Climbing the (Elastic) Beanstalk

One developer's journey from Amazon Web Services newbie to system admin of a brand new, HITRUST-Certified application in the AWS cloud.

Kris Hatcher

Development Lead @ Smart Data

My Name Is **Kris Hatcher**

- **Developer** with over 15 years experience
- Certified **Scrum Master** with experience on teams ranging from 2 to 20 people
- AWS Certified **Solutions Architect** with experience on a variety of systems from single app deployments to several multi-tenant apps in a single account
- Science Fiction TV fan, enjoy all Star Trek (except original series) but prefer Stargate: SG-1 & Atlantis
- Enjoy MCU movies a lot! #CaptainRogers
  (I haven't seen Infinity Wars yet, so NO SPOILERS!!!)

I work for **Smart Data**

- 50+ Staff Members
- Primarily focus on Cincinnati and Dayton markets
- Currently have clients across the Eastern United States
- Focus on consistent, reliable delivery of software by using Agile Principles and close, active discussion with Product Owners

smartdata

wearesmartdata.com

ASK QUESTIONS DURING THE SESSIONS!

slack

THERE IS A SEPARATE CHANNEL FOR EACH TRACK!

#2018--RED #2018--ORANGE #2018--YELLOW #2018--GREEN

#2018--BLUE #2018--PURPLE #2018--THANOS #2018--GAUNTLET

The Client & Project

Client

- Software as a Service company, specializing in
  - Healthcare Case Management
  - Assessments
  - Reporting
- Primary clients
  - Government Agencies
  - Managed Care Organizations
  - Case Management Agencies

Project

- Rewrite legacy case management and assessment application from scratch
- Support expanded assessment capabilities in new system
- Migrate users and content from legacy application to new application with minimal downtime
- Make use of modern infrastructure technologies for new platform in order to support cost-savings through scalability and flexibility

Back Story

- Client faced significant financial pressure and reduced their internal development staff, moving their support development to a sub-contracting development firm.
- After using that firm for several years, the Client became unable to meet timelines promised to clients and had significant problems communicating with the firm's development team.
- These and other problems drove the Client to look for a new partner in their efforts to complete work for their clients.

Back Story

- The Client approached Smart Data about the possibility of assisting with their development efforts in the Fall of 2016.
- Smart Data assembled a team dedicated to the Client and began working to understand the scope of the project.
- The Client & Smart Data faced significant problems while attempting to move development work (including source code and infrastructure resources) from the previous firm to Smart Data.

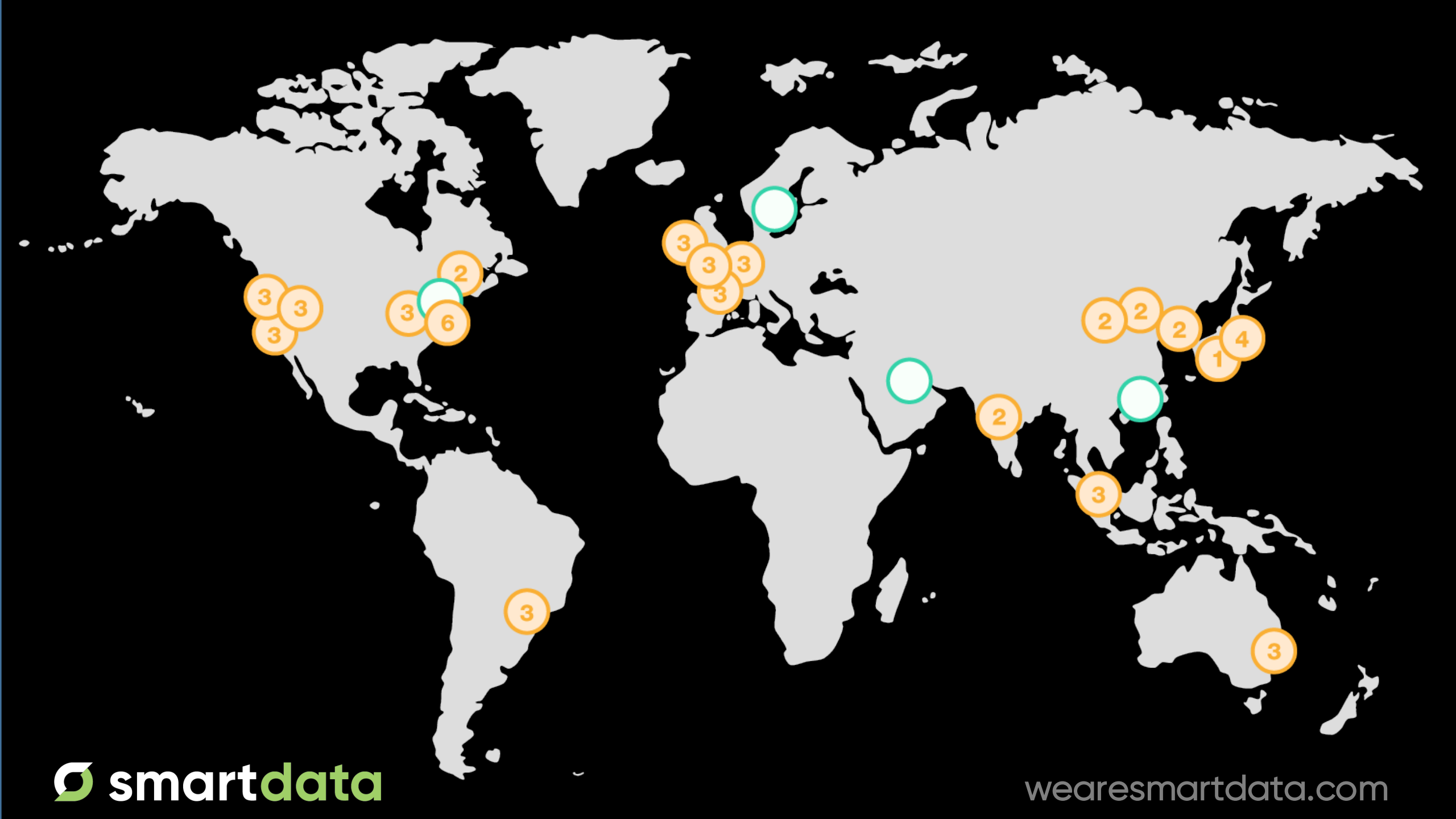
Initial Infrastructure

- Unit Testing framework was in place, but completely unused
- No part of deployment was automated
- Manually created & deployed AMIs
- Manually configured AWS environments, including scaling rules
- No standardization of naming, and use of multiple AWS Regions, resulted in an inability to know what resources were in Production use and what were for various testing environments

Security Concerns

- Application handles Personally Identifiable Information (PII) and Protected Health Information (PHI) & must follow guidelines put forth in the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act

