MICHIGAN STATE UNIVERSITY

Alpha Presentation
Endpoint Data Monitoring and Analysis Agent

The Capstone Experience

Team Rook

Jared Clark
Drew Gilbertson
Bohao Gao
Jeremy Specht
Vikram Thakur

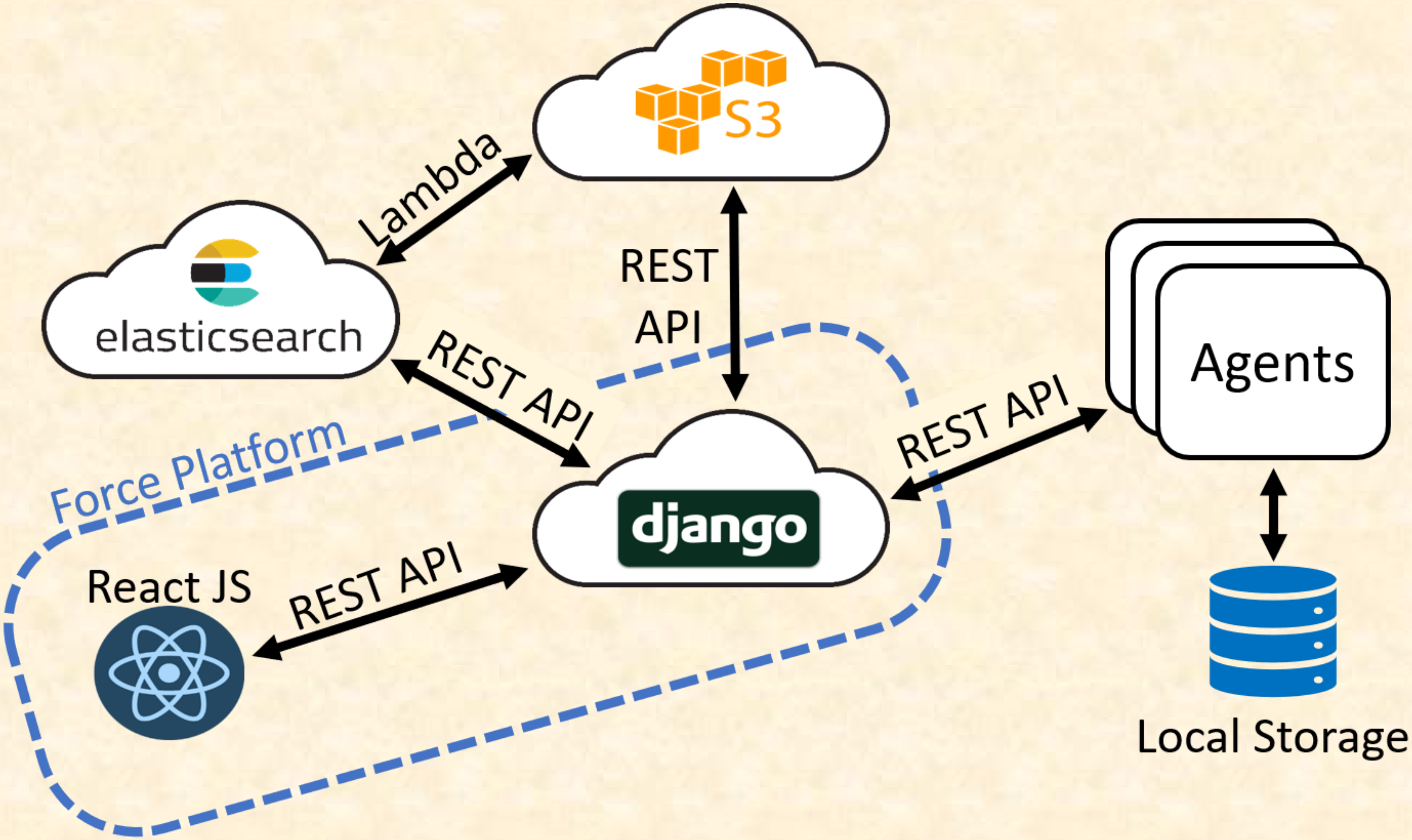
Department of Computer Science and Engineering
Michigan State University
Spring 2018

