abYsis

Using on AWS

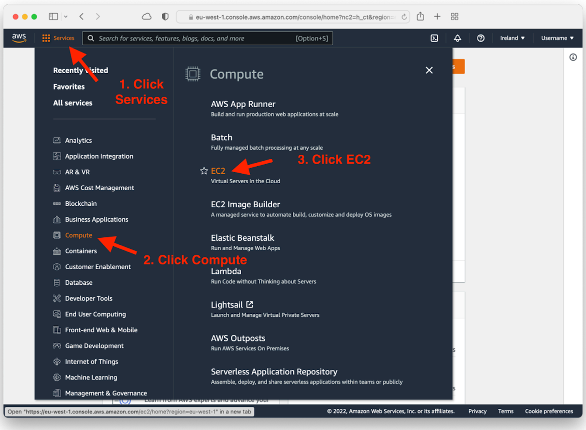
Table of Contents

Introduction

This manual is intended to give people an introduction to how abYsis might be used on a hosted service. We use AWS as an exemplar based but the information given here should not be considered comprehensive. Readers should access the AWS manuals and information. As always your own IT professionals should independently determine whether this is the appropriate option for your company and what steps are required to secure the system to your own requirement.

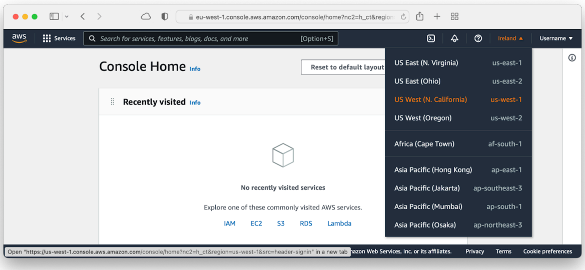
Installing a RHEL/Rocky 9 EC2 instance

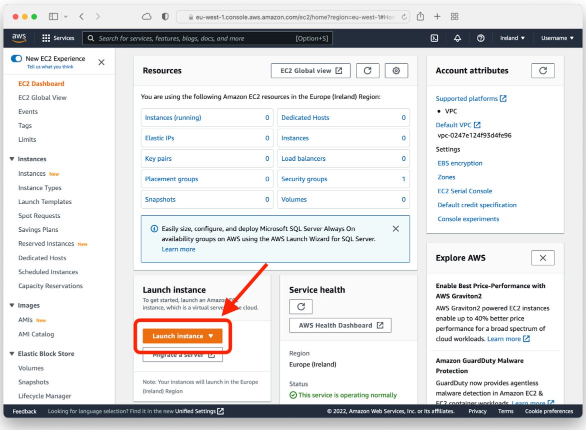
Launching an Instance



Before any work can begin you will need to create an Amazon AWS account and login to the Management Console.

Make sure that you select the appropriate cluster location - typically geographically close to your own location.

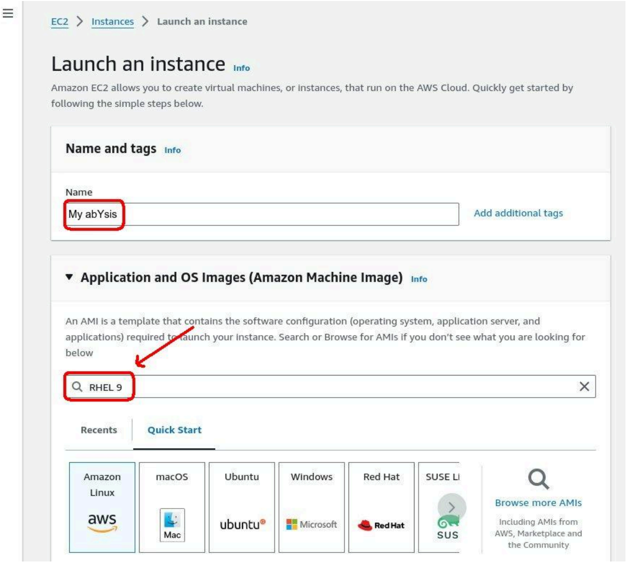

Console Home
US East (N. Virginia) us-east-1
US East (Ohio) us-east-2
US West (N. California) us-west-1
US West (Oregon) us-west-2
Africa (Cape Town) af-south-1
Asia Pacific (Hong Kong) ap-east-1
Asia Pacific (Jakarta) ap-southeast-3
Asia Pacific (Mumbai) ap-south-1
Asia Pacific (Osaka) ap-northeast-3



Now select the 'EC2' link under Services/Compute and click the 'Launch Instance' button.

Now go through the following steps:

a) Name your instance so you can easily recognise it later and then search for your preferred OS - RHEL 9 or Rocky 9.



Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name: My abYsis

▼ Application and OS Images (Amazon Machine Image)

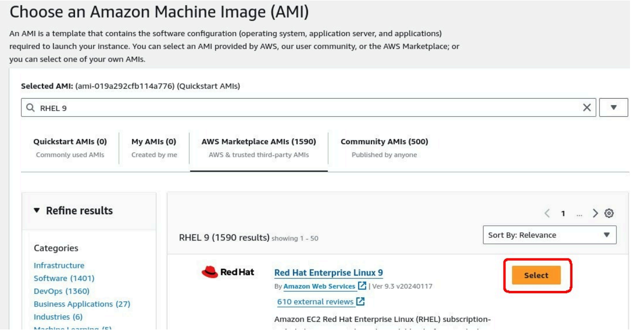
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

RHEL 9

b) The most suitable AMI is likely to be found in the AMI Marketplace indicating that a cost may be involved. We recommend

- Red Hat Enterprise Linux 9 by Amazon Web Services
- Rocky Linux 9 (Official) - x86_64 by Rocky Linux (not the "with LVM" variant)

c) Click ‘Select’ for the OS release you wish to use. You may be asked to confirm the cost of the subscription for using the OS.



Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

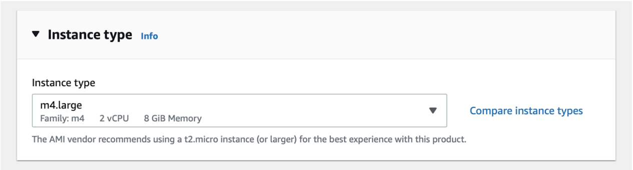
Selected AMI: (ami-019a292cfb114a776) (Quickstart AMIs)

RHEL 9

RHEL 9 (1590 results) showing 1 - 50

Red Hat Enterprise Linux 9
By Amazon Web Services | Ver 9.3 v20240117
610 external reviews
Amazon EC2 Red Hat Enterprise Linux (RHEL) subscription-

d) In the “Instance Type” panel, select your instance type. Below we have selected ‘m4.large’.



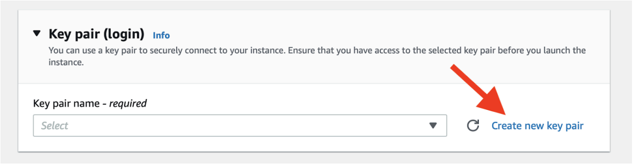
▼ Instance type

Instance type: m4.large
Family: m4 2 vCPU 8 GiB Memory

The AMI vendor recommends using a t2.micro instance (or larger) for the best experience with this product.

e) In the “Key pair (login)” panel create an SSH key.

- Select ‘Create a new key pair’

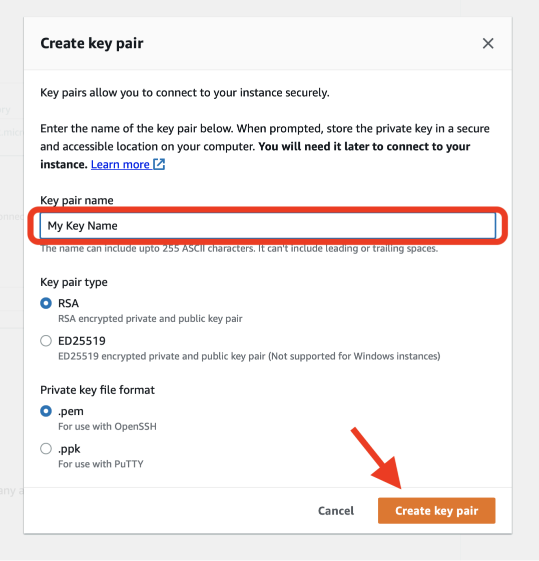


▼ Key pair (login)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

- Enter and name for the key.
- Click “Create key pair.



