# Windows Server 2022 – PostgreSQL 16 + pgAdmin4

| | |
|---|---|
| Version: | 1.0.0 |
| Created by: | cloudimg |

## Table of Contents



## 1.) Overview

This document is provided as a user guide for the Windows Server 2022 – PostgreSQL 16 + pgAdmin product offering on the AWS Marketplace. Please reach out to support@cloudimg.co.uk if any issues are encountered following this user guide for the chosen product offering.

## 2.) Access & Security

Please update the security group of the target instance to allow the below ports and protocols for access and connectivity.

| Protocol | Type | Port | Description |
|---|---|---|---|
| RDP | TCP | 3389 | Remote Desktop Access |
| TCP | TCP | 5432 | PostgreSQL Database Listener Port |

## 3.) System Requirements

The minimum system requirements for the chosen product offering can be found below

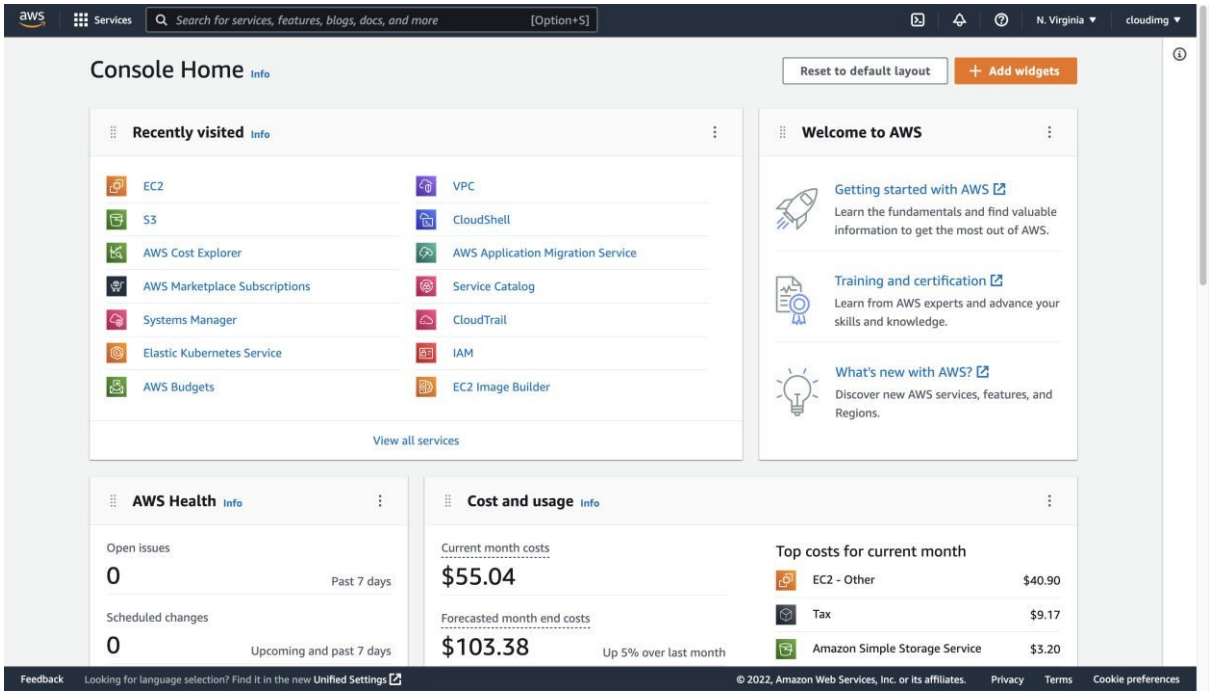
| Minimum CPU | Minimum RAM | Required Disk Space |
|---|---|---|
| 1 | 1 GB | 30GB |

## 4.) Connecting to the Instance

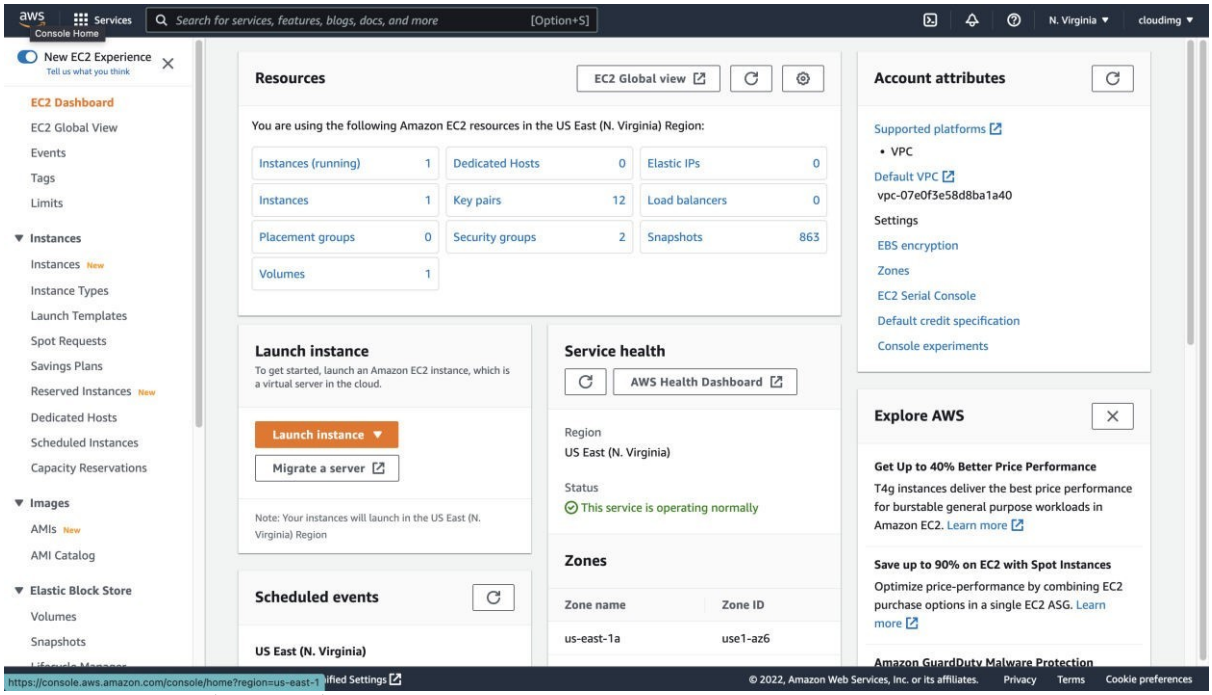
Once launched in the Amazon EC2 Service, please connect to the instance via an RDP client using the **Administrator** user. Please allow the EC2 Instance to pass 2/2 status checks before connecting via RDP to allow the system enough time to complete the boot process.

