Vidyavardhini's College of Engineering and Technology

Department of Artificial Intelligence & Data Science

AY: 2023-24

Class:		**Semester:**	
Course Code:		**Course Name:**	

Name of Student:	
Roll No. :	
Experiment No.:	7
Title of the Experiment:	To study and Implement Security as a Service on AWS/Azure
Date of Performance:	
Date of Submission:	

Evaluation

Performance Indicator	Max. Marks	Marks Obtained
Performance	5	
Understanding	5	
Journal work and timely submission	10	
Total	20	

Performance Indicator	Exceed Expectations (EE)	Meet Expectations (ME)	Below Expectations (BE)
Performance	4-5	2-3	1
Understanding	4-5	2-3	1
Journal work and timely submission	8-10	5-8	1-4

Checked by

Name of Faculty :

Signature :

Date :

Experiment No. 7

Aim: To study and Implement Security as a Service on AWS/Azure

Objective: To understand the Security practices available in public cloud platforms and to demonstrate various Threat detection, Data protection and Infrastructure protection services in AWS and Azure **Theory**:

As the use of file sharing increases across the industry, more attention is being paid to the inherent security of these solutions and the need for corporations to provide enterprise file sync and share (EFSS) solutions that meet IT's security parameters. **Security Features of ownCloud**

ownCloud's drivers for continued security improvement is to not only fix individual symptoms (e.g. the single bugs), but to also focus on identifying and resolving the root cause to prevent whole categories of vulnerabilities. ownCloud internal security processes and secure software development lifecycle aligns with industry standards such as ISOs 29147, 30111 and 27304.

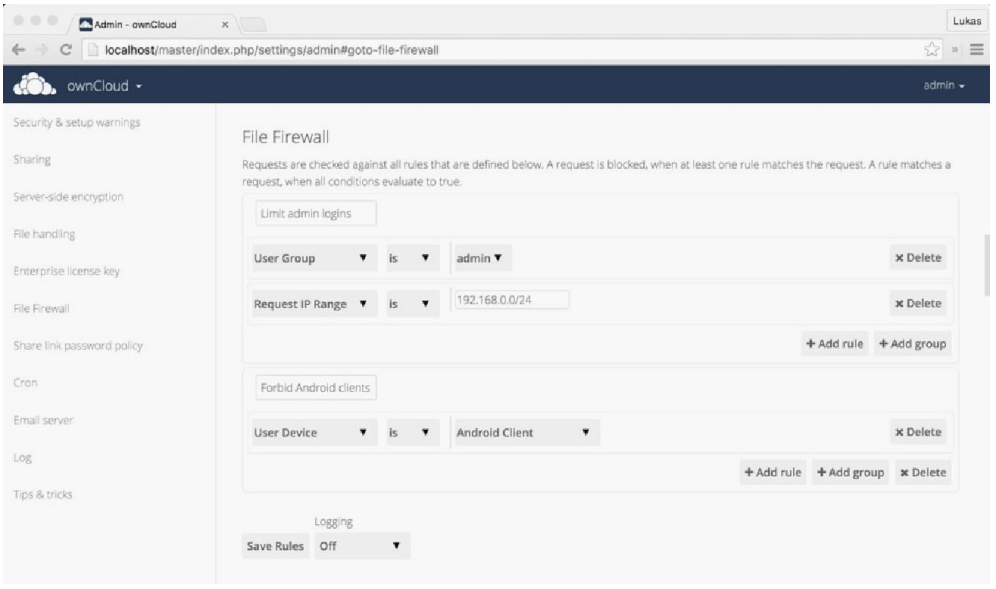
- **Strict Content Security Policy :** Content Security Policy (CSP) is one of the most useful and powerful web security features introduced in recent years. With CSP, applications can instruct the browser to follow a specified security model, including instructions to not execute any inline scripts or load remote resources.