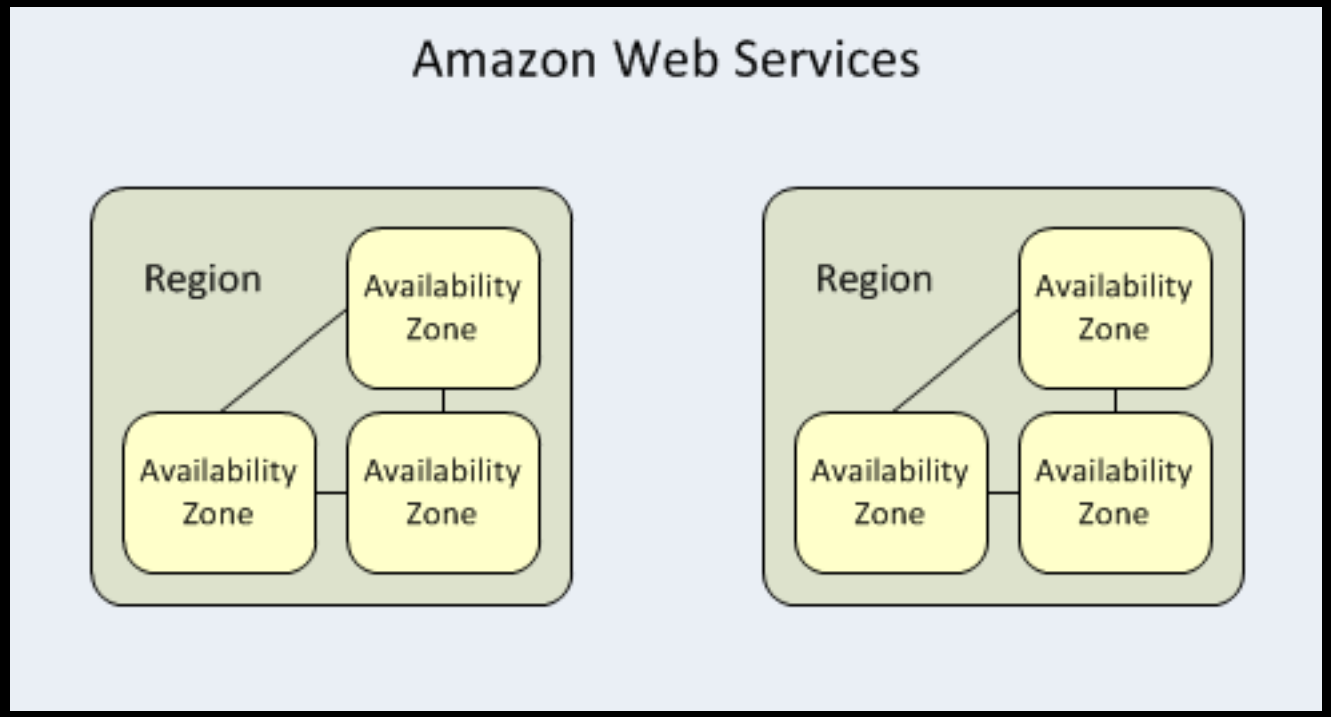
Amazon Web Services



smartdata

wearesmartdata.com

Regions & Availability Zones



Regions & Availability Zones

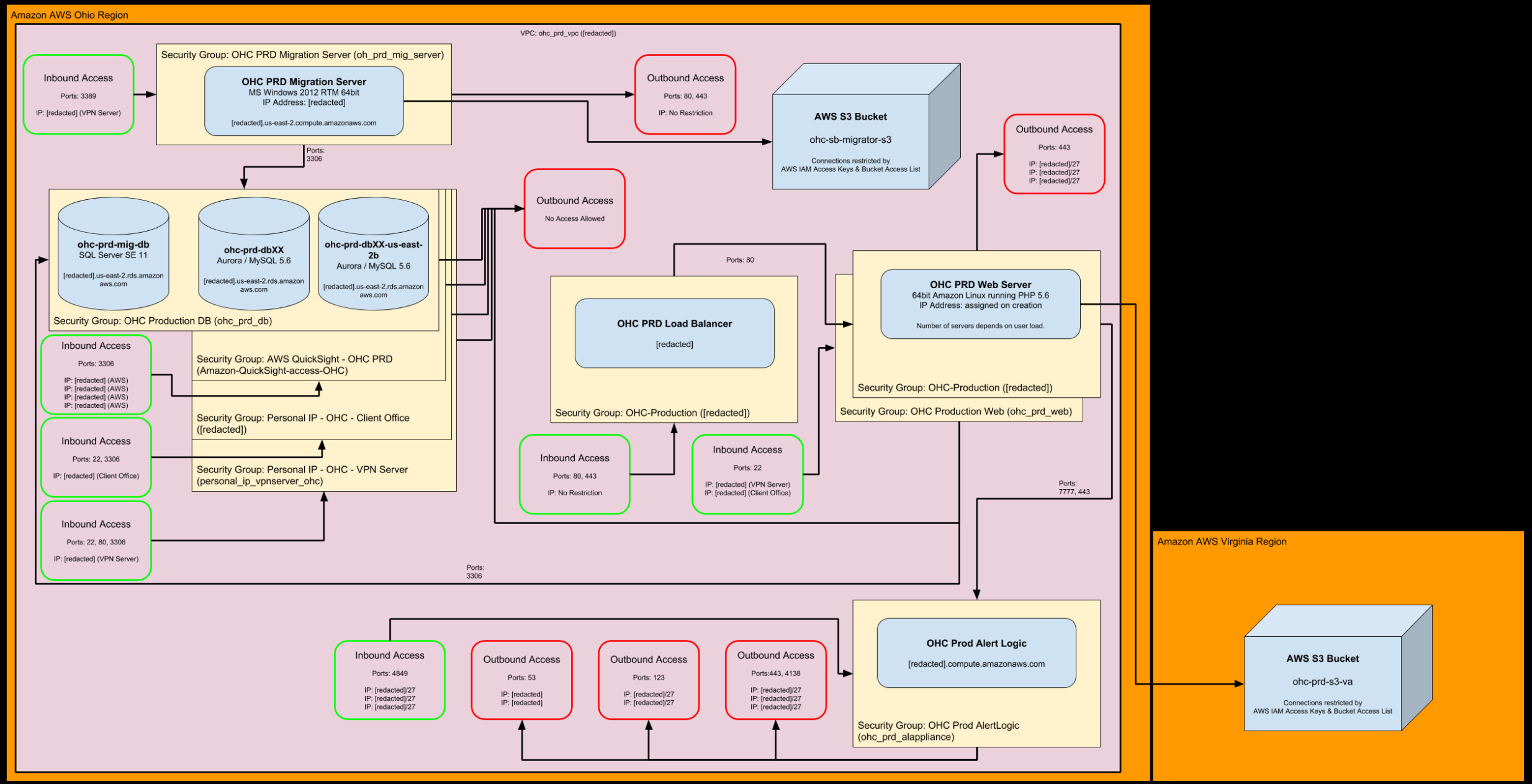
Region = Columbus *(us-east-2)*

AZ 1 = Dublin *(us-east-2a)*
AZ 2 = Hilliard *(us-east-2b)*
AZ 3 = New Albany *(us-east-2c)*

Glossary

- **Instance = Server**

- AZ = Availability Zone *(datacenter)*
- VPC = Virtual Private Cloud *(network)*
- EC2 = Elastic Cloud Compute *(server)*
- AMI = Amazon Machine Image
- RDS = Relational Database Service
- S3 = Simple Storage Service
- EB = Elastic Beanstalk


Amazon AWS Ohio Region
VPC: ohc_prd_vpc ([redacted])
Inbound Access
Ports: 3389
IP: [redacted] (VPN Server)
Security Group: OHC PRD Migration Server (oh_prd_mig_server)
OHC PRD Migration Server
MS Windows 2012 RTM 64bit
IP Address: [redacted]
[redacted].us-east-2.compute.amazonaws.com
Outbound Access
Ports: 80, 443
IP: No Restriction
AWS S3 Bucket
ohc-sb-migrator-s3
Connections restricted by
AWS IAM Access Keys & Bucket Access List
Outbound Access
Ports: 443
IP: [redacted]/27
IP: [redacted]/27
IP: [redacted]/27
Ports:
3306
ohc-prd-mig-db
SQL Server SE 11
[redacted].us-east-2.rds.amazonaws.com
ohc-prd-dbXX
Aurora / MySQL 5.6
[redacted].us-east-2.rds.amazonaws.com
ohc-prd-dbXX-us-east-2b
Aurora / MySQL 5.6
[redacted].us-east-2.rds.amazonaws.com
Security Group: OHC Production DB (ohc_prd_db)
Outbound Access
No Access Allowed
Ports: 80
OHC PRD Load Balancer
[redacted]
Security Group: OHC-Production ([redacted])
OHC PRD Web Server
64bit Amazon Linux running PHP 5.6
IP Address: assigned on creation
Number of servers depends on user load.
Security Group: OHC-Production ([redacted])
Security Group: OHC Production Web (ohc_prd_web)
Inbound Access
Ports: 3306
IP: [redacted] (AWS)
IP: [redacted] (AWS)
IP: [redacted] (AWS)
IP: [redacted] (AWS)
Security Group: AWS QuickSight - OHC PRD
(Amazon-QuickSight-access-OHC)
Inbound Access
Ports: 22, 3306
IP: [redacted] (Client Office)
Security Group: Personal IP - OHC - Client Office
([redacted])
Inbound Access
Ports: 22, 80, 3306
IP: [redacted] (VPN Server)
Security Group: Personal IP - OHC - VPN Server
(personal_ip_vpnserver_ohc)
Inbound Access
Ports: 80, 443
IP: No Restriction
Inbound Access
Ports: 22
IP: [redacted] (VPN Server)
IP: [redacted] (Client Office)
Ports:
7777, 443
Ports:
3306
Inbound Access
Ports: 4849
IP: [redacted]/27
IP: [redacted]/27
IP: [redacted]/27
Outbound Access
Ports: 53
IP: [redacted]
IP: [redacted]
Outbound Access
Ports: 123
IP: [redacted]/27
IP: [redacted]/27
Outbound Access
Ports:443, 4138
IP: [redacted]/27
IP: [redacted]/27
IP: [redacted]/27
OHC Prod Alert Logic
[redacted].compute.amazonaws.com
Security Group: OHC Prod AlertLogic
(ohc_prd_alappliance)
Amazon AWS Virginia Region
AWS S3 Bucket
ohc-prd-s3-va
Connections restricted by
AWS IAM Access Keys & Bucket Access List

Web Servers

Web Servers - Legacy

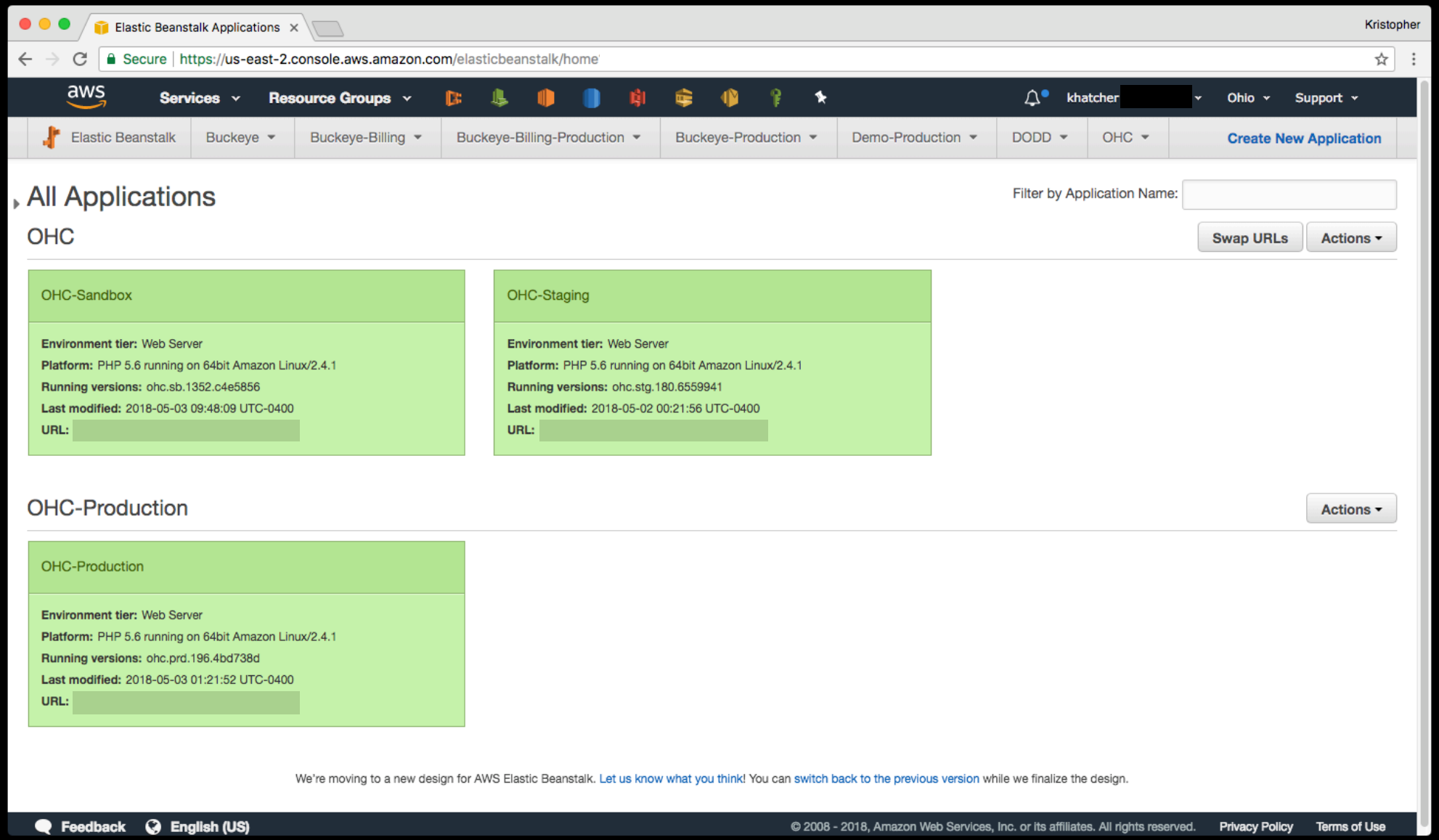
- Environment hosted on leased servers in shared datacenter.
- Physical servers, which require significant time to on-board if new servers are necessary
- Inconsistent backups, with minimal paths to restore in case of system failure