Create key pair

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** Learn more

Key pair name: My Key Name

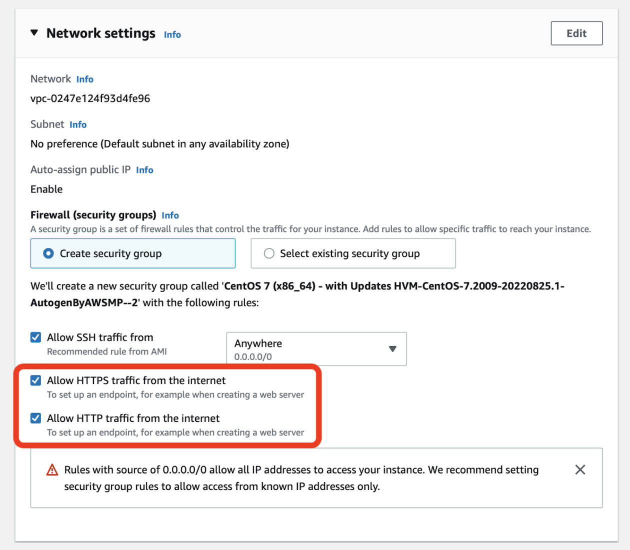
The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type
● RSA
RSA encrypted private and public key pair
○ ED25519
ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format
● .pem
For use with OpenSSH
○ .ppk
For use with PuTTY

- The ‘.pem’ key file will be downloaded. This file is important as it is required to connect to the server.

f) In the “Network Settings” panel select "Allow SSH", “Allow HTTPS” and “Allow HTTP" traffic from the internet.



▼ **Network settings** Info

Network Info
vpc-0247e124f93d4fe96

Subnet Info
No preference (Default subnet in any availability zone)

Auto-assign public IP Info
Enable

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

We'll create a new security group called '**CentOS 7 (x86_64) - with Updates HVM-CentOS-7.2009-20220825.1-AutogenByAWSMP--2**' with the following rules:

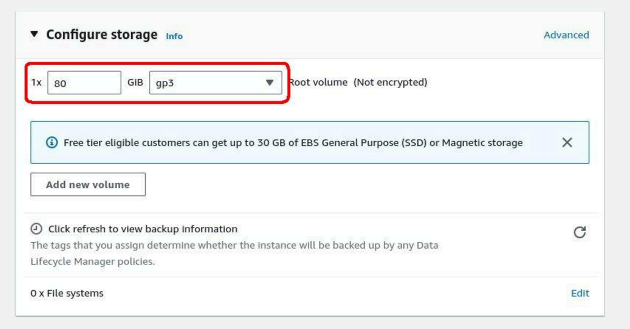
☑ Allow SSH traffic from — Anywhere 0.0.0.0/0
Recommended rule from AMI

☑ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☑ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

g) In the “Configure storage” panel, edit the size as required. 60Gb is the minimum currently recommended. Typical suitable storage media is either gp2 or gp3. It is best to review as their usage will involve cost.



▼ **Configure storage** Info

1x 80 GiB gp3 Root volume (Not encrypted)

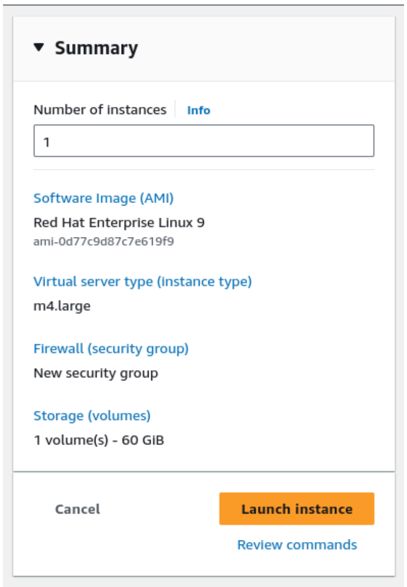
ⓘ Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

h) When your instance is **stopped**, the storage volume (disk) is retained (at a small cost) so that the instance can be started again. When your instance is **terminated** this volume is automatically deleted. Under “Advanced” there is an option for “Termination protection”. When it is **enabled** your instance cannot be terminated and your installation disk will not be deleted without first manually changing the termination protection to **disabled**.

i) The “Summary” panel to the right shows the options you have configured. Check they are correct and click “Launch instance”



▼ **Summary**

Number of instances Info
1

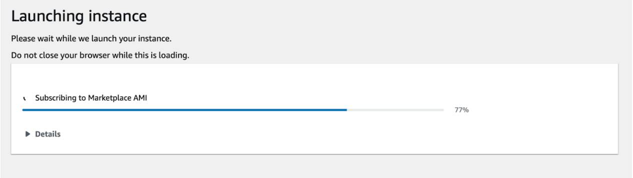
Software Image (AMI)
Red Hat Enterprise Linux 9
ami-0d77c9d87c7e619f9

Virtual server type (instance type)
m4.large

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 60 GiB

j) A screen will be shown with the progress of the instance setup, this can take a few minutes.



Launching instance

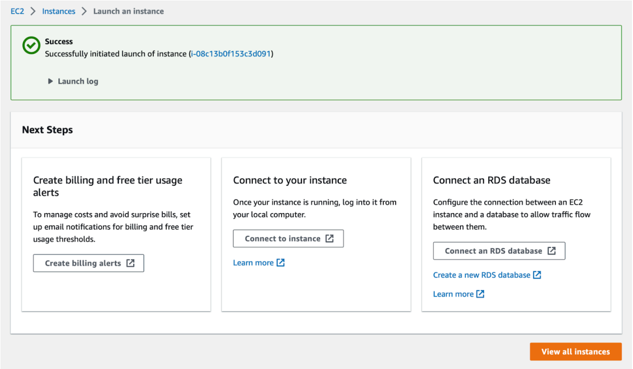
Please wait while we launch your instance.

Do not close your browser while this is loading.

Subscribing to Marketplace AMI 77%

▶ Details

k) You should be shown a confirmation screen once the instance is ready



EC2 > Instances > Launch an instance

Success
Successfully initiated launch of instance (i-08c13b0f153c3d091)

▶ Launch log

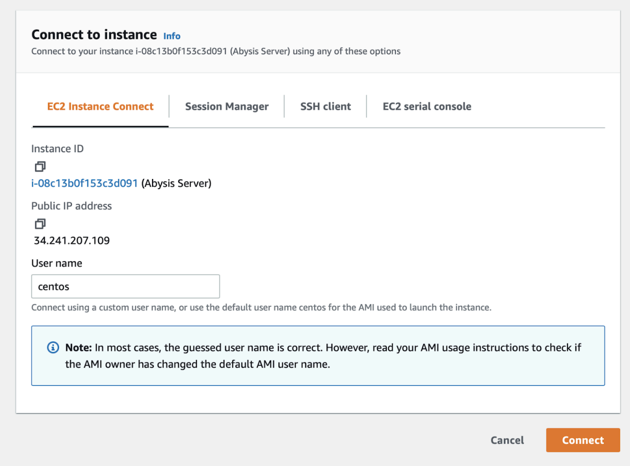
Next Steps

Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.

Connect to your instance
Once your instance is running, log into it from your local computer.

Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.

l) Clicking “Connect to instance” will take you to a screen with details on how to connect to your instance, including its public IP address.



Connect to instance Info

Connect to your instance i-08c13b0f153c3d091 (Abysis Server) using any of these options

Instance ID

i-08c13b0f153c3d091 (Abysis Server)

Public IP address

34.241.207.109

User name

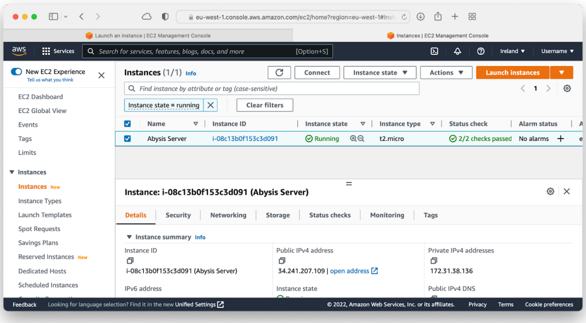
centos

Connect using a custom user name, or use the default user name centos for the AMI used to launch the instance.

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Please note that the login account for a RHEL machine is **ec2-user** and for a Rocky server it is **rocky**.

