

# WEEK 7 ASSIGNMENT 1

Large-Scale Data Storage Systems – DATA-5400 | Spring 2020

Christina Morgenstern

---

Securing AWS resources is important to specify who can access which services as well as to keep your data protected.

## I. Creating users on AWS

Enable access to billing to other users within my account settings. Go to IAM User and Role Access to Billing Information and Activate IAM Access.

### ▼ IAM User and Role Access to Billing Information

You can give IAM users and federated users with roles permissions to access billing information. This includes access to Account Settings, Payment Methods, and Report pages. You control which users and roles can see billing information by creating IAM policies. For more information, see [Controlling Access to Your Billing Information](#).



In the Identity and Access Management section choose Users in the left hand panel.

A screenshot of the AWS Identity and Access Management (IAM) dashboard. On the left, there's a sidebar with navigation links: 'Identity and Access Management (IAM)', 'Dashboard', 'Access management' (which is expanded), 'Groups', 'Users' (which is highlighted in orange), 'Roles', 'Policies', 'Identity providers', 'Account settings', 'Access reports', 'Access analyzer', 'Analyzer details', 'Credential report', 'Organization activity', and 'Service control policies (SCPs)'. The main content area is titled 'Your Security Credentials' and contains sections for 'Password', 'Multi-factor authentication (MFA)', 'Access keys (access key ID and secret access key)', 'CloudFront key pairs', 'X.509 certificate', and 'Account identifiers'. A note at the top says: 'Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity Console.' and 'To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#)'.

To add a new user select Add user.

A screenshot of the 'Add user' page in the AWS IAM dashboard. The left sidebar shows 'Identity and Access Management (IAM)' and 'Access management' (expanded) with 'Users' selected. The main page has a header with 'Add user' and 'Delete user' buttons. It features a search bar 'Find users by username or access key' and a table with columns: 'User name' (with a dropdown arrow), 'Groups', 'Access key age', and 'Password'. A message at the bottom right says 'There are no IAM users. [Learn more](#)'. There are also 'Dashboard' and 'Roles' links in the sidebar.

The Wizard guides through the set-up process and helps specifying user details, like user name and password, as well as access information. In our case finuser1, a prospective user from the finance department, was created.

**Set user details**

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name\*  [Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type\*  **Programmatic access**  
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.

**AWS Management Console access**  
Enables a password that allows users to sign-in to the AWS Management Console.

Console password\*  Autogenerated password  Custom password  
  Show password

Require password reset  User must create a new password at next sign-in  
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

**Add user**

1 2 3 4 5

▼ Set permissions

**Get started with groups**  
You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. [Learn more](#)

► Set permissions boundary

**Add user**

1 2 3 4 5

**Review**

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

**⚠ This user has no permissions**  
You haven't given this user any permissions. This means that the user has no access to any AWS service or resource. Consider returning to the previous step and adding some type of permissions.

**User details**

User name	finuser1
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

**Tags**

No tags were added.

The previous steps were repeated to create a second user, ituser1, a potential user from the IT department.

Add user

**Success**  
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.  
Users with AWS Management Console access can sign-in at: <https://023927144627.signin.aws.amazon.com/console>

**User**

ituser1

Email login instructions

Send email

Download .csv

The assigned users finuser1 and ituser1 should be assigned to separate groups. Groups were created through navigating to the left-hand panel and selecting Create New Group.

Identity and Access Management (IAM)

Dashboard

Access management

Groups

Users

Roles

Policies

Identity providers

Account settings

Create New Group

Group Actions

Search

Showing 0 results

Group Name	Users	Inline Policy	Creation Time
No records found.			

The create New Group Wizard guides through the set-up process.

First, specify a group name, such as FinanceGroup, the group responsible for dealing with e.g. salaries.

Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

**Set Group Name**

Specify a group name. Group names can be edited any time.

Group Name:

Example: Developers or ProjectAlpha  
Maximum 128 characters

Attach group relevant policies in the second step. The FinanceGroup should have access to Billing and full S3 services. Attach the policy through searching for the respective terms and selecting the policy type.

Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

**Attach Policy**

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type -

Showing 1 results

Policy Name	Attached Entities	Creation Time
Billing	0	2016-11-10 18:33 U...

Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

**Review**

Review the following information, then click **Create Group** to proceed.

To grant your IAM users and roles access to your account billing information and tools, the root user must follow the steps to enable billing access in [this procedure](#)

Group Name	FinanceGroup	Edit Group Name
Policy	arn:aws:iam::aws:policy/job-function/Billing	Edit Policies

Identity and Access Management (IAM)

Dashboard

Access management

**Groups**

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzer details

Credential report

Organization activity

Service control policies (SCPs)

Search IAM

IAM > Groups > FinanceGroup

Summary

Group ARN: arn:aws:iam::023927144627:group/FinanceGroup

Users (in this group): 0

Path: /

Creation Time: 2020-03-01 11:52 UTC+0100

Users Permissions **Access Advisor**

Managed Policies

The following managed policies are attached to this group. You can attach up to 10 managed policies.