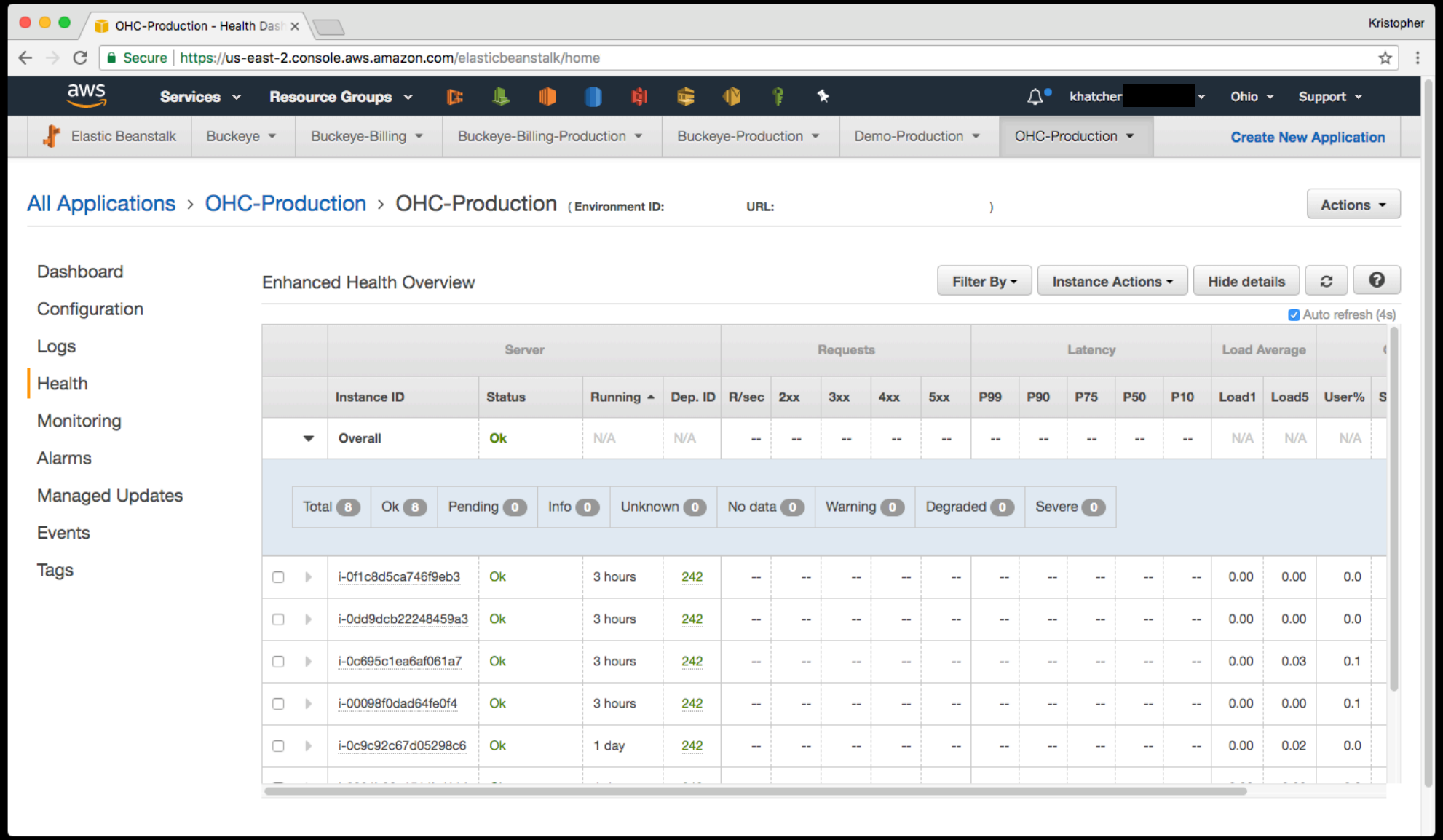
Web Servers – New System

- Based on AWS Elastic Cloud Compute (EC2) instances, environment scales as necessary based on load in the system
- Using AWS Elastic Beanstalk (EB), code deployments are rolling, with individual servers being pulled out of load balancer pool one at a time for updates before being placed back into the pool
- EB also monitors instance health and can terminate instances which are unhealthy after replacing them with new ones

Web Servers – Next Steps

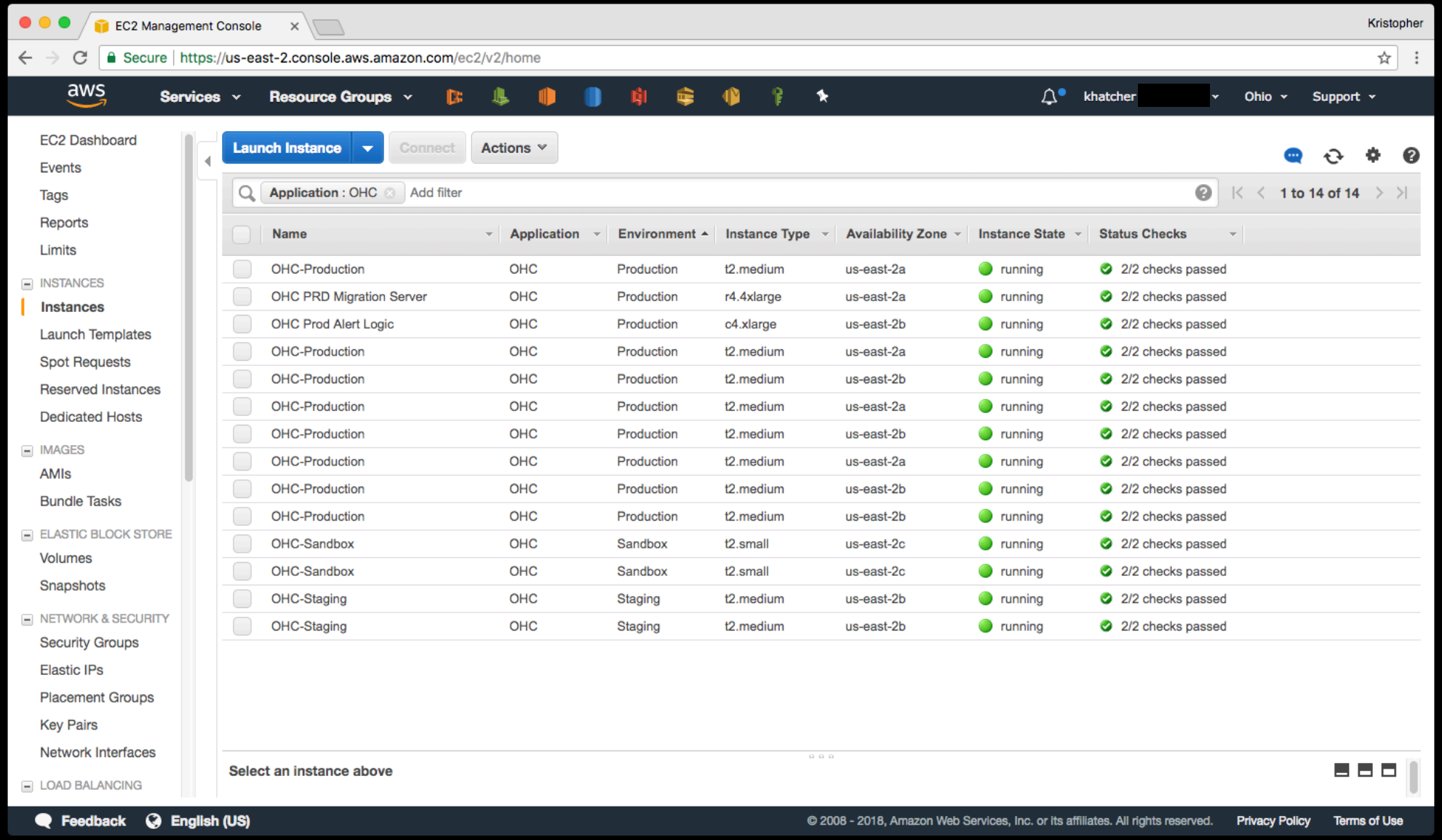
- Switch from Elastic Beanstalk to Cloud Formation
  - Provides more detailed control of process
- Modify deployment process to always create new instances, instead of “upgrading” instances currently in use
  - Prevents system from developing “ghosts” based on areas of code which are not operating as efficiently as they should be