To obtain the randomly generate password on boot for the Administrator user, please follow the below steps in the AWS Console.

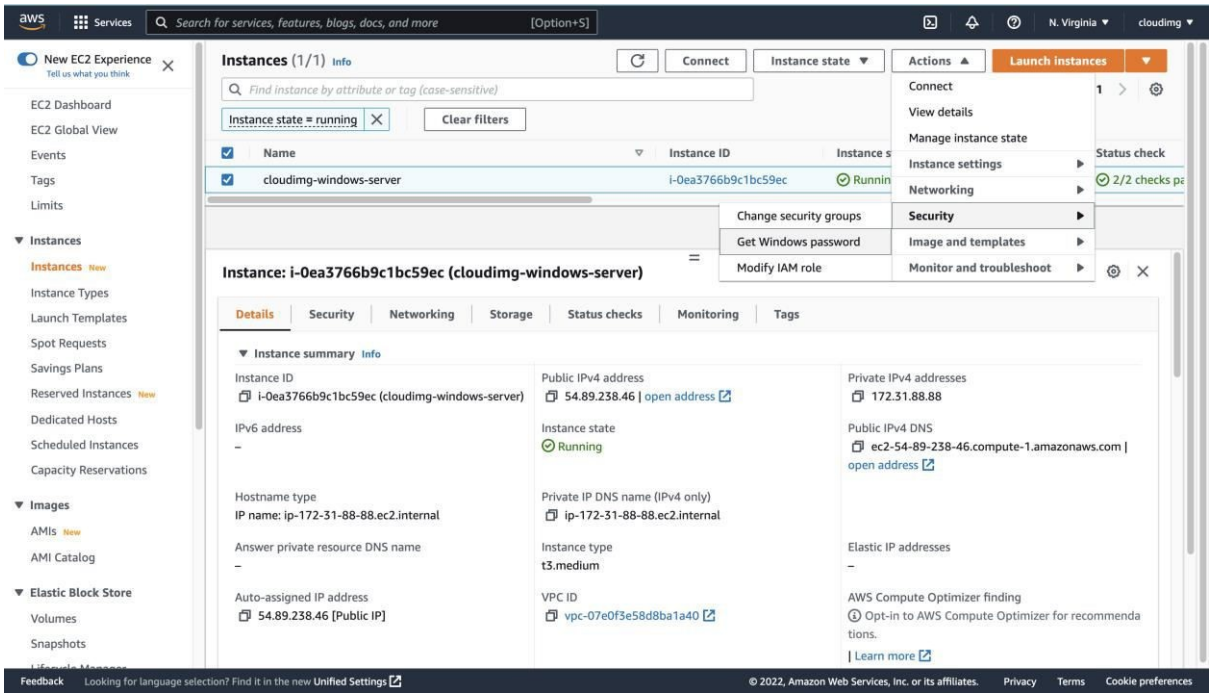
Log into the Target AWS Account > Select the region of which was chosen to host the newly launched cloudimg AMI



