

How to install VigorACS 2 in AWS Cloud

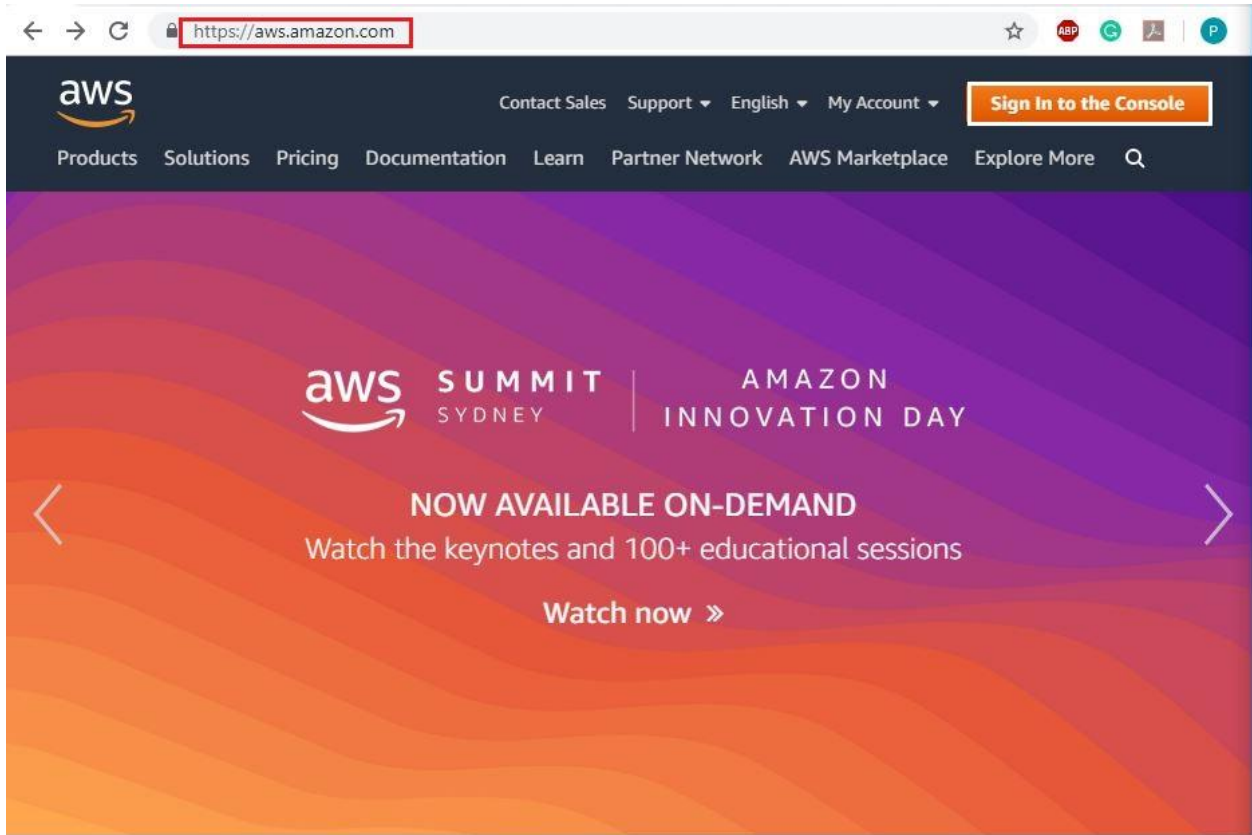
VigorACS 2 is a TR-069 based centralised management system for DrayTek's Vigor devices. It is a management tool that would help Network Engineers and Systems Integrators to configure, monitor and manage DrayTek devices remotely from the comfort of their offices or homes.

Amazon Web Services allows you to set up a cloud-based management system running VigorACS 2.

This guide shows you on how to install VigorACS 2 in Linux Ubuntu 18.04 using AWS cloud as our infrastructure server.



- I. Accessing AWS Cloud.
 - a. Go to <https://aws.amazon.com> and select **Sign in to the Console**.



b. Login using your AWS account.



Account ID or alias

IAM user name

Password

[Sign-in using root account credentials](#)

[Forgot password?](#)

Amazon Lightsail

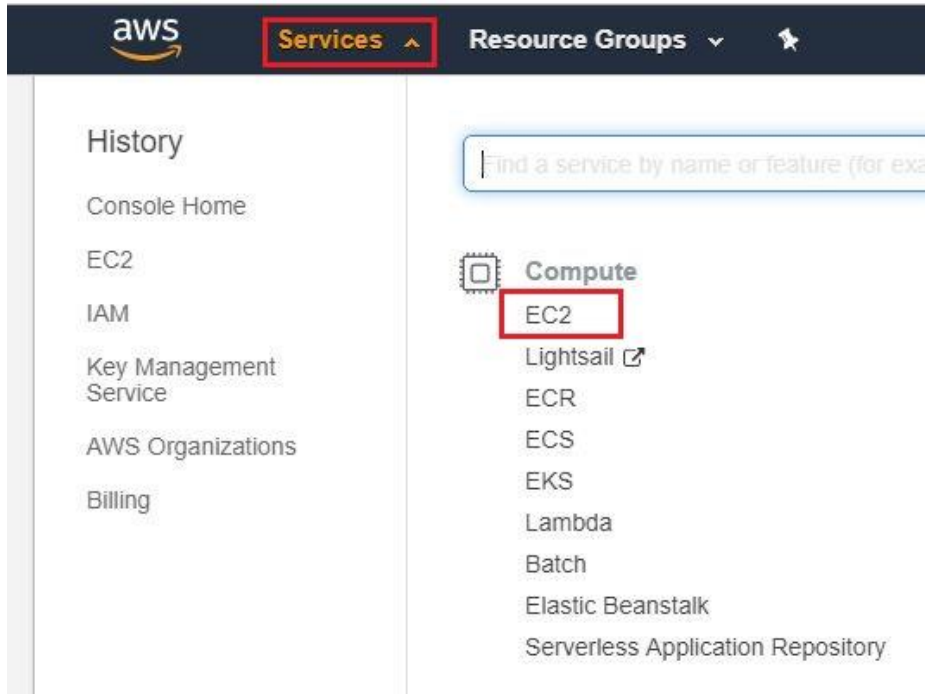
Lightsail is the easiest way to get started on AWS

[Learn more »](#)

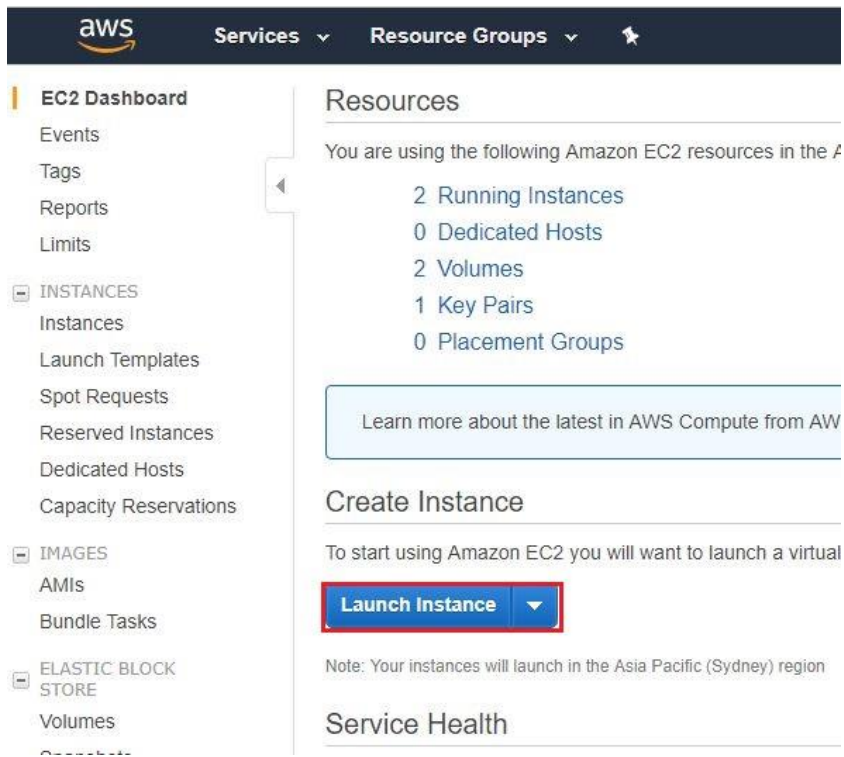
A white line-art cartoon robot character with a square head, two antennae, and a thumbs-up gesture, standing on a white horizontal line. The background of the banner is a dark space with a bright, glowing orange and yellow light source on the right, creating a lens flare effect.

