

MICHIGAN STATE
UNIVERSITY

Alpha Presentation

Endpoint Data Monitoring and Analysis

Agent

The Capstone Experience

Team Rook

Jared Clark

Drew Gilbertson

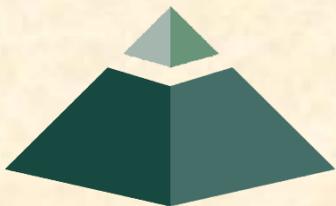
Bohao Gao

Jeremy Specht

Vikram Thakur

Department of Computer Science and Engineering
Michigan State University

Spring 2018



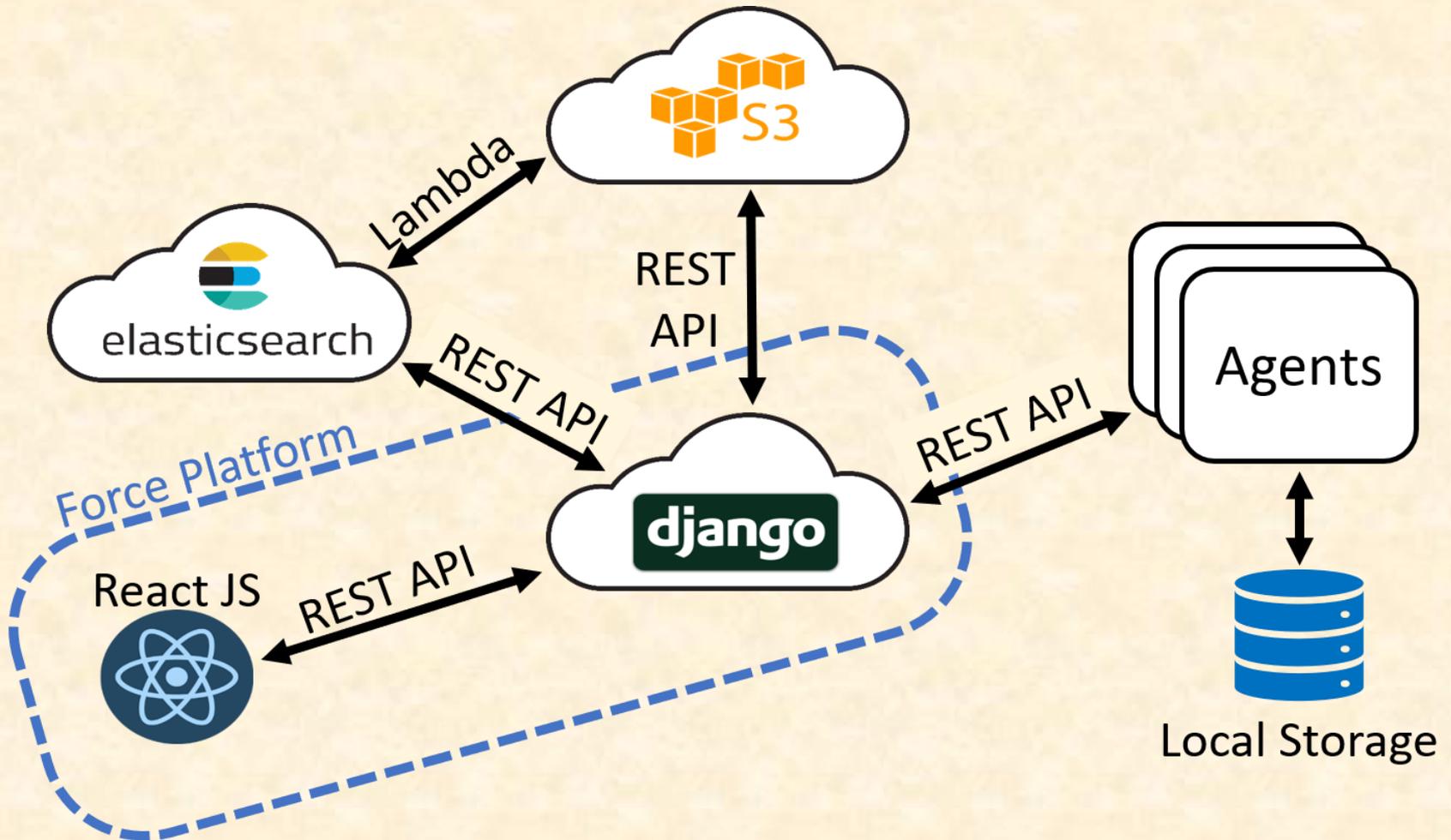
*From Students...
...to Professionals*

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

The screenshot shows a web browser window with the URL `localhost:8082/agents/config`. The page is titled "Agent Management Console" and features a dark theme with yellow accents. The navigation bar includes "ROOK SECURITY", "WORKSPACE", "CONSOLE", "SETTINGS", and "AGENTS", along with a "SEND FEEDBACK" button and a user profile "JS".

The main content area is divided into sections:

- AGENT HEALTH** (represented by a plus icon)
- CONFIGURATION** (represented by a gear icon)
- Select Client:** A dropdown menu currently showing "Meijer".
- Select Agent:** A dropdown menu currently showing "MeijerAgent1".
- DEFAULT STORAGE LOCATION** (represented by a yellow button)

The configuration section is further divided into three columns:

- Change Interval:** Includes a "Current Interval" field set to "15 Minutes" and a "New Interval" field.
- Log File Paths:** A list of log files: `corecaptured.log`, `displaypolicyd.stdout`, `hfs_convert.log`, `install.log`, and `system.log`. Below the list are "Add Path:" and "Remove Path:" buttons.
- Select Unique Location:** A dropdown menu currently showing "AMAZON S3 BUCKET".



Force Platform

The screenshot shows the Rook Security Agent Management Console in a web browser. The browser tab is labeled "DEV: Rook | FORCE" and the address bar shows "localhost:8082/agents/health". The interface has a dark theme with yellow accents. At the top, there is a navigation bar with icons for "ROOK SECURITY", "WORKSPACE", "CONSOLE", "SETTINGS", and "AGENTS". A "SEND FEEDBACK" button and a user profile "JS" are