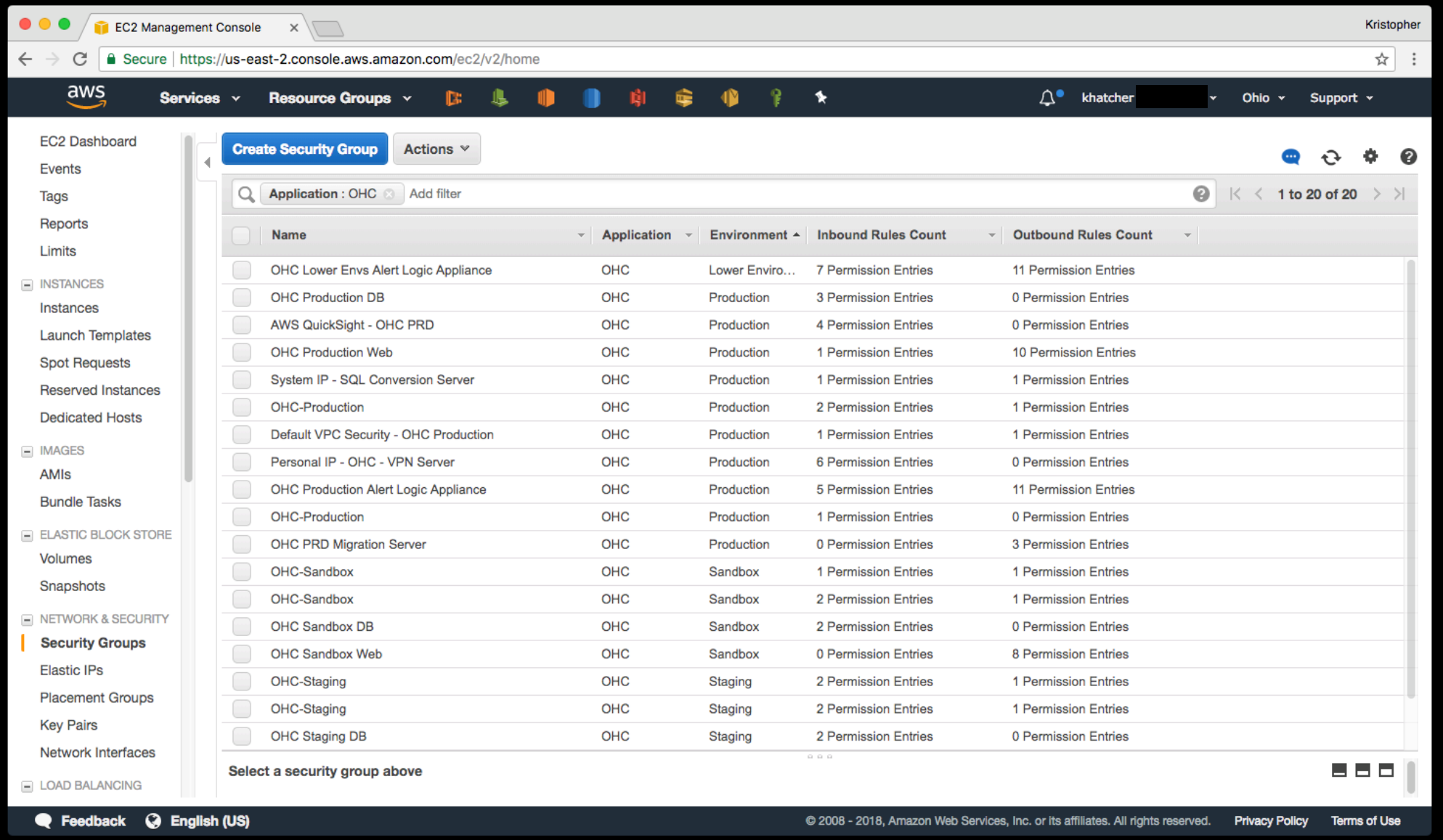




smartdata

wearesmartdata.com





Databases

Databases - Legacy

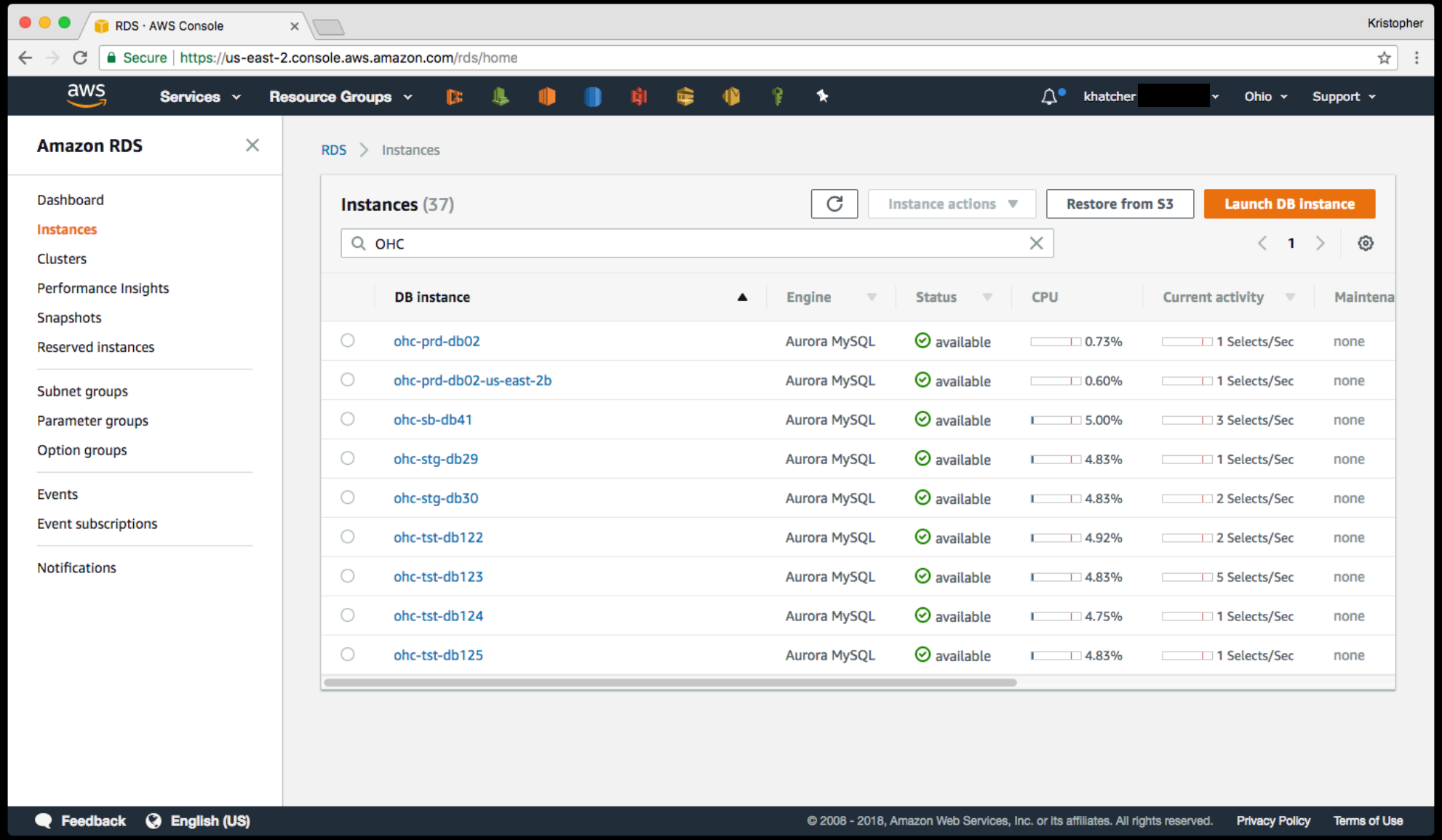
- Environment hosted on leased servers in shared datacenter.
- Physical servers, which require significant time to on-board if new servers are necessary
- Inconsistent backups, with minimal paths to restore in case of system failure
- Microsoft SQL system, which drove costs up due to licensing fees

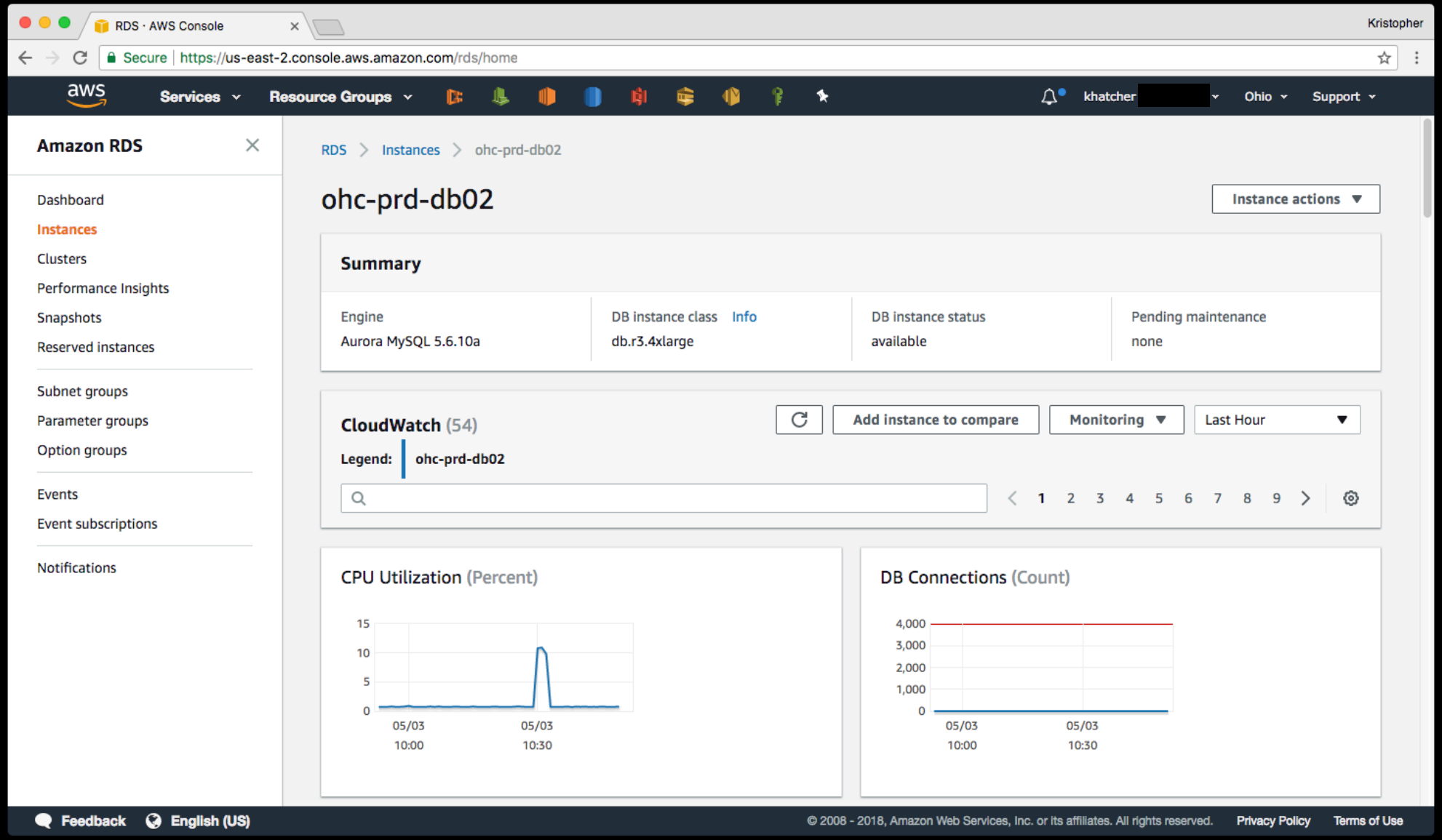
Databases – New System

- Used AWS Relational Database Service (RDS) and their “Aurora” database, based on MySQL technology with enhancements to improve speed & efficiency in cloud environments
- Flexible instance sizing provides the ability to have different sizes for different environments and to easily change that size as necessary
- Built-in backup technology provides
  - Every transaction for the last 24 hours
  - Daily backups stored for a configurable length of time
  - Hot-standby servers in a separate Availability Zone and/or Region