English ▼

- II. Creating a Virtual Machine Instance.
 - a. Select **Service** and **EC2**.



- b. Click **Launch Instance**.



c. Click **Select** under **Ubuntu Server 18.04 LTS**.

The screenshot shows the AWS console interface for selecting an Amazon Machine Image (AMI). The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information. Below the navigation bar, a progress indicator shows seven steps: '1. Choose AMI', '2. Choose Instance Type', '3. Configure Instance', '4. Add Storage', '5. Add Tags', '6. Configure Security Group', and '7. Review'. The main heading is 'Step 1: Choose an Amazon Machine Image (AMI)' with a 'Cancel and Exit' link in the top right.

On the left side, there is a filter for 'Free tier only'. The main content area displays a list of AMIs, each with a logo, name, ID, description, and a 'Select' button. The 'Ubuntu Server 18.04 LTS (HVM), SSD Volume Type' AMI is highlighted with a red dashed border, and its 'Select' button is highlighted with a red box.

OS	AMI Name	AMI ID	Architecture
Amazon Linux	Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type	ami-075caa3491def750b	64-bit (x86)
Red Hat	Red Hat Enterprise Linux 8 (HVM), SSD Volume Type	ami-0975ce566eec139c3	64-bit (x86)
SUSE Linux	SUSE Linux Enterprise Server 15 SP1 (HVM), SSD Volume Type	ami-0d0e2895dc0dcdbee	64-bit (x86)
Ubuntu	Ubuntu Server 18.04 LTS (HVM), SSD Volume Type	ami-06705195ce845509c	64-bit (x86)

d. Select the **Free tier eligible** VM instance and click **Next: Configure Instance Details**

The screenshot shows the AWS console interface for configuring an EC2 instance. The page title is "Step 2: Choose an Instance Type". Below the title, there is a paragraph explaining Amazon EC2 instance types. The "Filter by:" section shows "All instance types", "Current generation", and "Show/Hide Columns". The "Currently selected:" text indicates "t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)". A table lists various instance types with columns for Family, Type, vCPUs, Memory (GiB), Instance Storage (GB), EBS-Optimized Available, and Network Performance. The "t2.micro" row is selected and highlighted with a red box, and a green label "Free tier eligible" is visible next to the type name. At the bottom, there are buttons for "Cancel", "Previous", "Review and Launch", and "Next: Configure Instance Details", with the last button highlighted with a red box.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more about instance types and how they can meet your computing needs.](#)

Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate
<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate
<input type="checkbox"/>	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate
<input type="checkbox"/>	General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit
<input type="checkbox"/>	General purpose	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit
<input type="checkbox"/>	General purpose	t3a.small	2	2	EBS only	Yes	Up to 5 Gigabit
<input type="checkbox"/>	General purpose	t3a.medium	2	4	EBS only	Yes	Up to 5 Gigabit

Cancel Previous Review and Launch Next: Configure Instance Details

e. Leave it as default and click **Next: Add Storage**.

The screenshot shows the AWS Management Console interface for configuring an EC2 instance. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information. The breadcrumb trail indicates the current step is '3. Configure Instance Details'. The main heading is 'Step 3: Configure Instance Details', followed by a brief instruction: 'Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.'

The configuration options are as follows:

- Number of instances:** 1. Includes a 'Launch into Auto Scaling Group' link.
- Purchasing option:** Request Spot instances.
- Network:** vpc-fcba7b99 (default). Includes a 'Create new VPC' link.
- Subnet:** No preference (default subnet in any Availability Zone). Includes a 'Create new subnet' link.
- Auto-assign Public IP:** Use subnet setting (Enable).
- Placement group:** Add instance to placement group.
- Capacity Reservation:** Open. Includes a 'Create new Capacity Reservation' link.
- IAM role:** None. Includes a 'Create new IAM role' link.
- Shutdown behavior:** Stop.
- Enable termination protection:** Protect against accidental termination.
- Monitoring:** Enable CloudWatch detailed monitoring. Note: Additional charges apply.
- Tenancy:** Shared - Run a shared hardware instance. Note: Additional charges will apply for dedicated tenancy.
- T2/T3 Unlimited:** Enable. Note: Additional charges may apply.

At the bottom, there is a section for 'Advanced Details' and a navigation bar with buttons: 'Cancel', 'Previous', 'Review and Launch', and 'Next: Add Storage' (which is highlighted with a red border).

- f. Leave it as default and click **Next: Add Tags**.

The screenshot shows the AWS Management Console interface for the 'Add Storage' step. At the top, the AWS logo and navigation menu are visible. Below the navigation, a progress bar indicates the current step is '4. Add Storage'. The main content area is titled 'Step 4: Add Storage' and includes a descriptive paragraph about storage options. A table displays the configuration for the root volume. Below the table is an 'Add New Volume' button and a light blue informational box. At the bottom, a horizontal scroll bar is present, and a row of navigation buttons includes 'Cancel', 'Previous', 'Review and Launch', and 'Next: Add Tags', with the latter being highlighted by a red border.

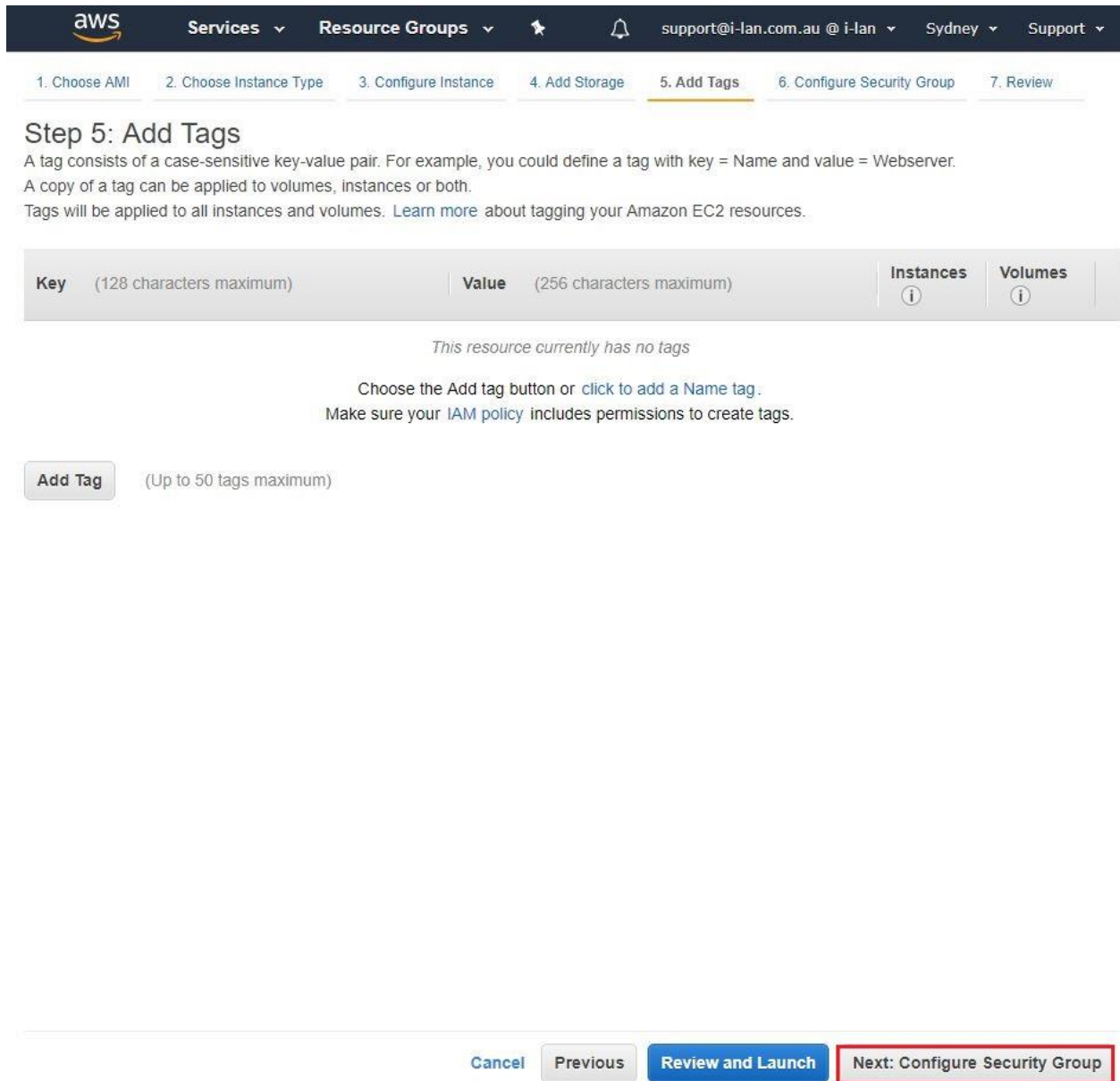
Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-01d5a58edadb2fbfd	8	General Purpose S	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Tags](#)

- g. Leave it as default and click **Next: Configure Security Group**.



aws Services Resource Groups support@i-lan.com.au @ i-lan Sydney Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes
This resource currently has no tags			

Choose the Add tag button or [click to add a Name tag](#).
Make sure your [IAM policy](#) includes permissions to create tags.

