

# PomoRobotics

## Handover Documentation - Runbook

### Document Information

|                |                              |
|----------------|------------------------------|
| Project name:  | PomoRobotics DriverlessTruck |
| Date:          | 24/09/2024                   |
| Author:        | Keval S/Chris F              |
| Document code: | 001                          |
| Version:       | V1.0                         |

### Approval

| Date                       | Name            | Title                    |
|----------------------------|-----------------|--------------------------|
| 24 <sup>th</sup> September | Keval S/Chris F | Solutions Architect      |
| 24 <sup>th</sup> September | Graham B        | Presales/Account manager |
| 24 <sup>th</sup> September | Gordon S        | CTO                      |

## Introduction

This handover document provides a seamless transition of ownership and knowledge for the recently completed running Machine Learning Workload on AWS . It contains essential information about the system architecture and functionalities, technical specifications, and other relevant details.

Our goal has been to align our expertise with your business objectives, delivering a tailored IT solution to meet your specific needs. This document serves as a valuable resource, empowering you to effectively maintain and enhance the system. Should you require any assistance during this transition phase, our team is available to support you.

## Project Outline

PomoRobotics have engaged transACT Cloud Services as their consulting partner to propose a design for architecting their Infrastructure in AWS for running ML workloads. Main goal was to Setup basic Infrastructure within AWS making sure that the environment is resilient/available/scalable /secured and setup as per AWS best practices.

Project Board:

| Role                | Person(s)   | Responsibilities                               |
|---------------------|-------------|--|
| Project Manager     | Graham B    | Responsible for the entire Project             |
| Solutions Architect | Keval Sheth | Design and Architecture of the system          |
| Solutions Architect | Chris F     | Creation & configuration of all infrastructure |

## Service Level Agreements (SLA's)

As per AWS transACT Business Support SLA's

## System Resources

Add all AWS services and third-party applications used in the application here.

- EC2
- ECR
- S3

- Lambda
- CloudFormation
- Identity & Access Management (IAM)
  - Roles
  - Policies
- SNS
- CloudWatch
- EBS
- Virtual Private Cloud (VPC)
  - Virtual Network
  - Subnets
  - Route Tables
  - Security Groups (SGs)
  - Flow Logs

## System Information

Add or remove tables/columns here to represent all core infrastructure

### Compute

| Name               | Type | OS           | Quantity       | Storage                      | AMI ID         |
|--------------------|------|--------------|----------------|------------------------------|----------------|
| Linux Bastion Host | EC2  | Amazon Linux | 1 – t3.micro   | EBS 8 GB                     | Amazon Linux 3 |
| ML Instance        | Ec2  | Windows 2022 | 2 – p3.8xlarge | EBS1- 100 GB<br>EBS2 – 10 GB | Amazon Linux 3 |

### Storage

| Name | Type           | Storage  | Multi-AZ |
|------|----------------|----------|----------|
| S3   | Object Storage | Scalable | Yes      |

## Network

### VPC

| Name                  | CIDR Range  | Flow Logs Enabled | NAT & Internet Gateway Attached | Number of Subnets |
|-----------------------|-------------|-------------------|---------------------------------|-------------------|
| vpc-0d1d9e408da2655ca | 10.0.0.0/16 | False             | True                            | 4                 |

*This VPC Was designed with expansion in mind, so there is space within the network for further subnets.*

### Ec2

| Instance Name          | Instance Id         | Instance Type | Instance State | Private IP Address | Public IP Address |
|------------------------|---------------------|---------------|----------------|--------------------|-------------------|
| Linux-BastionHost      | i-06233a7a04053eea2 | t2.micro      | running        | 10.0.3.192         | 35.176.37.95      |
| Production ML Instance | i-0101d8a519cd695af | p3.8xlarge    | stopped        | 10.0.1.103         | N/A               |