From Students…
…to Professionals

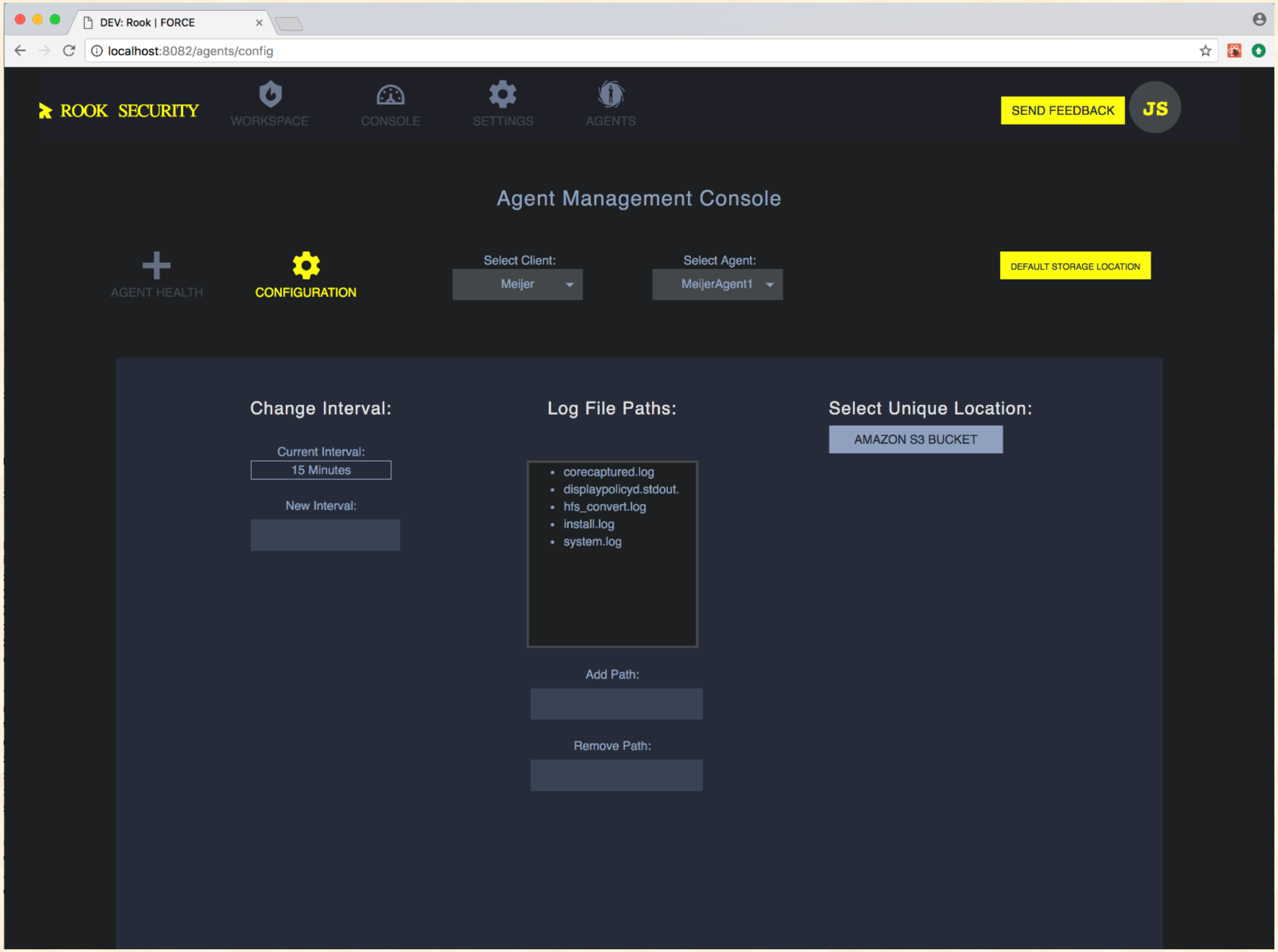
Project Overview

- Endpoint Agent Log Collection
  - Cross Platform Compatible
- Communication Channels for Data
  - Configurable
- Web Application to Analyze Agent
  - Configuration
    - Log Paths, Storage Location
  - Health Analysis
    - Alert Priorities

