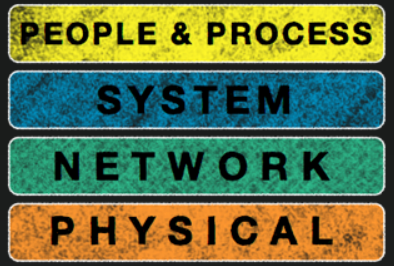
SECURITY IS JOB ZERO

Security – The Forefront For Any Online Business

Bill Murray – Sr. Mgr, AWS Security Programs

amazon web services

Security is Job Zero



Familiar security model

Validated by security experts

Collaboration on Enhancements

Every Customer Benefits

Physical Security	Network Security	Platform Security	People & Procedures

SECURITY IS SHARED

Build everything on a constantly improving security baseline

GxP
ISO 13485
AS9100
ISO/TS 16949

AWS is responsible for the security **OF** the Cloud

amazon web services

Security & compliance is a shared responsibility

Customers

Customer applications & content

Platform, Applications, Identity & Access Management

Operating System, Network, & Firewall Configuration

Client-side Data Encryption | Server-side Data Encryption | Network Traffic Protection

Customers have their choice of security configurations **IN** the Cloud

AWS Foundation Services

Compute | Storage | Database | Networking

amazon web services

AWS Global Infrastructure

Availability Zones | Regions | Edge Locations

AWS is responsible for the security **OF** the Cloud

amazon web services

SECURITY IS FAMILIAR

Security is Familiar

- We strive to make security at AWS as familiar as what you are doing right now
  - Visibility
  - Auditability
  - Controllability
  - Agility

AWS Marketplace: One-stop shop for familiar tools

Advanced Threat Analytics	Application Security	Identity and Access Mgmt	Server & Endpoint Protection	Network Security	Encryption & Key Mgmt	Vulnerability & Pen Testing
ALERTLOGIC	iMPERVA	CIPHERGRAPH networks	TREND MICRO	SOPHOS	SafeNet	tenable network security
ALIEN VAULT	FORTINET	SECUREAUTH	intel Security	FORTINET	Vormetric	QUALYSGUARD
	Barracuda	M-Pin SSO Authentication for Enterprises		Check Point We Secure the Internet	HYTRUST	
				paloalto networks.		