### Subnets

| SubnetName          | AvailabilityZone | CidrBlock   | RouteTableId          |
|---------------------|------------------|-------------|-----------------------|
| prod-privateSubnet2 | eu-west-2b       | 10.0.2.0/24 | rtb-0b100557e4c931f46 |
| prod-privateSubnet1 | eu-west-2a       | 10.0.1.0/24 | rtb-0b100557e4c931f46 |
| prod-publicSubnet2  | eu-west-2b       | 10.0.4.0/24 | rtb-01d5d9e7e7553b106 |
| prod-publicSubnet1  | eu-west-2a       | 10.0.3.0/24 | rtb-01d5d9e7e7553b106 |

### Endpoints

In order to facilitate connectivity to S3 bucket and ECR, endpoints have been created which provides seamless access to service privately

### Stacks:

| Stack Name  | Description  |
|-------------|--|
| prod-ml-ec2 | CloudFormation Template to create an EC2 instance with two EBS volumes (300GB and 100GB).    |
| ICO-Roles   | transACT IAM Control Roles   |
| prod-s3     | CloudFormation Template to create an S3 bucket with lifecycle rules for the raw-data folder. |

|                    |  |
|--------------------|--|
| prod-s3-monitoring | CloudFormation template for S3 bucket monitoring and alerting  |
| prod-network       | CloudFormation Template to create a VPC for PomoRobotics, 4 subnets (2 private and 2 public), IGW, NAT Gateway, and S3 Gateway Endpoint. |

## Disaster Recovery

No DR and Backup have been enabled at the moment since it was not decided as part of SoW. However, please go through the following Link and/OR let us know and we will be happy to guide you

## Patching

Patching and updating OS will be PomoRobotic's responsibility.

## IAM Control

To understand user access management and create new users, please refer to the IAM Control document that would have been provided to you during the handover.

## Access EC2 Hosts

If you need to connect to the ML EC2 instance, please note that since it resides in a private subnet, your initial point of access will be the Bastion Host. From there, you can access other instances within the private subnet.

