Genome Suite Analyzer User Guide for AWS

The Sequencing Center

Date: 2024-09-24

Repository: The-Sequencing-Center/GenomeSuite-Docs

Website: www.thesequencingcenter.com

Support: support@thesequencingcenter.com

Phone: +1 877-425-2235

Contents

Getting Started

GenomeSuite Analyzer runs on the Amazon Web Services (AWS) platform.
* If you do not have an AWS account, start with the **Create AWS Account** instructions below.
* If you do have an AWS account, you can skip to the step **Login to AWS Account**.

Some steps are identified as a "**one-time step**". This means you should only have to perform this step once during initial setup.

Creating an AWS Account

This is a **one-time** step.

To create an AWS account, follow these steps:

1. Open the AWS account creation page and **Create an AWS Account**.
2. Fill in the details and click **Verify email address**. You will receive an email with a verification code that you need to enter on the sign up page.
3. Set up your root user password and confirm it.
4. Choose between a Personal or Professional account. The features and functions are the same, but the information required might differ slightly.
5. Fill in your contact information and read the AWS Customer Agreement. Once done, click **Continue**.
6. Provide a valid payment method (credit/debit card). This step is mandatory even if you plan to use the free tier services. You may also need to verify your payment method by entering a code sent by AWS.
7. AWS will ask you to provide a phone number to verify your identity. You will receive a call or SMS with a verification code that you need to enter to proceed.

8. Choose one of the available support plans (Basic, Developer, Business, or Enterprise). The Basic support plan is free.
    - After selecting your support plan, AWS will begin activating your account. This process usually takes a few minutes but can take up to 24 hours. Once activation is complete, you will receive a confirmation email.

After your account is activated, you can sign in to the AWS Management Console and start using AWS services.

Logging into Your AWS Account

To log in to your AWS account, follow these steps:

1. Open your web browser and go to the AWS Management Console login page.
2. On the login page, you will see two options:
    - **Root user:** Use this if you are logging in as the account owner or the main administrator.
        - If you are the root user, click **Root user** and enter your email address associated with the AWS account. Click **Next**.
    - **IAM user:** Use this if you have been assigned a user account within an AWS organization.
        - If you are an IAM user, click **IAM user** and enter your IAM username along with the account ID or alias. Click **Next**.
3. Enter the password for your account, and click **Sign In**.
    - If Multi-Factor Authentication (MFA) is enabled for your account, you will be prompted to enter the code from your authentication device (like a mobile app). Enter the code and proceed.
4. After successful authentication, you will be directed to the AWS Management Console, where you can start managing your AWS services.

Creating an S3 Bucket

This is a **one-time** step.

You will now create an AWS S3 bucket that will contain all of your Nanopore POD5 sample files. To create an S3 bucket in your AWS account, follow these steps:

1. From the AWS Management Console, type **S3** into the search bar at the top. Choose **S3** from the drop-down list. This will take you to the Amazon S3 dashboard.
2. On the S3 dashboard, click the **Create bucket** button.

3. To configure the bucket settings, enter a name for the bucket in the **Bucket** name field.
    - Bucket names must be globally unique across all existing bucket names in Amazon S3. If you choose a name that is already taken, you'll have to try other names until you find a unique name.
    - The name must not contain spaces and must adhere to the bucket naming rules (e.g., lowercase letters, numbers, and hyphens).
    - Choose the region **US East (N. Virginia) us-east-1**. This is the region where the S3 bucket will be created.
4. By default, S3 buckets are set to block all public access. You can leave this option enabled unless you specifically need the bucket to be public.
5. To enable versioning, which keeps multiple versions of an object in the same bucket, you may optionally choose to enable this in **Bucket Versioning**.
6. You may also enable additional optional settings such as adding tags, enabling object lock, and set default encryption, but these are not necessary can be configured later.
7. After configuring the settings, review your choices and click **Create bucket**.
8. After the bucket is created, you will be taken back to the S3 dashboard, where you will see the bucket name listed among your S3 buckets.

Uploading POD5 Files to S3 Bucket

There are several methods available for uploading POD5 files to S3 buckets. These methods are beyond the scope of this document. For human whole genome sequencing, the aggregate size of these files is quite large, ca. 1TB or more, and may need special methods to upload in reasonable time. Please contact us at support@thesequencingcenter.com to review and discuss options for uploading large datasets.