Databases – Next Steps

- Automated process to pull backups from Production into lower environments for debugging & development purposes
  - Including capability to scramble PII
- Additional research to “right-size” the database instances to their use based on observed metrics
- Modify Testing & Development environments to use Aurora Serverless to minimize costs in less-used environments


RDS · AWS Console
Kristopher
Secure | https://us-east-2.console.aws.amazon.com/rds/home
aws
Services
Resource Groups
khatcher
Ohio
Support
Amazon RDS
Dashboard
Instances
Clusters
Performance Insights
Snapshots
Reserved instances
Subnet groups
Parameter groups
Option groups
Events
Event subscriptions
Notifications
RDS > Instances
Instances (37)
Instance actions
Restore from S3
Launch DB instance
OHC
1
DB instance
Engine
Status
CPU
Current activity
Maintena
ohc-prd-db02 Aurora MySQL available 0.73% 1 Selects/Sec none
ohc-prd-db02-us-east-2b Aurora MySQL available 0.60% 1 Selects/Sec none
ohc-sb-db41 Aurora MySQL available 5.00% 3 Selects/Sec none
ohc-stg-db29 Aurora MySQL available 4.83% 1 Selects/Sec none
ohc-stg-db30 Aurora MySQL available 4.83% 2 Selects/Sec none
ohc-tst-db122 Aurora MySQL available 4.92% 2 Selects/Sec none
ohc-tst-db123 Aurora MySQL available 4.83% 5 Selects/Sec none
ohc-tst-db124 Aurora MySQL available 4.75% 1 Selects/Sec none
ohc-tst-db125 Aurora MySQL available 4.83% 1 Selects/Sec none
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use