Alternatively going to your instance list should show your running instance:



Instances (1/1) Info

Instance state = running

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
Abysis Server	i-08c13b0f153c3d091	Running	t2.micro	2/2 checks passed	No alarms

Instance: i-08c13b0f153c3d091 (Abysis Server)

Instance summary Info

Instance ID: i-08c13b0f153c3d091 (Abysis Server)

Public IPv4 address: 34.241.207.109 | open address

Private IPv4 addresses: 172.31.38.136

IPv6 address

Instance state

Public IPv4 DNS

You are now able to connect to the server without being logged in to the AWS platform.

In the following example, our private key file is called abysis.pem and our Public DNS is ec2-123-456-789-101.eu-west-2.compute.amazonaws.com:

Logging in to EC2 Machine

Connect from a local Mac or Linux:

m) Open a terminal window.

n) Copy the *.pem file to a local directory and change the access rights as follows:

- chmod 400 abysis.pem

o) Connect to RHEL as follows:

ssh –i abysis.pem ec2-user@ec2-123-456-789-101.eu-west-2.compute.amazonaws.com

Connect to Rocky as follows:
ssh –i abysis.pem rocky@ec2-123-456-789-101.eu-west-2.compute.amazonaws.com

These users will have password-free sudo permissions.

p) You should now be connected.

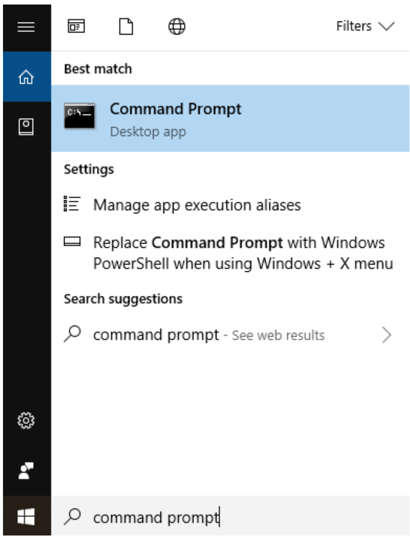
q) If you are installing abYsis yourself you can start from here.

Connect from a local Windows PC:

We do not recommend using a Windows machine for this work as the generation of an additional Key Pair (see later) is more complicated when using Windows. However, for the record this is how we believe a connection would be made.

a) Copy the *.pem file to a local directory

b) Open a windows command prompt window and change directory to the local directory


Filters
Best match
Command Prompt
Desktop app
Settings
Manage app execution aliases
Replace Command Prompt with Windows PowerShell when using Windows + X menu
Search suggestions
command prompt - See web results

command prompt

c) Connect to RHEL as follows:

```
ssh –i abysis.pem ec2-user@ec2-123-456-789-101.eu-west-2.compute.amazonaws.com
```

Connect to Rocky as follows:

```
ssh –i abysis.pem rocky@ec2-123-456-789-101.eu-west-2.compute.amazonaws.com
```

These users will have password-free sudo permissions.

d) You should now be connected.

e) If you are installing abYsis yourself you can start from here.

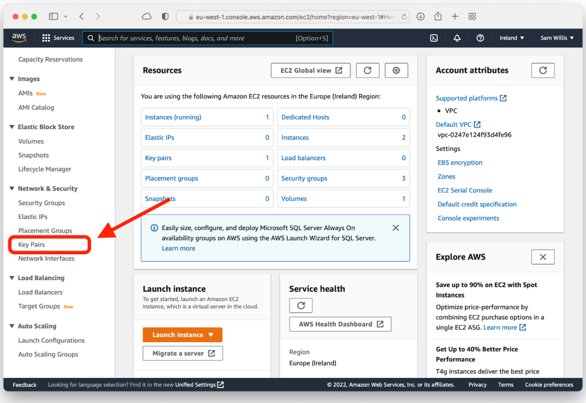
Generating separate Key Pair for an external user

If you are not installing abYsis yourself and are asking an external provider to perform the installation, you may want create an additional Key Pair which can be deleted at a later date to keep access under your control.

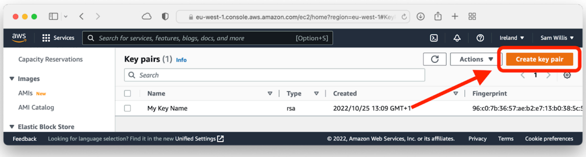
This can be achieved in the following manner.

On the AWS management console

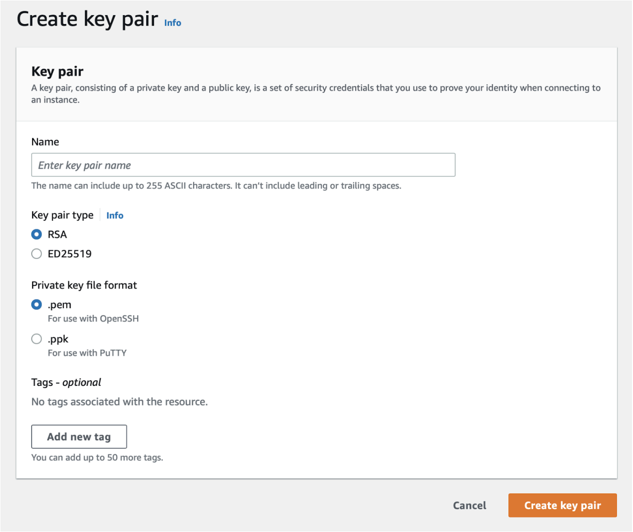
Go to ‘Key Pairs’ in the Network & Security section.



Click ‘Create Key Pair’.



Give the pair a name and click ‘Create key pair’.



Create key pair Info

Key pair

A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name

Enter key pair name

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type Info

● RSA

○ ED25519

Private key file format

● .pem
For use with OpenSSH

○ .ppk
For use with PuTTY

Tags - *optional*

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel | Create key pair

- The new Key Pair for this additional user we have called abysis_user. You can call the file whatever name you prefer.
- You will again be prompted to save the private key file (abysis_user.pem).

- You need to keep a local copy of this file and also send to the person who may require access.
- Now, you will need to add the associated Public Key to your user's authorization file.

On a local Mac or Linux machine:

In the local directory on your local machine, type

- ssh-keygen -y

You will be prompted for the file name, so type the file, e.g. abysis_user.pem

This will reveal the Public Key.

In a separate terminal window on your machine, connect to the **EC2 server** using the primary Private Key (i.e. the key generated in item (d) above that we called abysis).

- Change directory to /home/centos/.ssh
- Edit the file called 'authorized_keys' within the .ssh directory. (You will need to use the standard vi editor and switch to insert mode).
- You should see the Public Key for your current connection in the authorized_keys file.
- In the local window, highlight the text of new Public Key.
- Add the new Public key to this file.
- Save the file.

You have now added the extra Public Key to allow access using the new Key Pair.

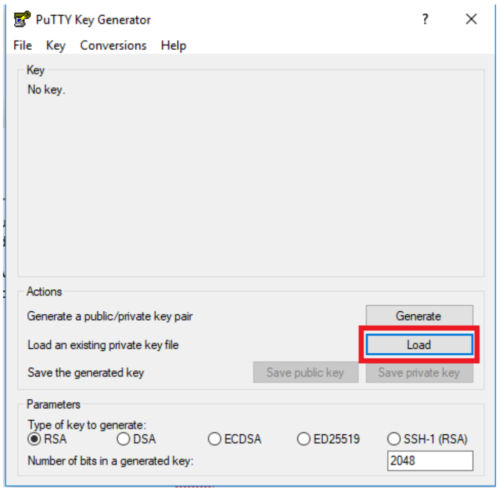
In the future, if you wish to revoke access by abysis_user, you can remove this line from the authorization file.

On a Windows machine:

We do not recommend using a Windows machine for this work. However, for the record this is how we believe it should be done.

You will need to install PuTTY on your Windows PC in order to generate the Public Key. PuTTY can be downloaded from https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html.

Once installed, open the PuTTYGen application and click 'Load'.

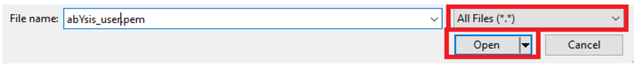


No key.

● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

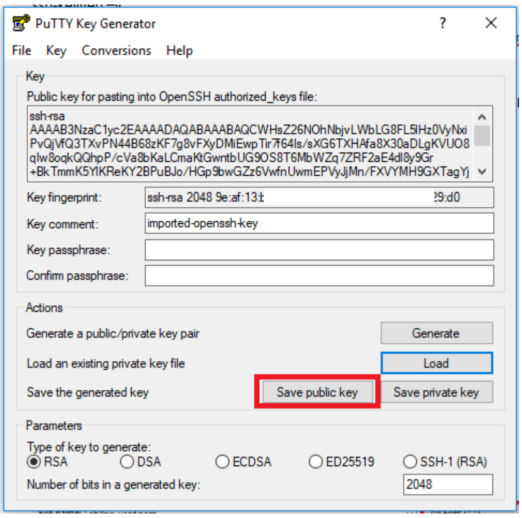
Select 'All files (*.*)' and navigate to the *.pem file. Click 'Open'.



File name: abYsis_user.pem

All Files (*.*)

You will see the Public Key listed in the dialog box.



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCWHsZ26NOhNbjvLWbLG8FL5lHz0VyNxi
PvQjVfQ3TXvPN44B68zKF7g8vFXyDMiEwpTir7f64ls/sXG6TXHAfa8X30aDLgKVUO8
qlw8oqkQQhpP/cVa8bKaLCmaKtGwntbUG9OS8T6MbWZq7ZRF2aE4dl8y9Gr
+BkTmmK5YlKReKY2BPuBJo/HGp9bwGZz6VwfnUwmEPVyJjMn/FXVYMH9GXTagYj
```

Key fingerprint: ssh-rsa 2048 9e:af:13:t [redacted] 29:d0

Key comment: imported-openssh-key

Key passphrase:

Confirm passphrase:

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Click ‘Save public key’ and give the file a name, say ‘PubKey.txt’. In a command prompt window, copy the file to the server using the following command and the Private Key generated in item 11 above:

scp –i abysis.pem PubKey.txt
ec2-user@ec2-123-456-789-101.eu-west-2.compute.amazonaws.com:/home/centos/.ssh/.

Connect to the server using your original Private Key (the key generated in item 11 above).

ssh –i abysis.pem
ec2-user@ec2-123-456-789-101.eu-west-2.compute.amazonaws.com

Change directory to /home/ec2-user/.ssh.

You should see the text file alongside the file called ‘authorized_keys’.

Edit the file called ‘authorized_keys’ using the vi editor and switch to insert mode.

You should see the Private Key for your current connection.

Add the new text on a new line at the end of this file.

Save the file.

You have now added the extra Public Key to allow access using the new Key Pair.

In the future, if you wish to revoke access by abysis_user, you can remove this line from the authorization file.

What to send to the person installing abYsis

You need to send the appropriate private key to the person installing abYsis.

In our example this is abysis_user.pem

Remember to keep a local copy of this file.

Security, Domain name, HTTPS

When installing abYsis it is important to consider how users will access the system and how to ensure it is not accessed by non-authorised persons. Below are suggestions on how you might secure access to abYsis. However, you should use your own IT facilities and personnel to ensure that securing abYsis access meets your own criteria.

For the purposes of these instructions it is assumed that you have already installed abYsis on an AWS server and it is running. It will be using HTTP by default which is unencrypted and should be secured to ensure that others cannot access.

Username and Password Protection

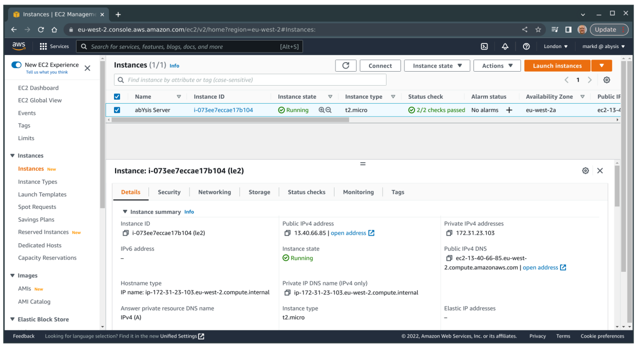
It is possible to configure your abYsis apache server to require users to provide a username and password before using it. Setting this up would be part of your abYsis installation process and can be found in the **Securing abYsis v4** document.

For this level of security you would not be required to change any AWS configurations.

Persistent IP address assignment

On an AWS server it is very likely that when the server reboots, a different IP address will be assigned unless action is taken to assign the server a static IP address to your instance.

Go to your Instance page on AWS. Take a note of the Instance ID, Private IP address and Availability Zone (under the Network tab)



eu-west-2.console.aws.amazon.com/ec2/v2/home?region=eu-west-2#Instances:

Instances (1/1)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IF
abYsis Server	i-073ee7eccae17b104	Running	t2.micro	2/2 checks passed	No alarms	eu-west-2a	ec2-13-4

Instance: i-073ee7eccae17b104 (le2)

Instance summary

Instance ID: i-073ee7eccae17b104 (le2)

Public IPv4 address: 13.40.66.85 | open address

Private IPv4 addresses: 172.31.23.103

IPv6 address: –

Instance state: Running

Public IPv4 DNS: ec2-13-40-66-85.eu-west-2.compute.amazonaws.com | open address

Hostname type: IP name: ip-172-31-23-103.eu-west-2.compute.internal

Private IP DNS name (IPv4 only): ip-172-31-23-103.eu-west-2.compute.internal

Answer private resource DNS name: IPv4 (A)

Instance type: t2.micro

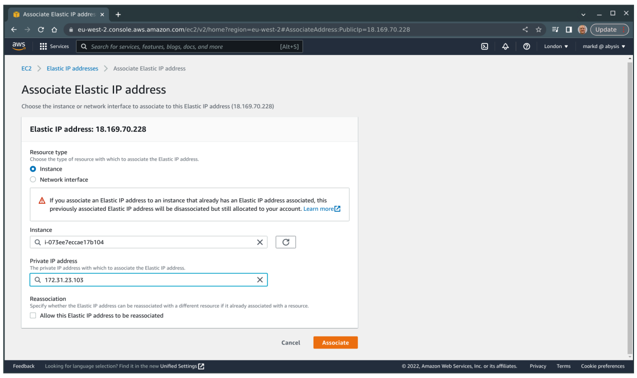
Elastic IP addresses: –

Scroll down the left hand menu and select Elastic IPs and then click the Allocate Elastic IP address button.

Make sure the Network Border Group is similar to your Availability Zone (you took note of above) and click the Allocate button.

A new IP will now be selected for you. To attach this to your instance click **Associate Elastic IP address** in the **Action** menu.

Select the Instance ID and the Private IP address (you took note of above) that this public IP address will point to and click Associate.



eu-west-2.console.aws.amazon.com/ec2/v2/home?region=eu-west-2#AssociateAddress:PublicIp=18.169.70.228

EC2 > Elastic IP addresses > Associate Elastic IP address

Associate Elastic IP address

Choose the instance or network interface to associate to this Elastic IP address (18.169.70.228)

Elastic IP address: 18.169.70.228

Resource type
Choose the type of resource with which to associate the Elastic IP address.
● Instance
○ Network interface

If you associate an Elastic IP address to an instance that already has an Elastic IP address associated, this previously associated Elastic IP address will be disassociated but still allocated to your account. Learn more

Instance: i-073ee7eccae17b104

Private IP address
The private IP address with which to associate the Elastic IP address.
172.31.23.103

Reassociation
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.
□ Allow this Elastic IP address to be reassociated

Associate Elastic IP addres
Update
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
London
markd @ abysis
Cancel
Associate
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Your instance now has a new public IP address that you can use to access your server.

- This will be important if you wish to provide an encrypted HTTPS connection

Domain name assignment

You will want to point your **Domain Name** to your static IP address. This will make it easier for users to access and is essentially necessary if you are planning to use HTTPS. Domain name assignment is implemented using the DNS Records editor supplied by the organisation that you bought the domain name from.

Once added to your DNS Records, you will also need to change your apache conf file on your abYsis server to include this domain name.

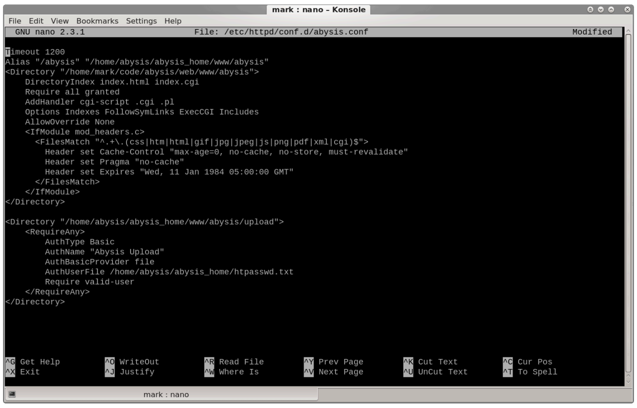
To do this, Log on to your abYsis server as a user with sudo permissions

If you used the default settings the name of your apache configuration file will be abysis.conf. The abysis part of the filename is the same as the abysis part of the URL you use to access the server.

http://81.123.45.45/**abysis**/index.cgi

To edit this file use a text editor such as **nano**

sudo nano /etc/httpd/conf.d/abysis.conf