Attach Policy

Policy Name	Actions
Billing	Show Policy   Detach Policy   Simulate Policy

Inline Policies

Repeat the steps for attaching a further policy that allows for full access to S3.

Attach Policy

AmazonS3ReadOnlyAccess

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type ▾ QS3 Showing 4 results

	Policy Name	Attached Entities	Creation Time
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	0	2016-04-20 19:05 U...
<input checked="" type="checkbox"/>	AmazonS3FullAccess	0	2015-02-06 19:40 U...
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	0	2015-02-06 19:40 U...
<input type="checkbox"/>	QuickSightAccessForS3StorageManagementAnalyticsReadOnly	0	2017-06-12 20:18 U...

The FinanceGroup has obtained permissions to access the billing and S3 full access.

Identity and Access Management (IAM)

Dashboard

Access management

**Groups**

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzer details

Credential report

Organization activity

Service control policies (SCPs)

Search IAM

AWS account ID:

IAM > Groups > FinanceGroup

Summary

Group ARN: arn:aws:iam::023927144627:group/FinanceGroup

Users (in this group): 0

Path: /

Creation Time: 2020-03-01 11:52 UTC+0100

Users Permissions **Access Advisor**

Managed Policies

The following managed policies are attached to this group. You can attach up to 10 managed policies.

Attach Policy

Policy Name	Actions
AmazonS3FullAccess	Show Policy   Detach Policy   Simulate Policy
Billing	Show Policy   Detach Policy   Simulate Policy

Inline Policies

Add finuser1 to the FinanceGroup.

User Name	Groups	Password	Password Last Used	Access Keys	Creation Time
<input checked="" type="checkbox"/> finuser1	0	✓	Never	None	2020-03-01 11:4...
<input type="checkbox"/> ituser1	0	✓	Never	None	2020-03-01 11:5...

Summary of FinanceGroup with one user.

User	Actions
finuser1	<a href="#">Remove User from Group</a>

Selecting policies can also be done in one go through ticking the relevant policy names from the list. The ITGroup should get full access to both, EC2 and S3.

Policy Name	Attached Entities	Creation Time
AmazonEC2ContainerRegistryFullAccess	0	2015-12-21 18:06 U...
AmazonEC2ContainerRegistryPowerUser	0	2015-12-21 18:05 U...
AmazonEC2ContainerRegistryReadOnly	0	2015-12-21 18:04 U...
AmazonEC2ContainerServiceAutoscaleRole	0	2016-05-13 01:25 U...
AmazonEC2ContainerServiceEventsRole	0	2017-05-30 18:51 U...
AmazonEC2ContainerServiceforEC2Role	0	2015-03-19 19:45 U...
AmazonEC2ContainerServiceFullAccess	0	2015-04-24 18:54 U...
AmazonEC2ContainerServiceRole	0	2015-04-09 18:14 U...
<input checked="" type="checkbox"/> AmazonEC2FullAccess	0	2015-02-06 19:40 U...
AmazonEC2ReadOnlyAccess	0	2015-02-06 19:40 U...
AmazonEC2RoleforAWSCodeDeploy	0	2015-05-19 20:10 U...
AmazonEC2RoleforDataPipelineRole	0	2015-02-06 19:41 U...

The ituser1 has access to EC2 and S3.

User ARN: arn:aws:iam::023927144627:user/ituser1  
Path: /  
Creation time: 2020-03-01 11:50 UTC+0100

**Permissions** **Groups (1)** **Tags** **Security credentials** **Access Advisor**

**Add permissions** **Add inline policy**

Policy name	Policy type
Attached from group	
AmazonEC2FullAccess	AWS managed policy from group ITGroup
AmazonS3FullAccess	AWS managed policy from group ITGroup
Permissions boundary (not set)	

Summary of groups and assigned users.

**Add user** **Delete user**

User name	Group	Access key age	Password age	Last activity	More
finuser1	FinanceGroup	None	Today	None	Nc
ituser1	ITGroup	None	Today	None	Nc

To confirm the settings and permissions of each user, log onto the console using my Account ID as well as user name and password of either the two users, ituser1 and finuser1, as specified above.

Log on as ituser1 who has access to S3 and EC2.