- **Data in Session is Stored Encrypted:** PHP stores session related data within sessions. These are usually small files on the server containing data such as the login state or the username. We have hardened the PHP session storage in such a way that the ownCloud server can only read session data at the same time the user is using ownCloud. This is done by encrypting the stored session data with an encryption key stored in another cookie. If the userrequests a page on ownCloud the encryption cookie will be sent by the sync clients or the web browser. Only with this cookie (which is not stored on the disk of the application server) can the session content be decrypted.

- **Secure by Default Model:** New ownCloud code uses the so called "ownCloud App Framework", a modern MVC-like framework to develop code for ownCloud. Code relying on this framework uses a lot of secure defaults such as requiring CSRF (another specific kind of web vulnerability caused by the original design of the web) and authentication checks being opt-out rather than the more common (and less safe) opt-in. The default mode for every critical security feature in ownCloud is "on", and requires the developer to deliberately "opt-out" of these security checks. These secure defaults are part of ownCloud's secure software development lifecycle. Secure defaults make it
more difficult to accidentally trigger a security vulnerability Instead, it allows internal and external security professionals to easily assess the overall security of an ownCloud component.

- **Strict Comparison in PHP Technically Enforced:** PHP has some peculiarities such as "Type Juggling". This means that it will automatically try to convert data types when applicable such as in comparisons. An example would be the following comparison: "0 == false" where PHP will try to convert both values (integer and Boolean value) into a comparable state and thus, will return true. This can lead to unexpected behavior and potential security bugs if developers don't take this into consideration. ownCloud forces PHP to confirm that the data is exactly the same type by verifying the data type using strict comparisons as a best practice.

- **File Firewall :** Using the internal File Firewall of ownCloud's Enterprise Edition, enterprises can limit access to sensitive data even further. File Firewall is an application-level firewall that inspects all incoming ownCloud requests and evaluates them based on rules set by the administrator to only allow through *"approved"* requests for a finely granular level of control. Administrators can, for example, limit administrative logins to a pre-defined internal network to enhance security or allow access to shared folders only from a specific location to implement internal security guidelines.

- 

Setting up your own private cloud storage service using ownCloud

There have been several reports of various cloud storage services getting hacked of late. You can actually create your own cloud storage solution that you can control with an open source service called ownCloud. It is a simple way to set up your own syncing and Dropbox-like cloud storage system on your own server or website. It is robust, quick and easy to set up, and does not require much advanced technical knowledge. Let's have a quick look at how you can set up a private cloud using ownCloud.

Prerequisites

You do not really need much to get started with setting up ownCloud, but should have the following handy before you start.

1. **Any Web host that supports PHP5 and MySQL (or SQLite):** You should be signed up for a service like Dreamhost. If you already have a domain name (like *http://www.name.com*) through a Web host, you can install ownCloud in a couple of minutes. You will not have to deal with things like MySQL and PHP for installing ownCloud. All of these are taken care of automatically. You just need to make sure that your hosting service supports them.
2. **A copy of ownCloud Server 5:** You can actually install ownCloud in different ways, but let's just stick to the simplest method, i.e., using the Web installer. If you know how to put a file onto your website, you can install this.
3. **A URL for remote access:** Since you would prefer to tap into ownCloud from anywhere, you will need a URL to do so. If you do not already have a domain name, you can buy one; but if you do, it's very easy to set up ownCloud in a sub-directory of your site.

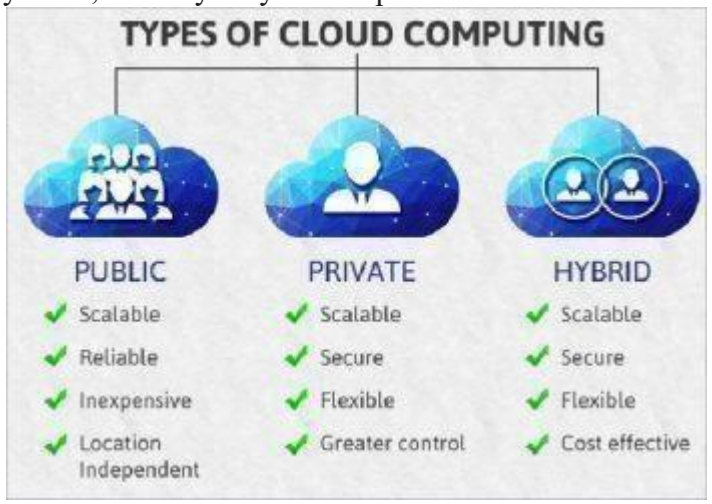


Figure : Different types of cloud storage systems (Image source: googleimages.com)