```
  GNU nano 2.3.1              File: /etc/httpd/conf.d/abysis.conf                     Modified

Timeout 1200
Alias "/abysis" "/home/abysis/abysis_home/www/abysis"
<Directory "/home/mark/code/abysis/web/www/abysis">
    DirectoryIndex index.html index.cgi
    Require all granted
    AddHandler cgi-script .cgi .pl
    Options Indexes FollowSymLinks ExecCGI Includes
    AllowOverride None
    <IfModule mod_headers.c>
      <FilesMatch "^.+\.(css|htm|html|gif|jpg|jpeg|js|png|pdf|xml|cgi)$">
        Header set Cache-Control "max-age=0, no-cache, no-store, must-revalidate"
        Header set Pragma "no-cache"
        Header set Expires "Wed, 11 Jan 1984 05:00:00 GMT"
      </FilesMatch>
    </IfModule>
</Directory>

<Directory "/home/abysis/abysis_home/www/abysis/upload">
    <RequireAny>
        AuthType Basic
        AuthName "Abysis Upload"
        AuthBasicProvider file
        AuthUserFile /home/abysis/abysis_home/htpasswd.txt
        Require valid-user
    </RequireAny>
</Directory>



^G Get Help    ^O WriteOut    ^R Read File   ^Y Prev Page   ^K Cut Text    ^C Cur Pos
^X Exit        ^J Justify     ^W Where Is    ^V Next Page   ^U UnCut Text  ^T To Spell
```

You need to add the following lines to the top of the file, using your registered domain name

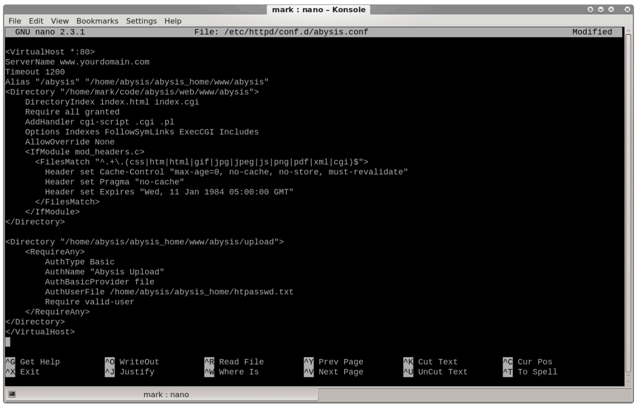
<VirtualHost *:80>

ServerName www.yourdomain.com

And add the following line to the very end of the file

</VirtualHost>

Your file should now look like the next image. Use Control-X and answer **Y**es to save the file.



```
  GNU nano 2.3.1              File: /etc/httpd/conf.d/abysis.conf                     Modified

<VirtualHost *:80>
ServerName www.yourdomain.com
Timeout 1200
Alias "/abysis" "/home/abysis/abysis_home/www/abysis"
<Directory "/home/mark/code/abysis/web/www/abysis">
    DirectoryIndex index.html index.cgi
    Require all granted
    AddHandler cgi-script .cgi .pl
    Options Indexes FollowSymLinks ExecCGI Includes
    AllowOverride None
    <IfModule mod_headers.c>
      <FilesMatch "^.+\.(css|htm|html|gif|jpg|jpeg|js|png|pdf|xml|cgi)$">
        Header set Cache-Control "max-age=0, no-cache, no-store, must-revalidate"
        Header set Pragma "no-cache"
        Header set Expires "Wed, 11 Jan 1984 05:00:00 GMT"
      </FilesMatch>
    </IfModule>
</Directory>

<Directory "/home/abysis/abysis_home/www/abysis/upload">
    <RequireAny>
        AuthType Basic
        AuthName "Abysis Upload"
        AuthBasicProvider file
        AuthUserFile /home/abysis/abysis_home/htpasswd.txt
        Require valid-user
    </RequireAny>
</Directory>
</VirtualHost>


^G Get Help    ^O WriteOut    ^R Read File   ^Y Prev Page   ^K Cut Text    ^C Cur Pos
^X Exit        ^J Justify     ^W Where Is    ^V Next Page   ^U UnCut Text  ^T To Spell
```

Finally, restart **apache** so that abYsis is running with the new credentials.