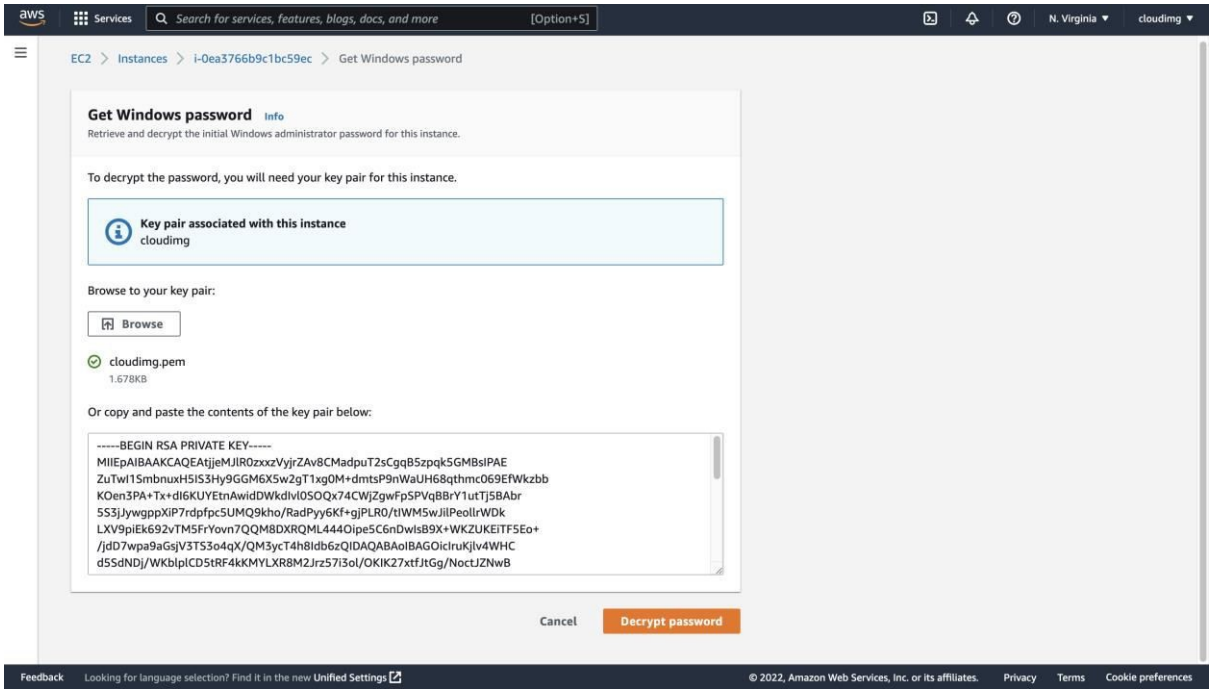

Select EC2



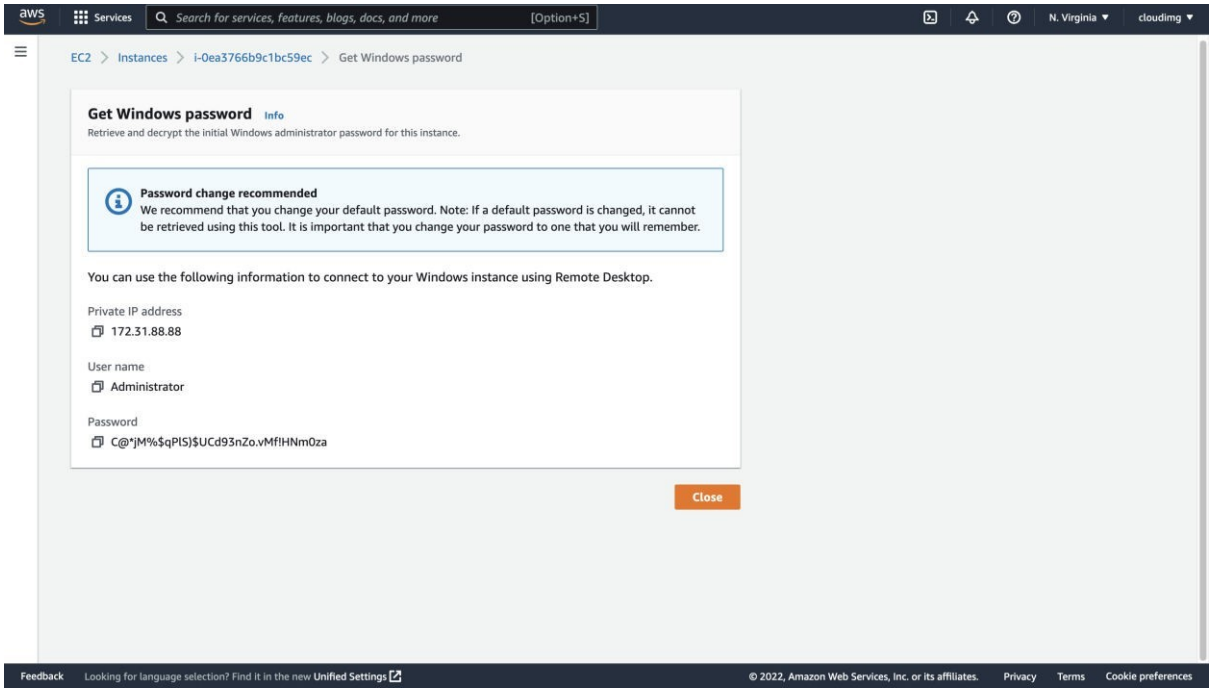

Select Instances (running)



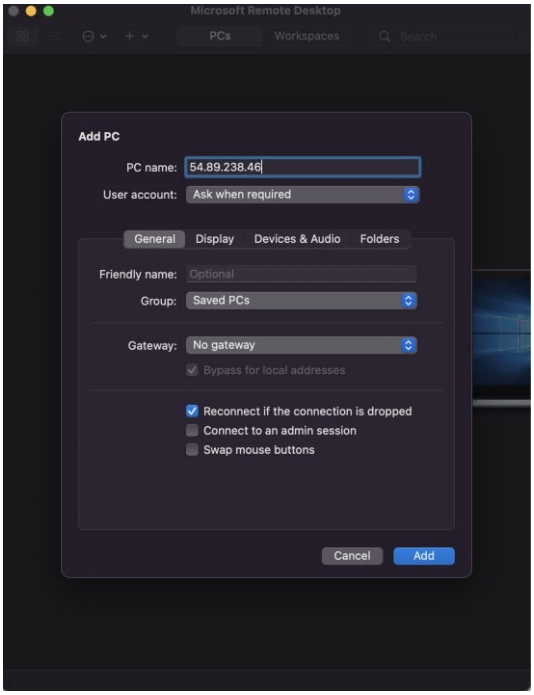

Search for the newly launched EC2 Instance
Select the Radio button above for the instance
Click Actions > Security > Get Windows password




Click Browse and upload the key pair selected during the launch of the EC2 instance from the AWS Marketplace. Click Decrypt password



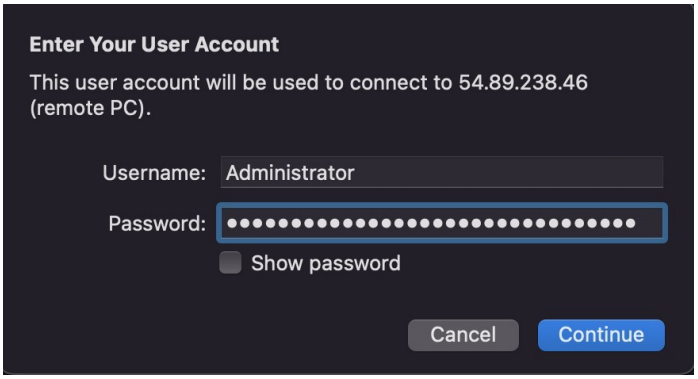

The Administrator password will now appear in plain text like the above example. Take a copy of this value and open a Remote Desktop Client Application.




Create a new connection and enter the IP address of the newly launched EC2 Instance. For this example, the public IP address will be used as the server has been launched in a public subnet. Use the private IP address where applicable for your environment if you have a private connection into the AWS VPC of which hosts the EC2 Instance. These Private connections often take the form of a VPN connection.

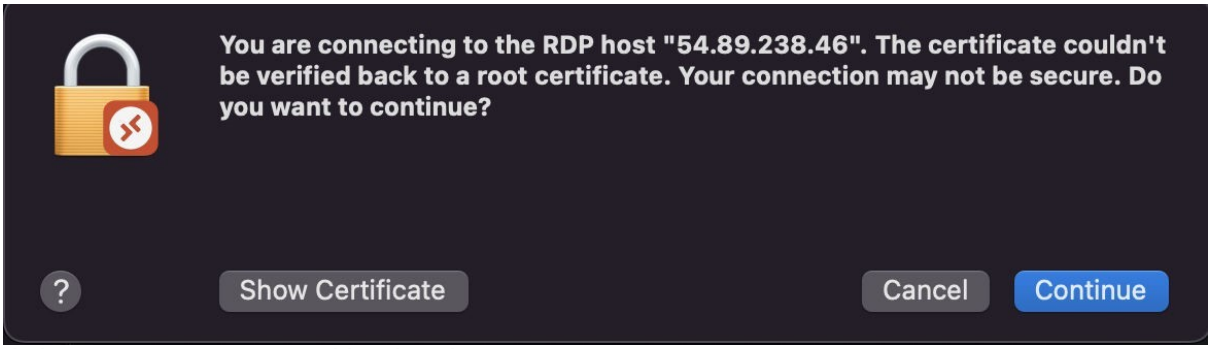
Click Add

Once added, double click the connection profile created in the above step, you will be prompted for a username & password. Enter the below values.

