Practical Cloud Security: Web/Dev Ops Edition

Jason Chan
chan@netflix.com

Agenda

- Background and Disclaimers
- Netflix in the Cloud
- Model-Driven Deployment Architecture
- APIs, Automation, and the Security Monkey
- Practical Cloud Security Gaps

Background and Disclaimers

Background and Disclaimers

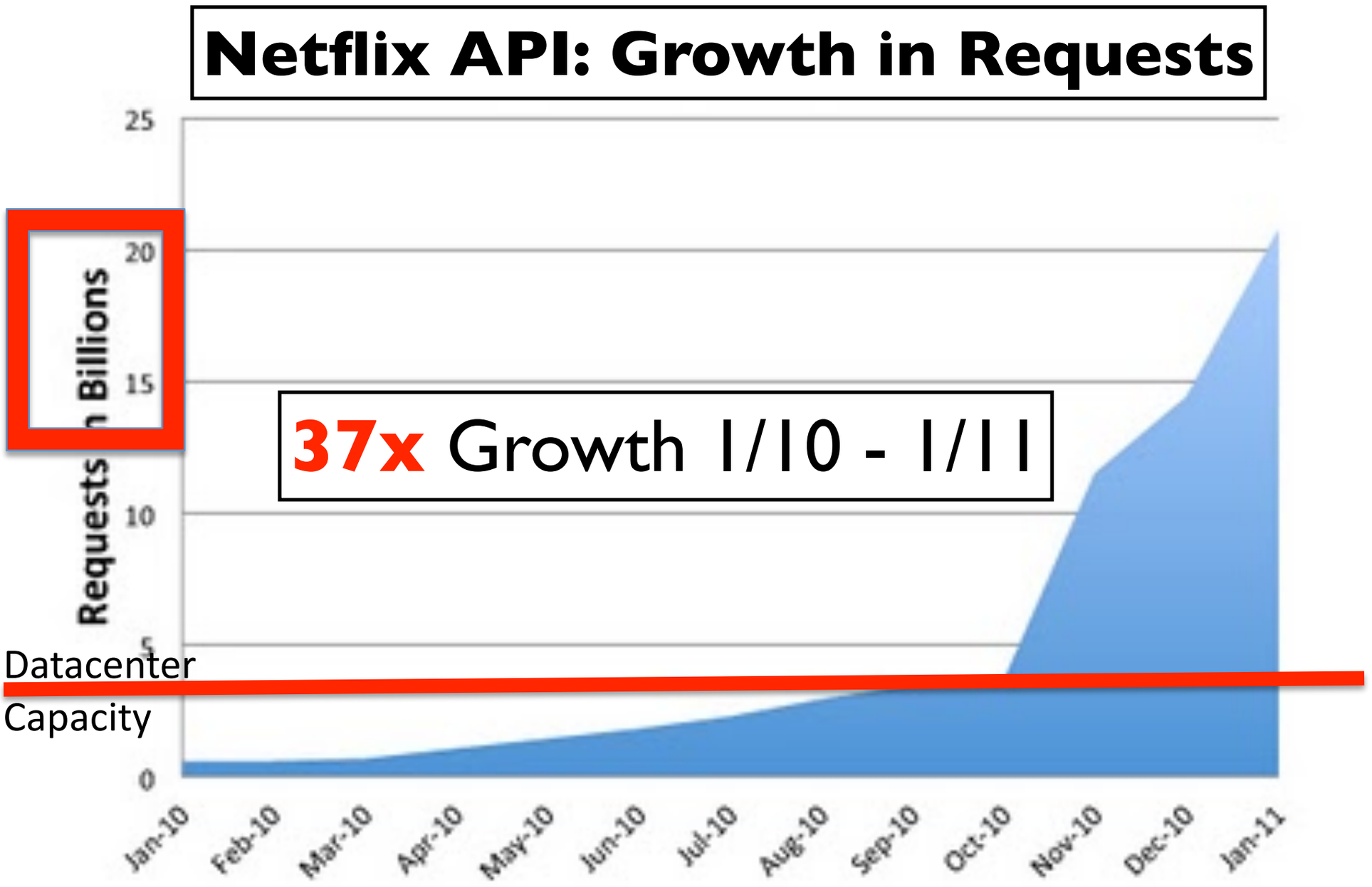
- No cloud definitions, but . . .
- I will focus on IaaS
- Netflix uses Amazon Web Services
  - Guidance should be generally applicable
- Works in progress . . .

Netflix in the Cloud

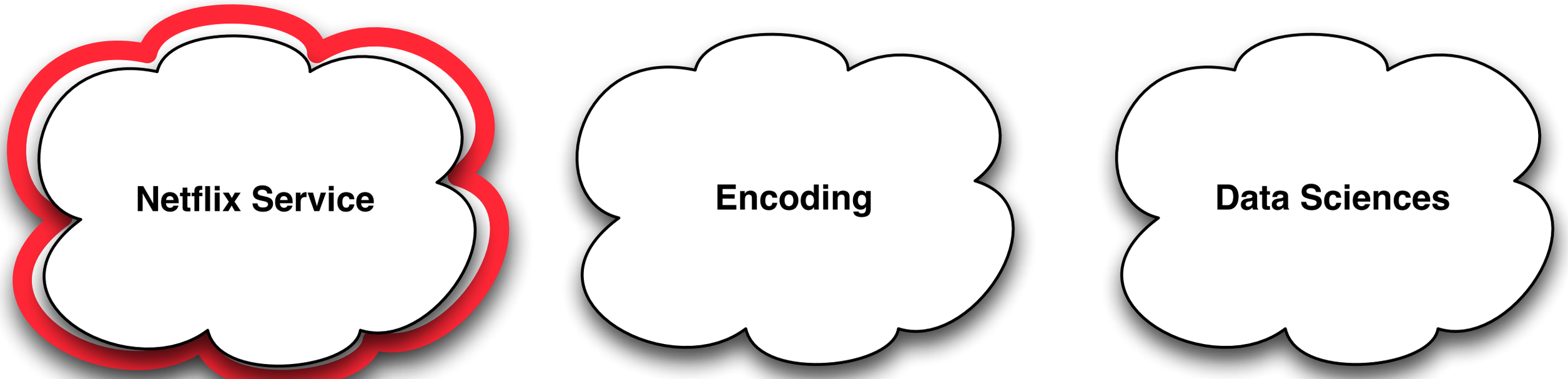
Why is Netflix Using Cloud?