Initial setup and installation

As was decided earlier, we will use the Web installer, with the help of which ownCloud automatically creates everything you need so that no special skills are required to get it set up. If you have multiple users wanting to access ownCloud, it is recommended that you manually create a database. Here is how you can install ownCloud using the Web installer.

1. Download and save the Web installer to the computer.
2. Upload the setup file – owncloud.php – to the Web space using the host's Web interface or an FTP application.
3. Enter the URL of the setup file into the Web browser. It should be something like ***http://www.yourdomainname.com/setup-owncloud.php***.
4. Follow the given on-screen instructions to install ownCloud. After a few minutes, you will be redirected to the login page.

The setup for desktop and mobile sync

Now that you have ownCloud installed on your Web server, it's time to set up desktop sync so that the files in ownCloud are the same format as those on your computer. For this, you need to install the desktop client (Linux, Windows or Mac).

From here onwards, the setup is pretty simple:

1. Open up ownCloud software on the computer, and select *Configure*.
2. Add the URL of the ownCloud server along with the login credentials.
3. Now, you need to select the folders and files that you want to sync. Click *Add folder* and select a folder that needs to be synced on the computer. All the files present in this folder will be uploaded and synced automatically to ownCloud. Similarly, you can add as many folders as you like.

As with Dropbox, you can simply drag files into the Web interface so that they can be uploaded and synchronised both locally as well as in the cloud, and you can also share files with friends by selecting the Share option when you hover the mouse over a file.

Syncing the calendar, address book and music

Syncing calendars: If you use a calendar app that supports CalDAV, you just need to point it to your ownCloud installation.

1. Click the *Calendar* icon on the right side.
2. Click the gear icon present in the top right.
3. Copy down the URL for the calendar (most of the calendars can access simple URLs, but iOS requires a slightly different URL).

Now, simply open the settings of your favourite calendar app, and add your account in the CalDAV section. All your appointments will be directly dumped into ownCloud and will be automatically synced across any other device you connect to it.

Sync your contacts: Similar to the calendar, you can easily import and sync your address book with ownCloud.

1. Export all the Contacts from the address book into a VCF file.
2. From ownCloud, select the Contacts sidebar, and then click the gear present in the bottom left corner.
3. Click Import and then select the VCF file to be uploaded.

It will take a few minutes to get all the contacts uploaded, but once they are up, you can synchronise them with any address book that supports CardDAV.