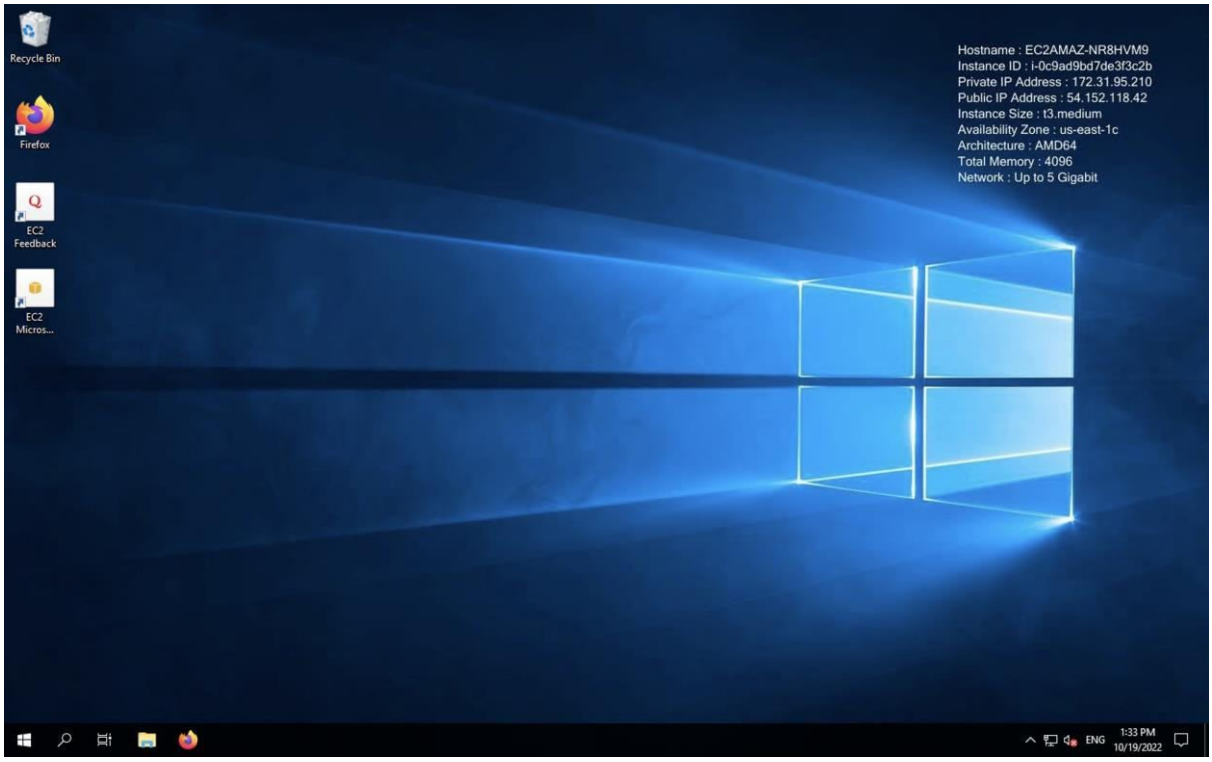



**Username: Administrator  Password: DECRYPTED VALUE RETRIEVED FROM THE ABOVE STEPS**

Click Continue



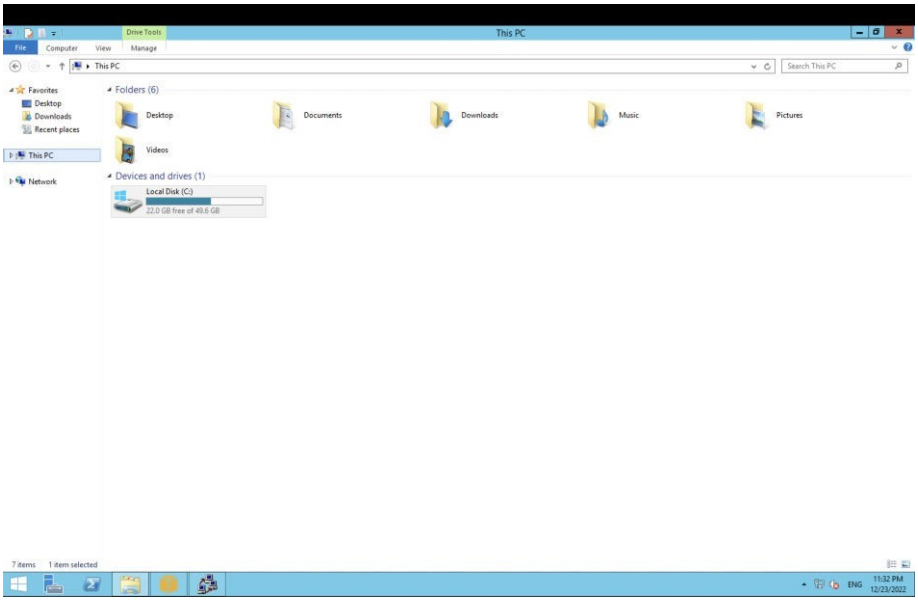

Click Continue if a pop up like the above appears.




You have now successfully connected to the Windows Server hosted in AWS.

## 5.) Filesystem Configuration

Please see below for a screenshot of the server disk configuration and specific mount point mappings for software locations.




## 6.) Server Components

Please see below for a list of installed server components.

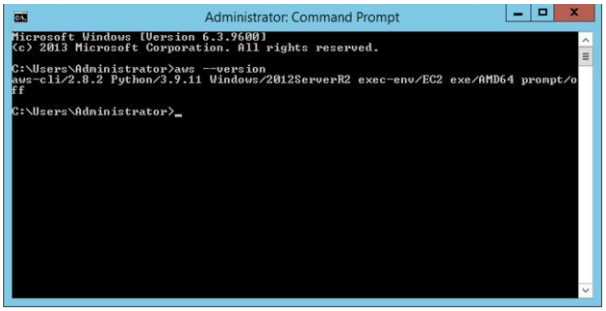
| Component | Version | Install Location |
|---|---|---|
| AWS CLI | 2.8.2 | |
| AWS CloudWatch Agent | 1.3.5 | |
| AWS Systems Manager Agent | 3.1.1 | |
| PostgreSQL | 16 | C:\Program Files\PostgreSQL\16 |
| pgAdmin | 4 | C:\Program Files\PostgreSQL\15\pgAdmin 4 |

## 7.) Using System Components

Instructions can be found below for using each component of the server build mentioned in section 7 of this user guide document.