Add Tag (Up to 50 tags maximum)

Cancel Previous **Review and Launch** **Next: Configure Security Group**

- h. Select **Create new security** and enter **Security group name** and **Description**; e.g **WebDMZ**. Click **Add Rule** and enter the following **Custom TCP ports**, **Source** and **Description** for VigorACS 2.
- HTTP = 8844
 - HTTPS = 8443
 - TR-069 = 8069
 - Source is all IP address 0.0.0.0/0
- i. Click **Review and Launch**.

Step 6: Configure Security Group

security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more about Amazon EC2 security groups.](#)

Assign a security group: Create a new security group
 Select an existing security group

Security group name:
 Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin De
Custom TCP f	TCP	8844	Custom 0.0.0.0/0	HTTP for VigorACS2
Custom TCP f	TCP	8443	Custom 0.0.0.0/0	HTTPS for VigorACS2
Custom TCP f	TCP	8069	Custom 0.0.0.0/0	TR-069 for VigorACS2

Add Rule

Warning
 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.

Cancel Previous **Review and Launch**

- j. Select **Launch**, then a small window will pop up for you to create a new key pair. Select **Create a new key pair** and name it as e.g **Mykey** and then click **Download key Pair**. The key pair that we downloaded is the private key that we will use to authenticate to gain access to our VM instance. Click **Launch instances** after downloading the key pair.

- 1. Choose AMI
- 2. Choose Instance Type
- 3. Configure Instance
- 4. Add Storage
- 5. Add Tags
- 6. Configure Security Group
- 7. Review

Step 7: Review Instance Launch

AMI Details [Edit AMI](#)

Free tier eligible **Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-06705195ce845509c**
 Ubuntu Server 18.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).
 Root Device Type: ebs Virtualization type: hvm

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups [Edit security groups](#)

Security Group ID	Name	Description
sg-0be432142827bf366	WebDMZ	WebDMZ

All selected security groups inbound rules

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	
Custom TCP Rule	TCP	8069	0.0.0.0/0	TR-069 for VigorAC...
Custom TCP Rule	TCP	8443	0.0.0.0/0	HTTPS for VigorACS...
Custom TCP Rule	TCP	8844	0.0.0.0/0	HTTP for VigorACS ...

Instance Details [Edit instance details](#)

Cancel Previous **Launch**

Select an existing key pair or create a new key pair



A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Create a new key pair

Key pair name

MyKey

Download Key Pair



You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel

Launch Instances

k. Lastly, click **View instance** and wait for the instance state to turn into **running**.

Launch Status

Your instances are now launching
The following instance launches have been initiated: i-0910be937c771d5f3 [View launch log](#)

Get notified of estimated charges
Create [billing alerts](#) to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. Find out [how to connect to your instances](#).

▼ **Here are some helpful resources to get you started**

- [How to connect to your Linux instance](#)
- [Learn about AWS Free Usage Tier](#)
- [Amazon EC2: User Guide](#)
- [Amazon EC2: Discussion Forum](#)

While your instances are launching you can also

- [Create status check alarms](#) to be notified when these instances fail status checks. (Additional charges may apply)
- [Create and attach additional EBS volumes](#) (Additional charges may apply)
- [Manage security groups](#)

[View Instances](#)

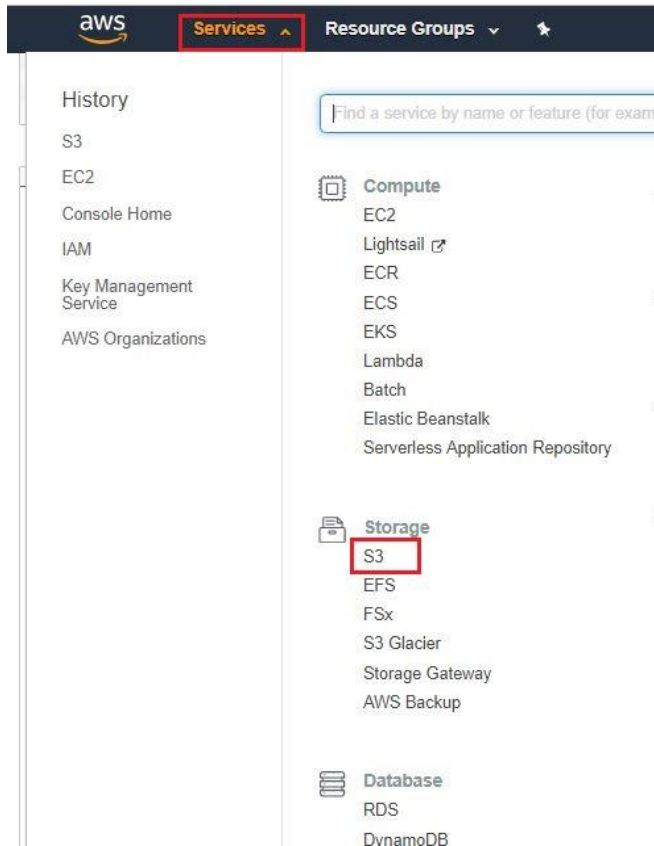
Instances

[Launch Instance](#) [Connect](#) [Actions](#)

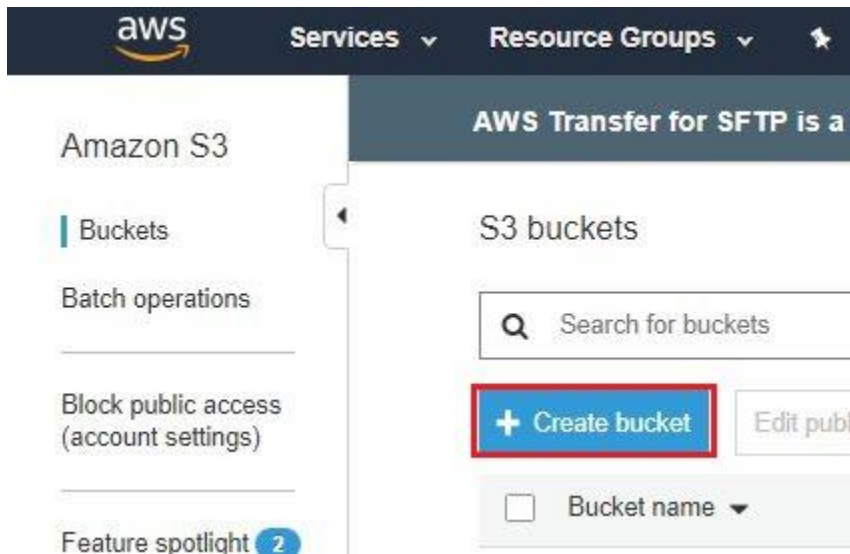
Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status
	i-0985e32ea210eb1cf	t2.micro	ap-southeast-2b	running	2/

- III. Creating a storage bucket in AWS Cloud and uploading Vigor ACS2 installer.
- a. Select **Service** and **S3**.



- b. Click **Create bucket**.



- c. Enter **Bucket name** as e.g **Vigoracs2** and select **Region** as e.g **Asia Pacific (Sydney)**, then click **Next**.

Create bucket



1 Name and region

2 Configure options

3 Set permissions

4 Review

Name and region

Bucket name ⓘ

vigoracs2

Region

Asia Pacific (Sydney)

Copy settings from an existing bucket

Select bucket (optional) 1 Buckets

Create

Cancel

Next

d. Leave it as default and click **Next**.

The screenshot shows the 'Create bucket' wizard in the AWS console, specifically the 'Configure options' step. The progress bar at the top indicates four steps: 1. Name and region (completed), 2. Configure options (current step), 3. Set permissions, and 4. Review. The main content area is titled 'Properties' and contains several sections with checkboxes and links:

- Versioning:** A checkbox labeled 'Keep all versions of an object in the same bucket.' with a 'Learn more' link.
- Server access logging:** A checkbox labeled 'Log requests for access to your bucket.' with a 'Learn more' link.
- Tags:** A section titled 'You can use tags to track project costs.' with a 'Learn more' link. Below this are two input fields labeled 'Key' and 'Value', and a '+ Add another' button.
- Object-level logging:** A checkbox labeled 'Record object-level API activity using AWS CloudTrail for an additional cost. See CloudTrail pricing or learn more.'
- Default encryption:** A checkbox labeled 'Automatically encrypt objects when they are stored in S3.' with a 'Learn more' link.
- Advanced settings:** A collapsed section indicated by a right-pointing arrow.