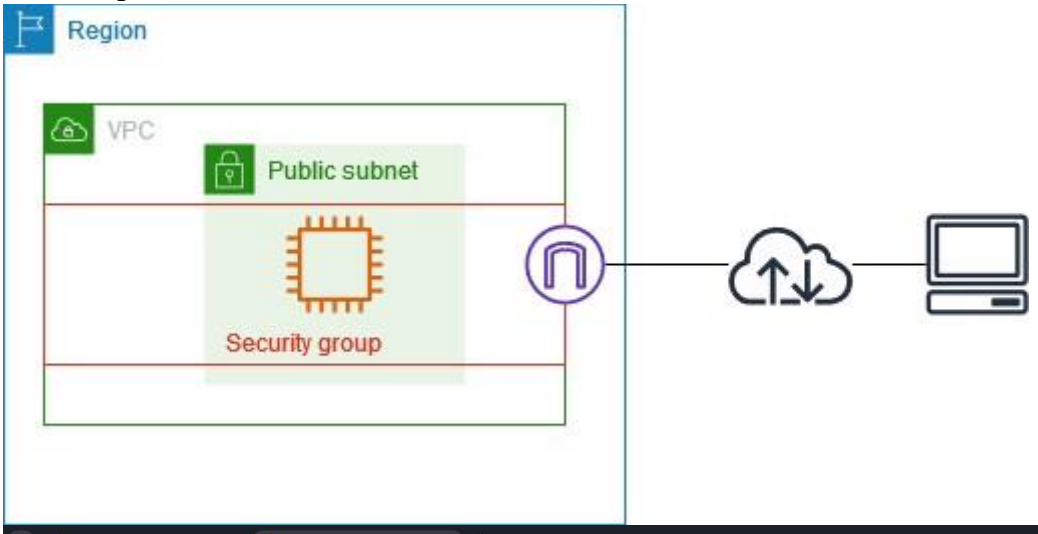
Add apps and extend ownCloud's power

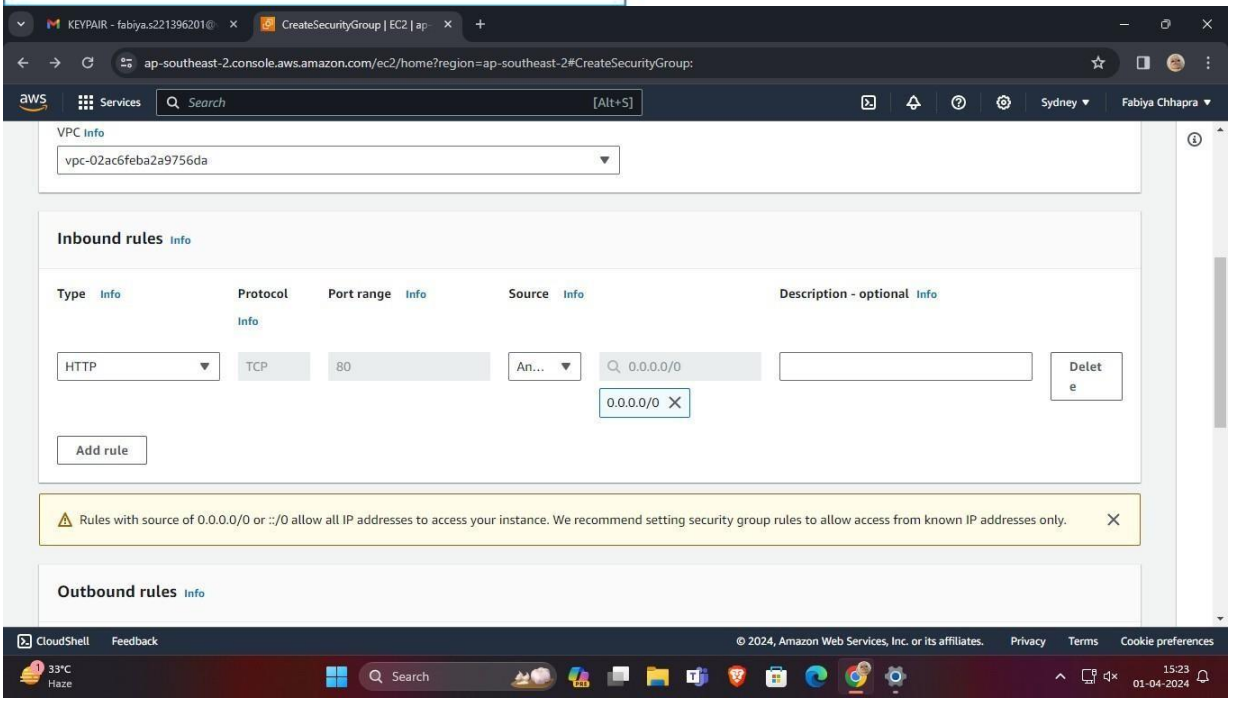
It is even possible to extend ownCloud's functionality with the help of additional applications. If you click your user name from the ownCloud Web interface and select Apps, you are taken to a list of the installable applications. You can also browse through a few more such applications over here. To install any of the external applications, you just need to select the app, and click Enable. After a few moments, it will be installed and you will find a new icon on the right panel.