**AWS CLI**

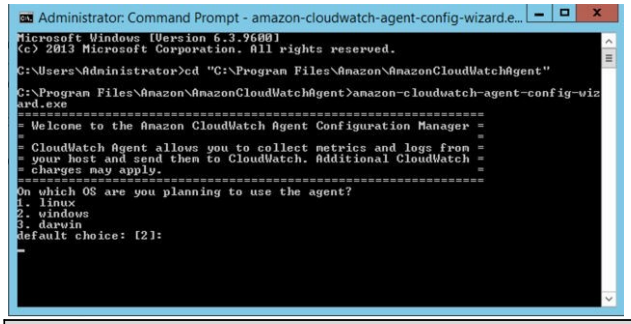
Using AWS CLI – as any OS user via the CMD programme.




```
aws --
help
```

**AWS CloudWatch Agent**

The CloudWatch Agent wizard can be launched via the below command for the configuration required pertaining to your specific use case. Run the below command from a CMD prompt.




```
cd "C:\Program Files\Amazon\AmazonCloudWatchAgent" amazon-cloudwatch-agent-config-wizard.exe
```

Once configured you will be able to start the AWS CloudWatch Agent via PowerShell by issuing the below command. Exchange the values below in bold to point to that of your configuration file.

```
& "C:\Program Files\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1" -a fetchconfig -m ec2 -s -c file:configuration-file-path
```

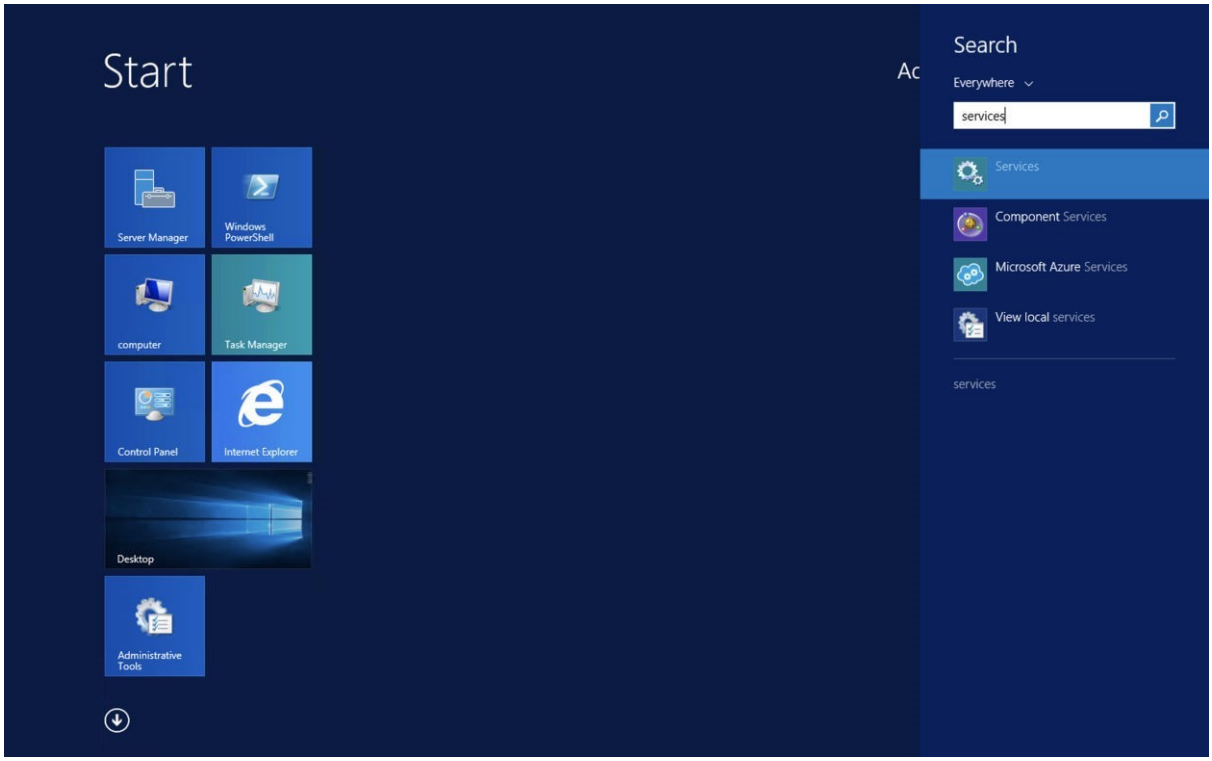
**AWS Systems Manager**

The AWS Systems Manager agent has been configured to start on boot.

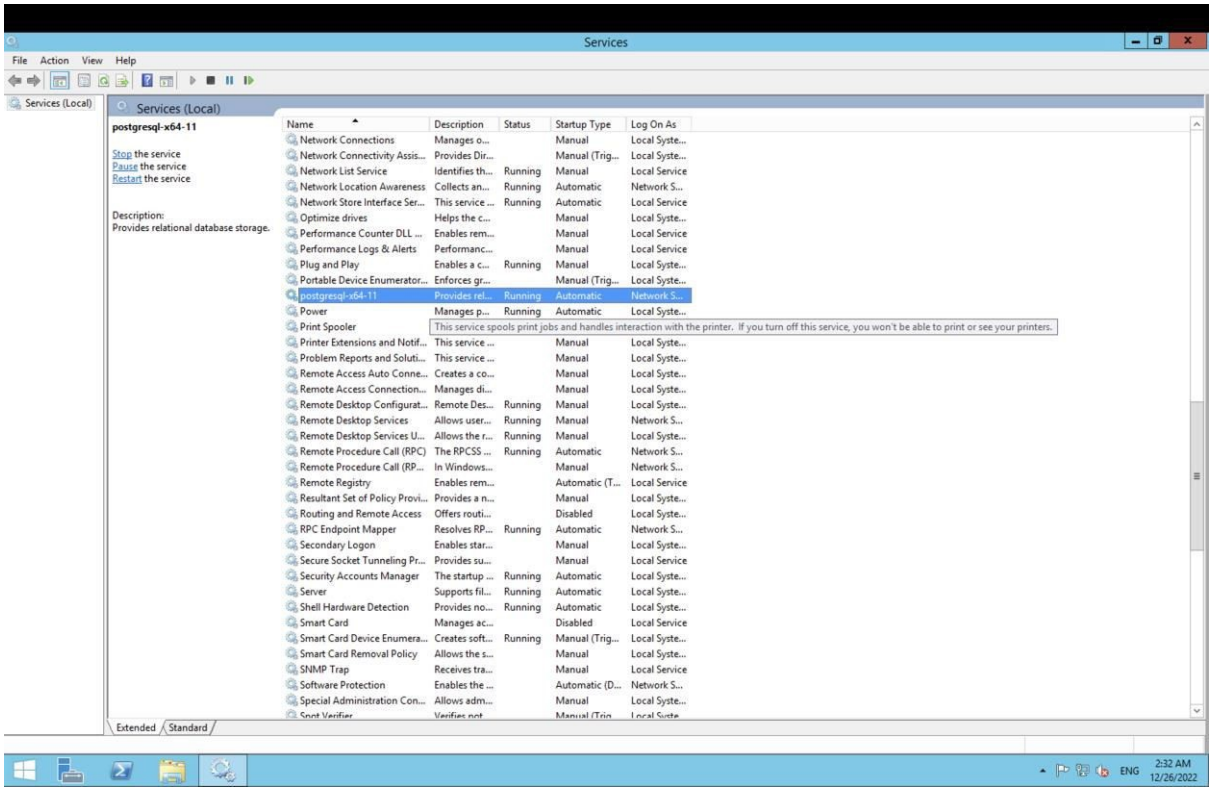
**PostgreSQL**

The postgres database service has been configured to start on boot via a Windows Service. You can stop, start or check the status of the postgres service by following the below steps.