Storing POD5 Files in S3 Bucket

If you already have an AWS account and an S3 bucket with POD5 files in it, you have two choices. You can use the existing Bucket name with GenomeSuite: Analyzer. Or you can copy or move the POD5 files from the existing bucket to another bucket within the same AWS account.

To copy or move files, follow these instructions:

Using the AWS Management Console

1. In the S3 dashboard, find and click the source bucket that contains the POD5 files you want to copy or move.

2. Browse through the folders in your source bucket and select the files you want to copy or move. You can select multiple files by holding the **Ctrl** key (or **Cmd** on Mac) while clicking.
3. After selecting the files, click on the **Actions** button at the top of the screen, and choose either **Copy** or **Move**.
    - A dialog box will appear asking where you want to copy or move the files.
4. In the **Destination** field, click **Browse S3** and navigate to the destination bucket.
    - You can specify the exact location within the bucket by selecting a folder or leave it blank to place the files directly in the bucket's root.
5. Once the destination is set, click **Copy** or **Move** to begin the operation. Depending on the size and number of files, this may take a few moments.
6. Navigate to the destination bucket and verify that the files have been successfully copied or moved.

Important Note: - In the S3 bucket that contains the POD5 files, make sure that all of the files are in the directory just below the S3 bucket name. There should be no other subdirectories under the main directory.

- For example: If your bucket name is `s3://your-bucket-name/`, all of the POD5 files should be immediately below this directory and there should be no subdirectories under `s3://your-bucket-name/`.

Creating a Key Pair

This is a one-time step.

To create a key pair in AWS, follow these steps:

Access the EC2 Dashboard

1. In the AWS Management Console, type **EC2** in the search bar and choose **EC2** from the drop-down menu.

Create a Key Pair

1. To open the key pair management page in the EC2 Dashboard, click on **Key Pairs** option under the **Network & Security** section on the left-hand side menu.
2. Click the **Create Key Pair** button.
3. Configure the key pair settings:

- **Name:** Enter a name for your key pair, such as **analyzer-keypair**. The name must be unique within your AWS region.
- **Key Pair Type:** Choose the key pair type, typically **ED25519**.
- **Private Key File Format:** Choose the format for the private key file. Options include:
  - .pem: For SSH clients (like OpenSSH) on Linux or macOS.
  - .ppk: For PuTTY, a popular SSH client on Windows.
- **Tags:** (Optional) You can add tags to your key pair for easier management.

4. Click **Create key pair**. AWS will generate the key pair and automatically download the private key file to your computer.

Secure the Private Key

1. Save the private key.
   - The private key file will automatically download to your computer. This file is crucial for connecting to your EC2 instances securely, so store it in a safe location. If you lose this file, you will not be able to connect to your instances using this key pair.
2. To set the correct permissions if you are using the key pair on a Linux or macOS system, run the following command:

   ```
   chmod 400 /path/to/your-keypair.pem
   ```

3. Make sure the private key is stored securely. Do not share it with anyone or commit it to version control systems like Git.

Important Notes: - **One-Time Download:** The private key file can only be downloaded once at the time of creation. If you lose the private key, you will need to create a new key pair and update your instances to use the new key. - **Accessing EC2 Instances:** When launching a new EC2 instance, you'll be able to select this key pair for SSH access. Ensure the correct permissions are set on your private key file before attempting to connect.

Creating a Security Group

This is a one-time step.

To create a security group in AWS for EC2 that allows SSH logins on port 22, follow these steps:

Access the EC2 Dashboard

1. In the AWS Management Console, type **EC2** in the search bar and choose **EC2** from the drop-down menu.

Create a Security Group

1. To open the security group management page in the EC2 Dashboard, click **Security Groups** option under the **Network & Security** section in the left-hand menu.
2. Click on the **Create security group** button to create a new security group.
3. **Configure Security Group Settings:**
   - **Name:** Enter a name for your security group, such as **sniffles-sg**.
   - **Description:** Provide a brief description of the security group, like "Security group for SSH access to EC2 instances".
   - **VPC:** Choose the appropriate VPC (Virtual Private Cloud) where you want this security group to be used. If you only have one VPC, it will be selected by default.

