**Experiment No. 7**

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

**Theory**:

In Amazon Web Services (AWS), a security group is like having bodyguards for your virtual machines (EC2 instances) in the cloud. These bodyguards protect your instances by controlling who can come in (inbound) and who can go out (outbound).

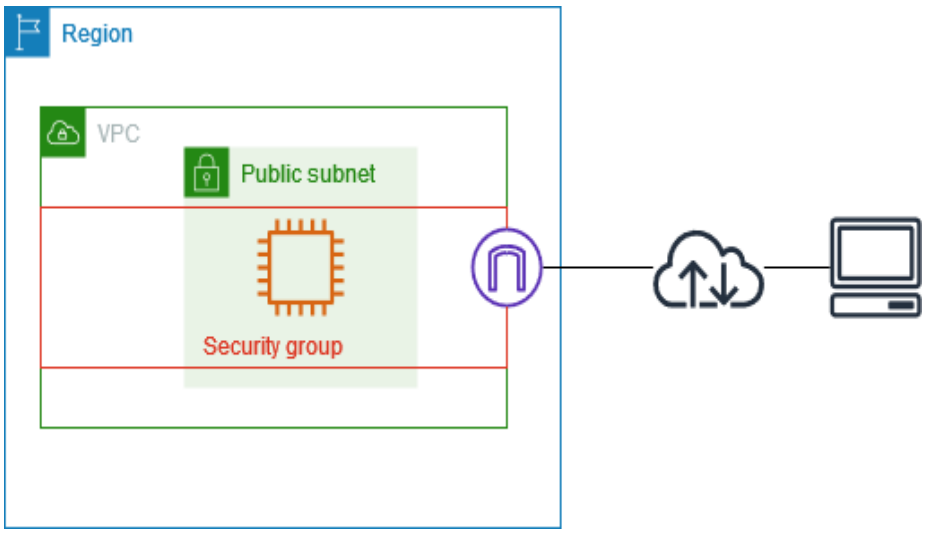
Security Group :- It's a set of rules that controls inbound and outbound traffic to and from your EC2 instances.

- Security Features of MVC Cloud: MVC Cloud's drivers for continued security improvement is to not only fix individual symptoms (e.g. insecure buffer handling, cross-site scripting) but also incorporating development lifecycle along with industry standards such as ISO/IEC 27001, COBIT and 27001.
- State Control Security Policy: Robust Security Suite (CSS) is one of the most useful and powerful web security features introduced in recent years. With CSS applications can institute the browser to follow a "Strict Security Model" including HTTPS and secure content decryption. In addition, any untrusted website content cannot be rendered.
- Data in Session is Stored Encrypted: PHP stores session related data within sessions files - usually small files on the server containing data (shared login state or the username). We have hardened the PHP Session store in such a way that the concurrent load server can only read session data at the same time the user is using MVC Cloud. This is done by encrypting the stored session data with an encryption key stored in another cookie. If the attacker gets a private copy of MVC Cloud, the encryption cookie will prevent the sync clients of the web browser private data which is not stored on the disk.
- Framework: A modern MVC-like framework to develop code for MVC Cloud. Code patching applies to protect the application code sets incorporated by MVC Cloud and specifically MVC Framework is reused by the original design of the web and authentication checks being operating rather than the more common (and less safe) operating the framework itself being injected as the session where classes cannot initiate part of MVC Cloud to secure software development lifecycle.
- 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 making a simple comparison. So in a case where the following comparison: "0 == "abc" would evaluate to true where PHP will try to convert both values (integer and boolean value) into a sametype (i.e. equal) even if the data is really not the same exact type. So it is good PHP coding practice and security guidelines for PHP to confirm that the data is exactly the same type by verifying the data type using strict comparison operators as a best practice.
- "File Firewall" using the internal file-pereval() on "own code" is memory edition purposes can run access control to allow only authorized file-fypes and a set of administration level of