From the Windows Start Menu > Search for Services




Click Services



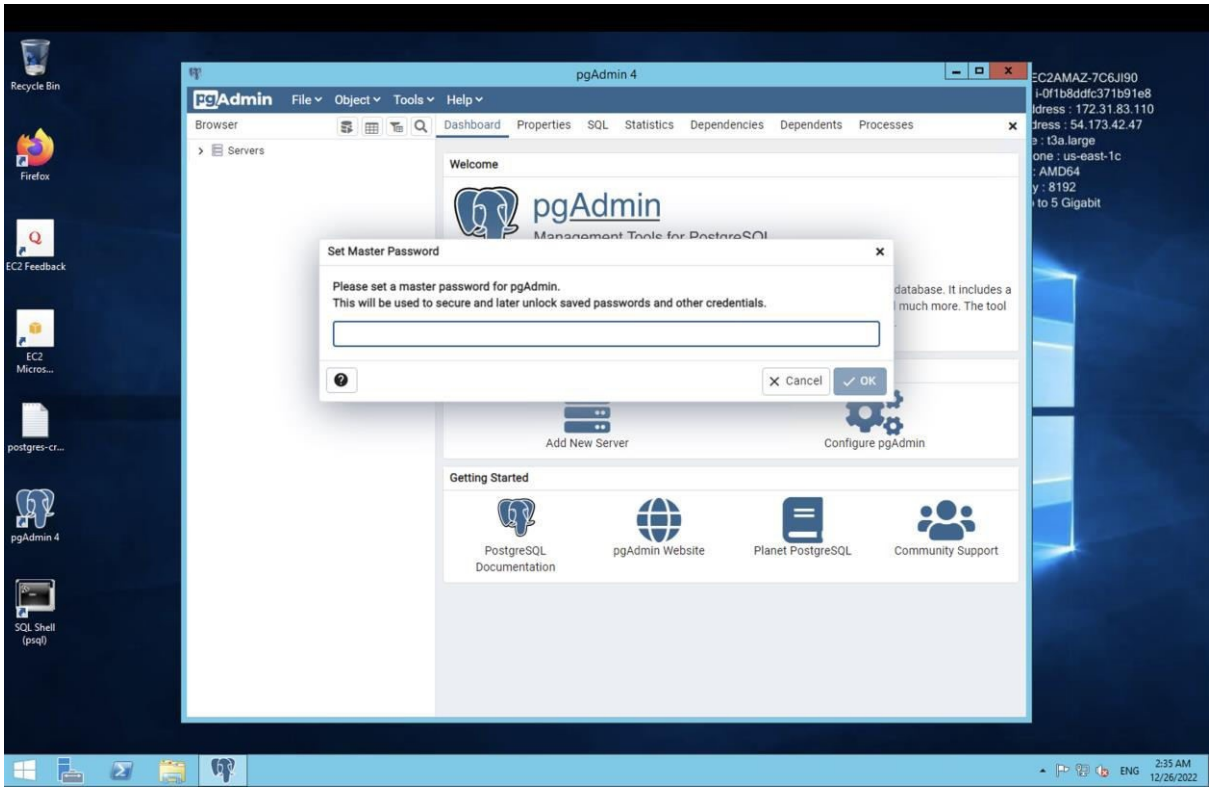
Search for the Service – postgresql-x64* > Double Click

From the above menu you can reconfigure the service to not start on boot, stop, start and or restart the service manually.

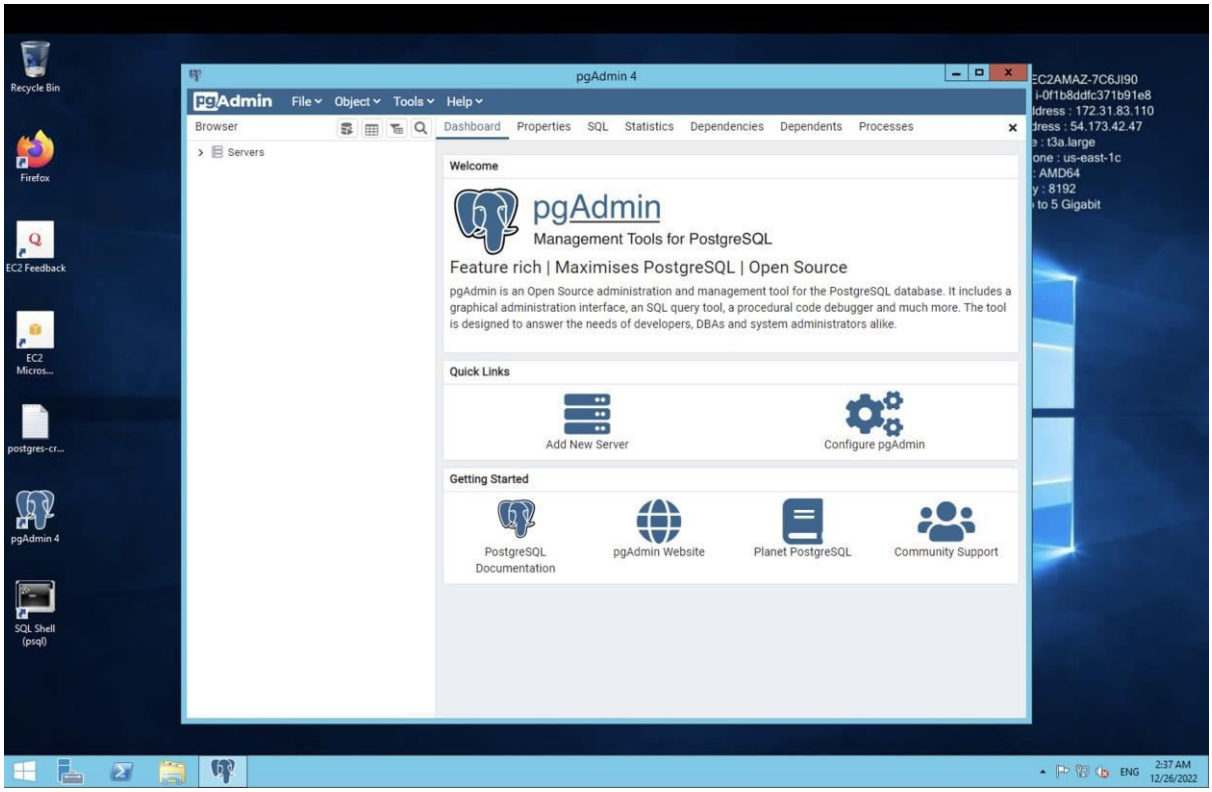
**pgdmin4**

A connection to the postgresql database running on the instance can be made from the pgAdmin4 programme preinstalled. You can access the program via the Desktop .exe shown below as the Administrator user.