Add an Inbound Rule for SSH Access

1. **Configure Inbound Rules:**
   - In the Inbound rules section, click on **Add Rule**.
   - Type: From the drop-down list, select **SSH**. This will automatically set the Port Range to 22.
   - Source:
     - You can choose **My IP** to allow SSH access only from your current IP address.
     - Alternatively, select **Anywhere** (0.0.0.0/0) to allow SSH access from any IP address, but note that this is less secure and should be used with caution.
     - You can also specify a custom IP range if you only want to allow SSH access from specific IP addresses or ranges.

Review and Create the Security Group

1. Review the rules you've added to ensure they match your requirements.
2. Once satisfied with the configuration, click **Create security group**.

Attach the Security Group to an EC2 Instance

1. **During EC2 Instance Launch:**
   - When launching a new EC2 instance, you can choose this security group under the **Configure Security Group** section.
2. **For Existing Instances:**
   - If you want to assign this security group to an existing instance, go to the **Instances** section, select your instance, click **Actions** > **Networking** > **Change Security Groups**, and then select the **analyzer-sg** security group.

Important Notes: - **Security Considerations:** Allowing SSH access from any IP address (0.0.0.0/0) is convenient but can expose your instance to potential attacks. It's recommended to restrict access to specific IP addresses whenever possible. - **Firewall Settings:** Ensure that any local firewalls on your machine or network allow outbound connections on port 22. # Launching GenomeSuite Analyzer on EC2

To launch the GenomeSuite Analyzer AMI (Amazon Machine Image) using EC2, follow these steps:

Step 1: Start at the EC2 Dashboard

1. **Navigate to the EC2 Dashboard:**
   - Once on the EC2 Dashboard, confirm you are in the correct region.

Step 2: Select a Region

```
1. GenomeSuite Analyzer is available in four AWS regions:
    * US East (N. Virginia) us-east-1
    * US East (Ohio) us-east-2
    * US West (Oregon) us-west-2
    * Canada (Central) ca-central-1
2. Choose a Region:
    * In the top-right corner of the EC2 Dashboard, click on the region selector drop-down.
    * Select one of the four regions from the list of regions.
```

Step 3: Find the GenomeSuite Analyzer AMI

1. **Navigate to AMIs:**
   - In the left-hand menu under **Images**, click on **AMIs**.
2. **Filter for Public Images:**
   - At the top of the AMIs page, find the drop-down list labeled **Owned by me**. Click on it and choose **Public images**.
3. **Search for the GenomeSuite Analyzer AMI:**
   - In the search bar, type **Sniffles_v.1.1.0** and press Enter.
4. **Select the AMI:**
   - Find the AMI named **Sniffles_v.1.1.0** in the results.
   - Click the checkbox next to this AMI to highlight the row.
5. **Launch the Instance:**
   - With the AMI row selected, click on the **Launch instance from image** button at the top right of the page.

Step 4: Configure the Instance

1. **Name the Instance:**

- On the **Launch an Instance** page, provide a name for your instance in the **Name** field.

2. **Select the Instance Type:**

   - Under **Instance Type**, select one of the following options:

   `For human exome, use these instance types:`

   1. `p3.2xlarge`
   2. `p3.8xlarge`
   3. `p3.16xlarge`

   `For human whole genome, use this instance type:`

   1. `p4d.24xlarge`

   These instance types are optimized for high-performance computing tasks using Nvidia GPU's.

3. **Configure Key Pair:**

   - Under **Key Pair (login)**, select the key pair you created earlier (e.g., `**sniffles-keypair**`).

4. **Set Network Settings:**

   - Under **Network Settings**, select **Edit**.
   - Choose **Select existing security group** and select the security group you created earlier (e.g., `**sniffles-sg**`).

5. **Configure Storage:**

   - Under **Configure Storage**, set the storage size to **2048 GiB**.
   - Ensure the storage type is set to **gp3** (General Purpose SSD).

Step 5: Launch the Instance

1. **Review the Settings:**
   - Double-check all configurations to ensure everything is set correctly.
2. **Launch the Instance:**
   - Click on the **Launch Instance** button at the bottom of the page.

