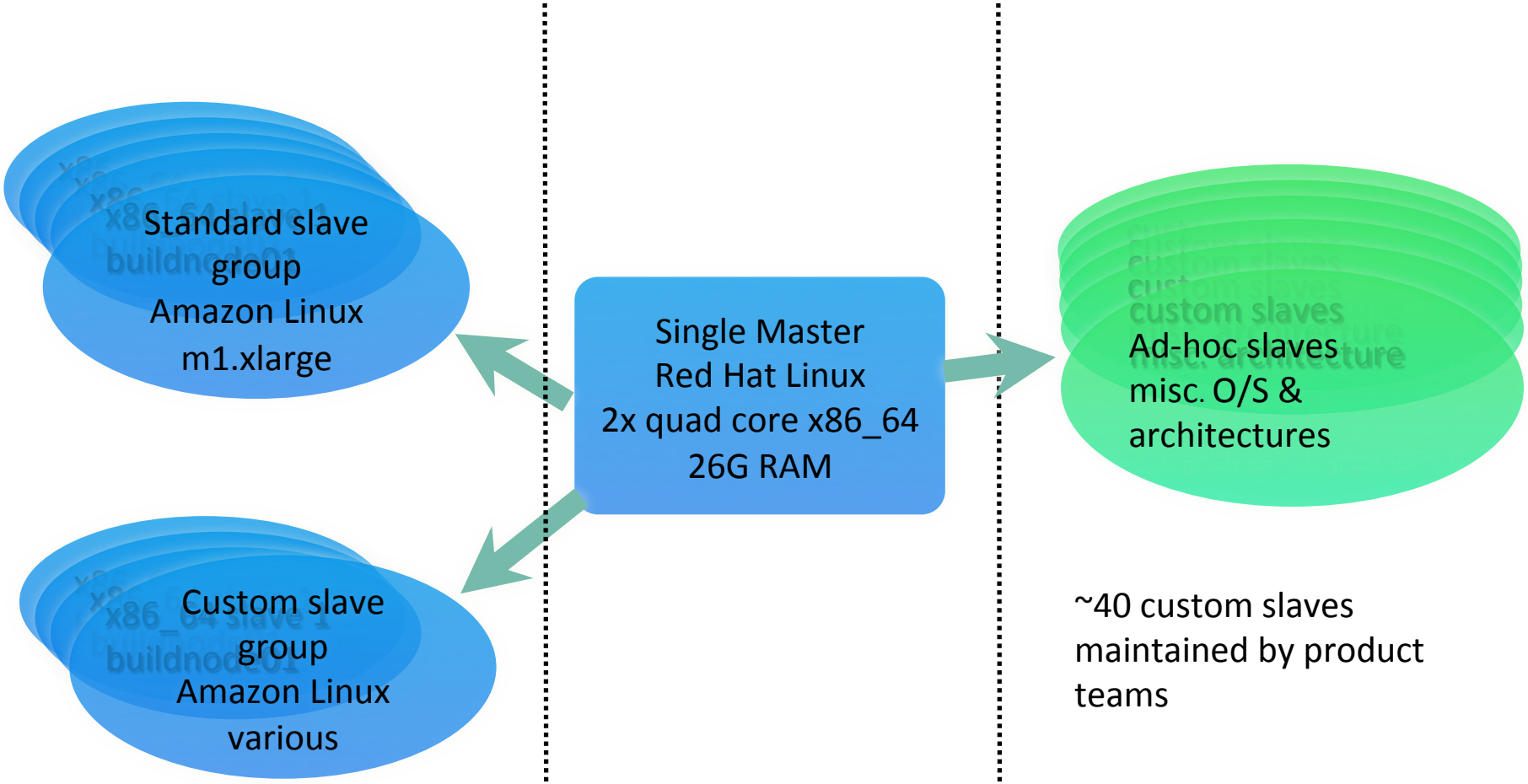
Extracted from
"Building and Deploying Netflix in the Cloud"
by @bmoyles and @garethbowles
On slideshare.net/netflix

Build Pipeline



NETFLIX

Jenkins Architecture



Netflix Extensions to Jenkins

Job DSL plugin: allow jobs to be set up with minimal definition, using templates and a Groovy-based DSL (Gradle)

Housekeeping and maintenance processes implemented as Jenkins jobs, system Groovy scripts