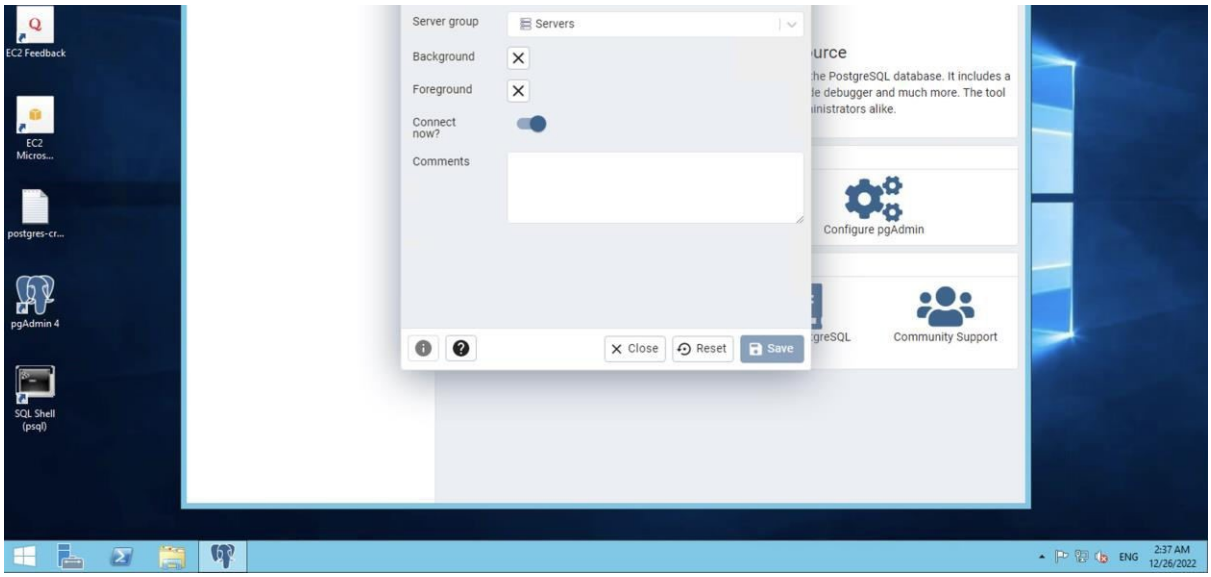

On first boot of the programme, you will be prompted to set a new master password to be used for securing & unlocking later defined passwords.




Enter your preferred password value for the above.

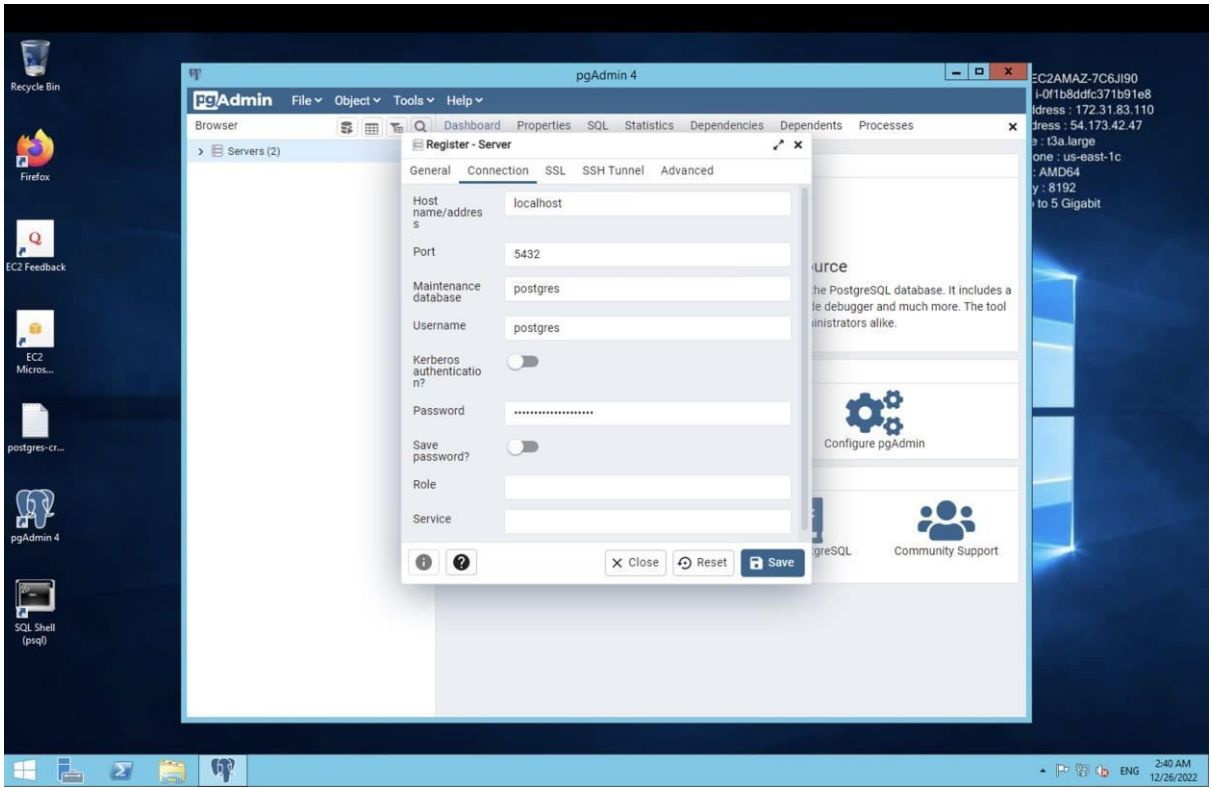


Select ‘Add New Server’




Enter a NAME for the new connection, in this example we will use EXAMPLE but any value could be used.

