



PROJECT

# Cloud Computing

Team Canada

## 1 INTRODUCTION

In recent years, Cloud Computing has become a necessity for businesses across all sectors and verticals. To keep a competitive edge, businesses leverage the cloud to develop solutions that can handle the demands of their customers and give them a positive customer experience given any load or fault scenario. There are key aspects to successfully building a cloud-based solution. These include system design, deployment, network design, high availability, scalability, automation, security, cost, and monitoring. This test project will assess Competitors based on their ability to effectively and securely deploy, maintain, and scale a web application.

These aspects are explained in more detail in the “Scaling A Web Application Break Down” section below.

## 2 DESCRIPTION OF PROJECT AND TASKS

This document describes the operational theory and practice for the production system powering the Unicorn Rentals website. The primary audience is the Unicorn Rentals DevOps team running the site. This team is responsible for deploying code, scaling the site in response to load, maintaining published SLAs (including response time and uptime), disaster recovery, troubleshooting activities, and any monitoring and alerting activities.

### Tasks

- Log into Gameday with your assigned hash (Provided on the day)
- Set your team/competitor name on the Dashboard – (Format: NAME SURNAME)
- Read the documentation thoroughly (Outlined below)
- Log into the AWS console (link provided from the Dashboard)
- Examine existing configurations in EC2 (Elastic Cloud Computer server)
- Examine existing configurations in VPC (Virtual Private Cloud, Network Segment)
- Configure application to auto scale to handle increasing load (Auto Scaling Groups, with Launch Configuration)
- Create/update the user data configuration correctly, including download locations of server binary and server configuration file

- Update the user data configuration to include any required local dependencies
- Configure any server dependencies as outlined in the technical details
- Configure necessary application monitoring, metrics and alarms in CloudWatch
- Monitor performance of the application servers in the “Score Events and Scoreboard” and through the AWS Console with CloudWatch
- Serve client requests to gain points, reference the “Score Events and Scoreboard” to ensure you are scoring positively by serving the requests.
- Monitor costs and do not scale up the infrastructure excessively to minimize penalties

## 2.1 Day 1: GameDay Experience




### 2.1.1 Initial States

At the start of the day, the minimal infrastructure needed to provide the public client API will be operational within the account. This infrastructure is neither scalable nor highly available. It does however provide a reference point for a functional deployment.

Please reference the TeamRole your account IAM console for any permissions based questions.

## Summary

[Delete role](#)

<b>Role ARN</b>	arn:aws:iam::117671164446:role/TeamRole 
<b>Role description</b>	<a href="#">Edit</a>
<b>Instance Profile ARNs</b>	arn:aws:iam::117671164446:instance-profile/TeamRoleInstanceProfile 
<b>Path</b>	/
<b>Creation time</b>	2019-08-21 03:17 CDT
<b>Maximum CLI/API session duration</b>	12 hours <a href="#">Edit</a>
<b>Give this link to users who can switch roles in the console</b>	<a href="https://signin.aws.amazon.com/switchrole?roleName=TeamRole&amp;account=117671164446">https://signin.aws.amazon.com/switchrole?roleName=TeamRole&amp;account=117671164446</a> 

[Permissions](#)
[Trust relationships](#)
[Tags](#)
[Access Advisor](#)
[Revoke sessions](#)

▼ Permissions policies (3 policies applied)

[Attach policies](#)
[+ Add inline policy](#)

Policy name ▼	Policy type ▼	
▶ <a href="#">restrict-policy</a>	Managed policy	✕
▶ <a href="#">ws-loadgen-aws-day2-policy</a>	Managed policy	✕
<a href="#">Show 1 more</a>		