also visible. Below the navigation bar, the main heading is "Agent Management Console". There are two sub-sections: "AGENT HEALTH" (with a plus icon) and "CONFIGURATION" (with a gear icon). The "Select Client:" dropdown is set to "Meijer" and the "Select Agent:" dropdown is set to "MeijerAgent1". A "DEFAULT STORAGE LOCATION" button is on the right. The main content area is divided into several panels: "Log Volume (Last Hour)" showing log counts for various files; "Agent Info" displaying client details like Meijer, Agent ID, Operating System, Storage Location, and Time Zone; "Health Status" showing "Agent Health Status: Good" and "System Health Status: Good"; "Agent Config Info" showing configuration changes like "Last Config Change: 2/18/18" and "Storage Change: Amazon S3 Bucket"; and "Agent Alerts" showing a list of 10 alerts.

DEV: Rook | FORCE
localhost:8082/agents/health

ROOK SECURITY WORKSPACE CONSOLE SETTINGS AGENTS SEND FEEDBACK JS

Agent Management Console

AGENT HEALTH CONFIGURATION Select Client: Meijer Select Agent: MeijerAgent1 DEFAULT STORAGE LOCATION

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

The screenshot displays the AWS S3 Management Console interface. The browser address bar shows the URL: <https://s3.console.aws.amazon.com/s3/buckets/msu-ss18-test/MACOSX/1234/?region=us-east-2&tab=overview>. The page title is "Amazon S3 > msu-ss18-test / MacOSX / 1234". The "Overview" tab is selected. A search bar is present with the placeholder text "Type a prefix and press Enter to search. Press ESC to clear." Below the search bar are buttons for "Upload", "Create folder", and "More". The region is set to "US East (Ohio)". A table lists 12 objects, with columns for Name, Last modified, Size, and Storage class. The objects are grouped into testAuthorization, testSystem, and testWifi categories.

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



What's left to do?

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



Questions?

?

?

?

?

?

?

?

?

?