Click Connection



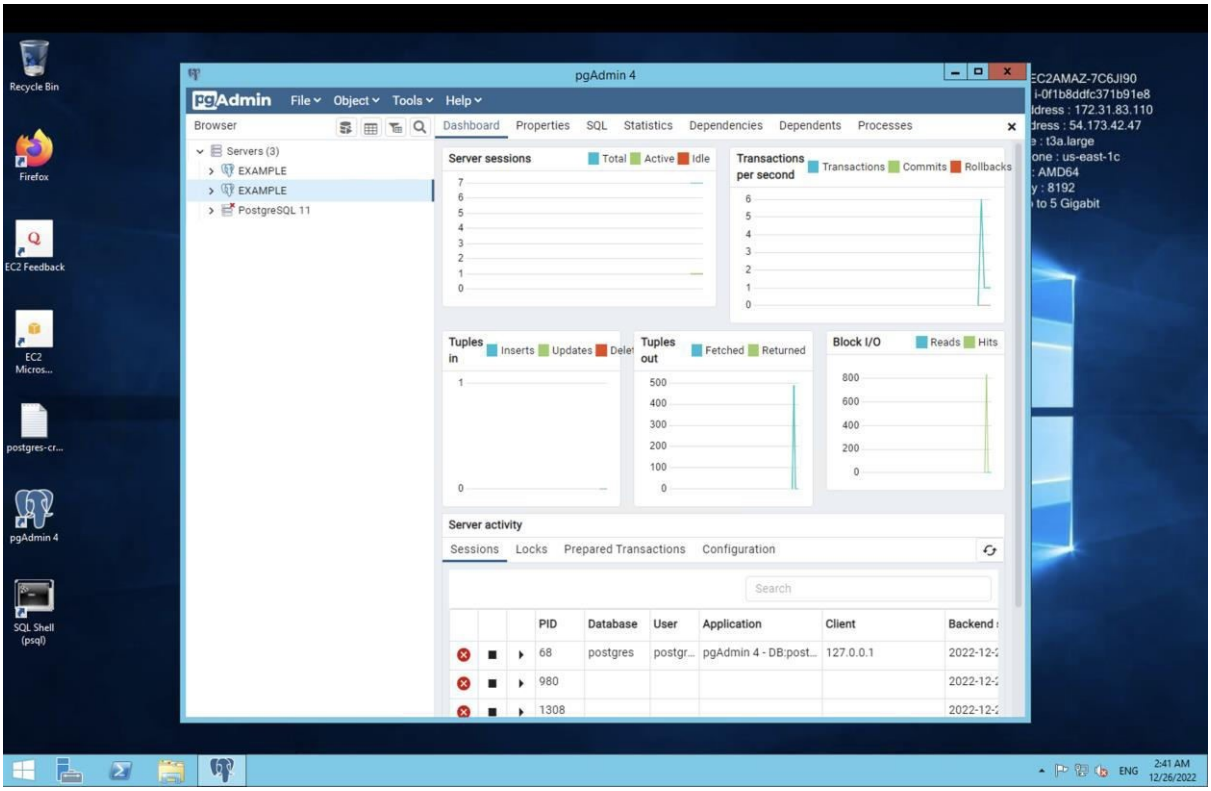

Host: localhost

Port: 5432

Username: postgres

Password: REFER TO THE RANDOMLY GENERATED PASSWORD VALUE FOUND IN THE postgres-credentials.txt FILE FOUND ON THE DESKTOP OF THE ADMINISTRATOR USER.

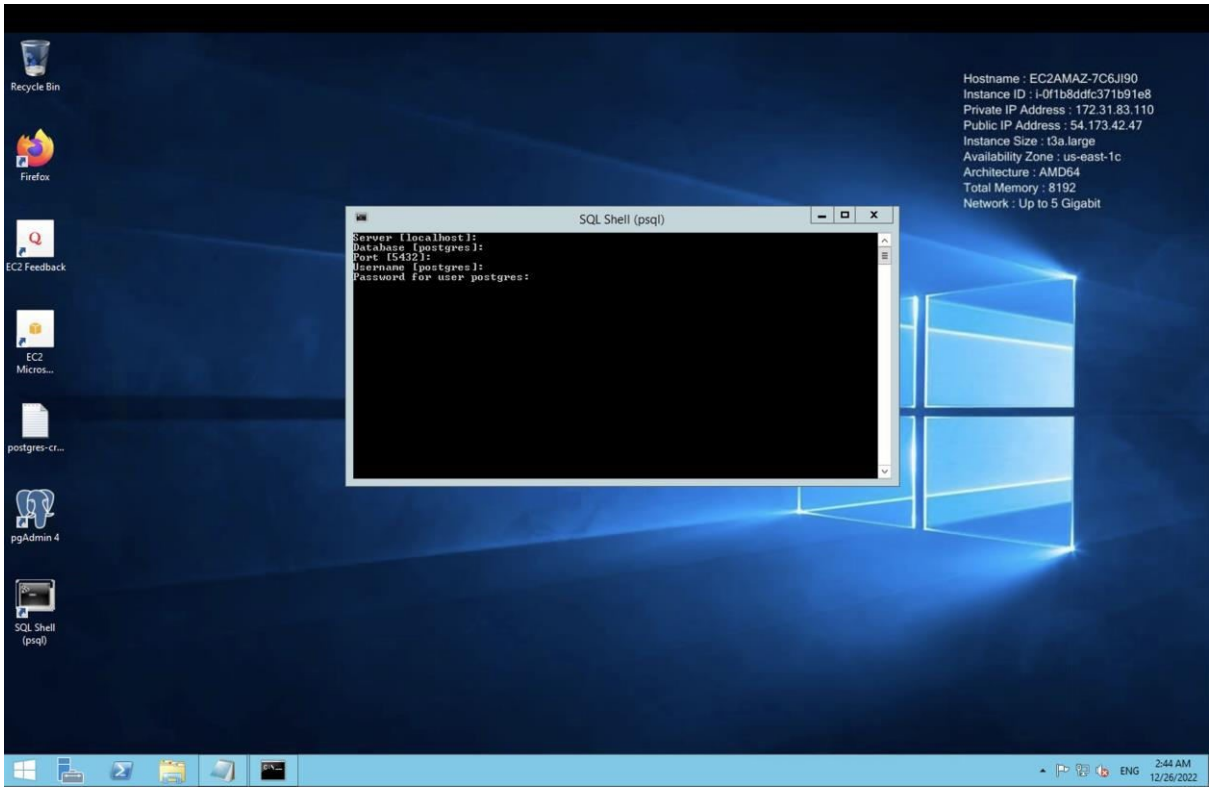
Click Save




You have now successfully connected to the locally running postgres database instance.

**SQL Shell (psql)**

SQL Shell has also been preinstalled on the system. You can access this programme via the below icon located on the Desktop of the Administrator user.




Upon starting the programme, you will be prompted for the below inputs.

Server: localhost

Database: postgres

Username: postgres

Password: REFER TO THE RANDOMLY GENERATED PASSWORD VALUE FOUND IN THE postgres-credentials.txt FILE FOUND ON THE DESKTOP OF THE ADMINISTRATOR USER.

Once successfully connected, you will now be able to perform postgres database administration tasks from the command line interface.