   - If you get an error message "Insufficient Capacity", this means all of the available computing resources are in use.
     At this point, you have two options:
     `1) Wait a few minutes and try to launch the instance again.`
     `2) Choose a different Region and try to launch the instance again.`
     Typically, there are computing resources available in one of the regions.
3. **Instance Initialization:**
   - Once launched, you will be taken to a page showing the status of your instance. The instance will take a few minutes to initialize.

4. **Verify the Instance:**
   - After the instance is running, you can find it under **Instances** in the EC2 Dashboard. Make sure the instance status is **running** before attempting to connect. # Configuring and Connecting to the EC2 Instance

Option 1: Configure Mac Terminal

This is a **one-time** step.

To connect to your EC2 instance using a Mac Terminal, you will first need to install the AWS CLI and then configure it. Below are the steps to do this:

Step 1: Install AWS CLI on Mac

1. **Open Terminal:**
   - On your Mac, open the Terminal application. This should be located in the Applications directory.
2. **Install Homebrew (if not already installed):**
   - Homebrew is a package manager for macOS that simplifies the installation of software. If you don't have Homebrew installed, run the following command in Terminal:
     `/bin/bash -c **$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD`
   - Follow the on-screen instructions to complete the installation.
3. **Install AWS CLI using Homebrew:**
   - Once Homebrew is installed, you can easily install the AWS CLI by running the following command:
     `brew install awscli`
   - This will download and install the AWS CLI on your Mac.
4. **Verify Installation:**
   - After installation, verify that the AWS CLI is installed correctly by typing:
     `aws --version`
   - You should see output showing the installed version of the AWS CLI.

Step 2: Configure the AWS CLI

1. **Run the AWS CLI Configuration Command:**
   - In Terminal, configure the AWS CLI by running:
     `aws configure`
2. **Enter Your AWS Credentials:**
   - The CLI will prompt you to enter the following information:
     - AWS Access Key ID: Enter your AWS Access Key ID (see below).
     - AWS Secret Access Key: Enter your AWS Secret Access Key (see below).
     - Default region name: Enter your preferred region (for example, us-east-1).

– Default output format: Enter None.

How to Obtain Your AWS Access Key ID and AWS Secret Access Key:

For New Users:

1. Sign in to the AWS Management Console and navigate to the IAM (Identity and Access Management) Console.
2. Create a New IAM User:
   - In the IAM Dashboard, click on **Users** in the left-hand menu.
   - Click **Add user**.
   - Provide a username and check the **Programmatic access** checkbox to generate an access key.
   - Click **Next: Permissions** to assign appropriate permissions, either directly or by attaching a policy (e.g., AmazonS3FullAccess if you need S3 access).
   - Follow the remaining prompts and then click **Create user**.
3. Download or View the Access Key:
   - After creating the user, you'll see a page with the Access Key ID and Secret Access Key. You can download these credentials as a .csv file or view them directly on the page.
   - Important: This is the only time you'll be able to view the Secret Access Key, so make sure to store it securely.

For Existing Users:

1. Sign in to the AWS Management Console and navigate to the IAM Console.
2. Access Your Existing IAM User:
   - In the IAM Dashboard, click on **Users** in the left-hand menu.
   - Click on your username to access the details.
3. Create a New Access Key (if none exists or if you need a new one):
   - Go to the **Security credentials** tab.
   - Scroll down to the **Access keys** section.
   - Click on **Create access key**. AWS will generate a new Access Key ID and Secret Access Key for you.
4. Download or View the Access Key:
   - As with new users, you'll have the option to download the key or view it once. Ensure it is stored securely.
5. **Verify Configuration:**
   - You can verify your configuration by listing the S3 buckets or EC2 instances:
     `aws s3 ls`
     or
     `aws ec2 describe-instances`
   - If configured correctly, this should return a list of your S3 buckets or EC2 instances.

Option 2: Configure Windows Terminal

This is a **one-time** step.

To configure the AWS CLI on a Windows machine and connect to an EC2 instance, follow these steps:

Step 1: Install AWS CLI on Windows

1. **Open PowerShell or Command Prompt:**
   - On your Windows machine, open PowerShell or Command Prompt by searching for it in the Start menu.
2. **Download the AWS CLI Installer:**
   - Download the AWS CLI installer for Windows from the AWS CLI official website. You can download the .msi installer directly by clicking here.
3. **Run the Installer:**
   - Once downloaded, run the .msi installer. Follow the on-screen instructions to complete the installation. The installer will automatically install the AWS CLI to your system.
4. **Verify Installation:**
   - After installation, verify that the AWS CLI is installed correctly by typing the following command in PowerShell or Command Prompt:
     `aws --version`
   - You should see output showing the installed version of the AWS CLI, confirming that it is ready to use.