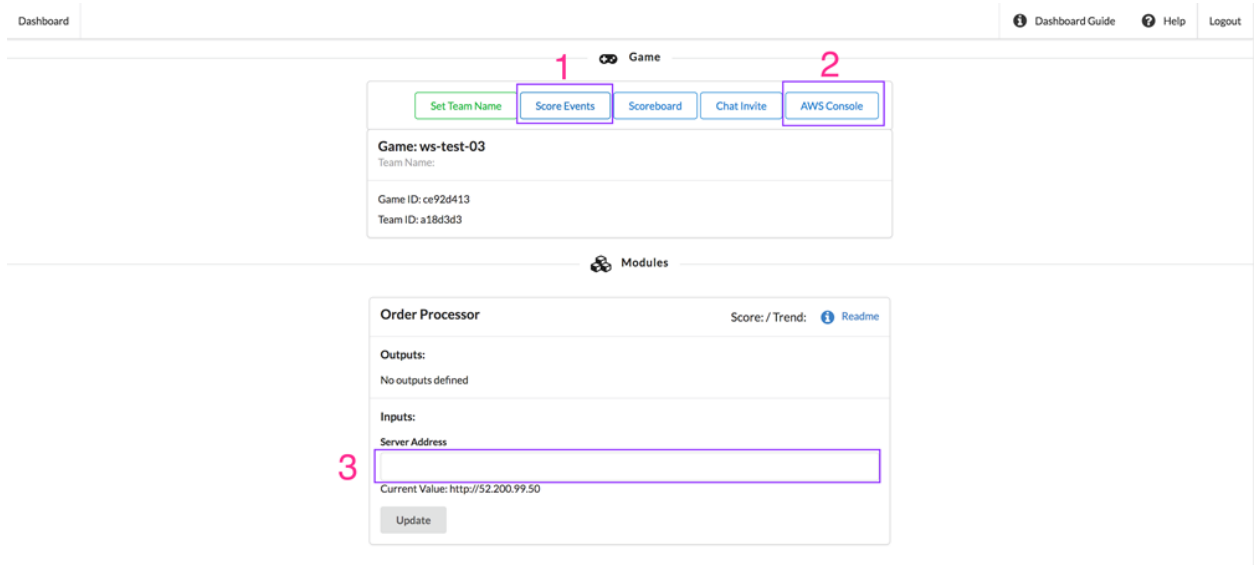
▶ Permissions boundary (not set)

## 2.1.2 Infrastructure Cost

Scaling the infrastructure horizontally brings an increase in the number of Amazon EC2 instances used. Each instance is associated with a cost. If there are more instances deployed than necessary to meet the demand of the load, Competitors will be penalized in points. Make sure to deploy the necessary number of instances to meet the demand (which changes throughout the day).

## 2.1.3 Personal Event Dashboard

The personal event dashboard and scoreboard is provided to give Competitors some visibility into how their application is performing based on web traffic served. This dashboard, however, does not include the Marks that are given based on Systems Design and Deployment, Systems Design and Deployment, Network Design and Deployment, Infrastructure Automation, Infrastructure Security, Infrastructure Active and Passive Monitoring. Each Criteria will provide marks that will be added up to meet the total amount. The sole purpose of the Personal event dashboard and Scoreboard for Competitors to have visibility into viability and how they are serving traffic and is not how the Competitors are performing in relation to other based on all the Criteria's where Marks can be accorded.



The screenshot shows the 'Dashboard' interface. At the top right, there are links for 'Dashboard Guide', 'Help', and 'Logout'. The main section is titled 'Game' and contains a row of buttons: 'Set Team Name', 'Score Events' (annotated with a pink '1'), 'Scoreboard', 'Chat Invite', and 'AWS Console' (annotated with a pink '2'). Below these buttons, the game details are displayed: 'Game: ws-test-03', 'Team Name:', 'Game ID: ce92d413', and 'Team ID: a18d3d3'. The 'Modules' section below contains a card for the 'Order Processor'. It shows 'Score: / Trend: 1 Readme'. Under 'Outputs', it says 'No outputs defined'. Under 'Inputs', there is a 'Server Address' field (annotated with a pink '3') and a 'Current Value: http://52.200.99.50'. An 'Update' button is at the bottom of the input field.