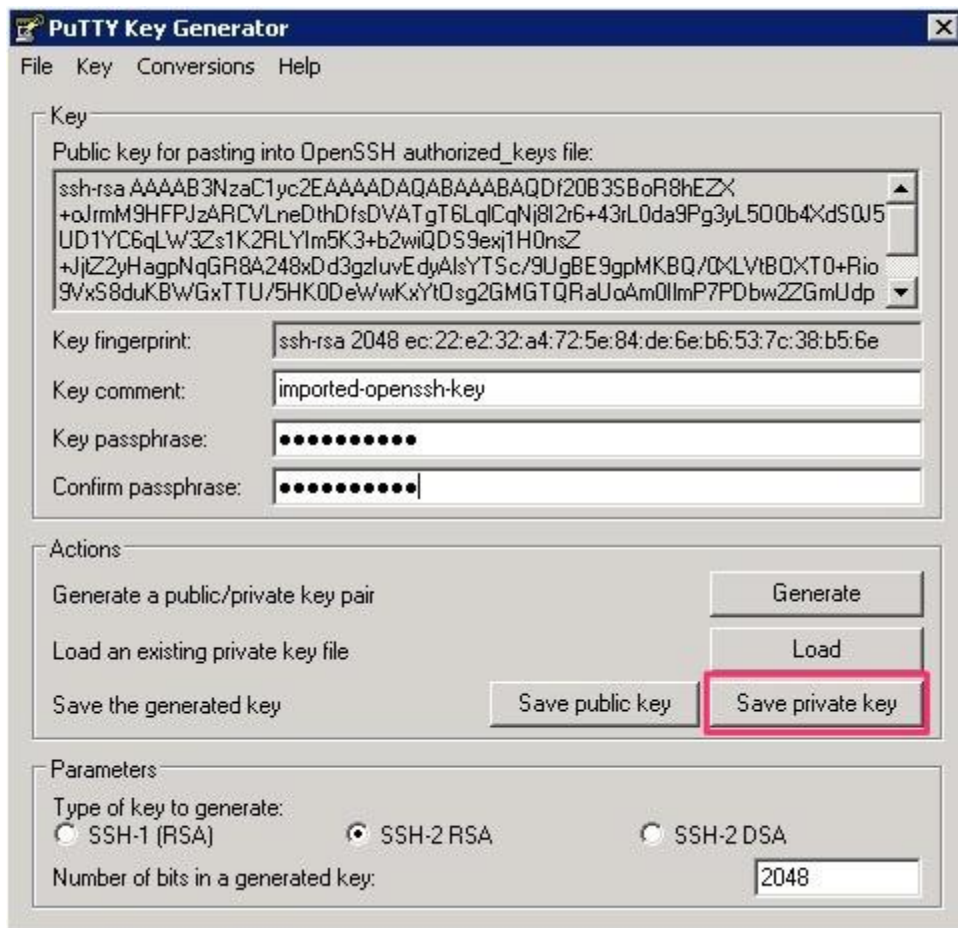
Configuring ssh-agent on Windows

In Windows, you can connect to Linux VPC instances using PuTTY. To get SSH agent functionality, you can use Pageant, which is available from the PuTTY [download page](#). When Pageant is installed, you can use the agent forwarding option in PuTTY to connect to instances in private subnets.

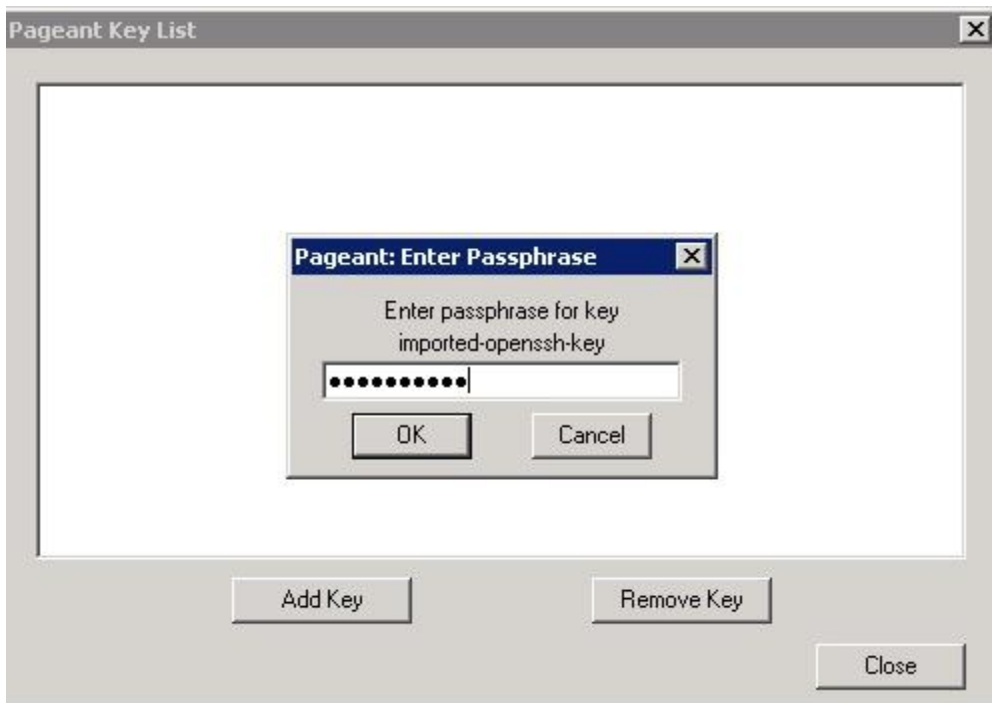
To use Pageant, you need to convert your private key from PEM format to PuTTY format using PuTTYGen (available from the PuTTY [download page](#)).