The Bakery

- Create base AMIs
  - We have CentOS, Ubuntu and Windows base AMIs
  - All the generic code, apache, tomcat etc.
  - Standard system and application monitoring tools
  - Update ~monthly with patches and new versions
- Add yummy topping and bake
  - Jenkins builds app specific AMI including all code etc.
  - Bakery mounts EBS snapshot, installs and bakes
  - One bakery per region, delivers into paastest
  - Tweak config and publish AMI to paasprod

NETFLIX

AWS Accounts

Accounts Isolate Concerns

- paastest – for development and testing
  - Fully functional deployment of all services
  - Developer tagged “stacks” for separation
- paasprod – for production
  - Autoscale groups only, isolated instances are terminated
  - Alert routing, backups enabled by default
- paasaudit – for sensitive services
  - To support SOX, PCI, etc.
  - Extra access controls, auditing
- paasarchive – for disaster recovery
  - Long term archive of backups
  - Different region, perhaps different vendor

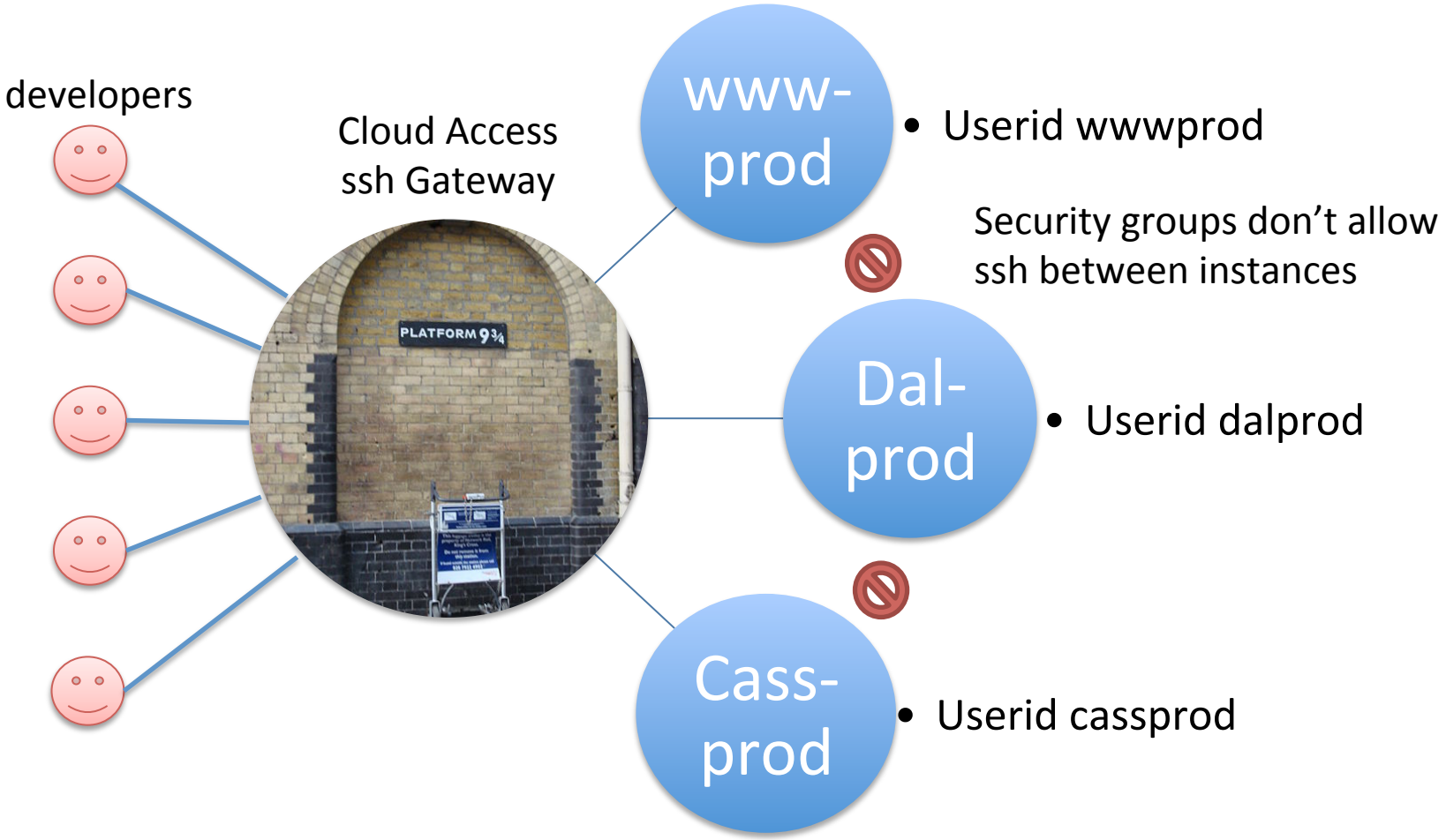
Reservations and Billing

- Consolidated Billing
  - Combine all accounts into one bill
  - Pooled capacity for bigger volume discounts

    http://docs.amazonwebservices.com/AWSConsolidatedBilling/1.0/AWSConsolidatedBillingGuide.html