System Architecture



Force Platform



Agent Management Console

Select Client: Meijer

Select Agent: MeijerAgent1

Change Interval:

Current Interval: 15 Minutes

New Interval:

Log File Paths:

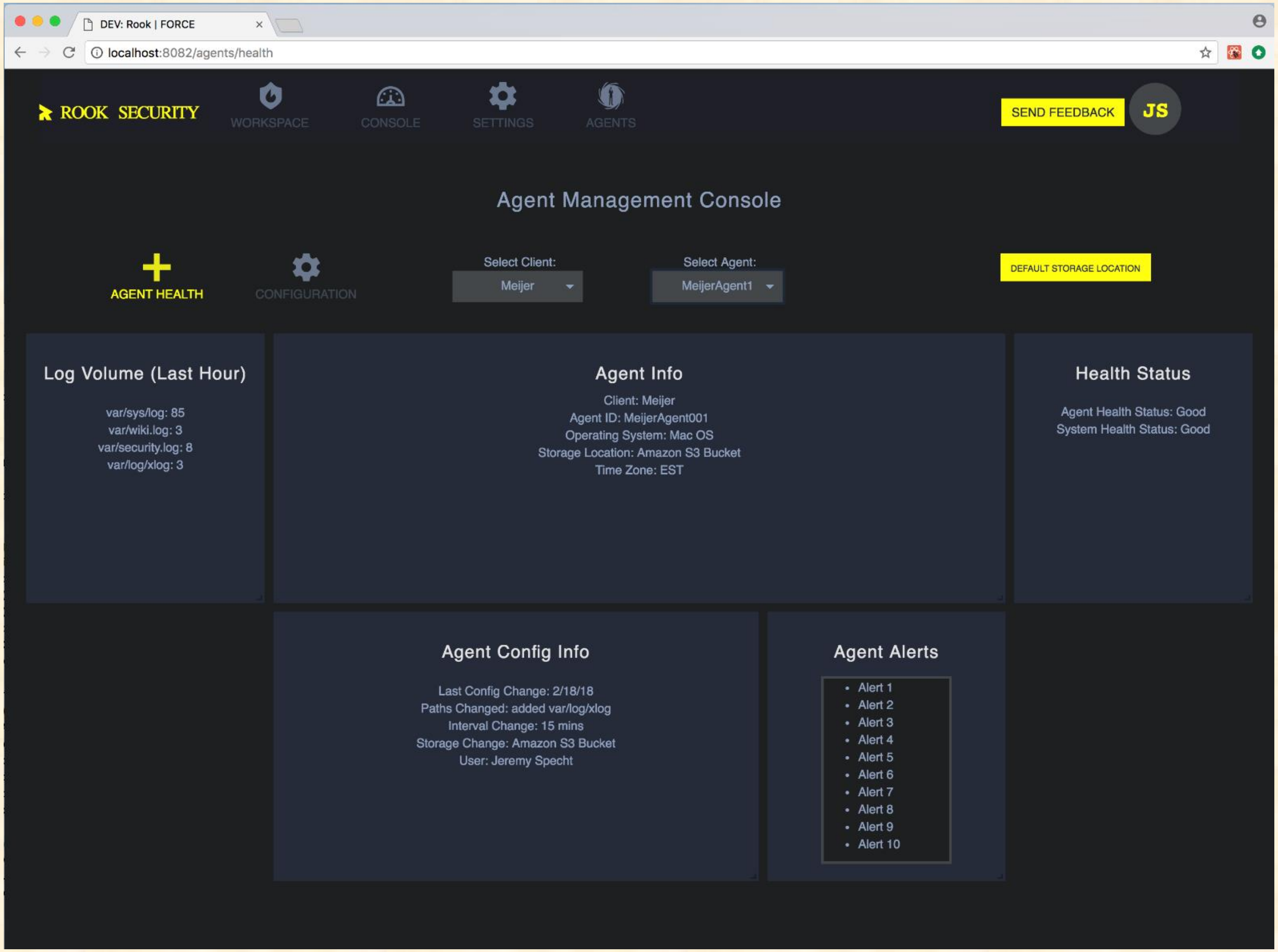
- corecaptured.log
- displaypolicyd.stdout.
- hfs_convert.log
- install.log
- system.log