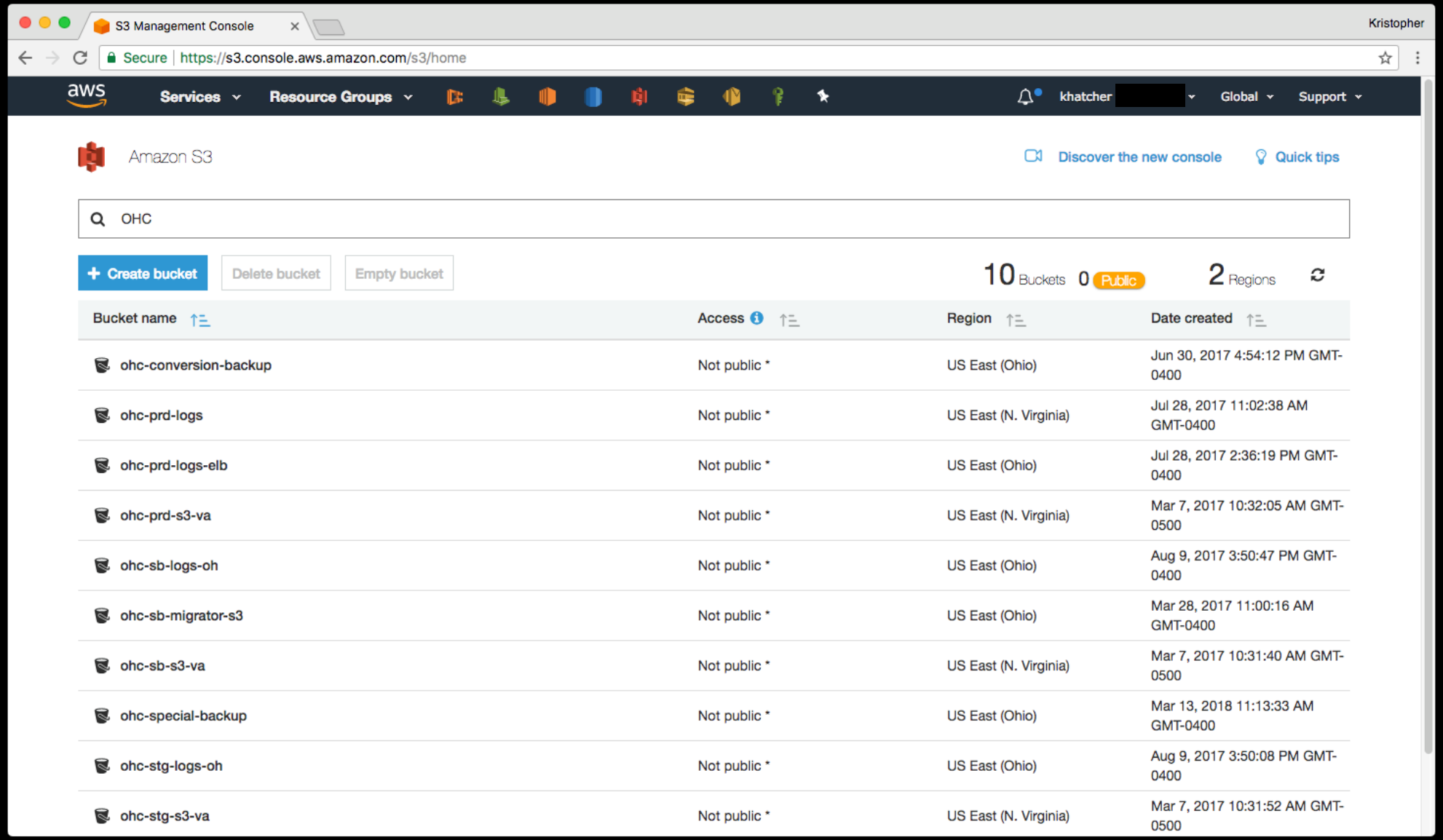
Document Storage

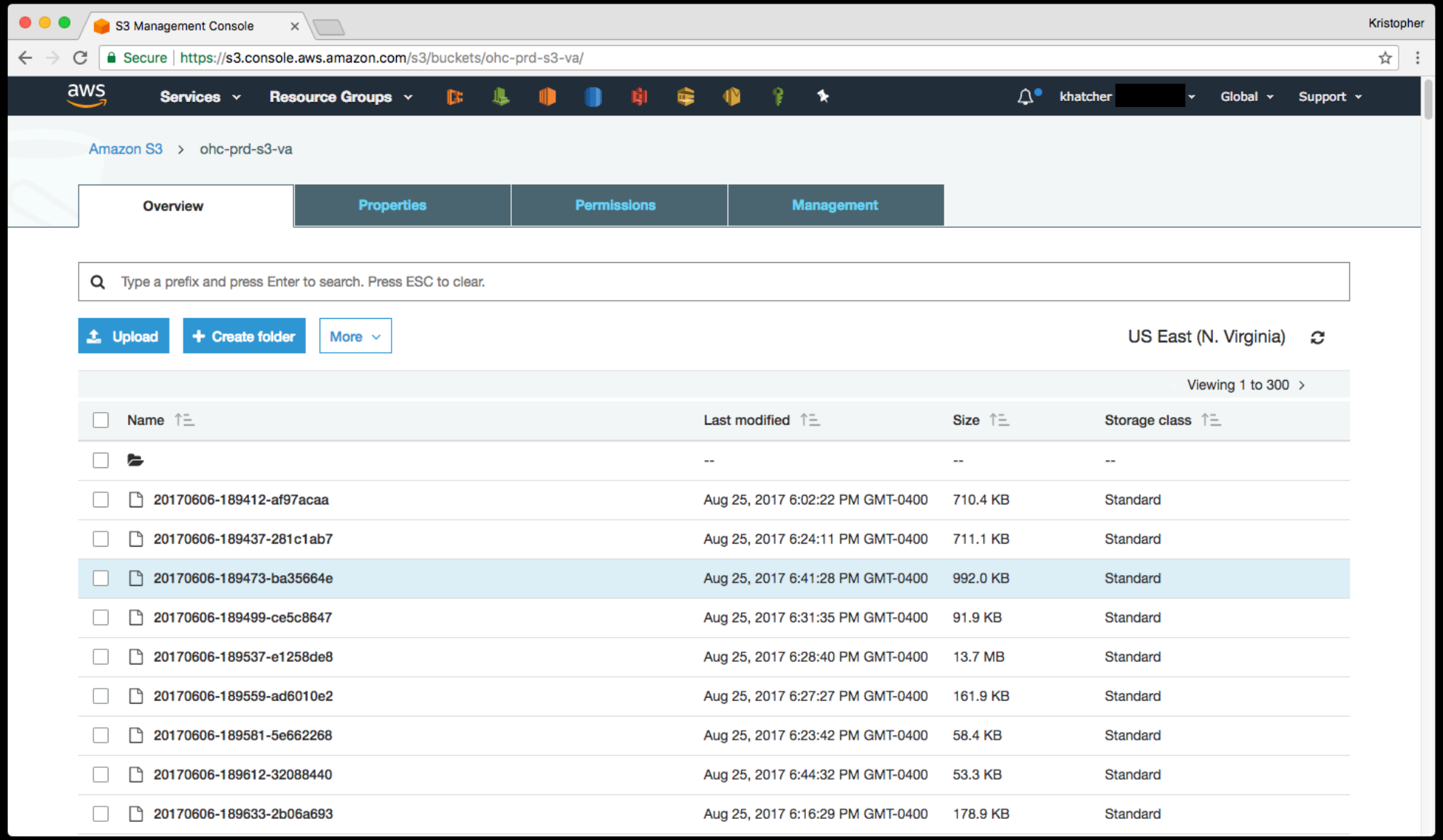
Document Storage - Legacy

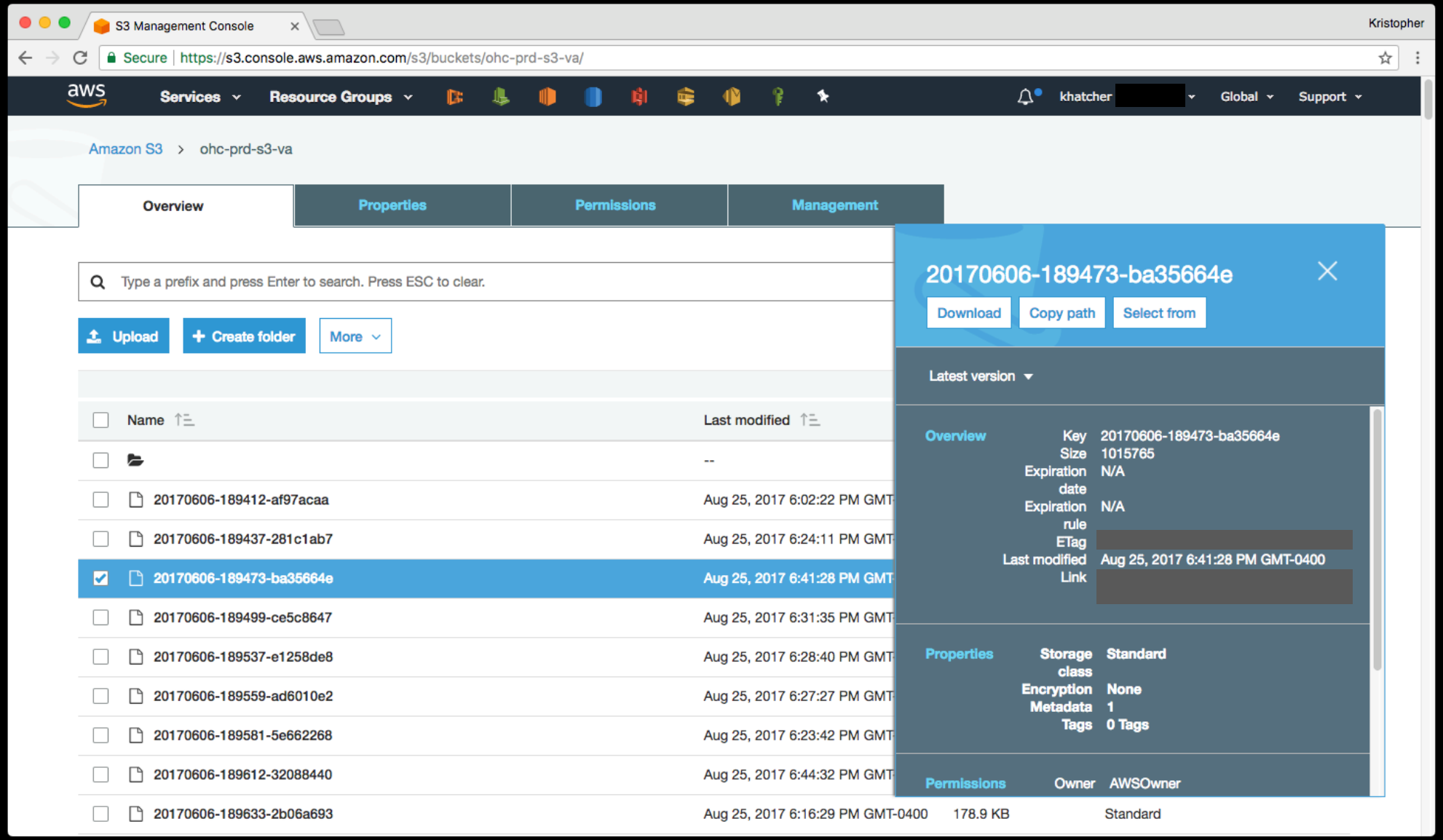
- Documents were stored on the web server
- No specific backup system in place
- Difficult to find documents for error report diagnosis

Document Storage – New System

- Documents are now stored in AWS Simple Storage Service (S3)
- Unified organizational structure provides ease of finding documents when necessary for error research
- AWS S3 provides built-in redundancy protections, promising 99.999999999% durability


S3 Management Console
Kristopher
Secure | https://s3.console.aws.amazon.com/s3/home
aws
Services
Resource Groups
khatcher
Global
Support
Amazon S3
Discover the new console
Quick tips
OHC
+ Create bucket
Delete bucket
Empty bucket
10 Buckets 0 Public
2 Regions
Bucket name
Access
Region
Date created
ohc-conversion-backup Not public * US East (Ohio) Jun 30, 2017 4:54:12 PM GMT-0400
ohc-prd-logs Not public * US East (N. Virginia) Jul 28, 2017 11:02:38 AM GMT-0400
ohc-prd-logs-elb Not public * US East (Ohio) Jul 28, 2017 2:36:19 PM GMT-0400
ohc-prd-s3-va Not public * US East (N. Virginia) Mar 7, 2017 10:32:05 AM GMT-0500
ohc-sb-logs-oh Not public * US East (Ohio) Aug 9, 2017 3:50:47 PM GMT-0400
ohc-sb-migrator-s3 Not public * US East (Ohio) Mar 28, 2017 11:00:16 AM GMT-0400
ohc-sb-s3-va Not public * US East (N. Virginia) Mar 7, 2017 10:31:40 AM GMT-0500
ohc-special-backup Not public * US East (Ohio) Mar 13, 2018 11:13:33 AM GMT-0400
ohc-stg-logs-oh Not public * US East (Ohio) Aug 9, 2017 3:50:08 PM GMT-0400
ohc-stg-s3-va Not public * US East (N. Virginia) Mar 7, 2017 10:31:52 AM GMT-0500




S3 Management Console
Kristopher
Secure | https://s3.console.aws.amazon.com/s3/buckets/ohc-prd-s3-va/
aws
Services
Resource Groups
khatcher
Global
Support
Amazon S3 > ohc-prd-s3-va
Overview
Properties
Permissions
Management
Type a prefix and press Enter to search. Press ESC to clear.
Upload
+ Create folder
More
Name
Last modified
--
20170606-189412-af97acaa
Aug 25, 2017 6:02:22 PM GMT
20170606-189437-281c1ab7
Aug 25, 2017 6:24:11 PM GMT
20170606-189473-ba35664e
Aug 25, 2017 6:41:28 PM GMT
20170606-189499-ce5c8647
Aug 25, 2017 6:31:35 PM GMT
20170606-189537-e1258de8
Aug 25, 2017 6:28:40 PM GMT
20170606-189559-ad6010e2
Aug 25, 2017 6:27:27 PM GMT
20170606-189581-5e662268
Aug 25, 2017 6:23:42 PM GMT
20170606-189612-32088440
Aug 25, 2017 6:44:32 PM GMT
20170606-189633-2b06a693
Aug 25, 2017 6:16:29 PM GMT-0400
178.9 KB
Standard
20170606-189473-ba35664e
Download
Copy path
Select from
Latest version
Overview
Key 20170606-189473-ba35664e
Size 1015765
Expiration date N/A
Expiration rule N/A
ETag
Last modified Aug 25, 2017 6:41:28 PM GMT-0400
Link
Properties
Storage class Standard
Encryption None
Metadata 1
Tags 0 Tags
Permissions
Owner AWSOwner