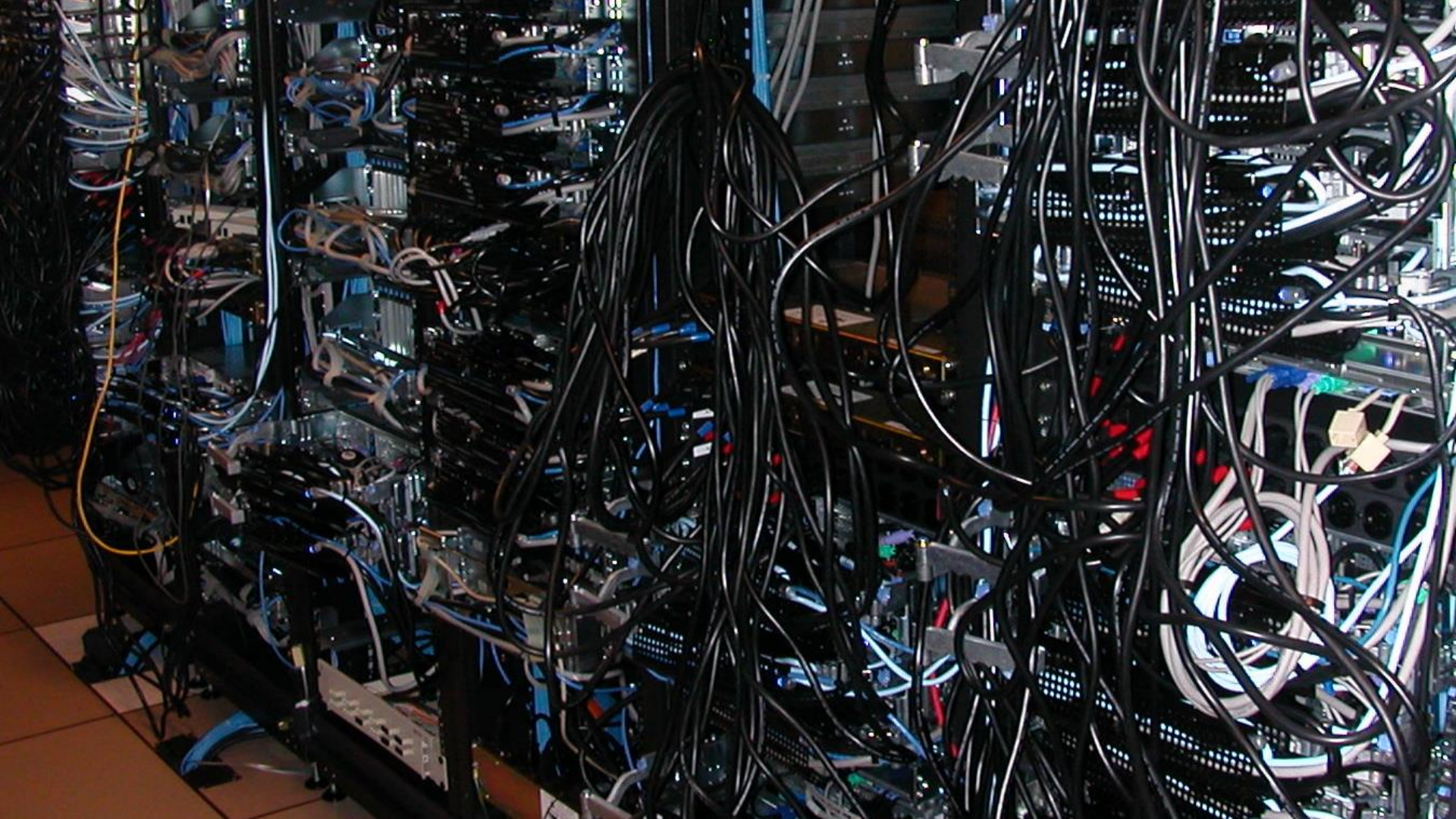
amazon web services

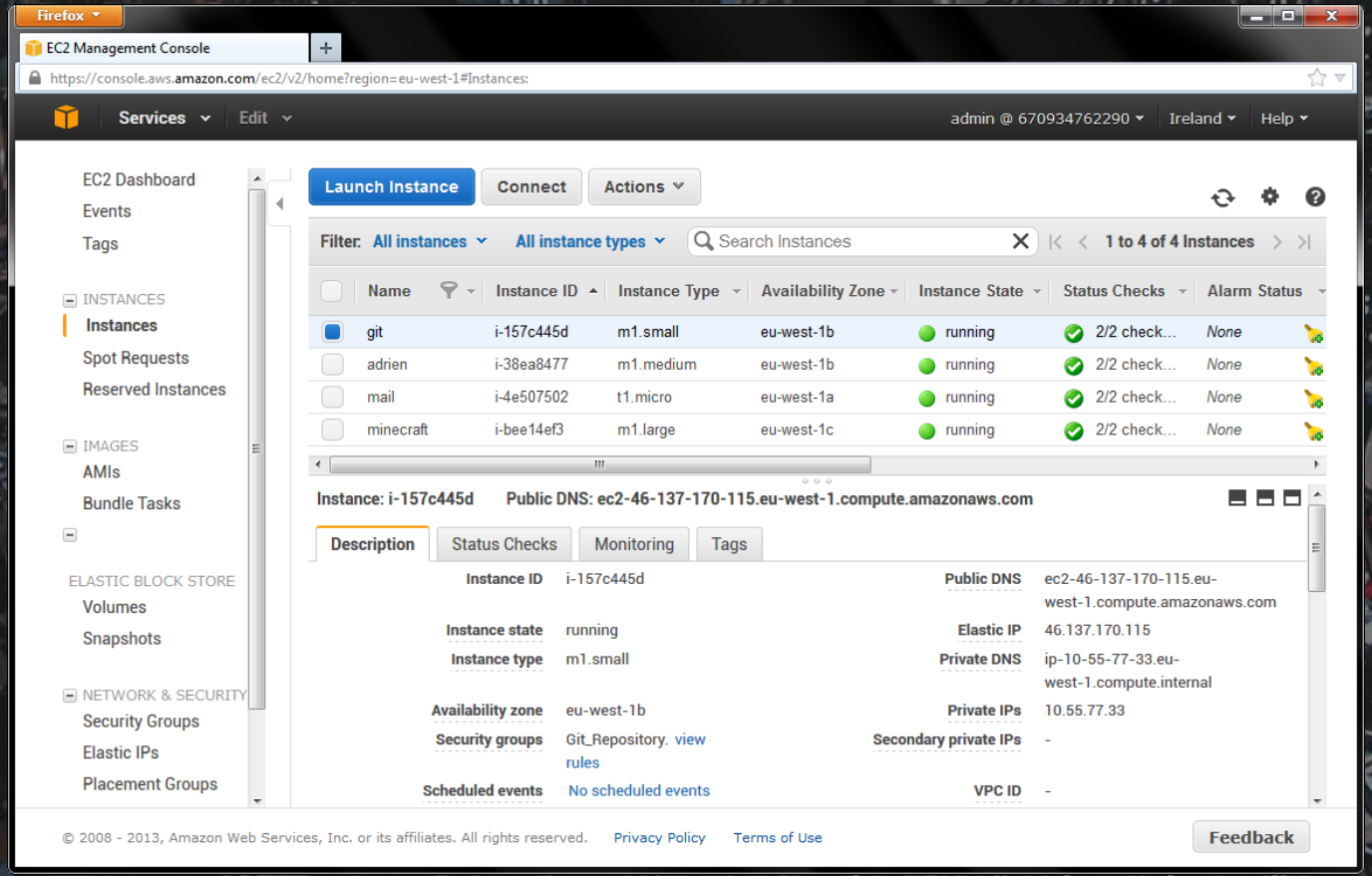
SECURITY REQUIRES VISIBILITY

VISIBILITY

HOW OFTEN DO YOU MAP YOUR NETWORK?

WHAT'S IN YOUR ENVIRONMENT
RIGHT NOW?

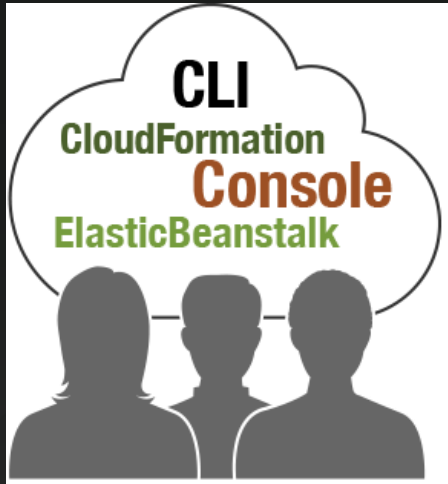


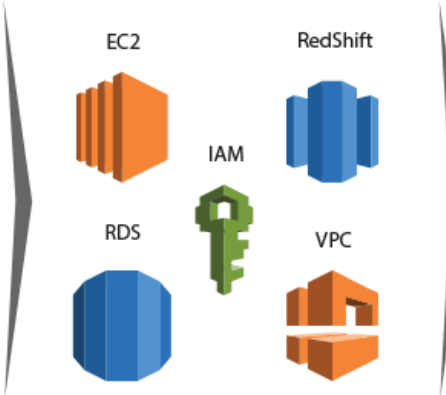

Firefox
EC2 Management Console
https://console.aws.amazon.com/ec2/v2/home?region=eu-west-1#Instances:
Services
Edit
admin @ 670934762290
Ireland
Help
EC2 Dashboard
Events
Tags
INSTANCES
Instances
Spot Requests
Reserved Instances
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Launch Instance
Connect
Actions
Filter: All instances
All instance types
Search Instances
1 to 4 of 4 Instances
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
Alarm Status
git i-157c445d m1.small eu-west-1b running 2/2 check... None
adrien i-38ea8477 m1.medium eu-west-1b running 2/2 check... None
mail i-4e507502 t1.micro eu-west-1a running 2/2 check... None
minecraft i-bee14ef3 m1.large eu-west-1c running 2/2 check... None
Instance: i-157c445d
Public DNS: ec2-46-137-170-115.eu-west-1.compute.amazonaws.com
Description
Status Checks
Monitoring
Tags
Instance ID i-157c445d
Instance state running
Instance type m1.small
Availability zone eu-west-1b
Security groups Git_Repository. view rules
Scheduled events No scheduled events
Public DNS ec2-46-137-170-115.eu-west-1.compute.amazonaws.com
Elastic IP 46.137.170.115
Private DNS ip-10-55-77-33.eu-west-1.compute.internal
Private IPs 10.55.77.33
Secondary private IPs -
VPC ID -
© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Feedback

Security is Visible

- Who is accessing the resources?
- Who took what action?
  - When?
  - From where?
  - What did they do?
  - Logs Logs Logs

AWS CLOUDTRAIL





User	Action	Time
Tim	Created	1:30pm
Sue	Deleted	2:40pm
Kat	Created	3:30pm

You are making API calls...