Add Path:

Remove Path:

Select Unique Location:

Force Platform



Agent Management Console

Select Client: Meijer

Select Agent: MeijerAgent1

Log Volume (Last Hour)

var/sys/log: 85
var/wiki.log: 3
var/security.log: 8
var/log/xlog: 3

Agent Info

Client: Meijer
Agent ID: MeijerAgent001
Operating System: Mac OS
Storage Location: Amazon S3 Bucket
Time Zone: EST

Health Status

Agent Health Status: Good
System Health Status: Good

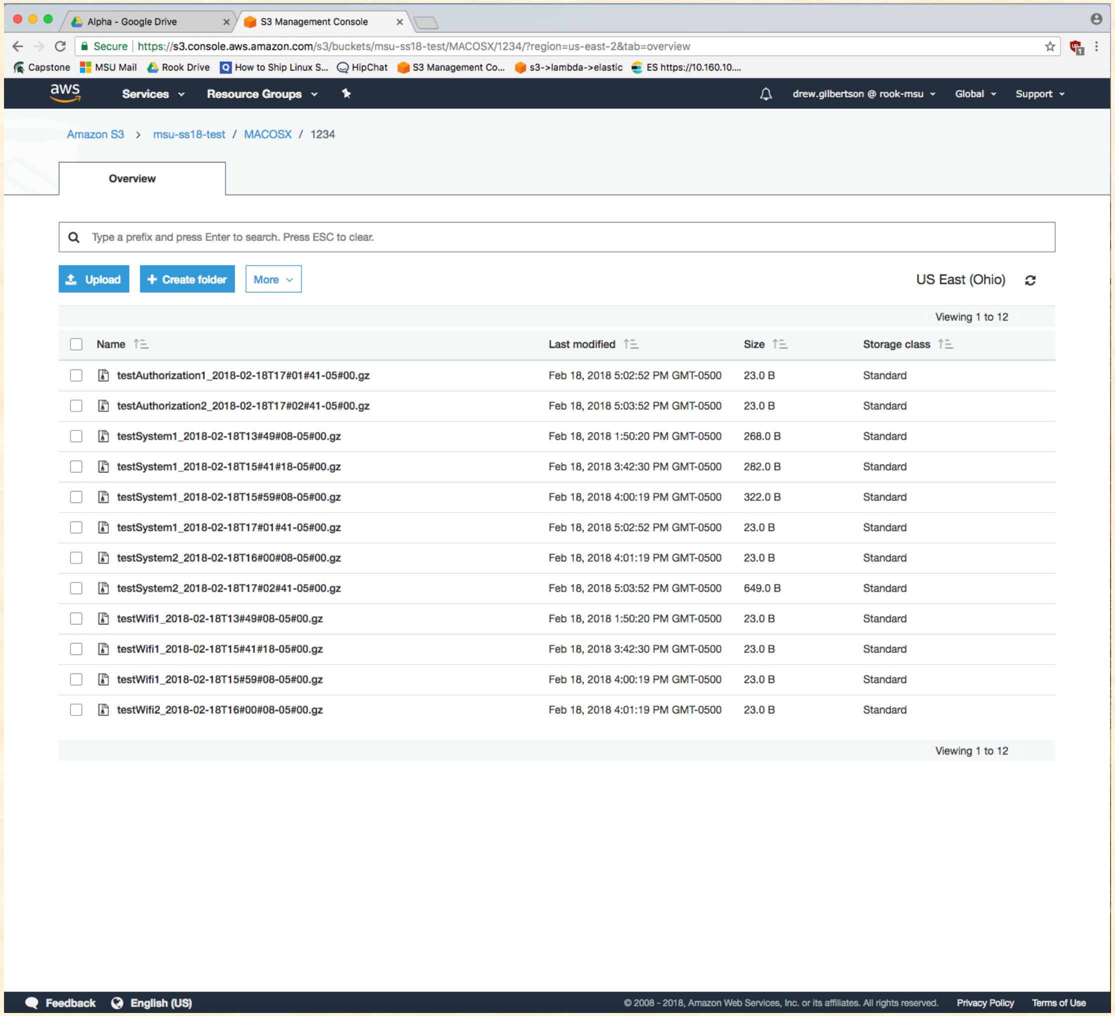
Agent Config Info

Last Config Change: 2/18/18
Paths Changed: added var/log/xlog
Interval Change: 15 mins
Storage Change: Amazon S3 Bucket
User: Jeremy Specht

Agent Alerts

- Alert 1
- Alert 2
- Alert 3
- Alert 4
- Alert 5
- Alert 6
- Alert 7
- Alert 8
- Alert 9
- Alert 10

Storage System



Secure | https://s3.console.aws.amazon.com/s3/buckets/msu-ss18-test/MACOSX/1234/?region=us-east-2&tab=overview

Amazon S3 > msu-ss18-test / MACOSX / 1234

Type a prefix and press Enter to search. Press ESC to clear.

US East (Ohio)

Viewing 1 to 12

□	Name	Last modified	Size	Storage class
□	testAuthorization1_2018-02-18T17#01#41-05#00.gz	Feb 18, 2018 5:02:52 PM GMT-0500	23.0 B	Standard