The dashboard has a few key components that you will interact with throughout the competition.

The top bar of the dashboard has a series of buttons that allow you to:

- Access your score events. These are individual entries of activity helpful in determining the availability of your application.
- Access your AWS account. Click on this button in order to get access to your AWS account. You are provided with an AWS account to use for this competition. On completion of each day, the account will be closed and unable to be accessed again.
- Input for your infrastructure address. Your web infrastructure will require a public hostname to access. Just as every website requires a name in a web browser, users of this web application you are deploying require an address to use in order to access the site. You can use an IP address for this address but will get more points for a hostname address.

#### 2.1.4 Scoreboard and Scoring Events

To get a deeper view your performance, you can click on the "Score Events" button on the player dashboard to access your point-by-point breakdown.

Points	Total	Source	Reason
-1	531.22	Order Processor	Request error: Get http://52.72.237.43/calc?input=SUNhbkhhelVuaWNvcm4%2FLTcwMzI%3D: dial tcp 52.72.237.43:80: i/o timeout
-1	532.22	Order Processor	Request error: Get http://52.72.237.43/calc?input=SUNhbkhhelVuaWNvcm4%2FLTEzNTI%3D: dial tcp 52.72.237.43:80: i/o timeout
-1	533.22	Order Processor	Request error: Get http://52.72.237.43/calc?input=SUNhbkhhelVuaWNvcm4%2FLTl5ODc%3D: dial tcp 52.72.237.43:80: i/o timeout
-1	534.22	Order Processor	Request error: Get http://52.72.237.43/calc?input=SUNhbkhhelVuaWNvcm4%2FLTYxNQ%3D%3D: dial tcp 52.72.237.43:80: i/o timeout
-1	535.22	Order Processor	Request error: Get http://52.72.237.43/calc?input=SUNhbkhhelVuaWNvcm4%2FLTgxNjU%3D: dial tcp 52.72.237.43:80: i/o timeout
-1	536.22	Order Processor	Request error: Get http://52.72.237.43/calc?input=SUNhbkhhelVuaWNvcm4%2FLTlyMTg%3D: dial tcp 52.72.237.43:80: i/o timeout
-1	537.22	Order Processor	Request error: Get http://52.72.237.43/calc?input=SUNhbkhhelVuaWNvcm4%2FLTMOMg%3D%3D: dial tcp 52.72.237.43:80: i/o timeout
-1	538.22	Order Processor	Request error: Get http://52.72.237.43/calc?input=SUNhbkhhelVuaWNvcm4%2FLTc0MQ%3D%3D: dial tcp 52.72.237.43:80: i/o timeout
-1	539.22	Order Processor	Request error: Get http://52.72.237.43/calc?input=SUNhbkhhelVuaWNvcm4%2FLTgxNDY%3D: dial tcp 52.72.237.43:80: i/o timeout

This page has two sections to note:

- Each row lists every score event that you have generated. The "Source" column tells you where the point awards or deductions came from. The "Points" column will tell you how many points you have received or lost.
- The "Reason" column will tell you the reason you received the points or lost the points. Pay very close attention to this column when you are losing points in order to understand what is going on and how to fix the problems.