Step 2: Configure the AWS CLI

1. **Run the AWS CLI Configuration Command:**
   - In PowerShell or Command Prompt, configure the AWS CLI by running:
     `aws configure`
2. **Enter Your AWS Credentials:**
   - The CLI will prompt you to enter the following information:
     - AWS Access Key ID: Enter your AWS Access Key ID (see below).
     - AWS Secret Access Key: Enter your AWS Secret Access Key (see below).
     - Default region name: Enter your preferred region (for example, us-east-1).
     - Default output format: Enter None.

How to Obtain Your AWS Access Key ID and AWS Secret Access Key:

For New Users:

1. Sign in to the AWS Management Console and navigate to the IAM (Identity and Access Management) Console.
2. Create a New IAM User:
   - In the IAM Dashboard, click on **Users** in the left-hand menu.
   - Click **Add user**.
   - Provide a username and check the **Programmatic access** checkbox to generate an access key.
   - Click **Next: Permissions** to assign appropriate permissions, either directly or by attaching a policy (e.g., AmazonS3FullAccess if you need S3 access).
   - Follow the remaining prompts and then click **Create user**.
3. Download or View the Access Key:
   - After creating the user, you'll see a page with the Access Key ID and Secret Access Key. You can download these credentials as a .csv file or view them directly on the page.
   - Important: This is the only time you'll be able to view the Secret Access Key, so make sure to store it securely.

For Existing Users:

1. Sign in to the AWS Management Console and navigate to the IAM Console.
2. Access Your Existing IAM User:
   - In the IAM Dashboard, click on **Users** in the left-hand menu.
   - Click on your username to access the details.
3. Create a New Access Key (if none exists or if you need a new one):
   - Go to the **Security credentials** tab.
   - Scroll down to the **Access keys** section.
   - Click on **Create access key**. AWS will generate a new Access Key ID and Secret Access Key for you.
4. Download or View the Access Key:
   - As with new users, you'll have the option to download the key or view it once. Ensure it is stored securely.
5. **Verify Configuration:**
   - You can verify your configuration by listing the S3 buckets or EC2 instances. Run one of the following commands:
     `aws s3 ls`
     or
     `aws ec2 describe-instances`
   - If configured correctly, this should return a list of your S3 buckets or EC2 instances.

Additional Steps (if required):

- **Set Environment Variables (Optional):**
  - If you want to make sure the AWS CLI is accessible from any directory, ensure that the installation path is included in your system's

environment variables. This is typically done automatically by the installer.

- **Connect to EC2 Instance Using SSH (Optional):**
  - To connect to your EC2 instance using SSH from Windows, you can use PuTTY or the Windows Subsystem for Linux (WSL) with an SSH client. Ensure that you have your .pem key file and that it is converted to .ppk if using PuTTY.

Connect to Sniffles on EC2

You can now access the Sniffles instance that is running on AWS EC2.

Connect to Your EC2 Instance

1. **Locate Your PEM File:**
   - Ensure you have the .pem key pair file that was created when you launched your EC2 instance.
2. **Set Permissions for the PEM File:**
   - Run the following command to set the correct permissions for the key pair file:
     `chmod 400 /path/to/your-keypair.pem`
   - Replace `/path/to/your-keypair.pem` with the actual path to your .pem file.
3. **Connect to the EC2 Instance:**
   - Use the SSH command to connect to your EC2 instance. Run the following command in Terminal:
     `ssh -i /path/to/your-keypair.pem ubuntu@your-instance-public-dns`
   - Replace `/path/to/your-keypair.pem` with the path to your .pem file and `your-instance-public-dns` with the Public DNS address of your EC2 instance. You can find the Public DNS in the AWS Management Console under the **Instances** section.
4. **Access Your EC2 Instance:**
   - Once connected, you will have shell access to your EC2 instance, allowing you to manage it as needed.