□	testAuthorization2_2018-02-18T17#02#41-05#00.gz	Feb 18, 2018 5:03:52 PM GMT-0500	23.0 B	Standard
□	testSystem1_2018-02-18T13#49#08-05#00.gz	Feb 18, 2018 1:50:20 PM GMT-0500	268.0 B	Standard
□	testSystem1_2018-02-18T15#41#18-05#00.gz	Feb 18, 2018 3:42:30 PM GMT-0500	282.0 B	Standard
□	testSystem1_2018-02-18T15#59#08-05#00.gz	Feb 18, 2018 4:00:19 PM GMT-0500	322.0 B	Standard
□	testSystem1_2018-02-18T17#01#41-05#00.gz	Feb 18, 2018 5:02:52 PM GMT-0500	23.0 B	Standard
□	testSystem2_2018-02-18T16#00#08-05#00.gz	Feb 18, 2018 4:01:19 PM GMT-0500	23.0 B	Standard
□	testSystem2_2018-02-18T17#02#41-05#00.gz	Feb 18, 2018 5:03:52 PM GMT-0500	649.0 B	Standard
□	testWifi1_2018-02-18T13#49#08-05#00.gz	Feb 18, 2018 1:50:20 PM GMT-0500	23.0 B	Standard
□	testWifi1_2018-02-18T15#41#18-05#00.gz	Feb 18, 2018 3:42:30 PM GMT-0500	23.0 B	Standard
□	testWifi1_2018-02-18T15#59#08-05#00.gz	Feb 18, 2018 4:00:19 PM GMT-0500	23.0 B	Standard
□	testWifi2_2018-02-18T16#00#08-05#00.gz	Feb 18, 2018 4:01:19 PM GMT-0500	23.0 B	Standard

Viewing 1 to 12

What's left to do?

- Remote Configuration of Agent
- Front-End Development
  - Refine Interface Functionality
- Back-End Development
  - Feature Expansion
- Elasticsearch
  - Integration

Questions?

? ? ? ?

? ?

? ? ?