```
sudo systemctl restart httpd
```

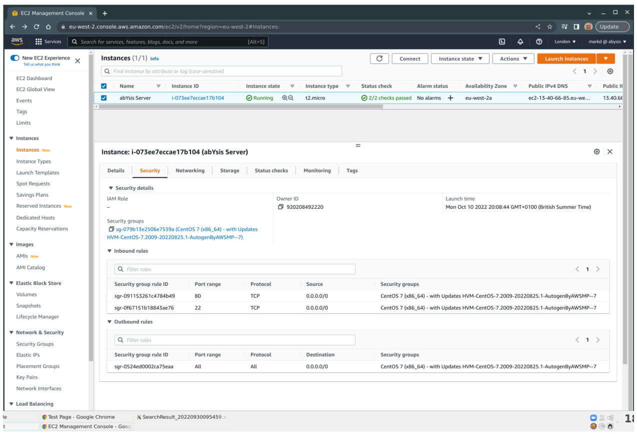
Your abYsis server is now ready to be recognised by your domain name.

Note

- If you have added site-wide username and password protection, make sure those changes are also inside the **</VirtualHost>** tag
- This will be important if you wish to provide an encrypted HTTPS connection

Control Access through Firewall

It is possible to configure a firewall so that only specific internet traffic can access your abYsis server. If you are using AWS to host your server you may have already configured your server to be accessed by **ssh (port 22)** and **HTTP (port 80)**. To add more firewall rules you need to login to your AWS account and go to your Instance page and click the **Security** tab.



Instances (1/1)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
abYsis Server	i-073ee7eccae17b104	Running	t2.micro	2/2 checks passed	No alarms	eu-west-2a	ec2-13-40-66-85.eu-we...

Instance: i-073ee7eccae17b104 (abYsis Server)

Security details

IAM Role: –

Owner ID: 920208492220

Launch time: Mon Oct 10 2022 20:08:44 GMT+0100 (British Summer Time)

Security groups: sg-079b13e2506e7539a (CentOS 7 (x86_64) - with Updates HVM-CentOS-7.2009-20220825.1-AutogenByAWSMP--7)

Inbound rules

Security group rule ID	Port range	Protocol	Source	Security groups
sgr-091153261c4784b49	80	TCP	0.0.0.0/0	CentOS 7 (x86_64) - with Updates HVM-CentOS-7.2009-20220825.1-AutogenByAWSMP--7
sgr-0f67151b18843ae76	22	TCP	0.0.0.0/0	CentOS 7 (x86_64) - with Updates HVM-CentOS-7.2009-20220825.1-AutogenByAWSMP--7

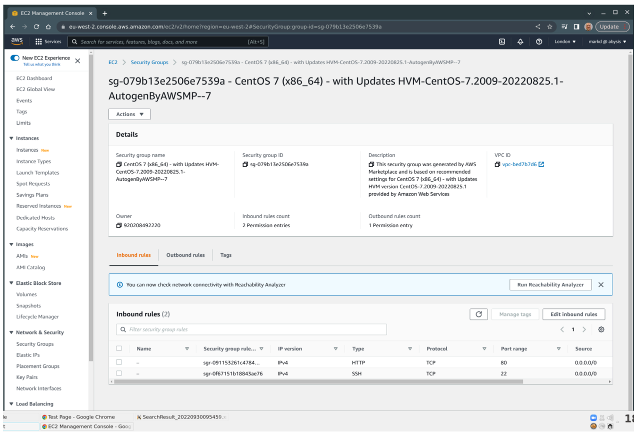
Outbound rules

Security group rule ID	Port range	Protocol	Destination	Security groups
sgr-0524ed0002ca75eaa	All	All	0.0.0.0/0	CentOS 7 (x86_64) - with Updates HVM-CentOS-7.2009-20220825.1-AutogenByAWSMP--7

You will see the list of **Inbound rules**. The example above has ports 22 and 80 open to everyone (represented by 0.0.0.0/0).

Below shows how it is possible to open a port so that **HTTPS (port 443)** traffic can access your server and how to limit access to only a select list of IP addresses.

On the **Security** tab click on the Security groups link. This will take you to a page where you can click on **Edit Inbound Rules.**


EC2 Management Console
eu-west-2.console.aws.amazon.com/ec2/v2/home?region=eu-west-2#SecurityGroup:group-id=sg-079b13e2506e7539a
London
markd @ abysis
EC2 > Security Groups > sg-079b13e2506e7539a - CentOS 7 (x86_64) - with Updates HVM-CentOS-7.2009-20220825.1-AutogenByAWSMP--7
Actions
Inbound rules
Outbound rules
Tags
Run Reachability Analyzer
Manage tags
Edit inbound rules

sg-079b13e2506e7539a - CentOS 7 (x86_64) - with Updates HVM-CentOS-7.2009-20220825.1-AutogenByAWSMP--7

Details

Security group name: CentOS 7 (x86_64) - with Updates HVM-CentOS-7.2009-20220825.1-AutogenByAWSMP--7

Security group ID: sg-079b13e2506e7539a

Description: This security group was generated by AWS Marketplace and is based on recommended settings for CentOS 7 (x86_64) - with Updates HVM version CentOS-7.2009-20220825.1 provided by Amazon Web Services

VPC ID: vpc-bed7b7d6

Owner: 920208492220

Inbound rules count: 2 Permission entries

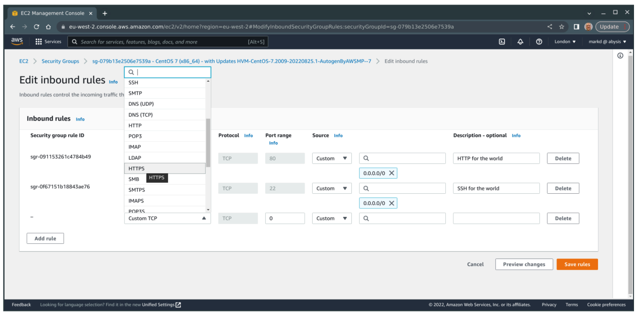
Outbound rules count: 1 Permission entry

You can now check network connectivity with Reachability Analyzer

Inbound rules (2)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
–	sgr-091153261c4784...	IPv4	HTTP	TCP	80	0.0.0.0/0
–	sgr-0f67151b18843ae76	IPv4	SSH	TCP	22	0.0.0.0/0

When you click the **Add rule** button a new line will appear.



EC2 Management Console
eu-west-2.console.aws.amazon.com/ec2/v2/home?region=eu-west-2#ModifyInboundSecurityGroupRules:securityGroupId=sg-079b13e2506e7539a
Update
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
London
markd @ abysis
SSH
SMTP
DNS (UDP)
DNS (TCP)
HTTP
POP3
IMAP
LDAP
HTTPS
SMB
HTTPS
SMTPS
IMAPS
POP3S
Add rule
Cancel
Preview changes
Save rules
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

EC2 > Security Groups > sg-079b13e2506e7539a - CentOS 7 (x86_64) - with Updates HVM-CentOS-7.2009-20220825.1-AutogenByAWSMP--7 > Edit inbound rules

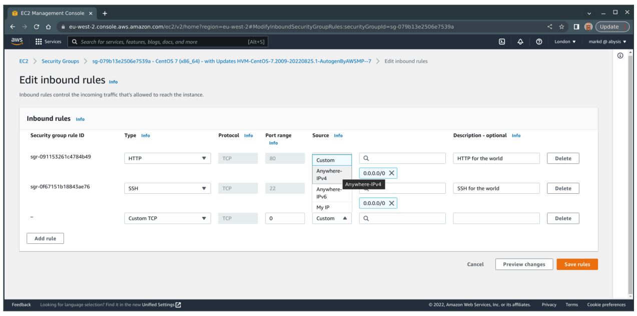
Edit inbound rules Info

Inbound rules control the incoming traffic th

Inbound rules Info

Security group rule ID	Type	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-091153261c4784b49		TCP	80	Custom	0.0.0.0/0	HTTP for the world	Delete
sgr-0f67151b18843ae76		TCP	22	Custom	0.0.0.0/0	SSH for the world	Delete
–	Custom TCP	TCP	0	Custom			Delete

The first drop down menu will allow you to choose from lots of preset configurations for different types of internet traffic. Choose HTTPS to allow HTTPS access to your server. Then you need to choose who can access the server using HTTPS.



EC2 Management Console
eu-west-2.console.aws.amazon.com/ec2/v2/home?region=eu-west-2#ModifyInboundSecurityGroupRules:securityGroupId=sg-079b13e2506e7539a
Update
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
London
markd @ abysis
Custom
Anywhere-IPv4
Anywhere-IPv4
Anywhere-IPv6
My IP
Add rule
Cancel
Preview changes
Save rules
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

EC2 > Security Groups > sg-079b13e2506e7539a - CentOS 7 (x86_64) - with Updates HVM-CentOS-7.2009-20220825.1-AutogenByAWSMP--7 > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-091153261c4784b49	HTTP	TCP	80	Custom	0.0.0.0/0	HTTP for the world	Delete
sgr-0f67151b18843ae76	SSH	TCP	22		0.0.0.0/0	SSH for the world	Delete
–	Custom TCP	TCP	0	Custom			Delete

The main options are:-

- Anywhere IPv4 - anyone on the internet