- Reservations
  - Save up to 71% on your baseline load
  - Priority when you request reserved capacity
  - Unused reservations are shared across accounts

Cloud Access Control



NETFLIX

Now Add Code

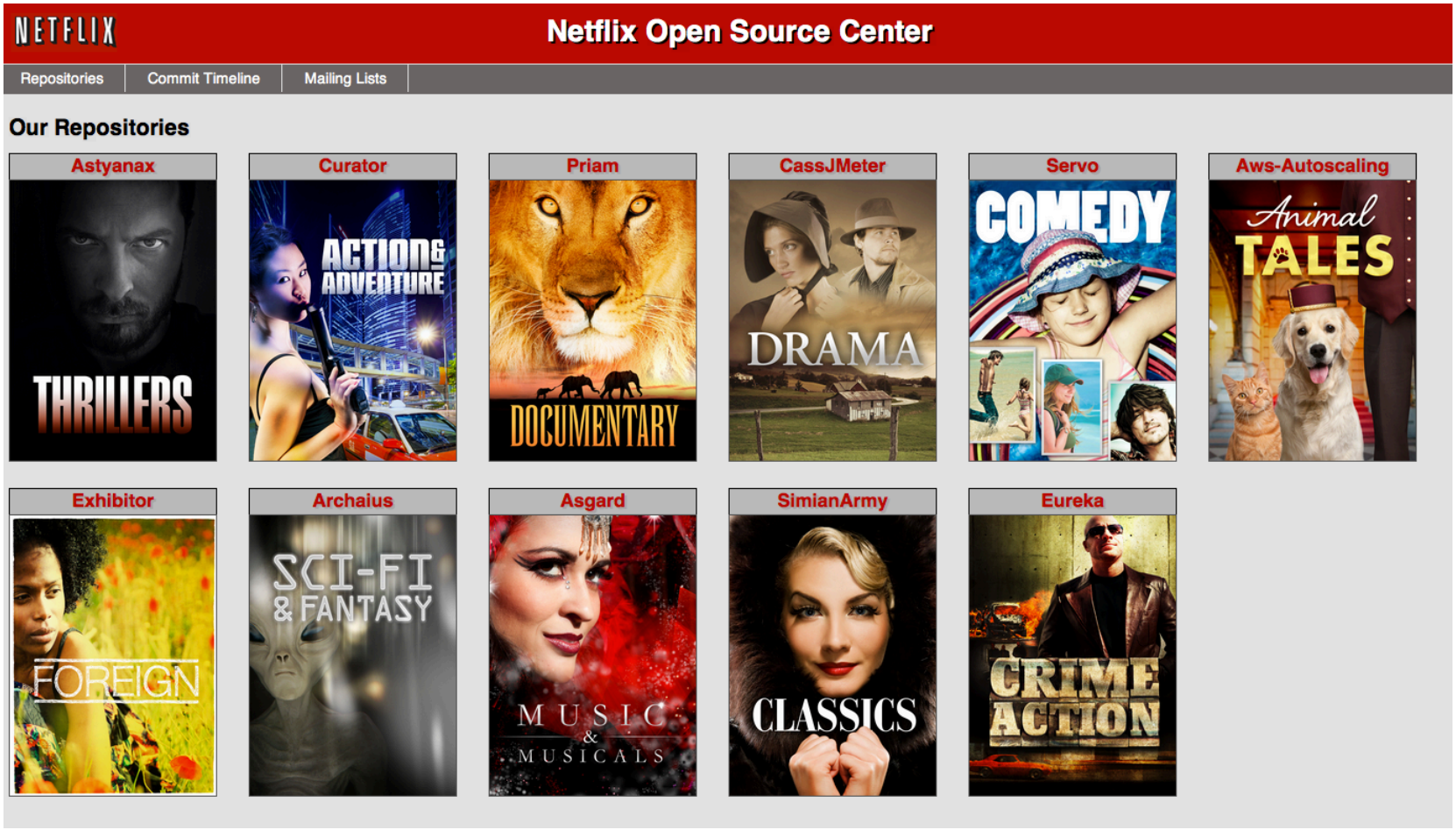
Netflix has open sourced a lot of what you need, more is on the way…

