

LAMP:



Guide – EC2 Security Group settings to open port 80

Web Application Development COP3834

Professor Navarro

LAMP stack should be installed by this point. This is step is necessary to send http request to apache web server.

Step 1: Open AWS Management Console for instance

Step 2: From AWS Management Console, Select Security Groups

Step 3: Create Security group button on left

The screenshot shows the AWS Management Console interface. The left sidebar contains navigation links for various services. The main content area displays the 'Security Groups (1/2)' page. A table lists the security groups, and the 'sg-b07028fb' group is selected. Below the table, the details for the 'sg-b07028fb - default' group are shown, including tabs for 'Details', 'Inbound rules', 'Outbound rules', and 'Tags'. A notification banner at the bottom indicates that the Reachability Analyzer can be used to check network connectivity.

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count
launch-wizard-1	sg-03145a71b55b7b23b	launch-wizard-1	vpc-6a3a5601	launch-wizard-1 create...	624176339369	1 Permission entry
default	sg-b07028fb	default	vpc-6a3a5601	default VPC security gr...	624176339369	1 Permission entry

sg-b07028fb - default

Details | Inbound rules | Outbound rules | Tags

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Step 4: Create rules as follows and press Create Security Group at bottom right

Edit inbound rules [Info](#)

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

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info		
sgr-0049fef43c33018ad	HTTP	TCP	80	Custom	Q	all ip http traffic	Delete
sgr-04e337f2c13bb182d	HTTPS	TCP	443	Custom	Q	secure https traffic	Delete

0.0.0.0/0 X

0.0.0.0/0 X

Add rule

Set inbound and outbound rules for EC2. Specifically for port 80 inbound.

Amazon tutorial can also be found at

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Tutorials.WebServerDB.CreateVPC.html#CHAP_Tutorials.WebServerDB.CreateVPC.SecurityGroupEC2

Step 5: Check status of apache with systemctl status httpd to ensure active

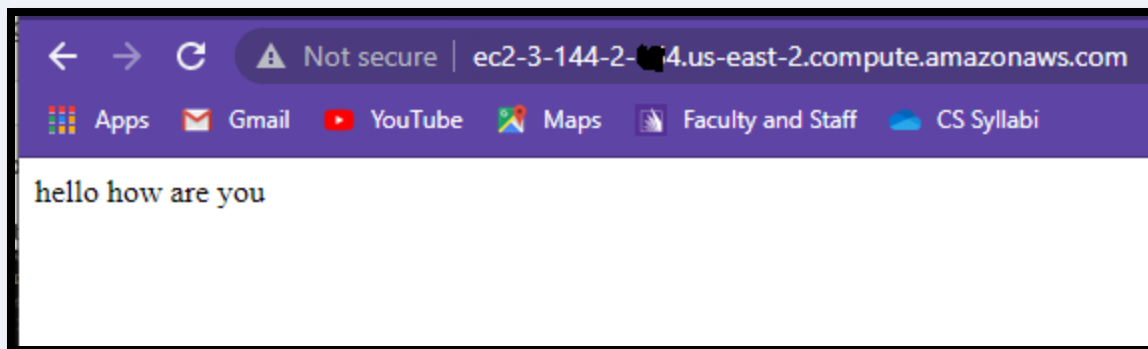
```
[ec2-user@ip-172-31-14-199 ~]$ systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Drop-In: /usr/lib/systemd/system/httpd.service.d
            └─php-fpm.conf
   Active: active (running) since Thu 2021-08-12 23:20:41 UTC; 1min 0s ago
     Docs: man:httpd.service(8)
  Main PID: 15823 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
    CGroup: /system.slice/httpd.service
            └─15823 /usr/sbin/httpd -DFOREGROUND
              15829 /usr/sbin/httpd -DFOREGROUND
              15830 /usr/sbin/httpd -DFOREGROUND
              15831 /usr/sbin/httpd -DFOREGROUND
              15832 /usr/sbin/httpd -DFOREGROUND
              15833 /usr/sbin/httpd -DFOREGROUND

Aug 12 23:20:41 ip-172-31-14-199.us-east-2.compute.internal systemd[1]: Starting The Apache HTTP Server...
Aug 12 23:20:41 ip-172-31-14-199.us-east-2.compute.internal systemd[1]: Started The Apache HTTP Server.
[ec2-user@ip-172-31-14-199 ~]$
```

Step 6: Create an index.html file to test. Place in /var/www/html directory

Step 7: Test http request to your public URL. (Use your public web address)

http:// <http://ec2-3-144-2-004.us-east-2.compute.amazonaws.com/>



Step 8: Disable apache when finished testing

```
[ec2-user@ip-172-31-14-199 ~]$ sudo service httpd stop
Redirecting to /bin/systemctl stop httpd.service
[ec2-user@ip-172-31-14-199 ~]$
```

Step 9: Review Security Group settings

EC2 > Security Groups > sg-03145a71b55b7b23b - launch-wizard-1

sg-03145a71b55b7b23b - launch-wizard-1

Actions ▼

Details

Security group name
launch-wizard-1

Security group ID
sg-03145a71b55b7b23b

Description
launch-wizard-1 created 2021-08-11T22:56:21.915-04:00

VPC ID
vpc-6a3a5601

Owner
624176339369

Inbound rules count
2 Permission entries

Outbound rules count
1 Permission entry

Inbound rules

Outbound rules

Tags

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Inbound rules (2)



Manage tags

Edit inbound rules

Filter security group rules

<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range	Source
<input type="checkbox"/>	-	sgr-0c5078521435e9e...	IPv4	SSH	TCP	22	0.0.0.0/0
<input type="checkbox"/>	-	sgr-004aeeb6450ce5069	IPv4	HTTP	TCP	80	0.0.0.0/0

Step 10: Go back and review security settings and httpd status if index.html not accessible
Complete