- My IP - only the computer you are currently using
- Custom - you can put a specific IP address (e.g. a colleagues) in the next box

You can add as many rules as you like. For example, if you want access to be limited to just 3 IP addresses then you will need 1 rule for each IP address and each access type.

At the end click Save rules. Those rules will now be enforced on your server.

Note

- You should always have a rule for ssh access. If you limit it to a specific IP and you can no longer use that IP address then you will lose access to your server. Therefore, it is best to leave ssh access open to everyone (it is password protected).
- If you have an SSL certificate installed on your server you need HTTPS rules. If not then it is not necessary to set them.
- If you use Let's Encrypt to install certificates on your server, always leave HTTP open to everyone.

Encrypt data using HTTPS

In order to provide HTTPS access to an abYsis server you need an SSL certificate from a Trusted Certificate Authority and configure apache on your abYsis server.

The instructions for configuring the server can be found in the **abYsis v4 Installation and Data Loading** document. You will need to configure the following on your AWS server to be able to set up an SSL certificate.

- You would need a persistent IP address. Instructions for this can be found above.
- You would need a domain name attached to the IP address above.

- You would need to make sure your HTTPS port 443 is open on your abYsis server for people to access your encrypted pages. This would be set during section (e) of the **Launching an Instance** section above.
- An SSL certificate provider such as Let's Encrypt generates a certificate that usually lasts for 90 days. It uses a certbot program to automatically renew a certificate. To enable this it is advisable to ensure that HTTP port 80 is accessible by everyone. Your abYsis site

At some point after an initial installation you might decide to bring back an abYsis installation via an AWS snapshot.

Whilst abYsis is not supplied as a Snapshot, this documentation is written to help people who might wish to generate their own and deploy at a later date.

A snapshot is of a fully configured OS (e.g. RHEL or Rocky 9) instance with an abYsis installation. By following the steps below you can turn a snapshot into an instance that is ready to go.

Create your instance

The first step is to create a machine to run abYsis on. This is the exact same process as outlined in the **Launching an Instance** process at the beginning of this document.

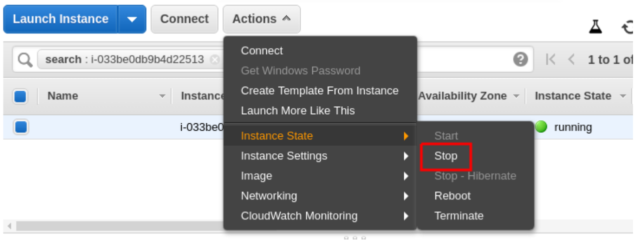
- You will then go to a page confirming that your instance has been launched. Scroll to the bottom of the page and click the **View Instance** button on the right.

should be secure because of the redirect to HTTPS, but should be checked.

- certbot ensures that normal HTTP traffic is automatically redirected to HTTPS.
- It may take a couple of hours for your certificate to be recognised and accepted by browsers

Snapshot for AWS

- This will take you to the **instance** page which lists all instances you have. Select the instance you just created (it may be pending or initializing). Using the **Action** button hover over **Instance State** and click on **Stop**.

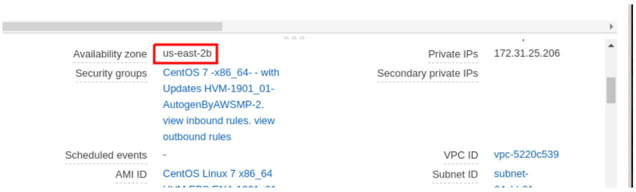


j) You will be asked to confirm stopping the instance.

Noting details and detaching the volume

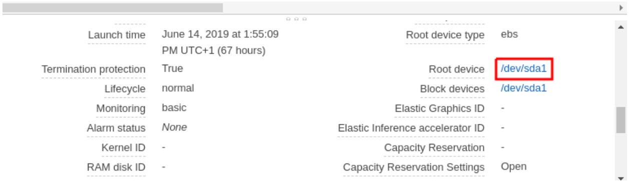
Attached to your new server (instance) is an 80GB volume, the server's harddrive. This is going to be replaced with the abYsis volume. While you do this you will need to take note of 2 things:- the **availability zone** and the **device name**.

On the instance page make sure your instance (and no other if there are more than one) is selected. Then, in the bottom panel scroll down until you find **Availability zone**. Take a note of this as you will need this later.



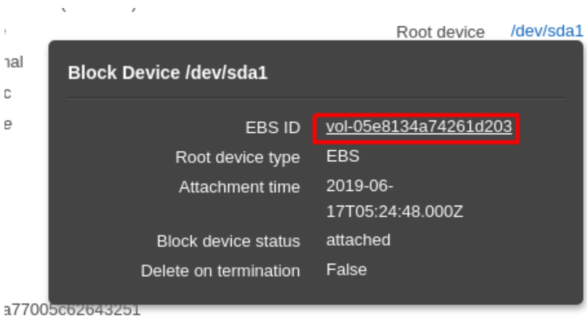
Availability zone	us-east-2b	Private IPs	172.31.25.206
Security groups	CentOS 7 -x86_64- - with Updates HVM-1901_01-AutogenByAWSMP-2. view inbound rules. view outbound rules	Secondary private IPs	
Scheduled events	-	VPC ID	vpc-5220c539
AMI ID	CentOS Linux 7 x86_64	Subnet ID	subnet-

Continue to scroll down until you find **Root device**. Again, take a note of this. It will probably be **/dev/sda1**.



Launch time	June 14, 2019 at 1:55:09 PM UTC+1 (67 hours)	Root device type	ebs
Termination protection	True	Root device	/dev/sda1
Lifecycle	normal	Block devices	/dev/sda1
Monitoring	basic	Elastic Graphics ID	-
Alarm status	*None*	Elastic Inference accelerator ID	-
Kernel ID	-	Capacity Reservation	-
RAM disk ID	-	Capacity Reservation Settings	Open

The device name is also a link. Click the link (such as /dev/sda1) and a **Block Device** pop-up will appear. Click the underlined EBS ID link and you will be taken to the **Volume** page.

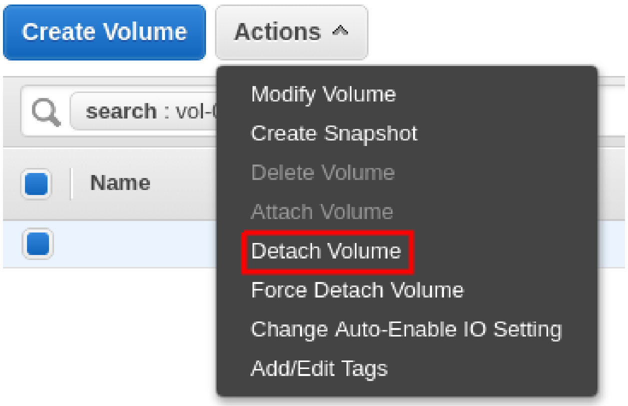


Root device /dev/sda1

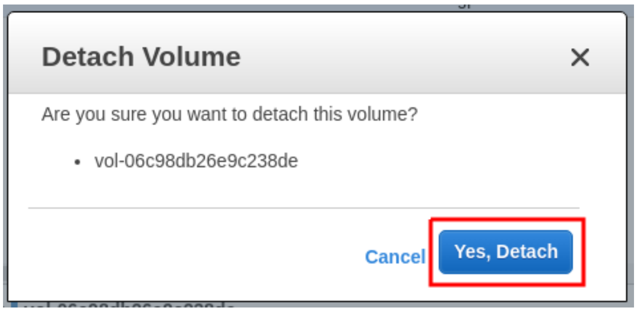
Block Device /dev/sda1

EBS ID	vol-05e8134a74261d203
Root device type	EBS
Attachment time	2019-06-17T05:24:48.000Z
Block device status	attached
Delete on termination	False

On the **Volume** page your 80GB volume should be selected. Using the **Action** button next to the Create Volume button, select **Detach Volume**.



You will be asked to confirm that you wish to detach the volume. Click **Yes, detach**. The instance is now detached and ready for you abYsis volume to be attached.



Detach Volume

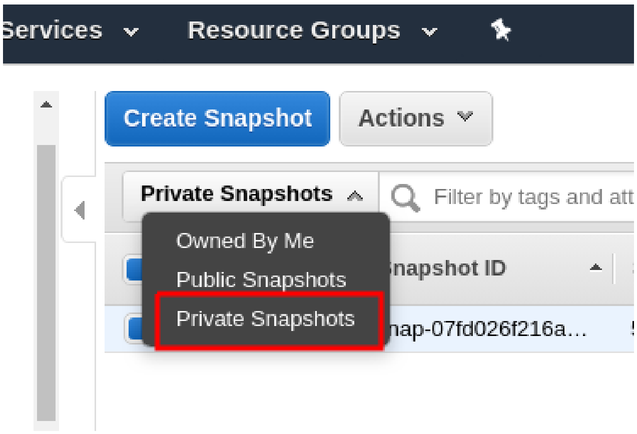
Are you sure you want to detach this volume?