On a growing set of services around the world…

AWS CloudTrail is continuously recording API calls…

And delivering log files to you

amazon web services

Use cases enabled by CloudTrail

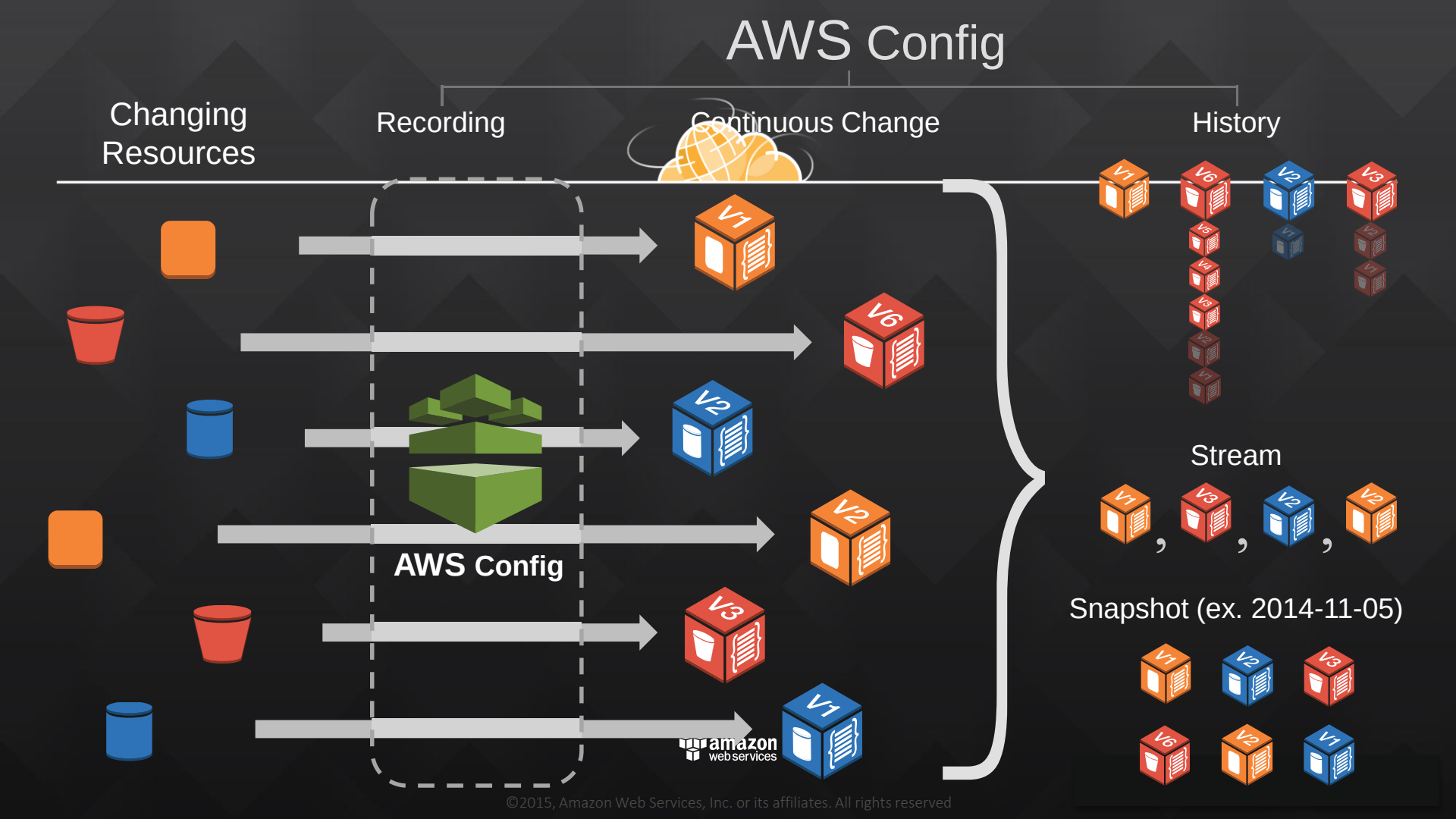
- Security Analysis
  - Use log files as an input into log management and analysis solutions to perform security analysis and to detect user behavior patterns
- Track Changes to AWS Resources
  - Track creation, modification, and deletion of AWS resources such as Amazon EC2 instances, Amazon VPC security groups and Amazon EBS volumes
- Troubleshoot Operational Issues
  - Identify the most recent actions made to resources in your AWS account
- Compliance Aid
  - Easier to demonstrate compliance with internal policies and regulatory standards

CloudTrail Regional Availability

SECURITY IS AUDITABLE

AWS Config

AWS Config is a fully managed service that provides you with an inventory of your AWS resources, lets you audit the resource configuration history and notifies you of resource configuration changes.



Use cases enabled by Config

- Security Analysis: Am I safe?
- Audit Compliance: Where is the evidence?
- Change Management: What will this change affect?
- Troubleshooting: What has changed?

Am I safe?

- Properly configured resources are critical to security

- Config enables you to continuously monitor the configurations of your resources and evaluate these configurations for potential security weaknesses

Where is the evidence?

- Many compliance audits require access to the state of your systems at arbitrary times (i.e. PCI, HIPAA)

- A complete inventory of all resources and their configuration attributes is available for any point in time

What will this change affect?

- When your resources are created, updated, or deleted, these configuration changes are streamed to Amazon SNS

- Relationships between resources are understood, so that you can proactively assess change impact

What changed?