Below the 'Properties' section is a 'Management' section, which includes a link for 'CloudWatch request metrics'. At the bottom right of the wizard, there are two buttons: 'Previous' and 'Next'. The 'Next' button is highlighted with a red border, indicating it is the recommended action.

- e. Untick **Block all public access** – this will allow us to access our bucket from outside the cloud network. Click **Next** to continue.

Create bucket

1 Name and region 2 Configure options **3 Set permissions** 4 Review

Note: You can grant access to specific users after you create the bucket.

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on **Block all public access**. These settings apply only to this bucket. AWS recommends that you turn on **Block all public access**, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

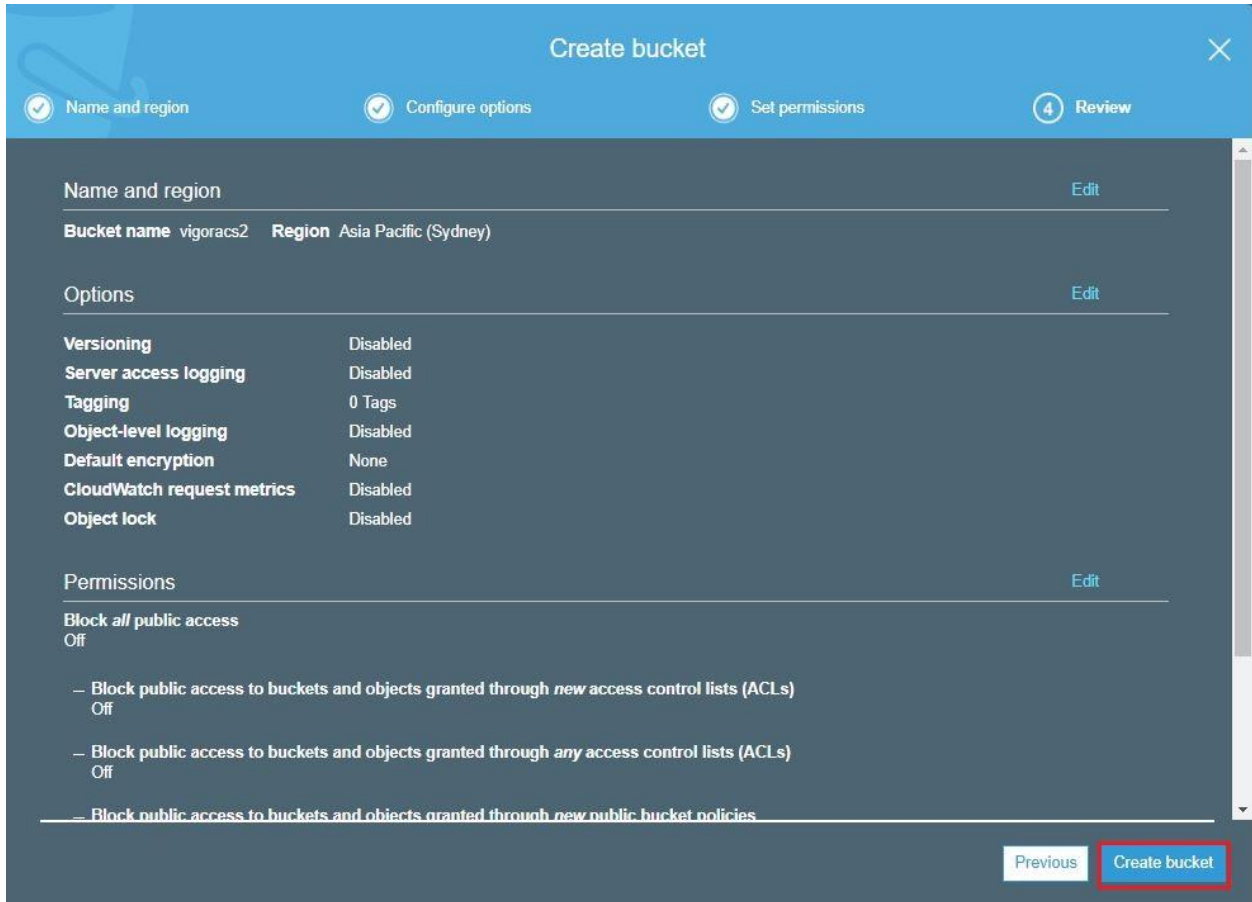
- Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket policies**
S3 will block new bucket policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket policies**
S3 will ignore public and cross-account access for buckets with policies that grant public access to buckets and objects.

Manage system permissions

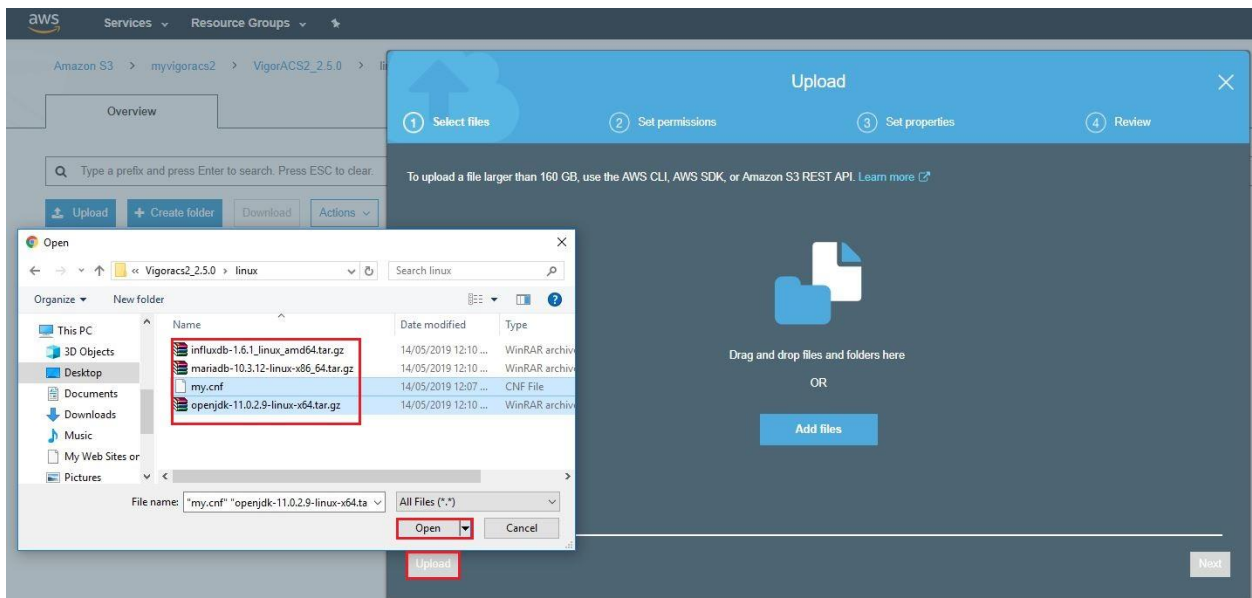
Do not grant Amazon S3 Log Delivery group write access to this bucket.

Previous **Next**

f. Click **Create bucket**.



g. Click **Upload** and **Add files** to browse the files from your computer that you want to upload to the bucket. We will upload VigorACS 2 installer. Finally, click **upload** again.







Upload

1 Select files 2 Set permissions 3 Set properties 4 Review

2 Files Size: 179.6 MB Target path: myvigoracs2/VigorACS2_2.5.0/linux/

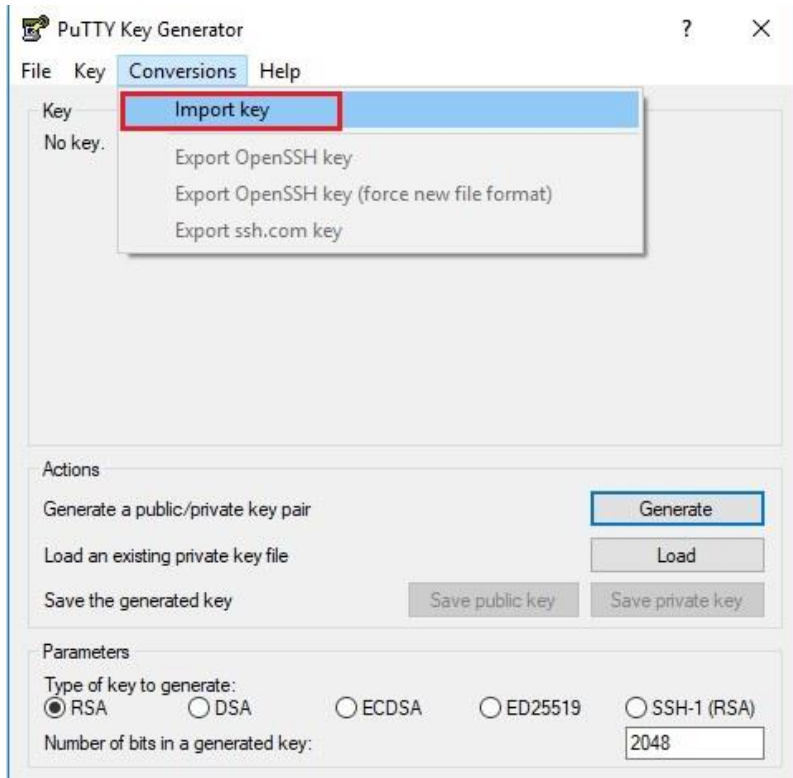
To upload a file larger than 160 GB, use the AWS CLI, AWS SDK, or Amazon S3 REST API. [Learn more](#)