- vol-06c98db26e9c238de

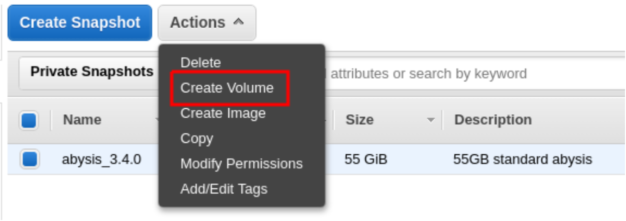
Turn Snapshot into a volume

When a snapshot is available to you it will be possible to create a new harddrive (volume) from it.

In the left hand side panel, scroll down and click Snapshot. In the main panel, just under the Create Snapshot button click the dropdown menu (which probably says **Owned By Me**). Change this to **Private Snapshots** and the relevant abYsis snapshot should appear.

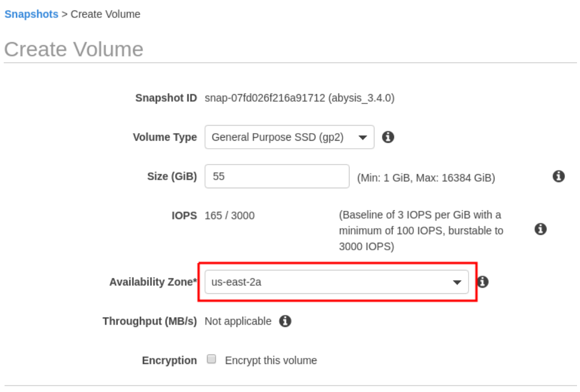


Click to select the abYsis snapshot and then using the **Actions** button above select **Create Volume**.



Name	Size	Description
abysis_3.4.0	55 GiB	55GB standard abysis

This will take you to a new **Create Volume** page. Take a note of the Half way down the page is the option **Availability zone**. Change that to the one that matches the one you noted earlier for your new instance. Then, scroll to the bottom and click the **Create Volume** button.


Snapshots > Create Volume

Create Volume

Snapshot ID snap-07fd026f216a91712 (abysis_3.4.0)

Volume Type General Purpose SSD (gp2)

Size (GiB) 55 (Min: 1 GiB, Max: 16384 GiB)

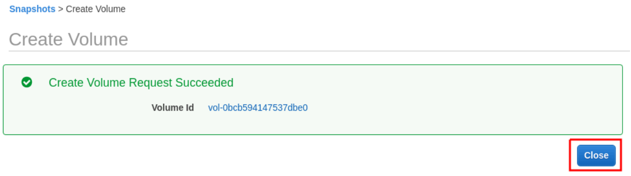
IOPS 165 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)

Availability Zone* us-east-2a

Throughput (MB/s) Not applicable

Encryption □ Encrypt this volume

You will be told that the volume was created successfully. Click the **Close** button and you will be returned to the snapshot page.


Snapshots > Create Volume

Create Volume

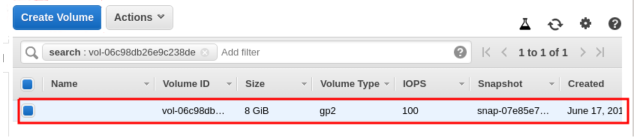
Create Volume Request Succeeded

Volume Id vol-0bcb594147537dbe0

Attach abYsis volume to your instance

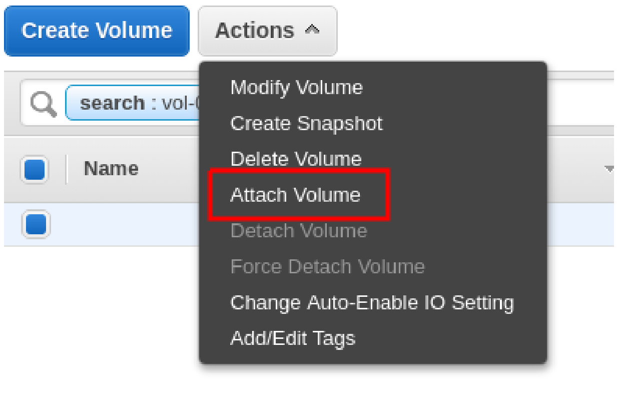
Your abYsis snapshot is now being built into a volume. You have essentially taken a copy of an installed disk and put it on a new disk. Now you have to attach it to your instance.

Use the left-hand panel to go to the **Volume** page. Find the volume you have created (you can use the **Created** date column for this) and select that volume.

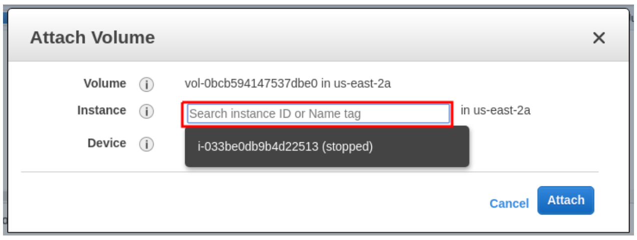


Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created
	vol-06c98db…	8 GiB	gp2	100	snap-07e85e7…	June 17, 201

Use the **Actions** menu and select **Attach Volume**



This will take you to a pop-up window, **Attach Volume**. The first thing to do is to click in the **Instance** box. It will display the instance that are in the same availability zone as the volume. Select the one you have just created.



Attach Volume

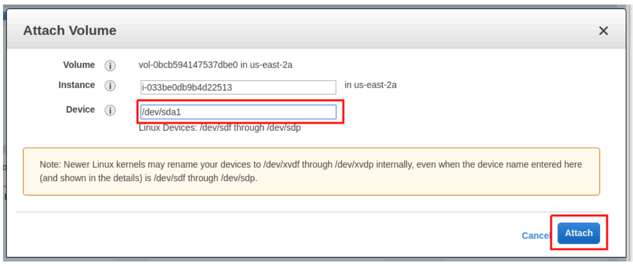
Volume vol-0bcb594147537dbe0 in us-east-2a

Instance Search instance ID or Name tag in us-east-2a

i-033be0db9b4d22513 (stopped)

Device

Then edit the **Device** from **/dev/sdf** to the device name you nated earlier, probably **/dev/sda1**. Then click the **Attach** button in the bottom right of the page to finish. You will then be returned to the **Volume** page.



Attach Volume

Volume vol-0bcb594147537dbe0 in us-east-2a

Instance i-033be0db9b4d22513 in us-east-2a

Device /dev/sda1

Linux Devices: /dev/sdf through /dev/sdp

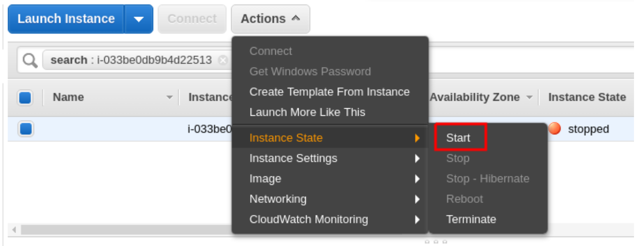
Note: Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdp internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp.

Start new abYsis instance

The abYsis instance has now been built. Now it needs to be started.

Use the left-hand panel to go to the **Instance** page.

Select the instance you created earlier and, using the **Actions** button, hover over **Instance State** and click **Start**. When asked to confirm click **Yes, Start**.

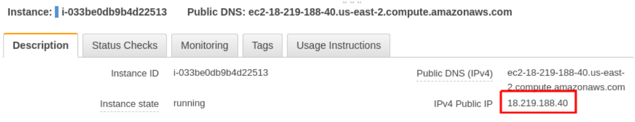


search : i-033be0db9b4d22513

Name	Instance	Availability Zone	Instance State
	i-033be0		stopped

Your instance will first go into a **pending** state and then **running** (use the ↻ icon to refresh the page).

When your instance is running, in the bottom panel you will see the **IPv4 Public IP**. Copy this address, paste it into your browser and add **/abysis** to the end of the URL. This will take you to your new abYsis server.



Instance: i-033be0db9b4d22513 Public DNS: ec2-18-219-188-40.us-east-2.compute.amazonaws.com

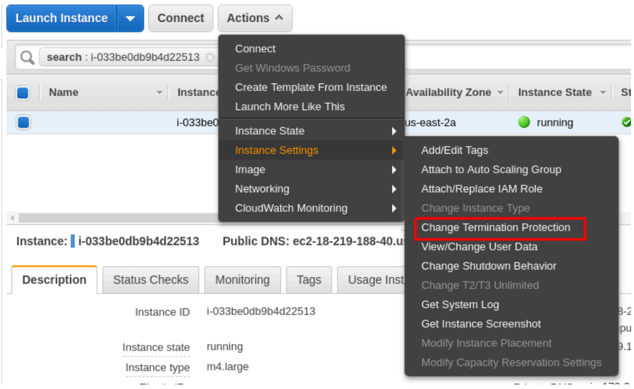
Instance ID i-033be0db9b4d22513

Instance state running

Public DNS (IPv4) ec2-18-219-188-40.us-east-2.compute.amazonaws.com

IPv4 Public IP 18.219.188.40

There is an option when controlling instances to **Terminate** the instance. In AWS terms this means stopping the instance and then deleting it **and** the EBS volume storage. To protect against that click the **Actions** button, hover over **Instance Settings** and click **Change Termination Protection**.



search : i-033be0db9b4d22513

Name	Instanc	Availability Zone	Instance State	St
	i-033be0	us-east-2a	● running	✓

Instance: i-033be0db9b4d22513 Public DNS: ec2-18-219-188-40.u

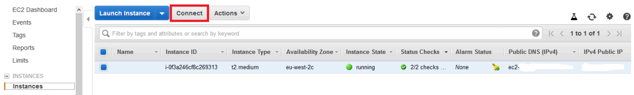
Instance ID i-033be0db9b4d22513

Instance state running

Instance type m4.large

If the current setting is **disabled** then click the Yes, Enable button. Now the instance and volume cannot be terminated unless this setting is manually altered.

Should you need to access the instance's command line using ssh, click **Connect** and follow the instructions on the pop-up page. Please note, for a **RHEL** server the sudo username is **ec2-user** and for a **Rocky** server the username is **rocky**.



Filter by tags and attributes or search by keyword

1 to 1 of 1

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
	i-0f3a246cf8c269313	t2.medium	eu-west-2c	● running	✓ 2/2 checks ...	None	ec2-[redacted]	[redacted]