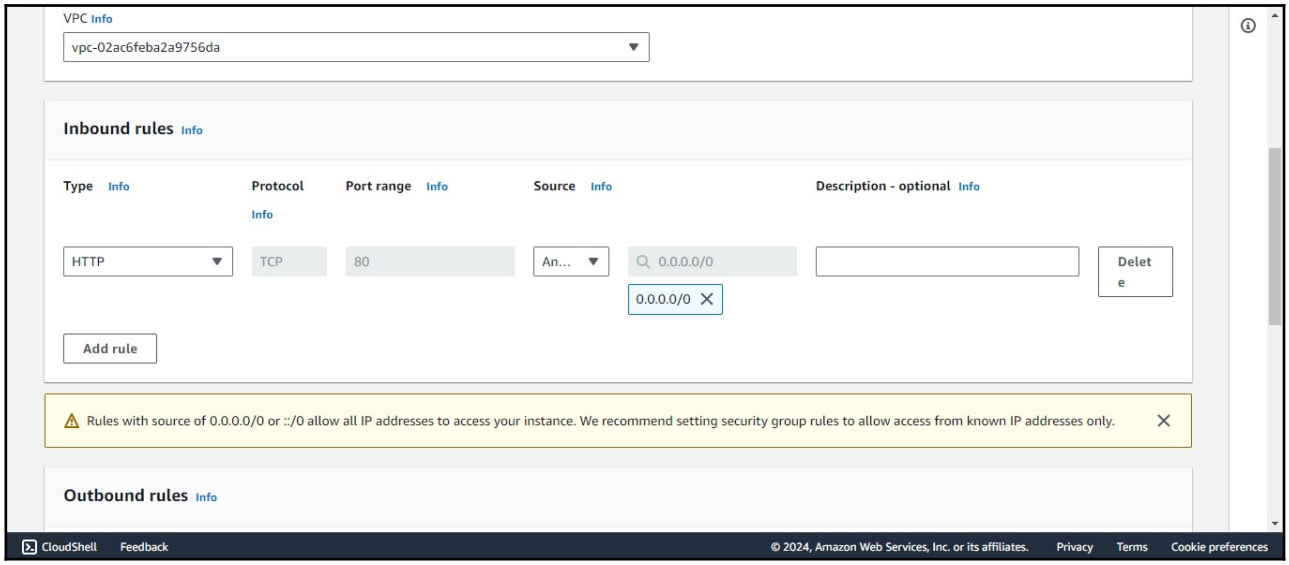
control within the app. This technique filters out any unapproved internal network outbound security allow access to shared folders only for mass-media occasion to implement internal security guidelines.

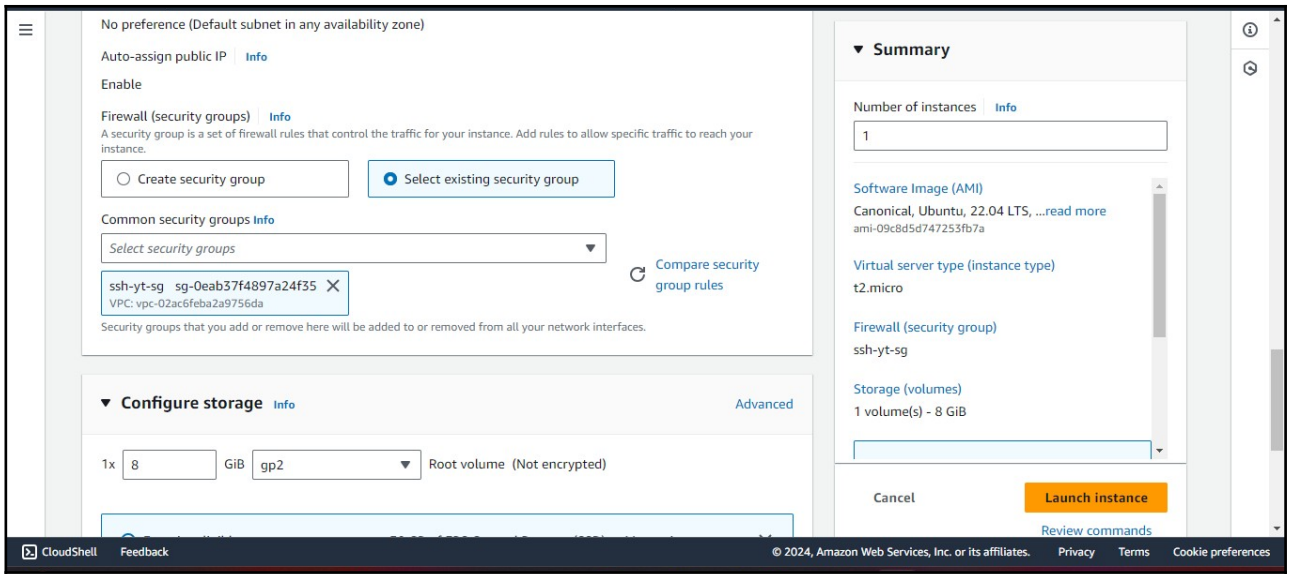
Security Group Rules:

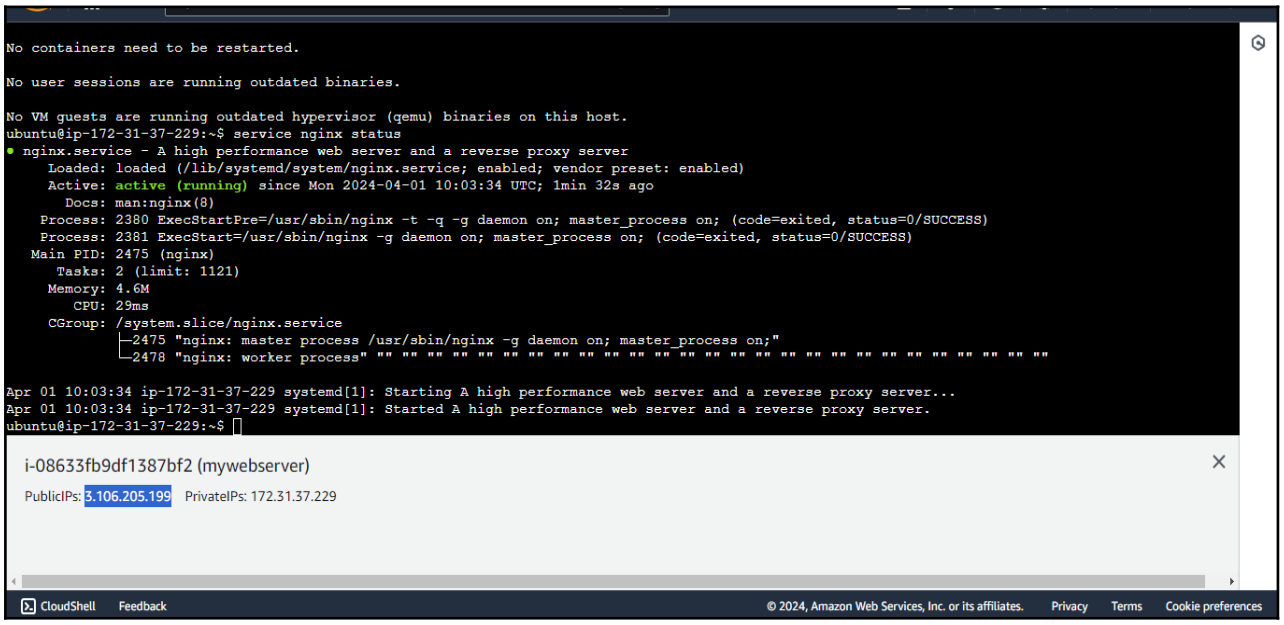
- Inbound Rules: These rules dictate who can enter your party (or access your EC2 instance). For instance, you might allow web traffic on port 80 or secure connections on port 443. In real life, these are like specifying that only guests with valid invitations can come inside your party.
- Outbound Rules: These rules determine where your guests (or your EC2 instance) can go. For example, you might allow your guests to leave and return but not take strangers with them. In AWS, this is akin to allowing your EC2 instance to connect to specific services or websites but not just anywhere on the internet.

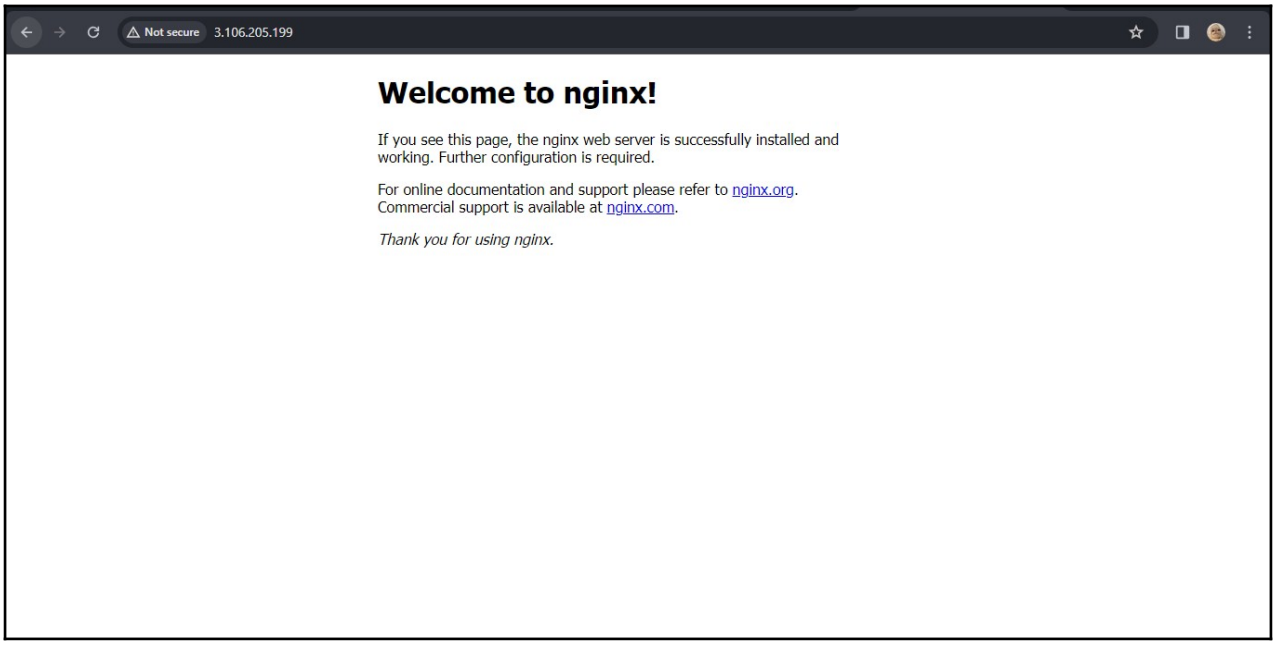



**Output:**




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


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


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.

**Conclusion:** In AWS, you can assign multiple security groups to a single instance. This allows you to apply different sets of firewall rules to control inbound and outbound traffic for that instance. Each security group acts as a virtual firewall, and the rules of all associated security groups are effectively aggregated. This approach provides flexibility and granularity in managing security for your AWS resources, enabling you to tailor access permissions based on specific requirements or roles within your infrastructure.