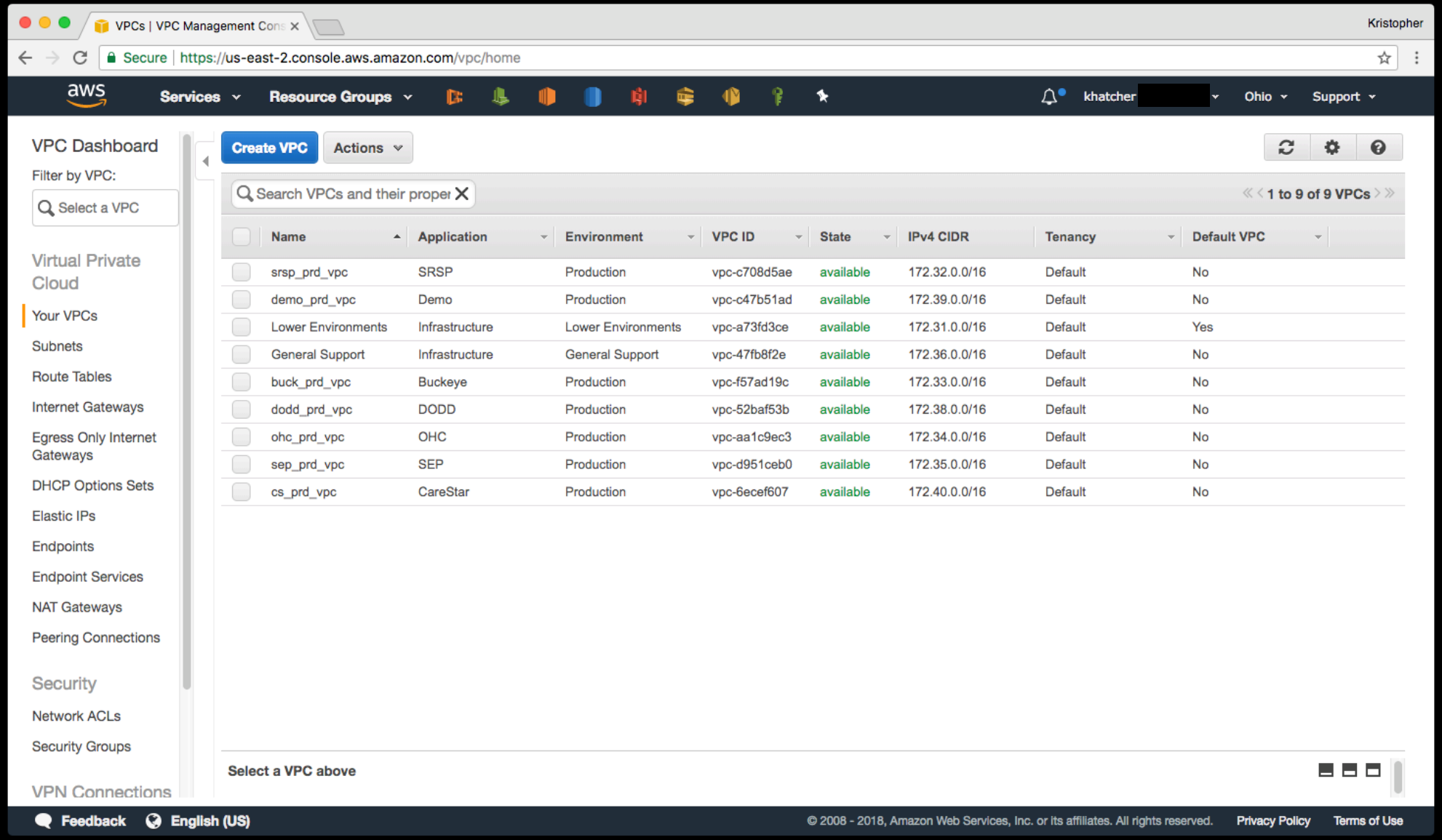
Infrastructure

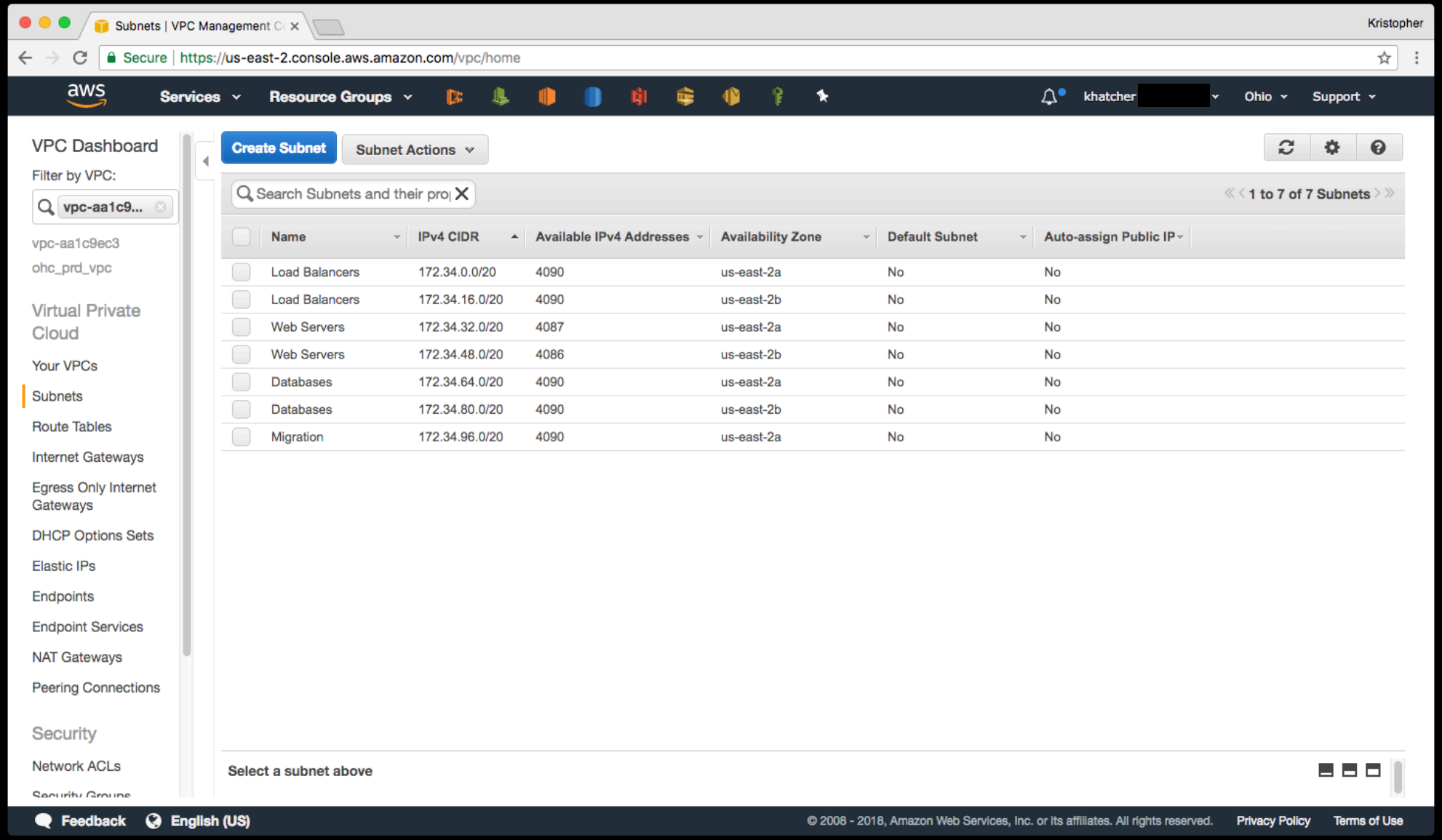
Infrastructure – Legacy

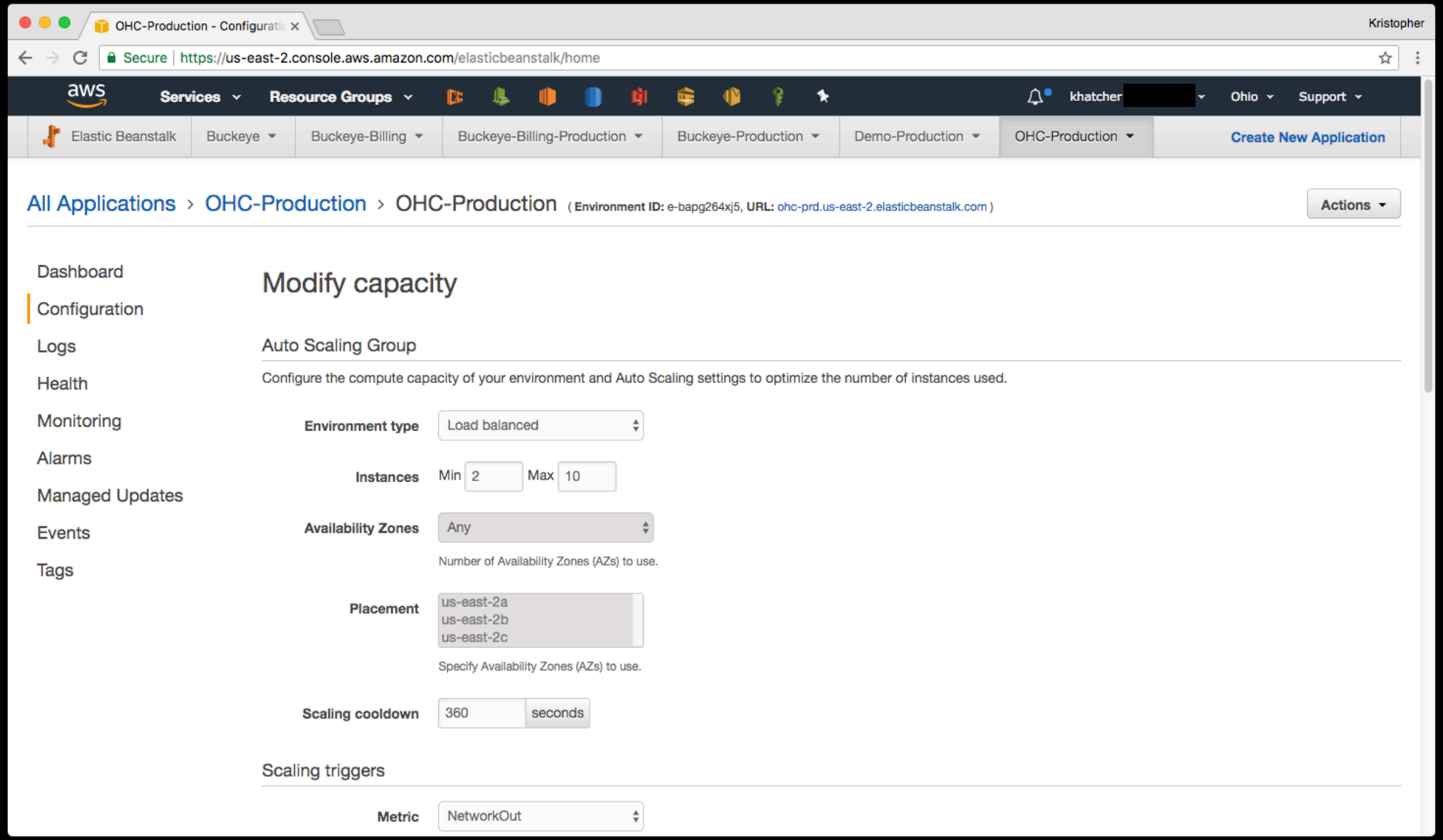
- No testing environments
- Physical servers
- No scaling

Infrastructure – New System

- Each application (6 total) has Sandbox, Staging, and Production environments
- Each production application is in it's own VPC, with access restricted and monitored
- Creating environments for new applications is a documented process that can be completed by anyone with a basic understanding of AWS
- All environments scale web instances based on usage
- All infrastructure for an environment is right-sized to that environment's needs and use-case