Outgrowing Data Center

http://techblog.netflix.com/2011/02/redesigning-netflix-api.html



netflix.com is now ~100% Cloud



- Remaining components being migrated

Netflix Model-Driven Architecture

Data Center Patterns

- Long-lived, non-elastic systems
- Push code and config to running systems
- Difficult to enforce deployment patterns
- ‘Snowflake phenomenon’
- Difficult to sync or reproduce environments (e.g. test and prod)

Cloud Patterns

- Ephemeral nodes
- Dynamic scaling
- Hardware is abstracted
- Automation/orchestration supports common deployment patterns

When Moving to the Cloud, Leave Old Ways Behind . . .

Generic forklift is generally a mistake

Adapt models appropriately

Netflix Build and Deploy

http://techblog.netflix.com/2011/08/building-with-legos.html

Continuous Integration

App-Specific Packages and Configuration

Customized, Cloud-Ready Image

Jenkins

Yum

AMI

Perforce

Artifactory

Bakery

Instance

SCM

Binary Repository

Combine Base and App-Specific Configuration

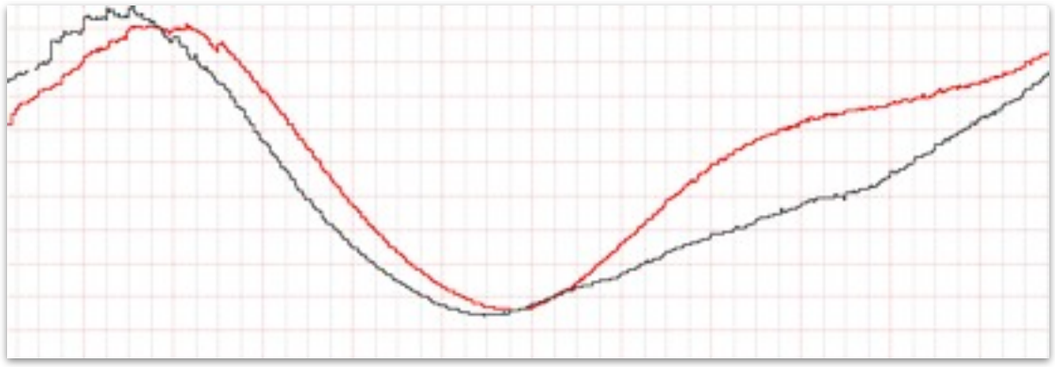
Live System!

Existing Components

Cloud-Specific Components

Autoscaling Group: Deployment Unit of Measure

Baked AMI	+	Launch Config	+	Autoscaling Group
• Base Linux • App code • App dependencies • App-specific config		• Instance type • Security group config		• Target data centers • Min/max/desired nodes



Autoscaling Results and Ramifications

- Continuously adding and removing nodes
  - Based on demand, system health
- **New nodes must mirror existing**

Every change is a new push

Operational Impact

- No changes to running systems
- No CMDB
- No systems management infrastructure
- No snowflakes
- Fewer logins to prod systems

Security Impact

- File integrity monitoring
- User activity monitoring
- Vulnerability management
- Patch management

APIs, Automation, and the Security Monkey

Common Challenges for Security Engineers

- Lots of data from different sources, in different formats
- Too many administrative interfaces and disconnected systems
- **Too few options for scalable automation**

Enter the Cloud . . .

How do you . . .

- Add a user account?
- Inventory systems?
- Change a firewall config?
- Snapshot a drive for forensic analysis?
- Disable a multi-factor authentication token?

- CreateUser()
- DescribeInstances()
- AuthorizeSecurityGroupIngress()
- CreateSnapshot()
- DeactivateMFADevice()

Security Monkey

http://techblog.netflix.com/2011/07/netflix-simian-army.html

- Centralized framework for cloud security monitoring and analysis
- Certificate and cipher monitoring
- Firewall configuration checks
- User/group/policy monitoring
- Next - web security scanning

‘Practical’ Cloud Security Gaps

Common Security Product Model

- Examples - AV, FIM, etc.
- “Management” station with client “nodes”
  - Limited tagging or abstraction
- Per node licensing

“Thundering Herd”

- Mass deployments
  - “Red/Black” push - concurrent clusters of 500+ nodes
- Elasticity related to traffic spikes
- Licensing constraints

Node Ephemerality and Service Abstraction

- Data related to individual nodes becomes less important
- Dealing with short-lived systems, IP and ID reuse
- Event and log archives and data relationships

Resource Usage Logging and Auditing

- Public-facing APIs make access controls more difficult and more important
- Programmable infrastructure needs robust logging and auditing capabilities
- Can metering data be repurposed?

“Trusted Cloud”

- Various components related to providing higher assurance/trust levels in the cloud
- Virtual TPM / hardware root of trust
- Credential management
- HSM in the cloud

Thanks!
Questions?

chan@netflix.com

References

- http://www.slideshare.net/adrianco
- http://aws.amazon.com
- http://techblog.netflix.com
- https://cloudsecurityalliance.org/
- http://www.nist.gov/itl/cloud/index.cfm