- It is critical to be able to quickly answer “What has changed?”
- You can quickly identifying the recent configuration changes to your resources by using the console or by building custom integrations with the regularly exported resource history files

SECURITY PROVIDES CONTROL

First class security and compliance starts (but doesn't end!) with encryption

Automatic encryption with managed keys

Bring your own keys

Dedicated hardware security modules

Encryption & Best Practices with AWS

Managed key encryption

Key storage with AWS CloudHSM

Customer-supplied key encryption

DIY on Amazon EC2

Create, store, & retrieve keys securely

Rotate keys regularly

Securely audit access to keys

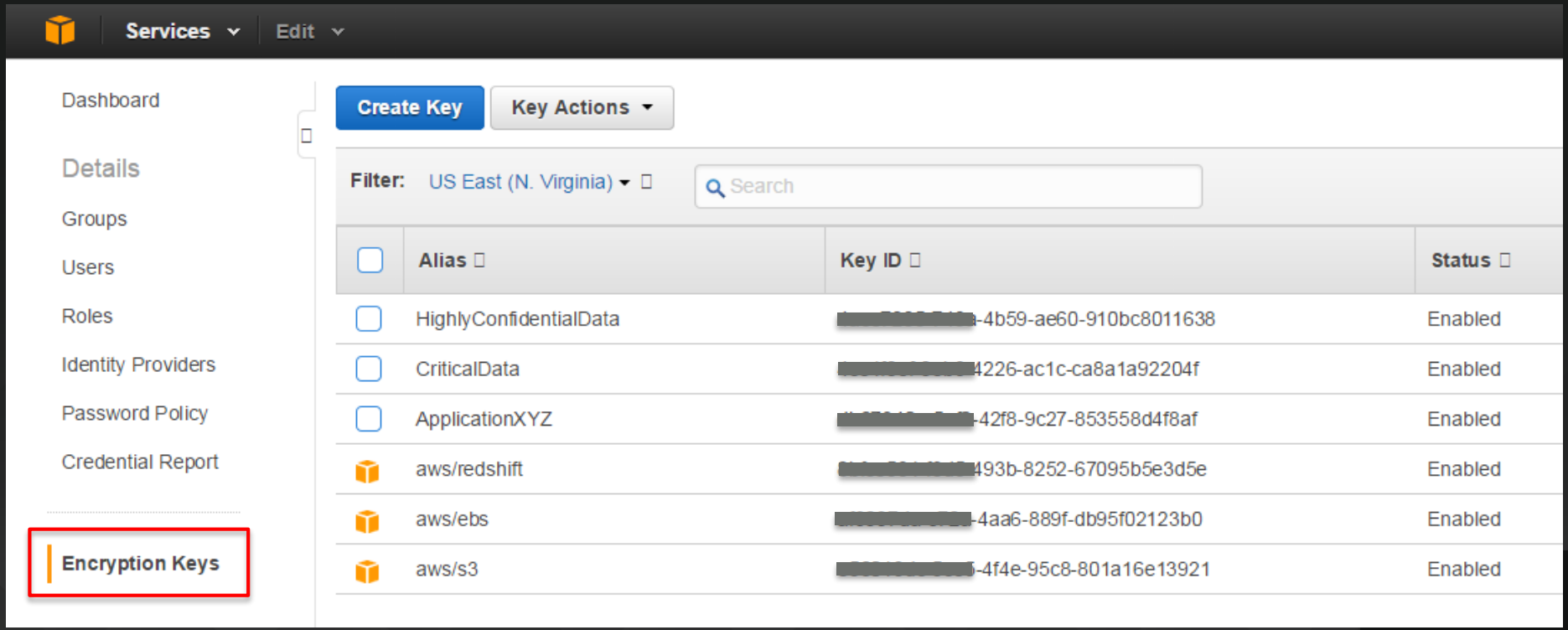
Partner enablement of crypto

AWS Key Management Service

- A managed service that makes it easy for you to create, control, and use your encryption keys
- Integrated with AWS SDKs and AWS services including Amazon EBS, Amazon S3, and Amazon Redshift
- Integrated with AWS CloudTrail to provide auditable logs to help your regulatory and compliance activities