Netflix Open Source Strategy

- Release PaaS Components git-by-git
  - Source at github.com/netflix – we build from it…
  - Intros and techniques at techblog.netflix.com
  - Blog post or new code every few weeks

- Motivations
  - Give back to Apache licensed OSS community
  - Motivate, retain, hire top engineers
  - "Peer pressure" code cleanup, external contributions

http://netflix.github.com



NETFLIX

Instance creation

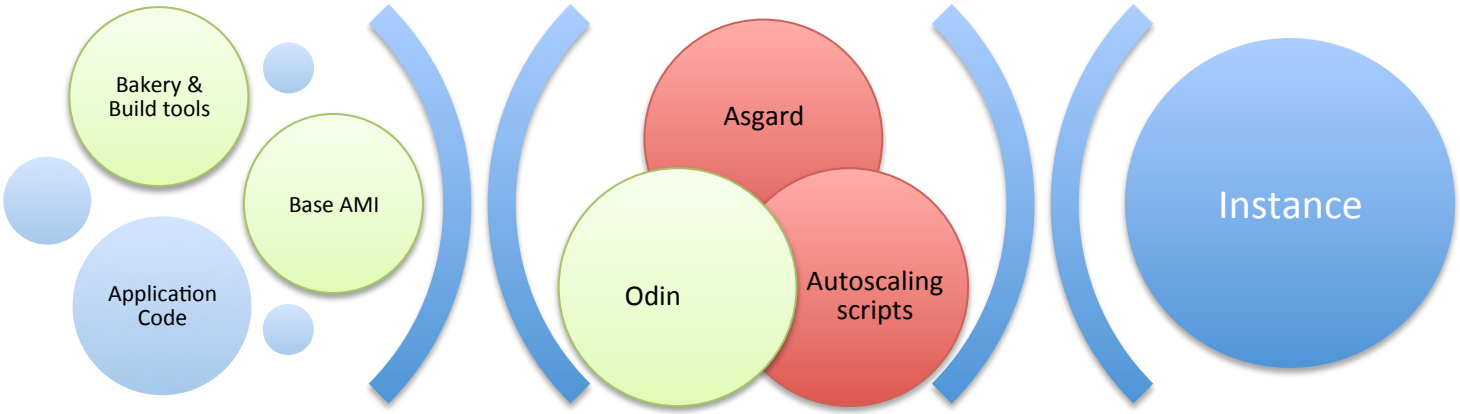


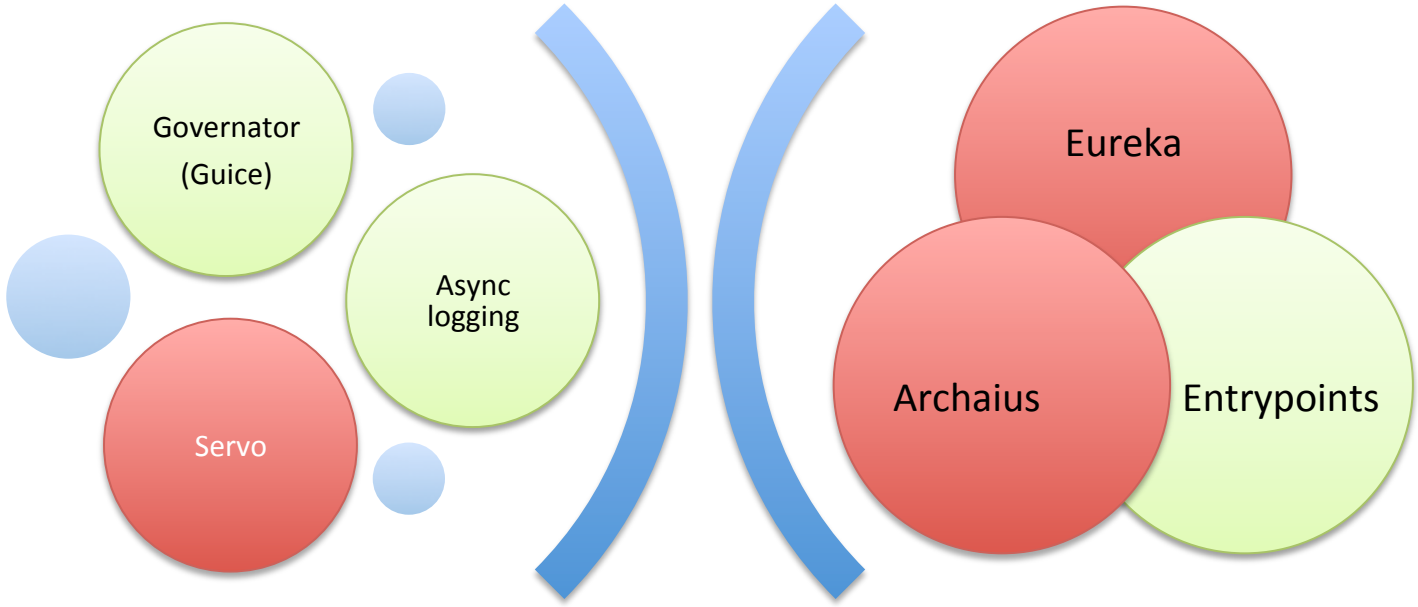
Image baked

ASG / Instance started

Instance Running

NETFLIX

Application Launch

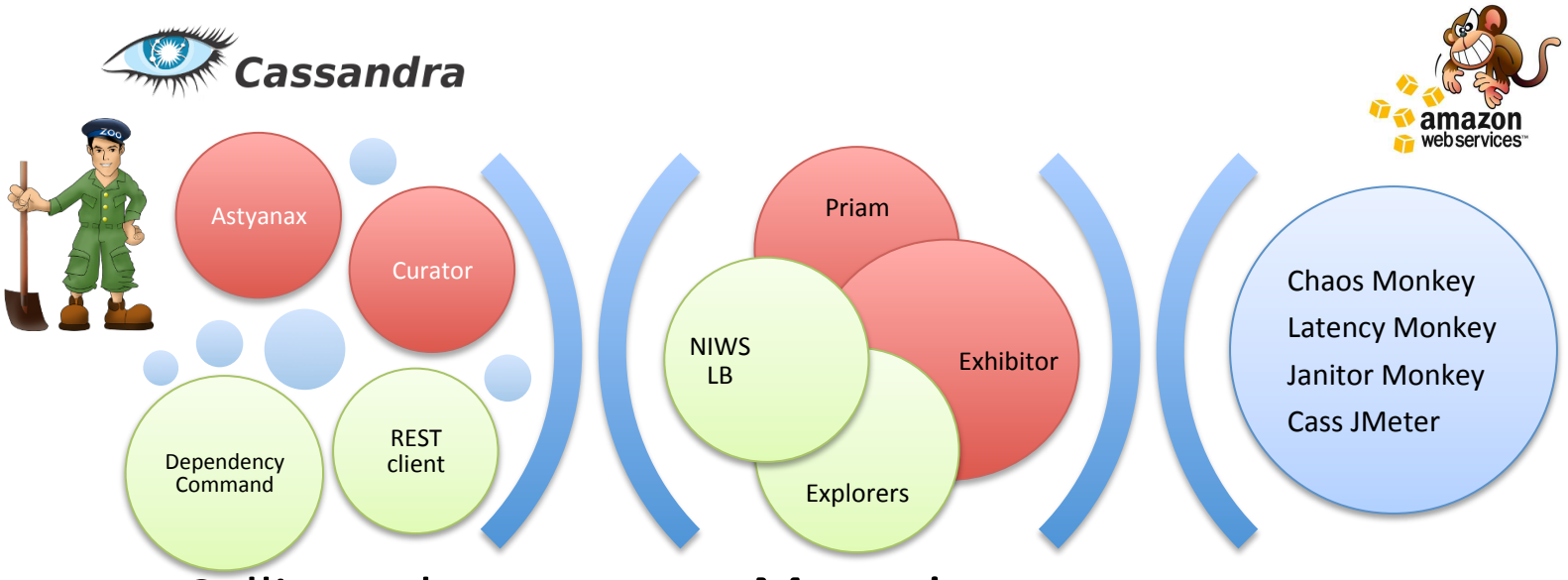


Application initializing

Registering,
configuration

NETFLIX

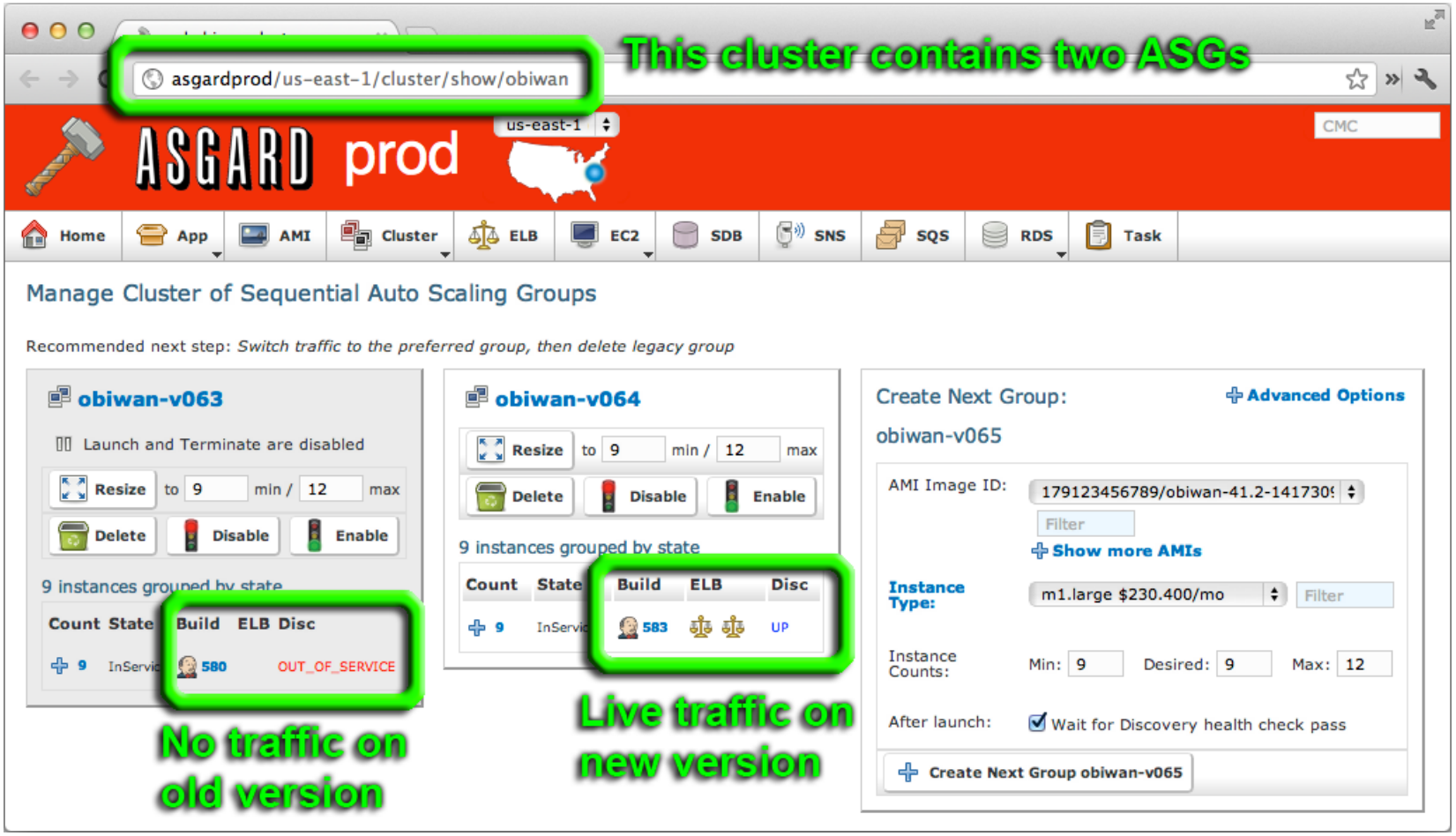
Runtime



NETFLIX

Asgard

http://techblog.netflix.com/2012/06/asgard-web-based-cloud-management-and.html



NETFLIX

Asgard

- Runs in a VM in our datacenter
  - So it can deploy to an empty account
  - Groovy/Grails/JVM based
  - Supports all AWS regions on a global basis
- Hides the AWS credentials
  - Use AWS IAM to issue restricted keys for Asgard
  - Each Asgard instance manages one account
  - One install each for paastest, paasprod, paasaudit