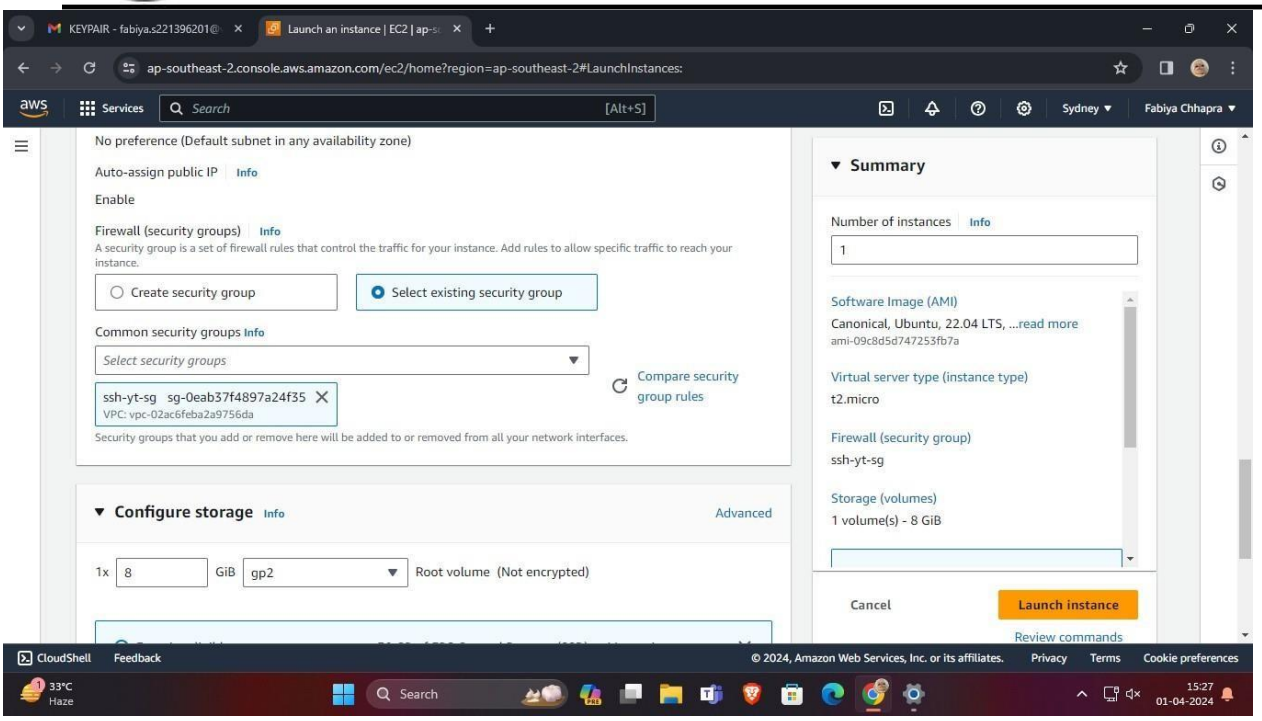
The benefits of setting up your own cloud storage system are many, some of which are:

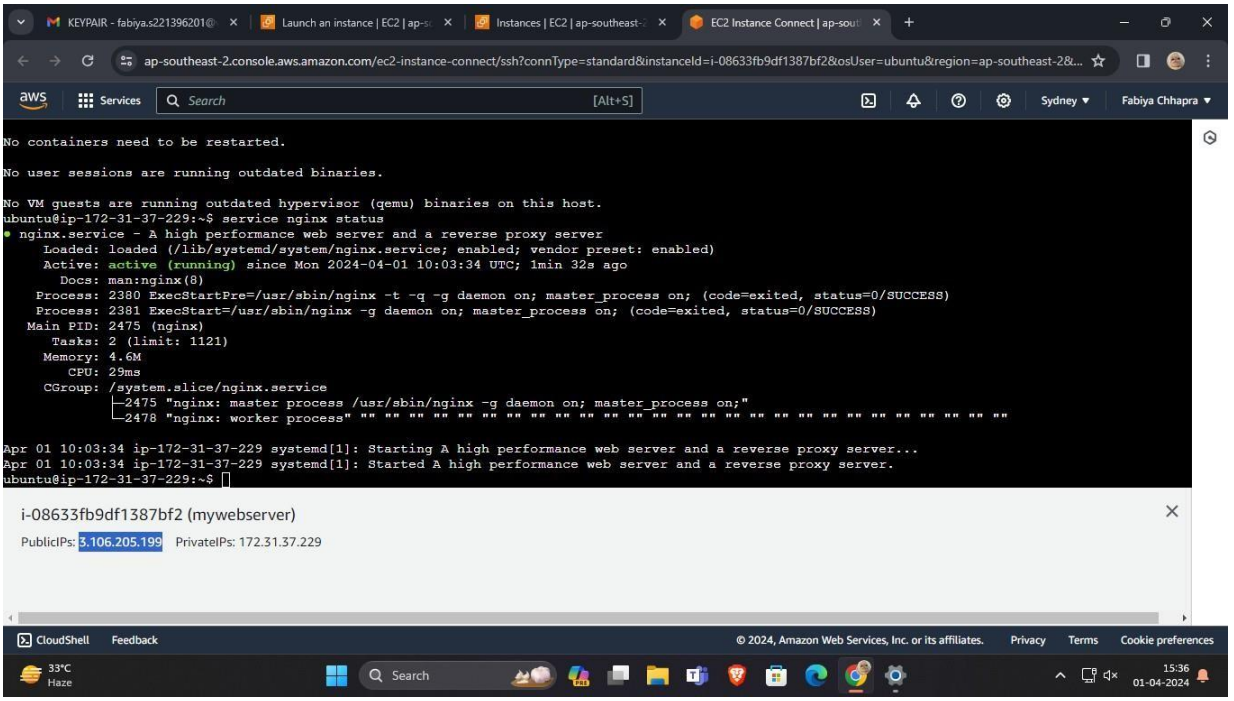
1. It helps to access the data present on the cloud from anywhere; hence, it's flexible.
2. It is highly scalable.
3. As it is a private cloud, it has got higher security.
4. It is easy to sync files from your desktop to the cloud.
5. It enables you to sync ownCloud with almost any desktop or mobile calendar and contacts application.

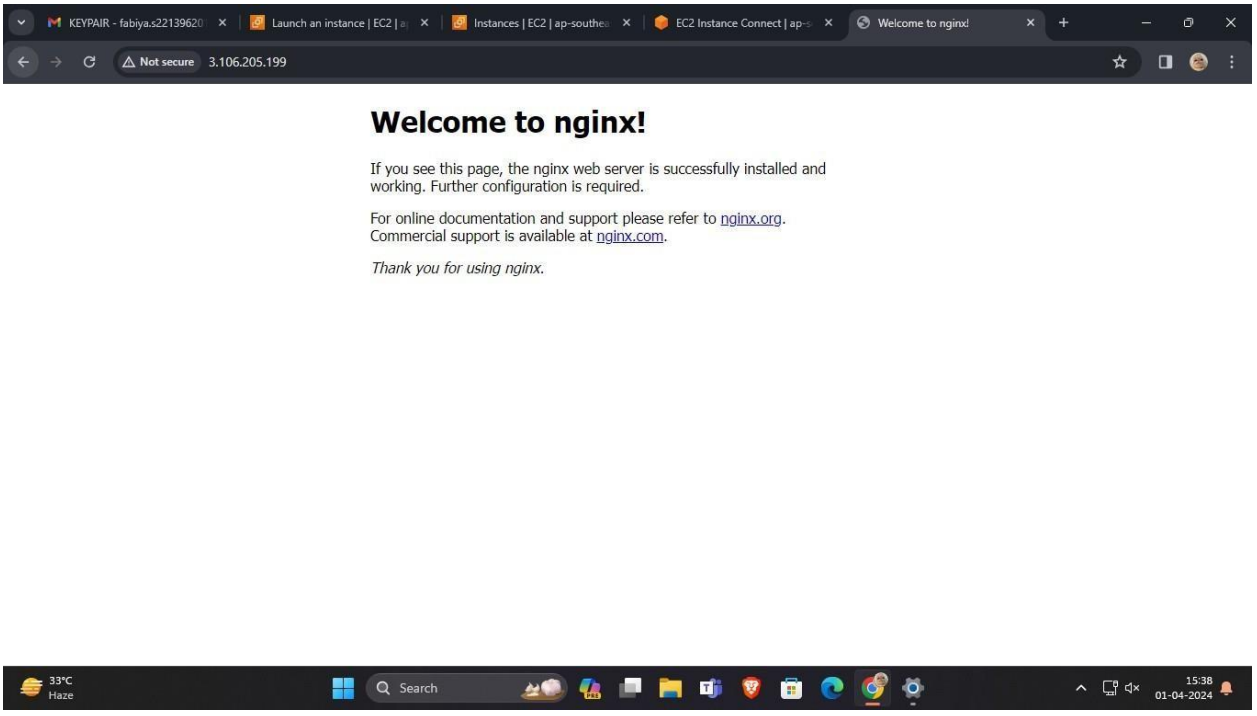
Output/Observation:






KEYPAIR - fabiya.s221396201@
Launch an instance | EC2 | ap-s
ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#LaunchInstances:
Services
Search
[Alt+S]
Sydney
Fabiya Chhapra
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
Common security groups Info
Select security groups
ssh-yt-sg sg-0eab37f4897a24f35
VPC: vpc-02ac6feba2a9756da
Compare security group rules
Security groups that you add or remove here will be added to or removed from all your network interfaces.
Configure storage Info
Advanced
1x 8 GiB gp2 Root volume (Not encrypted)
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-09c8d5d747253fb7a
Virtual server type (instance type)
t2.micro
Firewall (security group)
ssh-yt-sg
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
33°C
Haze
Search
15:27
01-04-2024


KEYPAIR - fabiya.s221396201@
Launch an instance | EC2 | ap-s
Instances | EC2 | ap-southeast-2
EC2 Instance Connect | ap-sout
ap-southeast-2.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-08633fb9df1387bf2&osUser=ubuntu&region=ap-southeast-2&...
Services
Search
[Alt+S]
Sydney
Fabiya Chhapra
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-37-229:~$ service nginx status
● nginx.service - A high performance web server and a reverse proxy server
Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
Active: active (running) since Mon 2024-04-01 10:03:34 UTC; 1min 32s ago
Docs: man:nginx(8)
Process: 2380 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
Process: 2381 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
Main PID: 2475 (nginx)
Tasks: 2 (limit: 1121)
Memory: 4.6M
CPU: 29ms
CGroup: /system.slice/nginx.service
├─2475 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
└─2478 "nginx: worker process"
Apr 01 10:03:34 ip-172-31-37-229 systemd[1]: Starting A high performance web server and a reverse proxy server...
Apr 01 10:03:34 ip-172-31-37-229 systemd[1]: Started A high performance web server and a reverse proxy server.
ubuntu@ip-172-31-37-229:~$
i-08633fb9df1387bf2 (mywebserver)
PublicIPs: 3.106.205.199 PrivateIPs: 172.31.37.229
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
33°C
Haze
Search
15:36
01-04-2024


KEYPAIR - fabiya.s2213962
Launch an instance | EC2 |
Instances | EC2 | ap-southea
EC2 Instance Connect | ap-s
Welcome to nginx!
Not secure
3.106.205.199
Welcome to nginx!
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.
Thank you for using nginx.
33°C
Haze
Search
15:38
01-04-2024

Conclusion:

The installation of OwnCloud offers an array of security features aimed at safeguarding sensitive data. Among these, the implementation of a Strict Content Security Policy enhances protection against cross-site scripting (XSS) attacks by limiting the sources from which resources can be loaded. Additionally, encrypting data stored in session ensures that even if unauthorized access occurs, the information remains inaccessible. These security measures not only fortify the platform against potential breaches but also foster user confidence in the integrity of their data. In our experiment, the deployment of OwnCloud coupled with these robust security protocols demonstrated a tangible enhancement in data protection, reinforcing the platform's reliability for secure file storage and sharing.