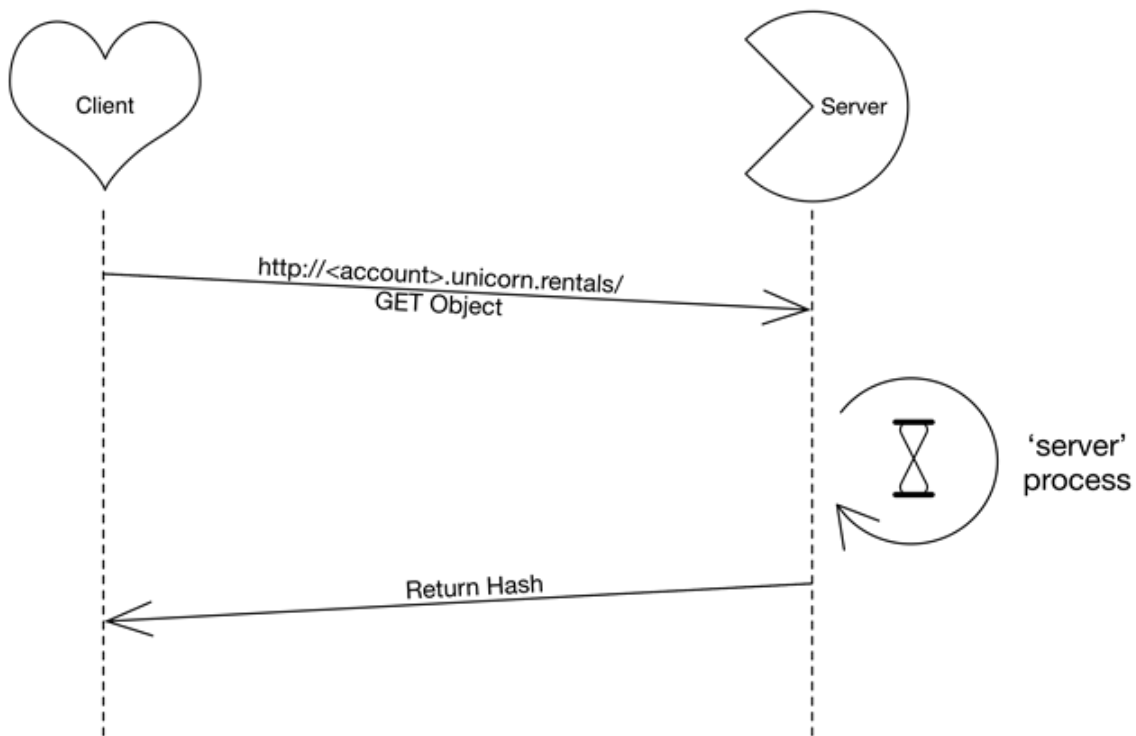
### **2.1.5 AWS Service Restrictions**

When working with AWS, you have access to most services. If you get an error such as "Permission Denied", check to make sure that you are operating in the correct AWS Region and using appropriate resources sizes (e.g. "t2" instance sizes).

### **2.1.6 Application Architecture**

The client below is making requests to the server that you are running. The address the client tries to connect on is defined by the address that you set in the dashboard.





### 2.1.7 Additional Operations

You can find additional application information on options by using the "-h" flag when running the server binary:

`./server -h`

- Create a new Launch Configuration based on the existing Launch Configuration that can be found in the account provided:
- (<http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/WorkingWithLaunchConfig.html>)
- Utilize a 'User Data' script
- Associate this new launch configuration with the Auto Scaling group.
- Scale-up new group / scale-in old group.
- Make sure instances are associated with the proper network resources.