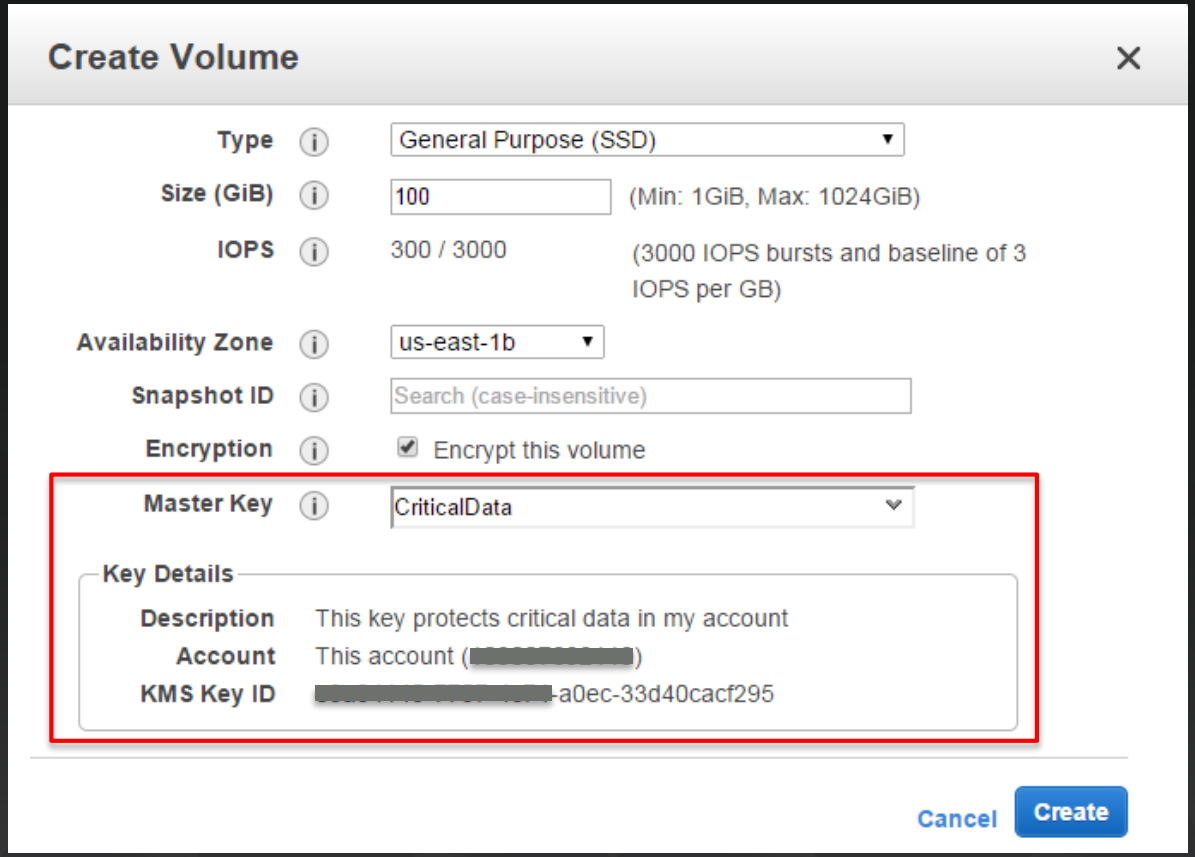
AWS Key Management Service

Integrated with AWS IAM Console



AWS Key Management Service

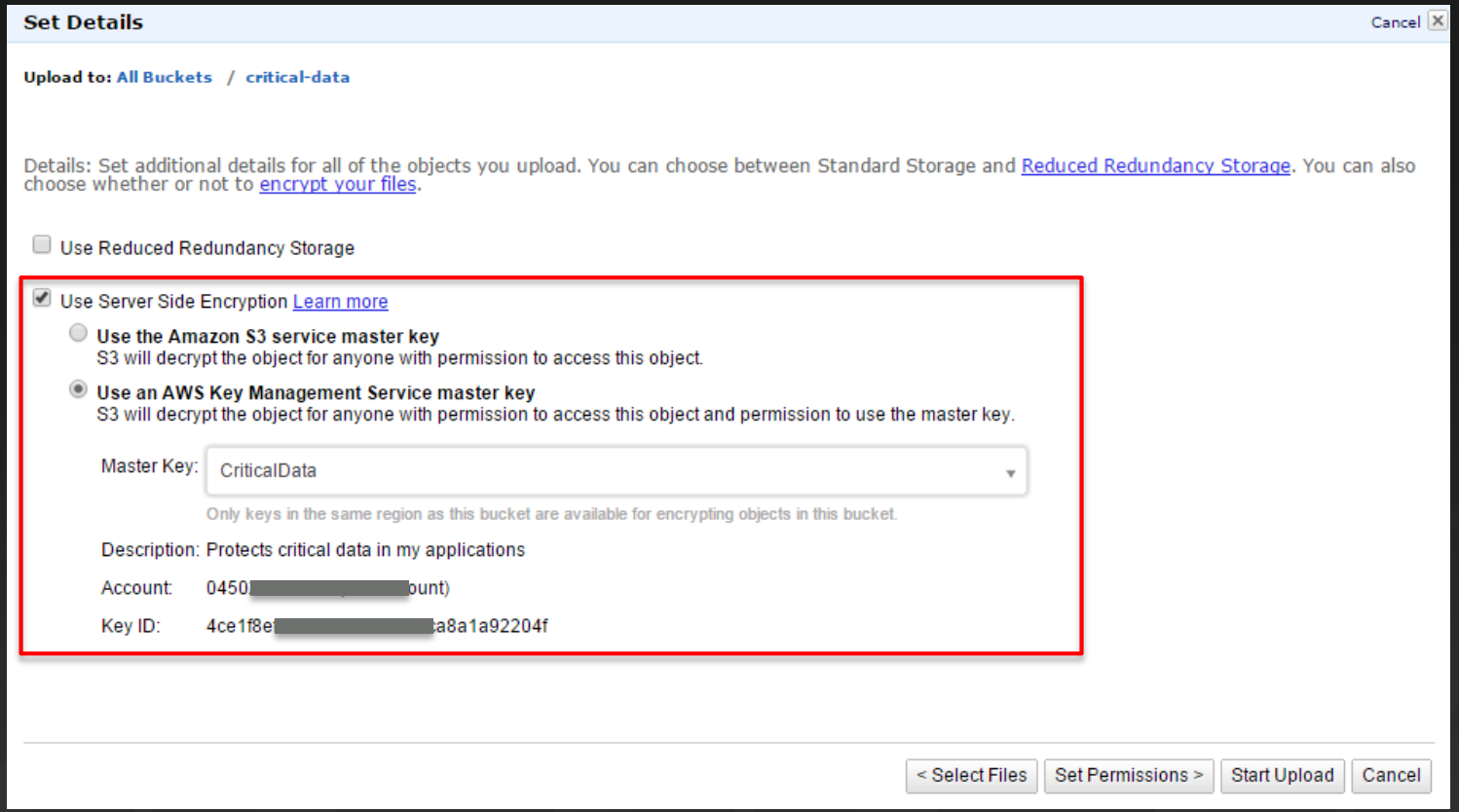
Integrated with Amazon EBS



amazon web services

AWS Key Management Service

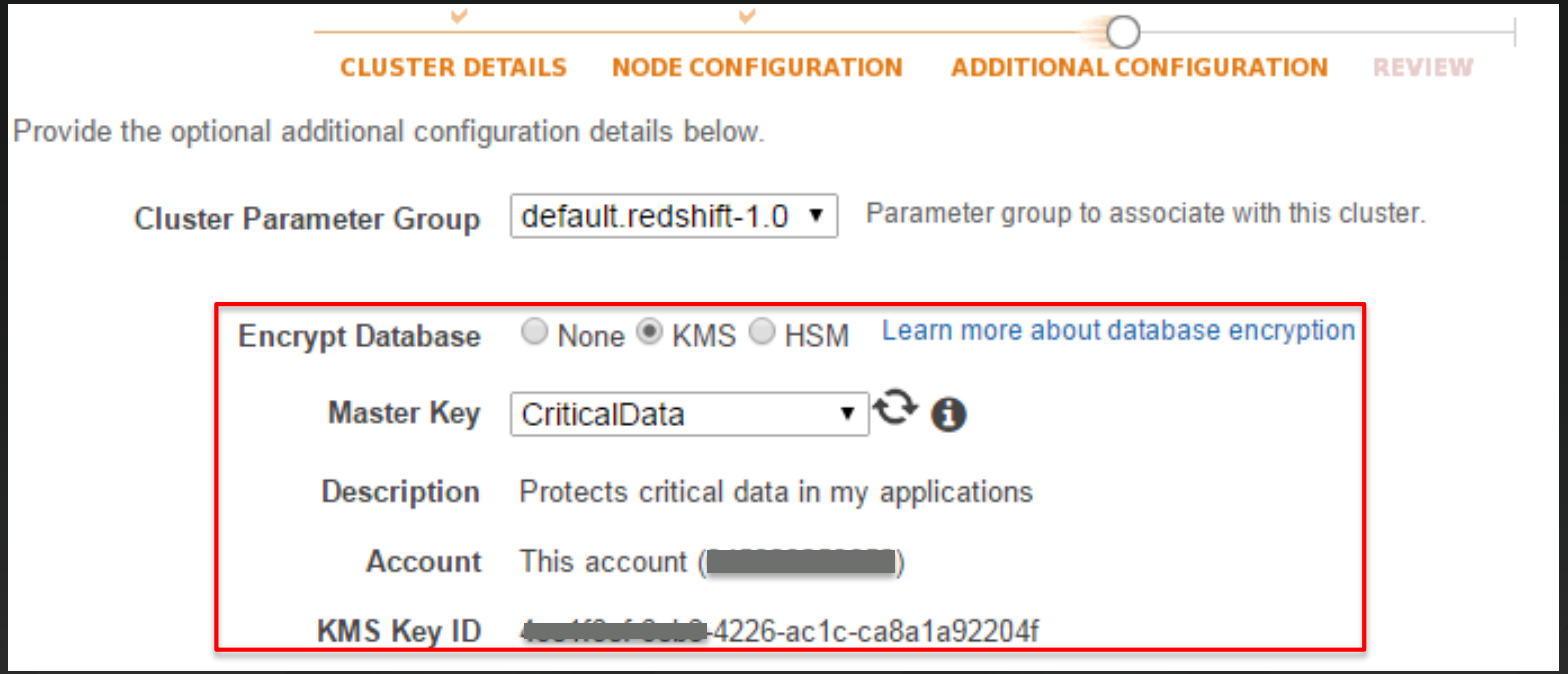
Integrated with Amazon S3



amazon web services

AWS Key Management Service

Integrated with Amazon Redshift



SECURITY IS AGILE

HOW DOES AWS PRACTICE SECURITY?

The practice of security at AWS is different, but the outcome is familiar:

So what does your security team look like?

- Operations
- Engineering
- Application Security
- Compliance

Our Culture:

Everyone's an owner

When the problem is "mine" rather than "hers" there's a much higher likelihood I'll do the right thing

Our Culture:

Measure constantly, report regularly, and hold senior executives accountable for security – have them drive the right culture

Our Culture:

Measure measure measure

- 5 min metrics are too coarse