Additional Tips:

- **Using SSH Config File:** If you frequently connect to the same instance, consider setting up an SSH config file to simplify the connection command.
- **Security Considerations:** Ensure your .pem file is kept secure, as it provides access to your EC2 instance.

Configure AWS Credentials

This is a one-time step.

After logging into the EC2 instance, you must configure your AWS credentials by following these steps:

Step 1: Connect to the EC2 Instance

- Ensure you are logged into the EC2 instance using SSH as previously explained.

Step 2: Configure AWS CLI with Your Credentials

1. **Run the AWS CLI Configuration Command:**
   - On your EC2 instance, configure the AWS CLI by running:
     `aws configure`
2. **Enter Your AWS Credentials:**
   - The CLI will prompt you to enter the following information:
     - AWS Access Key ID: Enter your AWS Access Key ID (see below).
     - AWS Secret Access Key: Enter your AWS Secret Access Key (see below).
     - Default region name: Enter the region where your S3 bucket is located (e.g., us-east-1).
     - Default output format: Enter None.

How to Obtain Your AWS Access Key ID and AWS Secret Access Key:

For New Users:

1. Sign in to the AWS Management Console and navigate to the IAM (Identity and Access Management) Console.
2. Create a New IAM User:
   - In the IAM Dashboard, click on **Users** in the left-hand menu.
   - Click **Add user**.
   - Provide a username and check the **Programmatic access** checkbox to generate an access key.
   - Click **Next: Permissions** to assign appropriate permissions, either directly or by attaching a policy (e.g., AmazonS3FullAccess if you need S3 access).
   - Follow the remaining prompts and then click **Create user**.
3. Download or View the Access Key:
   - After creating the user, you'll see a page with the Access Key ID and Secret Access Key. You can download these credentials as a .csv file or view them directly on the page.
   - Important: This is the only time you'll be able to view the Secret Access Key, so make sure to store it securely.

For Existing Users:

1. Sign in to the AWS Management Console and navigate to the IAM Console.
2. Access Your Existing IAM User:
    - In the IAM Dashboard, click on **Users** in the left-hand menu.
    - Click on your username to access the details.
3. Create a New Access Key (if none exists or if you need a new one):
    - Go to the **Security credentials** tab.
    - Scroll down to the **Access keys** section.
    - Click on **Create access key**. AWS will generate a new Access Key ID and Secret Access Key for you.
4. Download or View the Access Key:
    - As with new users, you'll have the option to download the key or view it once. Ensure it is stored securely.
5. **Verify Configuration:**
    - To verify that the credentials are configured correctly, you can try listing the contents of your S3 bucket.
      `aws s3 ls s3://your-bucket-name`
    - Replace `your-bucket-name` with the actual name of your S3 bucket.

Important Note: By configuring your AWS credentials directly on the EC2 instance, you enable the instance to interact with S3 buckets. This is essential for performing operations like uploading or downloading files from an S3 bucket.
Running and Terminating GenomeSuite Analyzer

To run GenomeSuite Analyzer on the EC2 instance, follow these steps:

Navigate to the GenomeSuite Analyzer Directory

1. **Change to the Home Directory:**
    - Once logged in, you should already be in the `/home/ubuntu` directory. To confirm, run:
      `cd /home/ubuntu`
    - If you're already there, this command won't change anything.
2. **Navigate to the GenomeSuite Analyzer Distribution Directory:**
    - Run the following command to change into the GenomeSuite Analyzer distribution directory:
      `cd Sniffles/dist`

Run GenomeSuite Analyzer

1. **Run GenomeSuite Analyzer with the Required Parameters:**
    - Execute GenomeSuite Analyzer by running the following command:
      `./sniffles -b bucketname -s samplename`
    - Replace `bucketname` with the name of the S3 bucket where your POD5 files are stored.
    - Replace `samplename` with an arbitrary name of your choice for the sample being processed.

Example Command: If your S3 bucket is named `sniffles-sample` and your sample name is `sample1`, the command would look like this:

```
./sniffles -b sniffles-sample -s sample1
```

Monitor GenomeSuite Analyzer Output

- GenomeSuite Analyzer will start processing the data. You should see output in the terminal indicating the progress of the operation. Depending on the size of the dataset, this may take some time.

Create a New AMI

This is a **one-time** step.