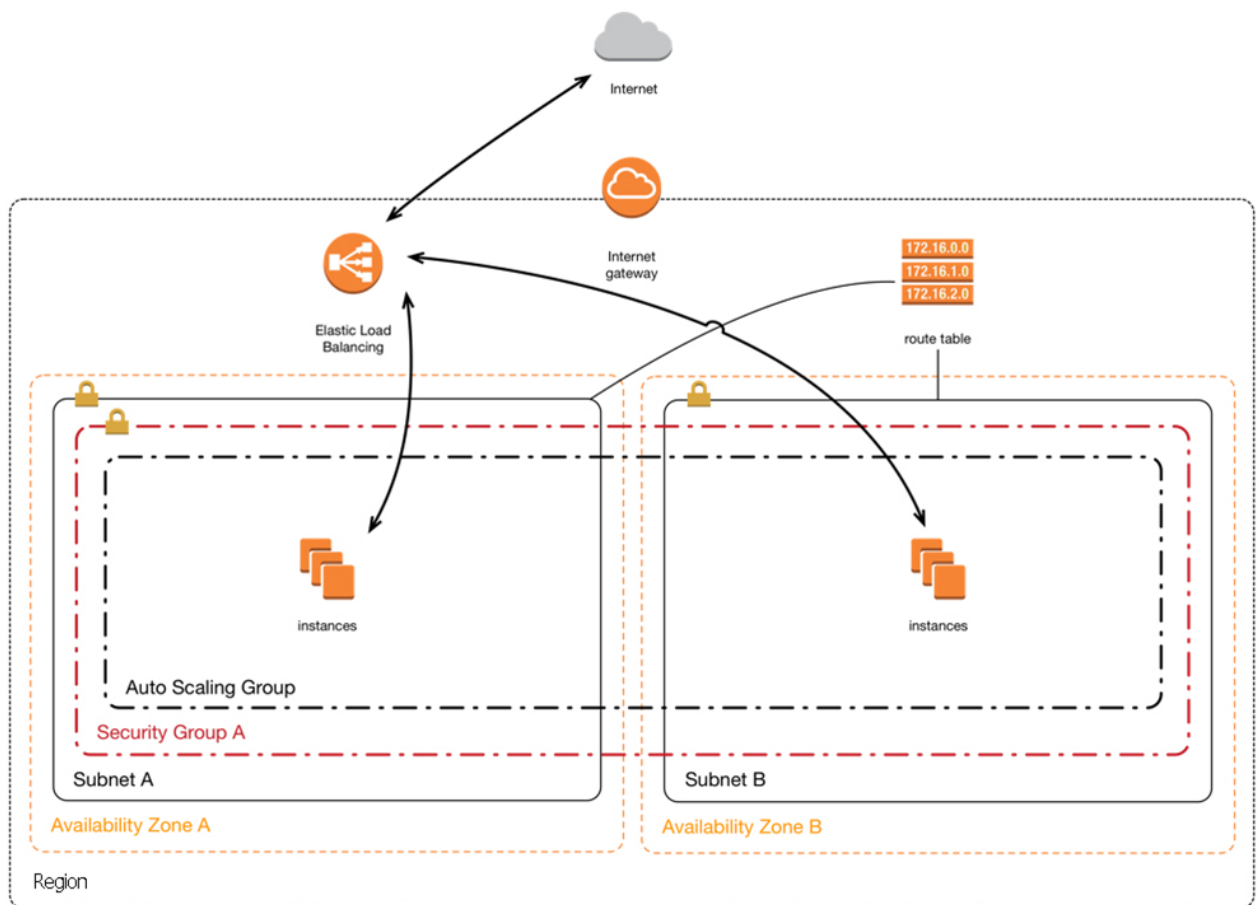


### 2.1.8 Add an SSH Key to the instance and Auto Scaling Groups

- Create an ssh-keypair  
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html>)
- Update the Launch Configuration (Same procedure as 'Update Application').
- Yes, this means you must relaunch the instances.
- Connect from Windows:  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html>
- Configure an Auto Scaling Policy:  
[http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/scaling\\_types.html](http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/scaling_types.html)

### 2.1.9 Troubleshooting Procedures

The AWS VPC / ELB environment must be healthy for the application to work. All production traffic flows through the ELB on both ingress and egress as shown in this diagram.



- Check the Security Group settings for your instances
- Make sure all required ports are allowed
- Check the Routing tables on your subnets
- Make sure the routing tables are applied to each subnet
- 'Default' table applies to all subnets without an explicit definition
- Make sure the routing table has the appropriate rules
- Things to check in your VPC.
- Are the Instances up?
- Is the Instance 'up' in the Auto Scaling group?
- Are your subnets configured properly?
- Subnet details and size are an important component
- Are the subnets added to the Elastic Load Balancer?
- Are the subnets added to the Auto Scaling Group?

