Cloud & DevOps
April Big Group

April 24, 2015
Friday
1:30-2:30 p.m.
Science Center Hall E
Agenda

• **Program Update** — Megan Parmar (10 min)
  – News and Announcements
  – Cloud & DevOps Open House: The Results

• **Network 1.0** — Jefferson Burson (20 min)

• **Security 1.0** — Bill Knox (20 min)
  – High-Level Responsibilities
  – Means to an End
  – How to Do This in the Cloud?

• **Q&A** (10 min)
Program Update: News and Announcements

• Since our last meeting, the Cloud & DevOps team has been building the foundation to enable Wave 1 migrations:
  – Designing and building DevOps Platform v1.0
  – Creating application server patterns and refining the toolset used to orchestrate and deploy applications to AWS

• We have also spent time refining and rethinking our approach for onboarding applications into the migration process:
  – Preparing to pilot a more Agile approach for engagement that leverages Scaled Agile principles

• We continue to work with application teams on migrations, but not at the pace originally planned
  – Continued progress with QlikView and IAM migrations
  – Working to re-baseline the schedule for Wave 1 migrations
Program Update: News and Announcements

• Lesson: It’s important to focus on training
  – Piloted AWS DevOps class built around our program needs — and we will be opening the class to HUIT as a whole
  – Dedicated time to building our Python development skills

• Lesson: We need more transition time to support ongoing operational work and provide the right level of support for migrated applications

• Plus: Our team is growing!
  – Joel Fanton, Director of DevOps Platform
  – Magnus Bjorkman, Director of Solution Architecture (embedded)
  – Tom Vachon, Senior Cloud Architect

• Soon: Focus on Wave 2 transition planning based on what we’ve learned from Wave 1
Cloud & DevOps Open House: The Results

• Thank you for attending our Open House!
  – 125 people from across HUIT attended
  – Generated excellent feedback for us to incorporate into our plans and communications

• You asked, we listened:
  – The two key topics respondents want to learn the most about: Security 1.0 and Network 1.0
  – Other top results:
    • Training (update at next Big Group)
    • Migration and transition (update at next Big Group)
    • Cloud architecture and its impact on software engineering
    • Future operational support model and its team impact
Network
Jefferson Burson
Hi!
Agenda

• **Network 1.0**
  – Direct Connect
  – VPC Architecture
  – IP Addressing
  – Integrated Monitoring

• **Toward Network 2.0**
  – Automation
  – NFV
Network 1.0
It’s All About Integration
Until Recently ...

If you wanted to connect to Harvard, you either did it over the open Internet, had HUIT build you a VPN tunnel, or did something weird on your own.
VPN tunnel to Amazon
Many VPN tunnels to Amazon
Many VPN tunnels to Amazon
AWS Direct Connect
Dedicated 2x10GB Fiber Connection to AWS
What’s Next for Direct Connect?

Expand to include more customers
- Add the rest of the Wave 1 VPCs
- Establish as formal service offering for multiple Schools and affiliates
- Billing and cost recovery
- Ensure scalability

Technology roadmap
- Improve redundancy with a second dual-path circuit
- Increase automation
AWS VPC
What is a VPC?
It’s a Virtual Private Cloud
(That’s Not Very Helpful)
A Network Boundary

The network inside the VPC can be visible to all virtual machines or segments within the VPC.

However, you can selectively choose what addresses and services are seen from outside the VPC.
A Trust Zone

We can bind identities and roles of administrators and developers to the VPC.

Thus, if an entity has rights in one part of the VPC, he or she will likely have those rights in all of the VPC.
A Functional Boundary

My team is different than your team.
My applications are different than your applications.
VPC Design Patterns

Cloud Ops, the Architecture Decision Group, and Network Services are all working together on this.
IP Addresses at AWS

Services at Amazon need IP addresses just like everything else.

HUIT is centrally managing IP addresses for our use of AWS.
Harvard Routable Addresses

Why should you use Harvard routable addresses?

Connecting back to Harvard
Can’t connect back to the rest of Harvard if you’re using someone else’s IP address

Connecting to other VPCs
Can’t have two VPCs with the same IP addresses connect together

Network security
Unique IP addressing improves logging and traceability
Don’t Screw This Up, Because ...

You can’t re-address an AWS VPC.
You have to delete it and start over.
So, the Moral of the Story is:

Get an IP address assignment from HUIT Network Services before you create your VPC.
Seriously:

Get an IP address assignment from HUIT Network Services before you create your VPC.
Integrated Monitoring

A common approach to monitoring networks, systems, and services in the cloud and on-premise.

A HUIT Top 40 goal.
Integrated Monitoring at Harvard

“Best-of-breed” configuration management and orchestration:

- vCenter SCOM
- Puppet
- Continuous Integration
- Git
- CloudFormation/
- Code Deploy
- NetMRI
- Fortinet
- Infoblox
- Other

Integrated Monitoring System:
- Discovery, Monitoring, Performance, Alerting

ServiceNow CMDB
Due by June 30

Complete Comparative Analysis

Product Selection

Staffing Proposal

Budget Model

Final Recommendation
Toward Network 2.0
Iterate, Improve, Automate
Security 1.0
Security for HUIT Wave 1 Cloud Deployment
BLUF*, a.k.a. TB;DL**

• Work in progress – change is likely
  – Could be changes to how we do similar things
  – Could be changes to how we approach information security overall
• For now, implementing security in a similar fashion to the way we do it today to avoid holding things up
• Detailed read is available at http://tinyurl.com/huit-cloud-security-principles
• Feedback is both welcome and critical to everyone’s success

* Bottom Line Up Front
** Too Boring, Didn’t Listen
High-Level Responsibilities for Information Security

• Protect
• Detect
• Respond

From what?
“Activities that are counter to established information protection policies and requirements”
Means to an End: 8 Requirements for Better Security

- See network traffic as it flows to and from systems (traffic insight)
- See detail of what is being done on systems (activity insight)
- Be able to associate what is observed with specific systems (traffic association)
- Know who to talk to about specific systems (owner association)
- Ability to restrict network traffic to only that which is required for the system to perform necessary business functions (traffic control)
- Gain insight and effect control through standard IT services (standard services)
- Insertion of additional inspection and control in the application layer on the network (Layer 7 controls)
- Limitation to the extent by which one party can undermine system security controls (separation of duties)
How to Do This in the Cloud?

• **Traffic insight:** Virtual firewall in each VPC, logging flow information about traffic between the VPC and the Internet

• **Activity insight:** Centralized logging to Splunk

• **Traffic association:** IP address management and logging where required

• **Owner association:** You tell me (tagging? registration?)

• **Traffic control:** Virtual firewall to control Internet-facing traffic; security groups to control intra-VPC traffic

• **Standard services:** Deployment by HUIT of services

• **Layer 7 controls:** Use of web proxy for outbound web connections

• **Separation of duties:** Separate group (NOC?) that handles virtual firewall rules (in this model, DevOps teams can control security groups)
Thank you!