Private Key can be obtained from Secrets Manager in PEM format: Prod-lhr-keypair

In PuTTYGen, choose Conversions > Import Key and select your PEM-formatted private key. Enter a passphrase and then click Save private key, as shown in the following screenshot. Save the key as a .ppk file.



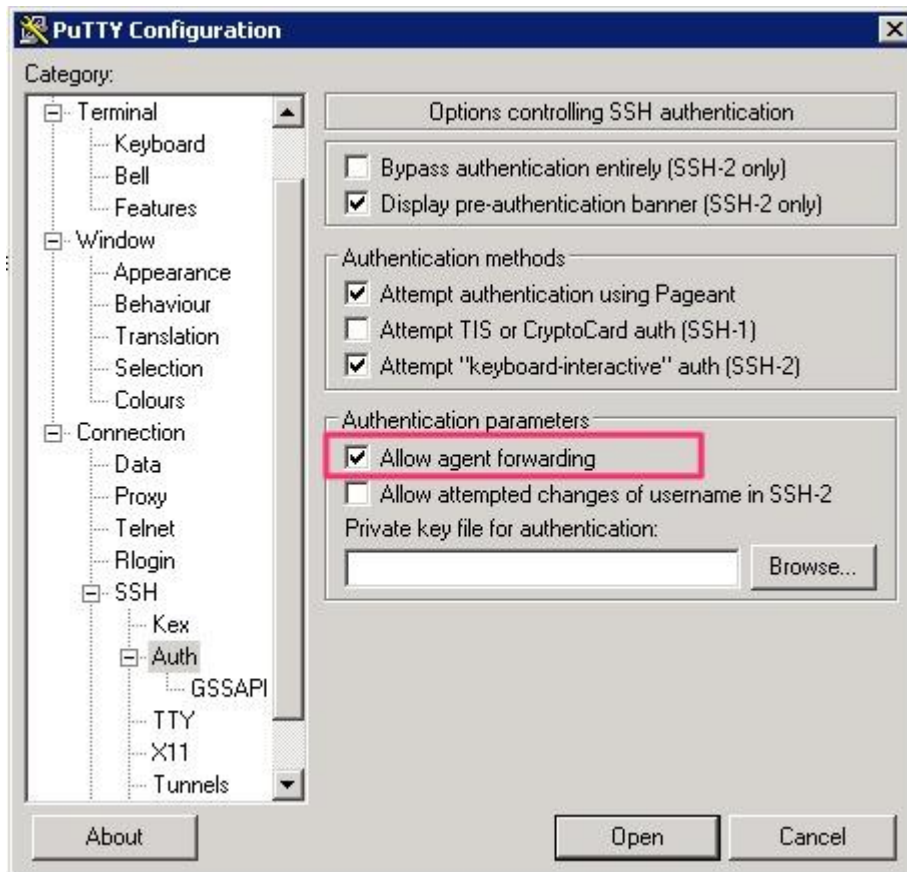
After you convert the private key, open Pageant, which runs as a Windows service. To import the PuTTY-formatted key into Pageant, double-click the Pageant icon in the notification area and then click Add Key. When you select the .ppk file, you're prompted to enter the passphrase you chose when you converted the key, as shown in the following screenshot.



After you add the key, close the Pageant Key List window.

Finally, when you are configuring the connections for SSH in PuTTY, check the Allow agent forwarding box and leave the Private key file for authentication field empty.

When you use PuTTY to connect to the public IP address of your bastion, you will see that the Pageant PuTTY component provides the SSH key for authentication, as shown in the following screenshot.



With agent forwarding enabled in the PuTTY configuration, you can connect from the bastion to any other instance in the VPC without having the SSH private key on the bastion. To connect to other instances, use the following command:

```
ssh user@<instance-IP-address of ML Ec2 or DNS-entry>
```

As long as the matching private key for the instance is loaded into Pageant, the connection will be successful,



## Architecture Diagrams

### Pomorobotics AWS Architecture