- Are Routes correct / intact? See the above diagram.
- Are ACL set on subnet? Are they too restrictive/permissive?
- Are you using the correct Security groups?
- Internet Gateway (IGW) Do you have routes to flow traffic through the IGW? Required to grab the server code from S3.
- DNS settings: Are the records pointing to the correct resources?
- You can try connecting to the instance using SSH to verify the server application is working correctly and to access the application logs. You must install a ssh key first (see 'Add ssh-key to instance', above)
- Performance: The server process can get slow if it is handling too many connections. Try restarting the server if it becomes overloaded.
- Security consideration: you will have created a configuration file containing database credentials and other sensitive data. Is this something that you want available for public download?

#### **2.1.10 Application Versions**

During the course of the test, you will be required to "update" your application. A new version of the application will be made available to download. Once it is available, you will want to start rolling out that new version. At the defined time, the old version of the application will no longer function.

#### **2.1.11 System Monitoring**

How to check ELB metrics?

[http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/policy\\_creating.html](http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/policy_creating.html)

<http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-cloudwatch-metrics.html>

## 2.2 Day 2: AWS Jams

### 2.2.1 The Jam Platform

The first day of competition will be mainly focused on your ability to create new scalable architectures. In addition to testing your creativity and technical ability in creating architectures, you will also be tested on specific skills that are necessary as a cloud computing expert. For this part of the competition we will be using a module-based platform for testing specific skills.

### 2.2.2 Registering on the jam platform



If you haven't already just click the register button.

Fields:

Email: Your Email

Display Name: [Name]-[Province]

Password: A password of your choosing. Never share this with another person

You can choose whether or not to give consent to distribute your email. For this event it will not matter.

Complete the Captcha

### 2.2.3 Using the Jam Platform

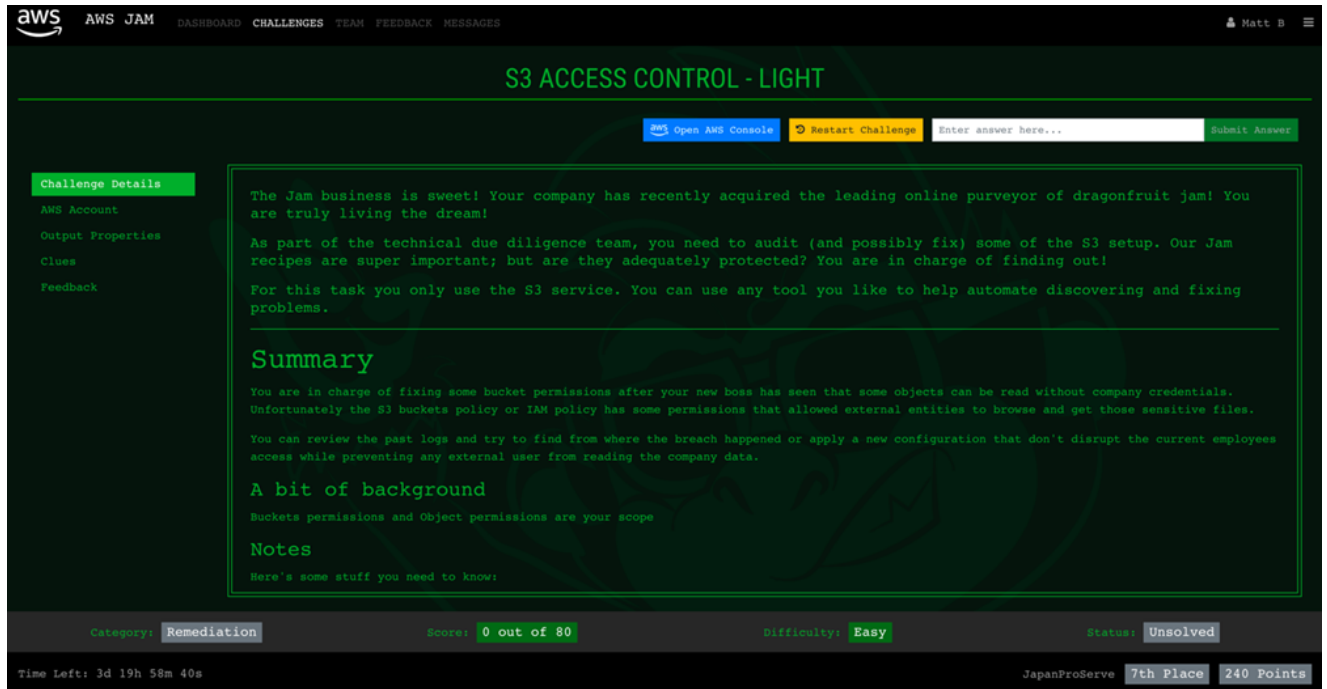
You will be using the jam platform every day for the competition. Days 1 and 2 will be small modules that will open towards the end of the day. Days 3 and 4 will be exclusively jam platform based. Once the jam event opens, you'll be able to complete the challenges in any order that you wish.