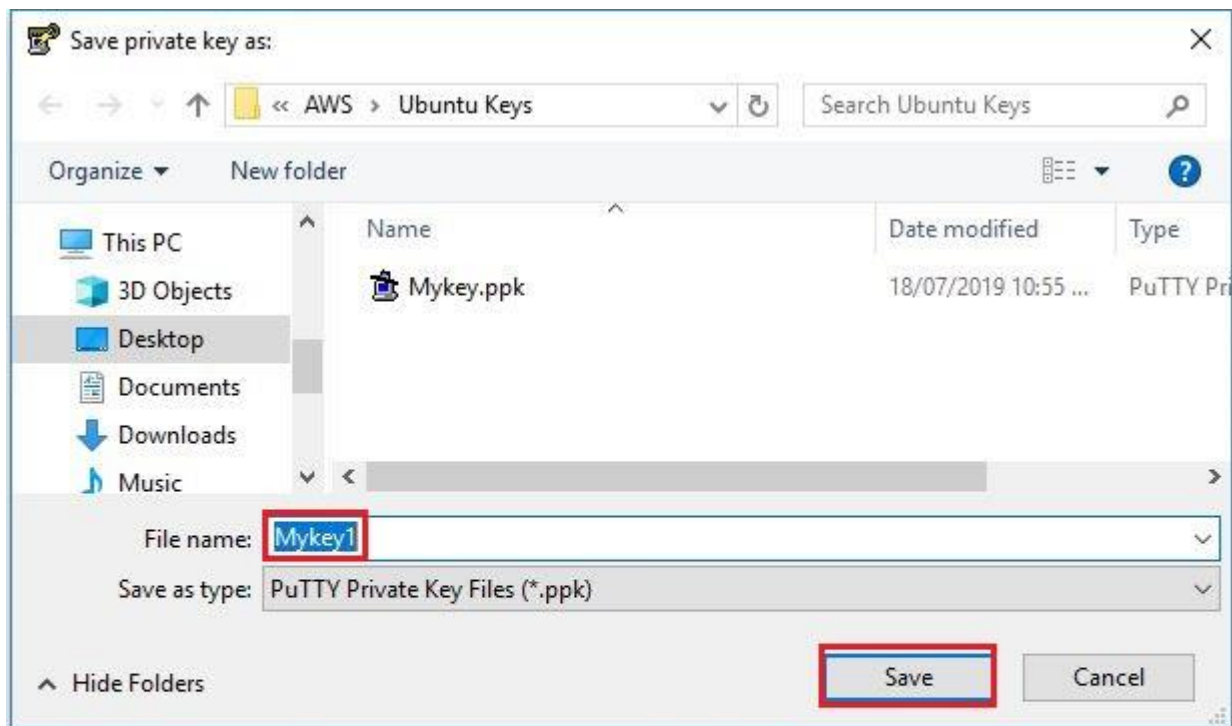
[+ Add more files](#)

	my.cnf - 562.0 B	
	openjdk-11.0.2.9-linux-x64.tar.gz - 179.6 MB	

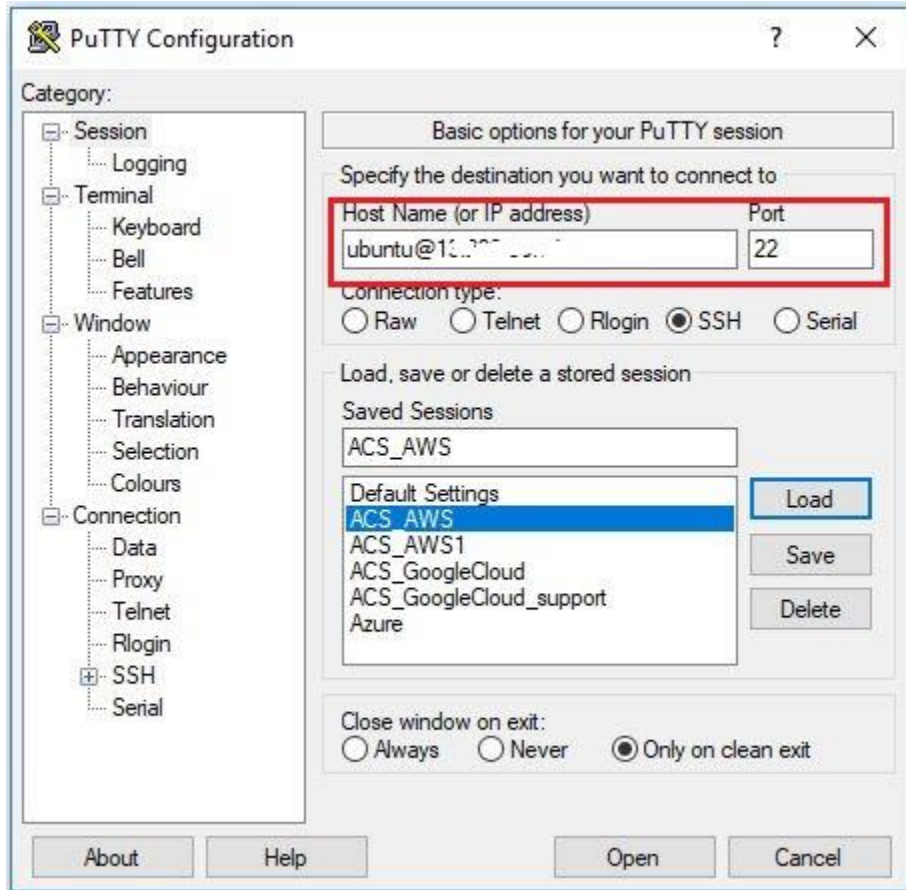
[Upload](#) [Next](#)

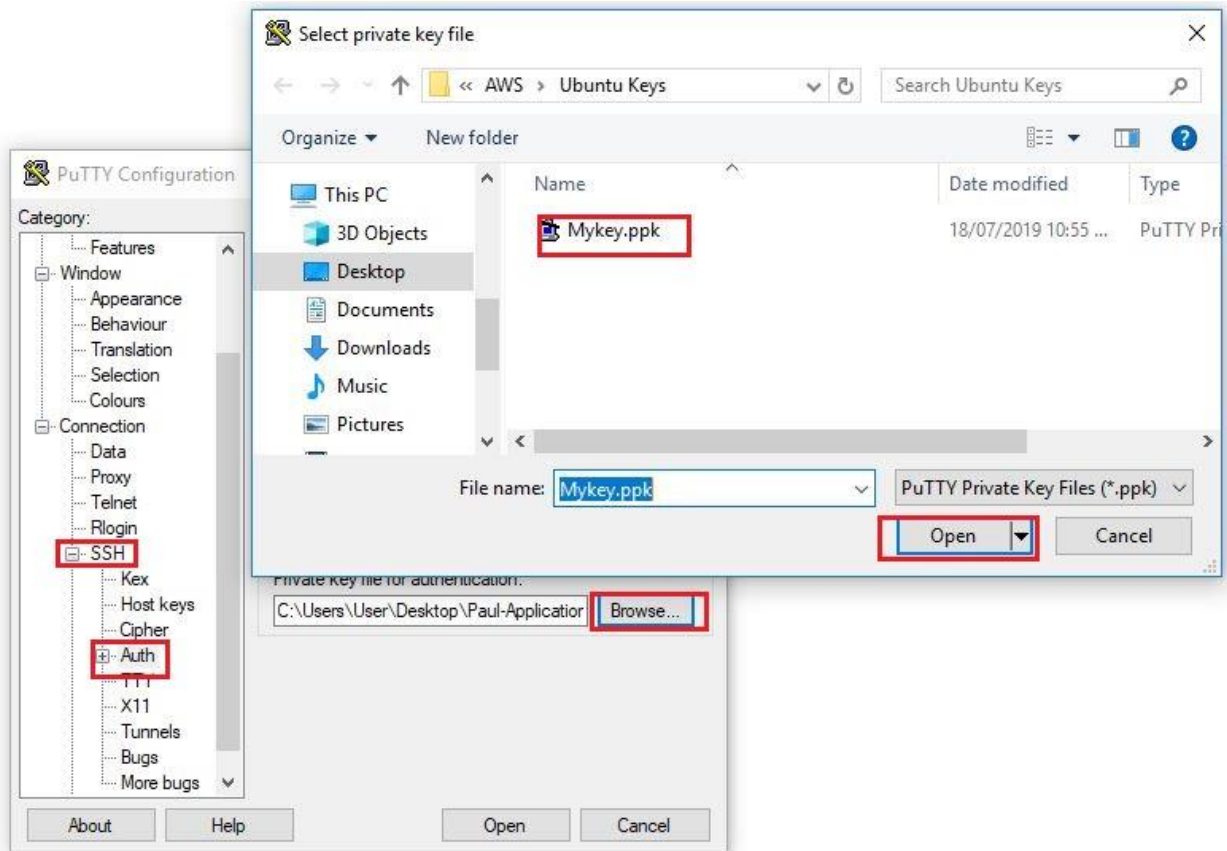
- IV. Manage the VM instance via SSH using Putty.
- a. Convert the Private Key (MyKey.pem) that we downloaded from AWS to MyKey.pkk.
The **.pem** format is not supported by putty.
 1. Run **Putty Key Generator** and go to **Conversions>>Import Key**.
 2. Click **Save private key** and save it to your computer.