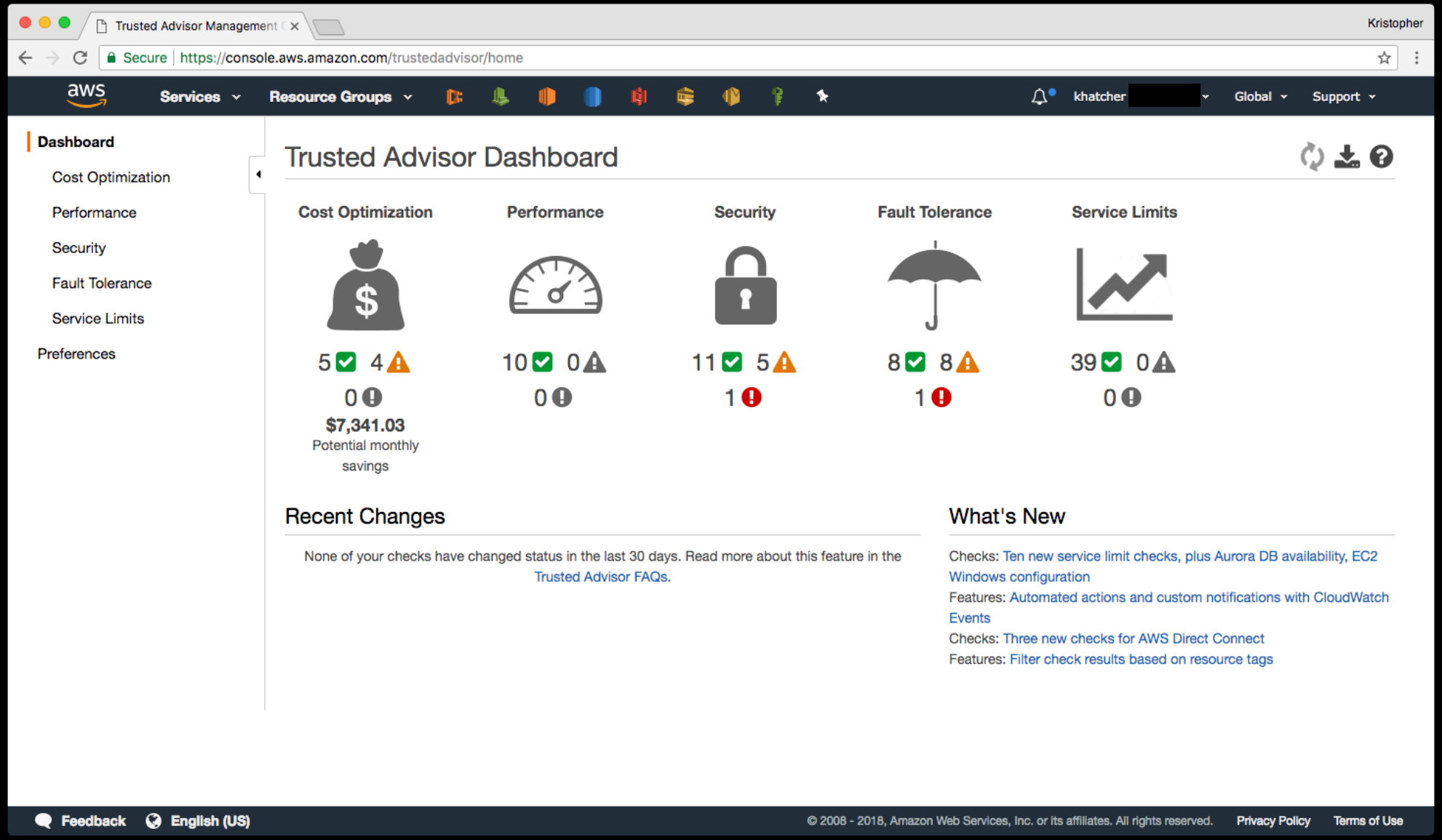


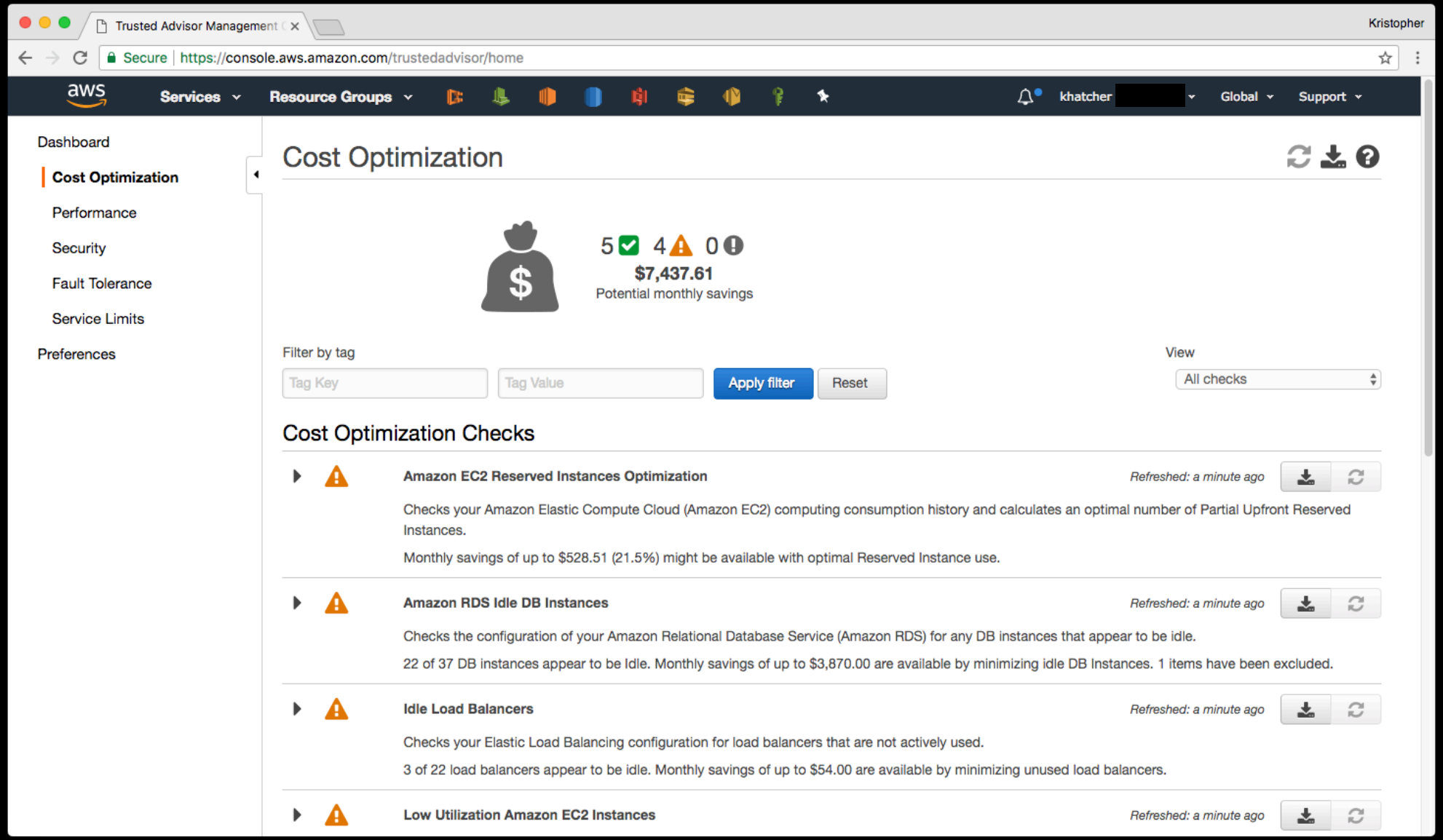

OHC-Production - Configuratic
Kristopher
Secure | https://us-east-2.console.aws.amazon.com/elasticbeanstalk/home
aws
Services
Resource Groups
khatcher [redacted]
Ohio
Support
Elastic Beanstalk
Buckeye
Buckeye-Billing
Buckeye-Billing-Production
Buckeye-Production
Demo-Production
OHC-Production
Create New Application
All Applications › OHC-Production › OHC-Production (Environment ID: e-bapg264xj5, URL: ohc-prd.us-east-2.elasticbeanstalk.com)
Actions
Dashboard
Configuration
Logs
Health
Monitoring
Alarms
Managed Updates
Events
Tags
Modify capacity
Auto Scaling Group
Configure the compute capacity of your environment and Auto Scaling settings to optimize the number of instances used.
Environment type
Load balanced
Instances
Min 2 Max 10
Availability Zones
Any
Number of Availability Zones (AZs) to use.
Placement
us-east-2a
us-east-2b
us-east-2c
Specify Availability Zones (AZs) to use.
Scaling cooldown
360
seconds
Scaling triggers
Metric
NetworkOut

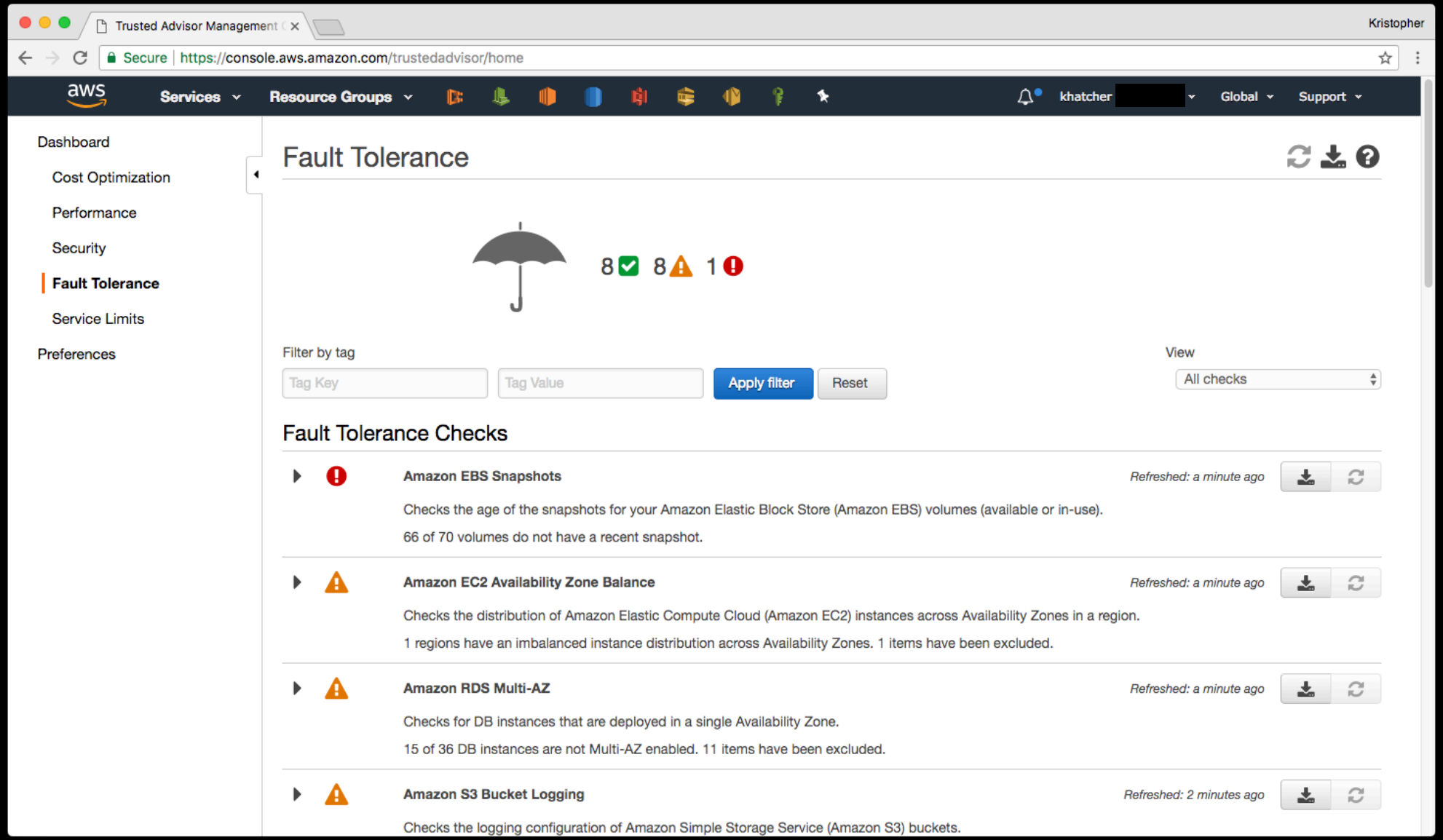
Lessons Learned & Next Steps

Lessons Learned & Next Steps

- Separate general infrastructure
- Use Elastic Beanstalk for rapid prototyping and initial development, then use Cloud Formation for long-term implementation and Production use-cases
- Take advantage of AWS tools to minimize spend on non-critical portions of system







Thank you!

speakerdeck.com/krishatcher/climbing-the-elastic-beanstalk

linkedin.com/in/krishatcher/