Once we are ready to start the jam event, you will all be given an event password. This will unlock your tasks for that day.



The default view of the jam platform is a map. This is just a fun layout, but is not important for this event. You can complete any challenge in any order.

Once you select a challenge you will see a screen like this:



The screenshot shows the AWS IAM challenge interface for "S3 ACCESS CONTROL - LIGHT". The top navigation bar includes "aws", "AWS IAM", "DASHBOARD", "CHALLENGES", "TEAM", "FEEDBACK", and "MESSAGES". The user "Matt B" is logged in. The challenge title "S3 ACCESS CONTROL - LIGHT" is displayed in green. Below the title, there are buttons for "Open AWS Console", "Restart Challenge", an input field for "Enter answer here...", and a "Submit Answer" button. On the left, a sidebar lists "Challenge Details", "AWS Account", "Output Properties", "Clues", and "Feedback". The main content area contains the following text:

The Jam business is sweet! Your company has recently acquired the leading online purveyor of dragonfruit jam! You are truly living the dream!

As part of the technical due diligence team, you need to audit (and possibly fix) some of the S3 setup. Our Jam recipes are super important; but are they adequately protected? You are in charge of finding out!

For this task you only use the S3 service. You can use any tool you like to help automate discovering and fixing problems.

---

### Summary

You are in charge of fixing some bucket permissions after your new boss has seen that some objects can be read without company credentials. Unfortunately the S3 buckets policy or IAM policy has some permissions that allowed external entities to browse and get those sensitive files.

You can review the past logs and try to find from where the breach happened or apply a new configuration that don't disrupt the current employees access while preventing any external user from reading the company data.