When the GenomeSuite Analyzer job is done, and before terminating the running EC2 instance, it is VERY IMPORTANT that you create a new AMI. By creating a new AMI you will save all your configuration settings from above. You can then use this new AMI for all future runs.

To create a new AMI from a running EC2 instance using the EC2 console, follow these steps:

Step 1: Access the EC2 Console

1. **Navigate to the EC2 Dashboard:**
   - In the AWS Management Console, type **EC2** in the search bar and select **EC2** from the drop-down menu.
2. **Access the Instances Section:**
   - In the EC2 Dashboard, click on **Instances** in the left-hand menu under the **Instances** section. This will display a list of all running EC2 instances.

Step 2: Create an AMI from the Running Instance

1. **Select the Instance:**
   - Locate the running instance from which you want to create an AMI. Click the checkbox next to the instance to select it.
2. **Open the Instance Actions Menu:**
   - With the instance selected, click on the **Actions** drop-down menu at the top right of the page.
3. **Select Create Image:**
   - From the **Actions** drop-down menu, navigate to **Image and templates** and then select **Create image**. This will open the Create Image dialog box.
4. **Configure the Image Settings:**
   - Image Name: Enter a name for your AMI in the **Image name** field.

- Image Description (optional): You can provide a description of the AMI for future reference.

5. **Create the Image:**
   - Once you have configured all the settings, click on the **Create image** button at the bottom of the dialog box.

Step 3: Monitor the AMI Creation Process

1. **View the Image Creation Progress:**
   - AWS will start creating the AMI. To monitor its progress, click on **AMIs** in the left-hand menu under the **Images** section.
   - You will see your new AMI listed with a status of **pending**. Once the status changes to **available**, the AMI is ready to use.

Terminate GenomeSuite Analyzer EC2 Instance

When the GenomeSuite Analyzer job is finished, it's very important that you terminate the running GenomeSuite Analyzer EC2 instance. You do not want to accumulate unnecessary charges by letting the instance continue running.

To terminate an EC2 instance, follow these steps:

Step 1: Access the EC2 Dashboard

1. **Navigate to the Instances Section:**
   - On the EC2 Dashboard, in the left-hand menu, click on **Instances** under the **Instances** section.

Step 2: Select the Instance to Terminate

1. **Find the Instance:**
   - Locate the instance you want to terminate. You can use the search bar at the top to filter instances by name, instance ID, or other attributes.
2. **Select the Instance:**
   - Click the checkbox next to the instance you want to terminate to select it.

Step 3: Terminate the Instance

1. **Terminate the Instance:**
   - With the instance selected, click on the **Instance state** button at the top of the page.
   - From the dropdown menu, select **Terminate instance**.
2. **Confirm the Termination:**
   - A confirmation dialog will appear asking if you're sure you want to terminate the instance. Confirm by clicking **Terminate**.
3. **Monitor Termination Process:**

- The instance will begin shutting down and its state will change to **shutting-down** and then to **terminated**. Once terminated, the instance will no longer incur charges. # Retrieving the VCF File

GenomeSuite Analyzer will generate a **VCF** file and store it in your S3 bucket. To download the VCF file from the S3 bucket, follow these steps:

Step 1: Sign in to the AWS Management Console

1. **Navigate to the AWS Console:**
   - Open your web browser and go to the AWS Management Console.
   - Sign in with your AWS account credentials.

Step 2: Access the S3 Service

1. **Open the S3 Dashboard:**
   - In the AWS Management Console, type **S3** into the search bar and select **S3** from the dropdown list to navigate to the S3 service.

Step 3: Locate the VCF File in the S3 Bucket

1. **Find the Bucket:**
   - In the S3 Dashboard, find and click on the bucket name where the VCF file is stored (e.g., `sniffles-sample`).
2. **Locate the VCF File:**
   - Search for the VCF file using the naming convention `sample_name.vcf.gz`, where `sample_name` is the name you provided in the `-s` parameter when running GenomeSuite Analyzer. For example, if the sample name was `sample1`, look for the file named `sample1.vcf.gz`.

Step 4: Download the VCF File

1. **Select the File:**
   - Once you locate the `sample_name.vcf.gz` file, click on the checkbox next to the file name to select it.
2. **Download the File:**
   - With the file selected, click on the **Download** button. The file will begin downloading to your local machine.