Discovery and Coordination

- Eureka – Service Directory
  - Map an instance to a service in a private namespace
  - Load balance over clusters of instances
  - Foundation service, first to deploy

- Highly available distributed coordination
  - Netflix Curator for common Zookeeper usage patterns
  - Netflix Exhibitor manages Zookeeper reliably

http://techblog.netflix.com/2012/09/eureka.html
http://techblog.netflix.com/2011/11/introducing-curator-netflix-zookeeper.html
http://techblog.netflix.com/2012/04/introducing-exhibitor-supervisor-system.html

Archaius Dynamic Properties Service

http://techblog.netflix.com/2012/06/annoucing-archaius-dynamic-properties.html

- Dynamic hierarchical & propagates in seconds
  - Client timeouts, feature set enables
  - Region specific service endpoints
  - etc. etc.

- Used to configure everything
  - So everything depends on it…
  - Pluggable backend storage interface
  - Files, SimpleDB, Cassandra

Open Source Projects

Legend

- Github / Techblog
- Apache Contributions
- Techblog Post
- Coming Soon

Priam Cassandra as a Service	Exhibitor Zookeeper as a Service	Servo and Autoscaling Scripts
Astyanax Cassandra client for Java	Curator Zookeeper Patterns	Honu Log4j streaming to Hadoop
CassJMeter Cassandra test suite	EVCache Memcached as a Service	Circuit Breaker Robust service pattern
Cassandra Multi-region EC2 datastore support	Eureka / Discovery Service Directory	Asgard - AutoScaleGroup based AWS console
Aegisthus Hadoop ETL for Cassandra	Archaius Dynamics Properties Service	Chaos Monkey Robustness verification
Explorers	EntryPoints	Latency Monkey
Governator - Library lifecycle and dependency injection	Server-side latency/error injection	Janitor Monkey
Odin Workflow orchestration	REST Client + mid-tier LB	Bakeries and AMI
Async logging	Configuration REST endpoints	Build dynaslaves

NETFLIX

Roadmap for 2012

- More resiliency and improved availability
- More automation, orchestration
- “Hardening” the platform, code clean-up
- Lower latency for web services and devices
- IPv6 – now running in prod, rollout in process
- More open sourced components
- See you at AWS Re:Invent in November…

NETFLIX

Takeaway

Netflix has built and deployed a scalable global Platform as a Service.

Key components of the Netflix PaaS are being released as Open Source projects so you can build your own custom PaaS.

http://github.com/Netflix
http://techblog.netflix.com
http://slideshare.net/Netflix

http://www.linkedin.com/in/adriancockcroft
http://www.linkedin.com/in/ruslanmeshenberg

@adrianco @rusmeshenberg #netflixcloud

Amazon Cloud Terminology Reference

See http://aws.amazon.com/ This is not a full list of Amazon Web Service features

- AWS – Amazon Web Services (common name for Amazon cloud)
- AMI – Amazon Machine Image (archived boot disk, Linux, Windows etc. plus application code)
- EC2 – Elastic Compute Cloud
  - Range of virtual machine types m1, m2, c1, cc, cg. Varying memory, CPU and disk configurations.
  - Instance – a running computer system. Ephemeral, when it is de-allocated nothing is kept.
  - Reserved Instances – pre-paid to reduce cost for long term usage
  - Availability Zone – datacenter with own power and cooling hosting cloud instances
  - Region – group of Avail Zones – US-East, US-West, EU-Eire, Asia-Singapore, Asia-Japan, SA-Brazil, US-Gov
- ASG – Auto Scaling Group (instances booting from the same AMI)
- S3 – Simple Storage Service (http access)
- EBS – Elastic Block Storage (network disk filesystem can be mounted on an instance)
- RDS – Relational Database Service (managed MySQL master and slaves)
- DynamoDB/SDB – Simple Data Base (hosted http based NoSQL datastore, DynamoDB replaces SDB)
- SQS – Simple Queue Service (http based message queue)
- SNS – Simple Notification Service (http and email based topics and messages)
- EMR – Elastic Map Reduce (automatically managed Hadoop cluster)
- ELB – Elastic Load Balancer
- EIP – Elastic IP (stable IP address mapping assigned to instance or ELB)
- VPC – Virtual Private Cloud (single tenant, more flexible network and security constructs)
- DirectConnect – secure pipe from AWS VPC to external datacenter
- IAM – Identity and Access Management (fine grain role based security keys)