### A bit of background

Buckets permissions and Object permissions are your scope

### Notes

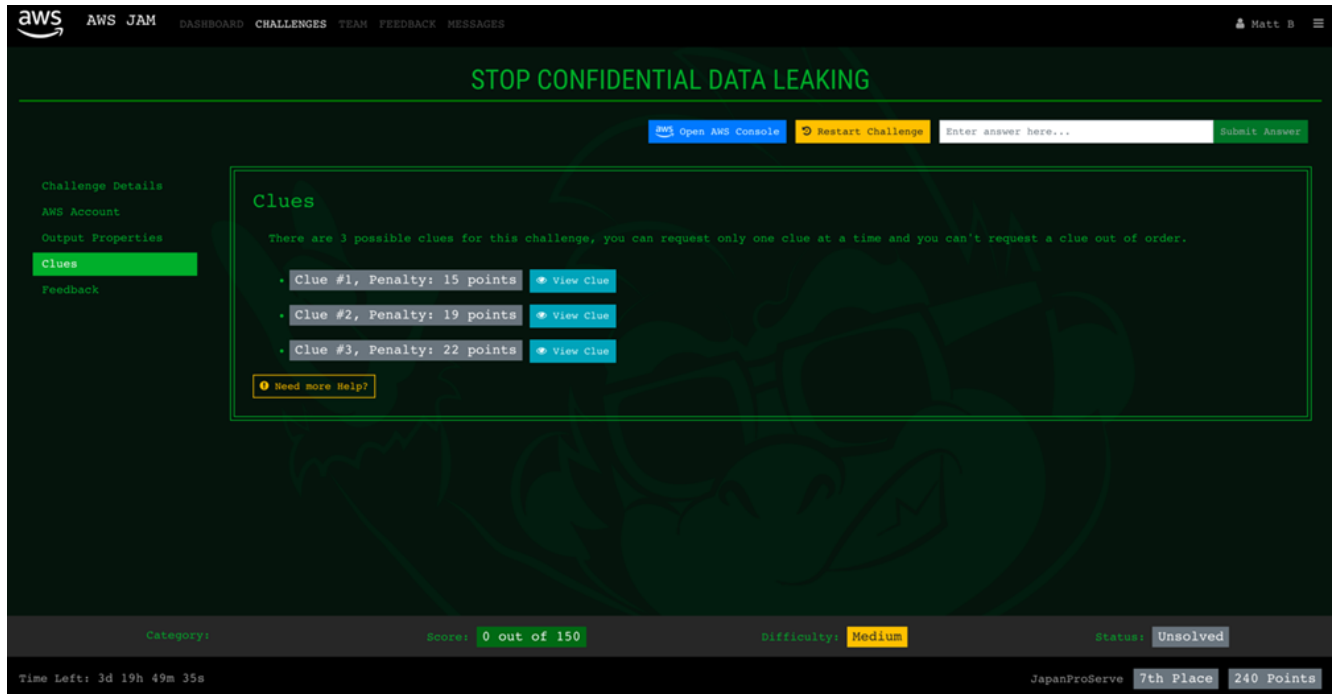
Here's some stuff you need to know:

At the bottom, the challenge status is shown: Category: Remediation, Score: 0 out of 80, Difficulty: Easy, Status: Unsolved. The time left is 3d 19h 58m 40s. The leaderboard shows JapanProServe in 7th Place with 240 Points.

This will give you the instructions for the task, access to your account, and the ability to restart the challenge if you believe you've broken something and cannot repair it yourself.

clues

The jam modules can be very difficult, but all can and have been solved using only the instructions given to you. However, you do have the option of revealing clues.



The screenshot shows the AWS JAM challenge interface. At the top, the navigation bar includes 'aws', 'AWS JAM', 'DASHBOARD', 'CHALLENGES', 'TEAM', 'FEEDBACK', and 'MESSAGES'. The user 'Matt B' is logged in. The challenge title 'STOP CONFIDENTIAL DATA LEAKING' is displayed in green. Below the title, there are buttons for 'Open AWS Console', 'Restart Challenge', an input field 'Enter answer here...', and a 'Submit Answer' button. On the left, a sidebar lists 'Challenge Details', 'AWS Account', 'Output Properties', 'Clues' (highlighted in green), and 'Feedback'. The main content area, titled 'Clues', states: 'There are 3 possible clues for this challenge, you can request only one clue at a time and you can't request a clue out of order.' It lists three clues: 'Clue #1, Penalty: 15 points', 'Clue #2, Penalty: 19 points', and 'Clue #3, Penalty: 22 points', each with a 'View Clue' button. A 'Need more Help?' button is also present. At the bottom, a status bar shows 'Category:', 'Score: 0 out of 150', 'Difficulty: Medium', 'Status: Unsolved', 'Time Left: 3d 19h 49m 35s', 'JapanProServe', '7th Place', and '240 Points'.

Clues are designed to help you make progress toward the final solution but it is important to remember that you will not receive full points for the module if you use a clue. Determine your own strategy, and be mindful of the consequences of using a clue.