- b. Create a session profile using putty.
 1. Run Putty configuration and enter **ubuntu@IP address of the server** and port **22**
 2. Go to **SSH>>Auth**, click **Browse** to select the private key that we download from AWS and then click open to connect to our VM instance.





- V. Copy the Vigor ACS2 installer from the bucket to the VM instance.
 - a. Installing awscli API in our VM instance.
 - 1. Enter the command **sudo -s** to switch to root access.

```
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.
```

```
ubuntu@ip-172-31-7-83:~$ sudo -s
```

2. Enter the command **apt update** to install and update awscli API dependencies, then type **y** to proceed with the installation.

```
root@ip-172-31-7-83:~# apt update
Hit:1 http://ap-southeast-2.ec2.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://ap-southeast-2.ec2.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:3 http://ap-southeast-2.ec2.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:4 http://ap-southeast-2.ec2.archive.ubuntu.com/ubuntu bionic/universe amd64 Packages [8570 kB]
Get:5 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:6 http://ap-southeast-2.ec2.archive.ubuntu.com/ubuntu bionic/universe Translation-en [4941 kB]
Get:7 http://ap-southeast-2.ec2.archive.ubuntu.com/ubuntu bionic/multiverse amd64 Packages [151 kB]
Get:8 http://ap-southeast-2.ec2.archive.ubuntu.com/ubuntu bionic/multiverse Translation-en [108 kB]
Get:9 http://ap-southeast-2.ec2.archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [693 kB]
Get:10 http://ap-southeast-2.ec2.archive.ubuntu.com/ubuntu bionic-updates/main Translation-en [254 kB]
Get:11 http://ap-southeast-2.ec2.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 Packages [976 kB]
Get:12 http://ap-southeast-2.ec2.archive.ubuntu.com/ubuntu bionic-updates/universe Translation-en [295 kB]
Get:13 http://ap-southeast-2.ec2.archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 Packages [6640 B]
Get:14 http://ap-southeast-2.ec2.archive.ubuntu.com/ubuntu bionic-updates/multiverse Translation-en [3556 B]
Get:15 http://ap-southeast-2.ec2.archive.ubuntu.com/ubuntu bionic-backports/main amd64 Packages [2512 B]
Get:16 http://ap-southeast-2.ec2.archive.ubuntu.com/ubuntu bionic-backports/main Translation-en [1644 B]
```

3. Enter the command **apt install awscli** to install awscli API.

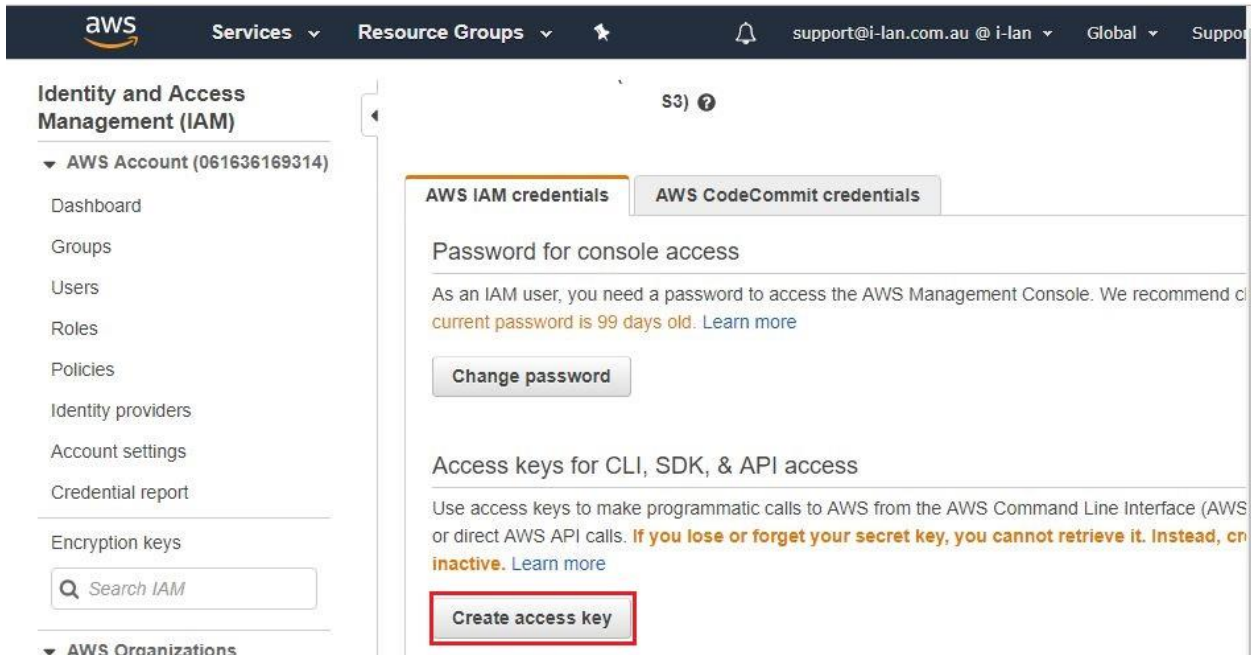
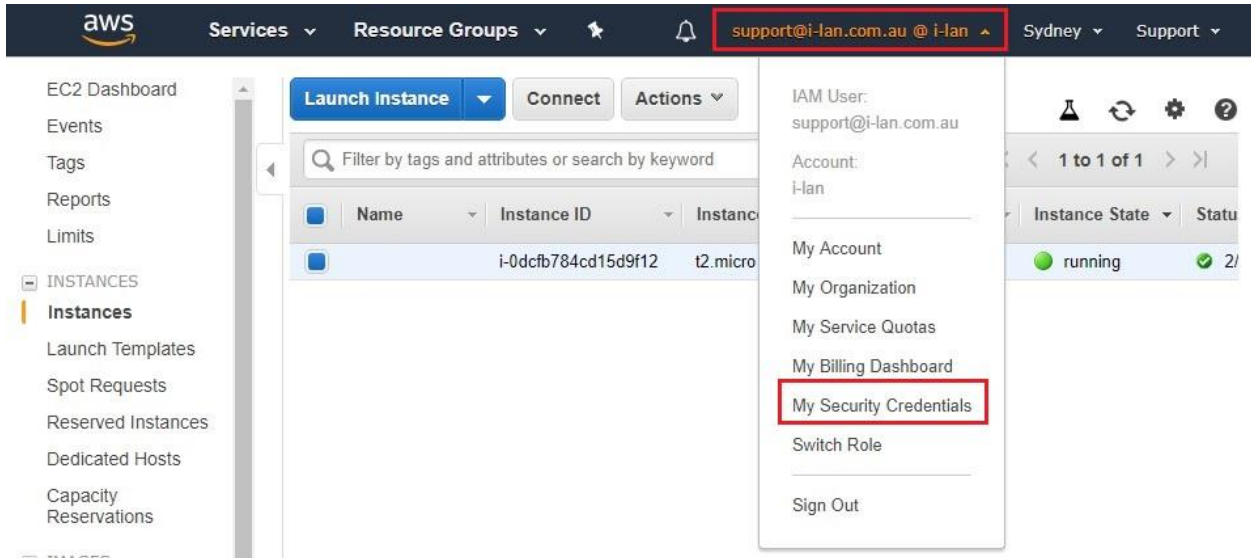
```
root@ip-172-31-7-83:~# apt install awscli
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  docutils-common libjbig0 libjpeg-turbo8 libjpeg8 liblcms2-2 libpaper-utils lib
  python3-pygments python3-roman python3-rsa python3-s3transfer sgml-base xml-co
Suggested packages:
  liblcms2-utils docutils-doc fonts-linuxlibertine | ttf-linux-libertine texlive
The following NEW packages will be installed:
  awscli docutils-common libjbig0 libjpeg-turbo8 libjpeg8 liblcms2-2 libpaper-ut
  python3-pygments python3-roman python3-rsa python3-s3transfer sgml-base xml-co
0 upgraded, 24 newly installed, 0 to remove and 40 not upgraded.
Need to get 4550 kB of archives.
After this operation, 40.8 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

4. Enter the command **aws configure** and enter the following access keys below for CLI, SDK, & API access.

- AWS Access Key ID
- AWS Secret Access Key
- Default region name = ap-southeast-2 (for Sydney)
- Default output format = can be json, text and table