- 1 min metrics just barely OK

Our Culture:

Saying “no” is a failure

Our Culture:

Apply more effort to the “why” rather than the “how”

Why is what really matters

When something goes wrong, ask the “five whys”

Our Culture:

Decentralize - don’t be a bottleneck

It’s human nature to go around a bottleneck

Our Culture:

Produce services that others can consume through hardened APIs

Our Culture:

Test, CONSTANTLY

- Inside/outside
- Privileged/unprivileged
- Black-box/white-box
- Vendor/self

Our Culture:

Proactive monitoring rules the day

- What's "normal" in your environment?
- Depending on signatures == waiting to find out WHEN you've been had

Our Culture:

Collect, digest, disseminate, & use intelligence

Our Culture:

Make your compliance team a part of your security operations

Our Culture:

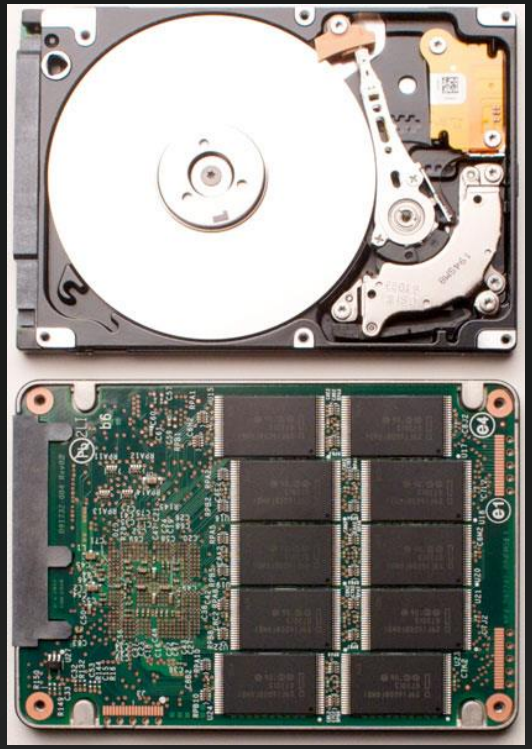
Base decisions on facts, metrics, & detailed understanding of your environment and adversaries

Simple Security Controls

Easy to Get Right

Easy to Audit

Easy to Enforce



This

To This

CONSTANT REDUCTION IN SURFACE AREA

CONSTANT REDUCTION IN HUMAN ACCESS POTENTIAL

UBIQUITOUS ENCRYPTION

EVEN MORE GRANULAR SEPARATION

Security is Job Zero

YOU ARE BETTER OFF IN AWS THAN YOU ARE IN YOUR OWN ENVIRONMENT

- *"Based on our experience, I believe that we can be even more secure in the AWS cloud than in our own data centers."*

  -Tom Soderstrom, CTO, NASA JPL

- "Nearly 60% of organizations agreed that CSPs [cloud service providers] provide better security than their own IT organizations."

  Source: IDC 2013 U.S. Cloud Security Survey, doc #242836, September 2013

amazon web services

AWS Security days

April 21st & 23rd

@ AWS Pop-up Loft

925 Market Street

San Francisco

Ask an Architect 1:1, 60-minute sessions

Talks by AWS Experts

Talks by AWS Partners

http://aws.amazon.com/start-ups/loft/

amazon web services

Thank You

SAN FRANCISCO

amazon web services