```
root@ip-172-31-7-83:~# aws configure
AWS Access Key ID [None]: 
AWS Secret Access Key [None]: 
Default region name [None]: ap-southeast-2
Default output format [None]: json
```

5. The keys can be found by going to *username*>>*My Security Credentials*, then click *Create access key*.



- b. Enter the command ***aws s3 sync s3://myvigoracs2 installer***
 - The ***vigoracs2*** is our bucket directory name and the ***installer*** is the directory to where the VigorACS 2 files would be save.

```
Default output format [None]: json
root@ip-172-31-7-83:~# aws s3 sync s3://myvigoracs2 installers
download: s3://myvigoracs2/VigorACS2_2.4.1/Install VigorACS on Synology Guide.txt
download: s3://myvigoracs2/VigorACS2_2.4.1/Install VigorACS Guide.txt to installers
download: s3://myvigoracs2/VigorACS2_2.4.1/ImportPEM2Keystore.sh to installers/Vig
download: s3://myvigoracs2/VigorACS2_2.4.1/acs_lib.sh to installers/VigorACS2_2.4.
download: s3://myvigoracs2/VigorACS2_2.4.1/install_acs_jdk.sh to installers/VigorA
download: s3://myvigoracs2/VigorACS2_2.4.1/install_sqlite.sh to installers/VigorAC
download: s3://myvigoracs2/VigorACS2_2.4.1/install_Synology_NAS.sh to installers/V
download: s3://myvigoracs2/VigorACS2_2.4.1/install_acs_jboss.sh to installers/Vigo
download: s3://myvigoracs2/VigorACS2_2.4.1/install.sh to installers/VigorACS2_2.4.
download: s3://myvigoracs2/VigorACS2_2.4.1/jcelib/US_export_policy.jar to installe
download: s3://myvigoracs2/VigorACS2_2.4.1/install_sqlite_openjdk.sh to installers
download: s3://myvigoracs2/VigorACS2_2.4.1/jcelib/local_policy.jar to installers/V
download: s3://myvigoracs2/VigorACS2_2.4.1/install_acs.sh to installers/VigorACS2_
download: s3://myvigoracs2/VigorACS2_2.4.1/install_user_vigoracs.sh to installers/
download: s3://myvigoracs2/VigorACS2_2.4.1/jcelib/java.security to installers/Vigo
download: s3://myvigoracs2/VigorACS2_2.4.1/linux/influxdb-1.6.1_linux_amd64.tar.gz
download: s3://myvigoracs2/VigorACS2_2.4.1/Quick Start Guide.txt to installers/Vig
```

- VI. Installing dependencies, database and VigorACS2.
 - a. Enter the command `cd installers/Vigoracs_2.4.1`
 - b. Allow root to execute `install.sh` file by entering the command `chmod 755 install.sh`
 - c. Enter the command `./install.sh` to run the VigorACS 2 installer.
 - d. Type `y` to proceed with the installation.

```
root@ip-172-31-7-83:~# cd installers/VigorACS2_2.4.1
root@ip-172-31-7-83:~/installers/VigorACS2_2.4.1# chmod 755 install.sh
root@ip-172-31-7-83:~/installers/VigorACS2_2.4.1# ./install.sh
ping IPv4 address success

entering /home/ubuntu/installers/VigorACS2_2.4.1/linux.....

Please create /usr/local/vigoracs
Create it now? (y/n)
```

- e. Install the following below:
 - ***press 1 and enter*** to install mysql/mariadb
 - ***press 3 and enter*** to install influxdb
 - ***press 4 and enter*** to install or upgrade Java
 - ***press 5 and enter*** to install VigorACS

```

Notice:
  * Installation ACS Server requires root privileges.
  * After installing the ACS server, need to configure the Firewall to Allow HTTP and HTTPS port

[1] Install mysql/mariadb
[2] Change root password and security configuration of mysql/mariadb ( Default root password is blank )
[3] Install influxdb
[4] Install or Upgrade java
[5] Install VigorACS ( It will build one mysql/mariadb database : tr069 )
[6] Upgrade VigorACS ( It will upgrade local tr069 database )

*****For Remote Database Only*****
[7] Redirect the database path of VigorACS to remote host ( It will not upgrade remote database )

[8] Exit
input select num :

```

- f. Type “y” and **press enter** to continue creating ACS database.
- g. Type “1” and **press enter** to select Local side database.
- h. Type “1” and **press enter** to use ACS for Mysql.
- i. **Press enter** to use blank password for MySQL/MariaDB.
- j. Type “y” and **press enter** to test password for MySQL/MariaDB.

```

[Install VigorACS]
[Warning] It will clear the existing ACS database and create a new one.Do you want to continue? (y/n)
y
Do you want to use remote/local database? (1: Local side database, 2: Remote side database, Enter for Local side da
tatabase)
1
Which Mysql do you want to use ? (1: ACS , 2: OS default, Enter for ACS mysql)
1
Starting vigoracsmysqld (via systemctl): [ OK ]
Please keyin password of root of MySQL/MariaDB.

Do you want to test password now ?(y/n)
y
Access Database Success
Restarting influxdb (via systemctl): [ OK ]
Start to install VigorACS....
Archive: VigorACS.zip
  creating: VigorACS/server/default/deploy/ACSServerAPP.ear/
  creating: VigorACS/server/default/deploy/ACSServerAPP.ear/ACSServer.war/

```

VII. Starting database and VigorACS 2.

- a. Enter the command `cd /usr/local/vigoracs/VigorACS/bin` and `./vigoracs.sh` to start the installation page.
- b. Start mysql/mariadb, influxdb and VigorACS2.
 - **press 1 and enter** to start mysql/mariadb
 - **press 3 and enter** to start influxdb
 - **press 5 and enter** to start VigorACS

```
*****For Remote Database Only*****
[7] Redirect the database path of VigorACS to remote host ( It will not upgrade remote da

[8] Exit
input select num :
^C
root@ip-172-31-7-83:~/installers/VigorACS2_2.4.1# cd /usr/local/vigoracs/VigorACS/bin
root@ip-172-31-7-83:/usr/local/vigoracs/VigorACS/bin# ./vigoracs.sh

Mysql process id : 14958 15044
Influxdb process id :
Vigoracs process id :

1. start mysql/mariadb
2. shutdown mysql/mariadb
3. start influxdb
4. shutdown influxdb
5. start VigorACS
6. shutdown VigorACS
7. edit bind IP of VigorACS Server(please keyin IP or servername)
8. set the MAX. and MIN. memory value of running java (It will be valid after restarting
9. view the MAX. and MIN. memory value of running java
```

- c. Enter the following below after selecting 5 (start VigorACS).
 1. Bind IP to **0.0.0.0**
 2. Optional: enter http port **8844** instead of 80.
 3. Optional: enter https port **8443** instead of 443.
 4. **Press enter** to select default ports **347** and **514** for stun and syslog.
 5. **Press enter** to accept default **max memory** and **minimum memory**.

```
Vigoracs process id :
1. start mysql/mariadb
2. shutdown mysql/mariadb
3. start influxdb
4. shutdown influxdb
5. start VigorACS
6. shutdown VigorACS
7. edit bind IP of VigorACS Server (please keyin IP or servername)
8. set the MAX. and MIN. memory value of running java (It will be valid after restarting VigorACS )
9. view the MAX. and MIN. memory value of running java
10. exit
input select num :
5
Which ip address do you want to bind for VigorACS service ( x.x.x.x or Enter for bind 0.0.0.0 address)?
0.0.0.0
Which http port do you want to bind for VigorACS service ( port number or Enter for 80 port)?
8844
Which https port do you want to bind for VigorACS service ( port number or Enter for 443 port)?
8443
Which stun port do you want to bind for VigorACS service ( port number or Enter for 3478 port)?
3478
Which syslog port do you want to bind for VigorACS service ( port number or Enter for 514 port)?
514
How many memory do you want to set for VigorACS service? (Enter for default MAX Memory is 1024, MIN Memory is 900 M
B)
MAX Memory What you want? (Unit: MB)
MIN Memory What you want? (Unit: MB)
Starting vigoracs:
[OK]
Mysql process id : 2882 3121
Influxdb process id : 6136
Vigoracs process id :
```

- VIII. Change the time zone to AEDT (Australian Eastern Daylight Time).
 - a. Enter the command **"date"** to verify the time zone.
 - b. Enter the command **"mv /etc/localtime /etc/localtime.bak"**.
 - c. Enter the command **"ln -s /usr/share/zoneinfo/Australia/NSW /etc/localtime"**.
 - d. Enter again the command **"date"** to verify the time zone – should be set to **AEDT**.

```
root@ip-172-31-7-83:~# date
Thu Jul 25 03:41:29 UTC 2019
root@ip-172-31-7-83:~# mv /etc/localtime /etc/localtime.bak
root@ip-172-31-7-83:~# ln -s /usr/share/zoneinfo/Australia/NSW /etc/localtime
root@ip-172-31-7-83:~# date
Thu Jul 25 13:42:08 AEST 2019
root@ip-172-31-7-83:~#
```


- IX. Accessing the VigorACS 2 web interface and activating the trial license.
- a. Type the **public IP address, port number** and enter **username** as " **root**" and **password** as " **admin123**".



Login to VigorACS 2

User Name

Password

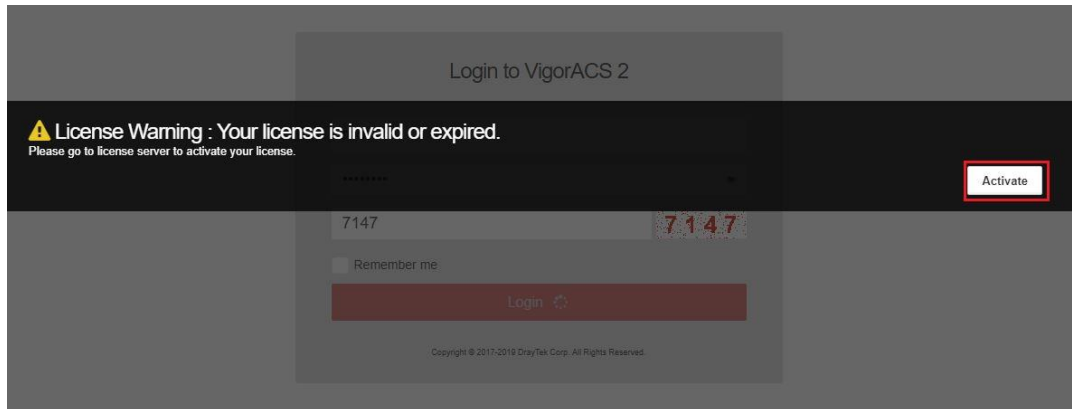
Validation Code **5218**

Remember me

Login

Copyright © 2017-2019 DrayTek Corp. All Rights Reserved.

- b. After selecting " **Activate**" the VigorACS2 will redirect us to the **MyVigor** website to register our VigorACS 2 and activate the 30 days trial license.



The MyVigor website does not record any personal identifiable information with the exception of your IP Address which is recorded after login for security purposes.



c. Select "On" under Status and "Login to ACS".

DrayTek MyVigor

Login User: itan_support_acs (Logout)

My Information - My Products

Device Information

Device Name: ACSGC-2445
Host ID: ACS190200091
Model: VigorACS2 Series

Rename Add Main Key ACS License Help Transfer Back

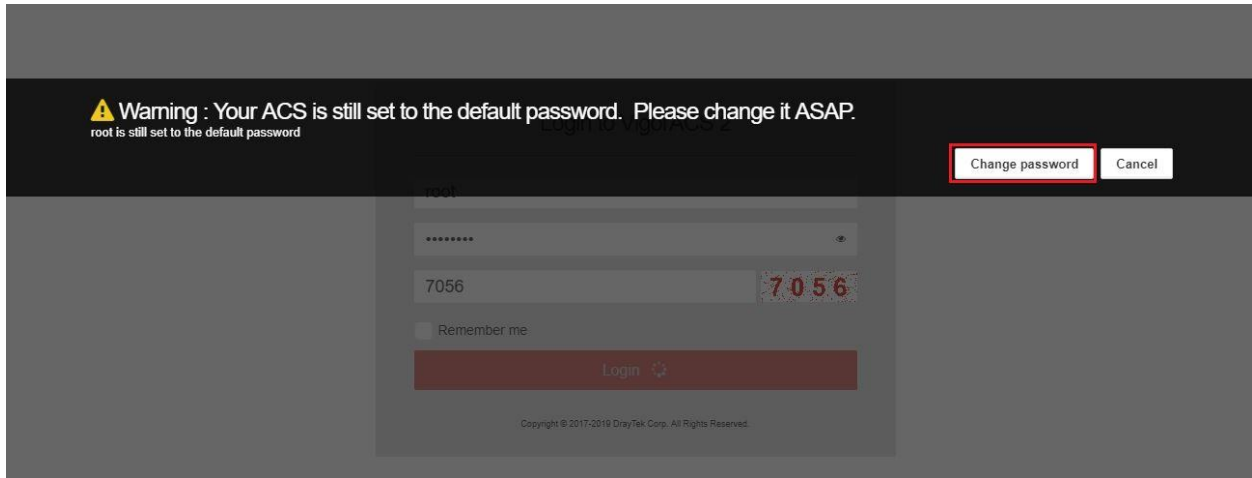
Service	Provider	Action	Status	Start Date	Expired Date	Nodes	Note
ACS	DT-ACS-2	Add Main Key	On	2019-02-26	2019-03-28	20	-

VigorACS License Information

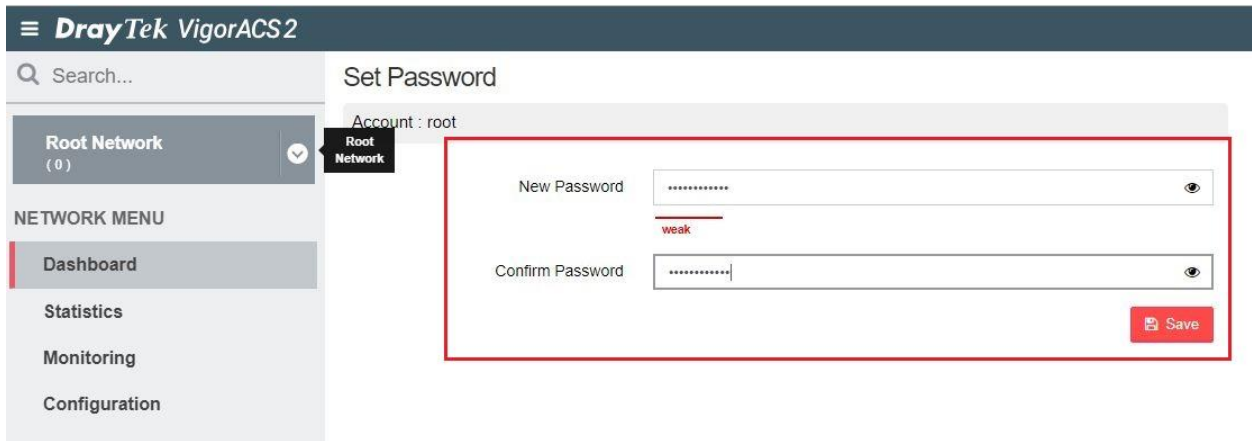
Operation	1000 - License Key OK
License id	00024e59
Start date	2019-02-26
Expire date	2019-03-28
Max node	00000020
Trial license	Yes

Login to ACS

d. Select **“Change password”** for security purposes.



e. **Enter new password** and confirm new password.



f. Go to “**About**”, to verify the license information on the VigorACS 2.

The screenshot displays the DrayTek VigorACS2 web interface. On the left is a navigation menu with sections for NETWORK MENU and SYSTEM MENU. The 'About' menu item is highlighted with a red box, and its sub-item 'License Information' is also highlighted with a red box. The main content area shows the 'License Information' page, which contains a table of license details and an 'Activate License' link.

License Information	
Host ID	ACS190200051
License ID	00024e59
License Type	Trial
Start Date	2019-02-26
Expire Date	2019-03-28
Max Node	20
Activate License	+ Click here to activate license