**EC2**

**Resources**

You are using the following Amazon EC2 resources in the Europe (Frankfurt) Region:

Running instances	0	Elastic IPs	0
Dedicated Hosts	0	Snapshots	0
Volumes	3	Load balancers	0
Key pairs	1	Security groups	3
Placement groups	0		

**Account attributes**

Supported platforms: VPC, Default VPC (vpc-72cb0918), Console experiments, Settings

**Explore AWS**

Optimize your EC2 cost and performance with Spot Instances, Combine EC2 On-Demand,

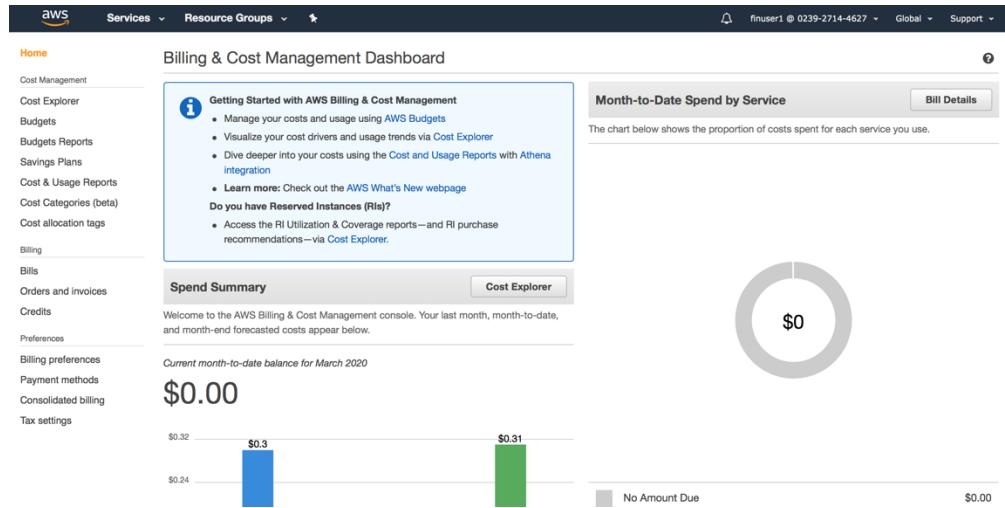
Access to billing information by ituser1 is prohibited.

**Billing & Cost Management Dashboard**

**You Need Permissions**

You don't have permission to access billing information for this account. Contact your AWS administrator if you need help. If you are an AWS administrator, you can provide permissions for your users or groups by making sure that (1) this account allows IAM and federated users to access billing information and (2) you have the required IAM permissions.

In contrast, finuser1, can see the billing and cost management dashboard.



However, setting up an EC2 instance is not possible for the finuser1.

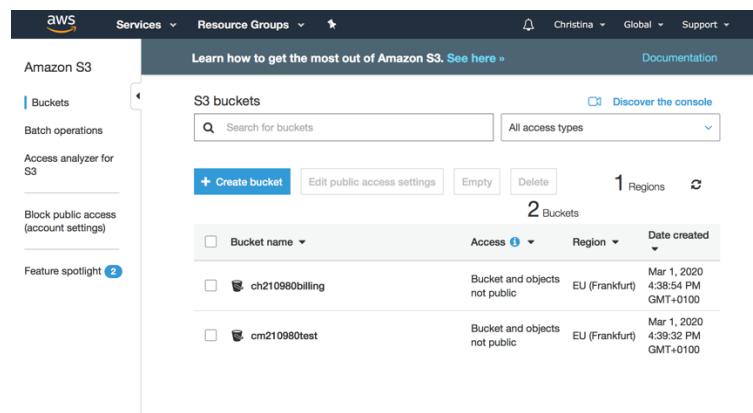
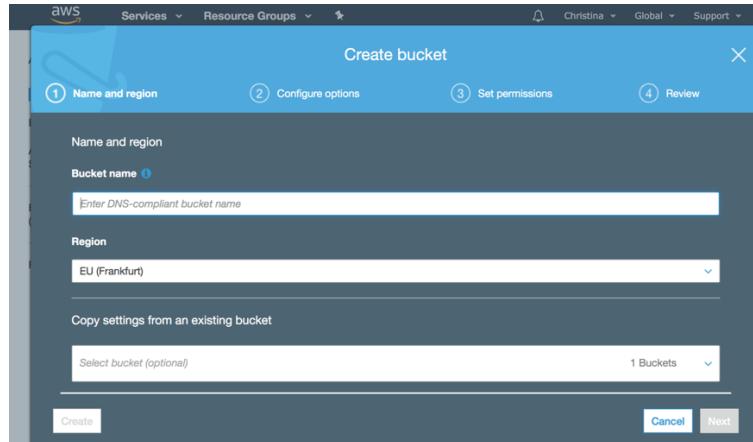
The screenshot shows the "Step 1: Choose an Amazon Machine Image (AMI)" page of the EC2 instance creation wizard. The user is on step 1, "Choose AMI". An error message in a red-bordered box says "An error occurred describing your selected AMI. You are not authorized to perform this operation." Below the message is a search bar with placeholder text "Search for an AMI by entering a search term e.g. "Windows"" and a "Select" button. To the left is a "Quick Start" sidebar with "My AMIs", "AWS Marketplace", and "Community AMIs". On the right, there's a list of AMIs, with the first one being "Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0df0e7600ad0913a9 (64-bit x86) / ami-0a3ab28b9d065f7c5 (64-bit Arm)". It shows it's "Free tier eligible". There are checkboxes for "64-bit (x86)" and "64-bit (Arm)".

Delete groups and users as follows:

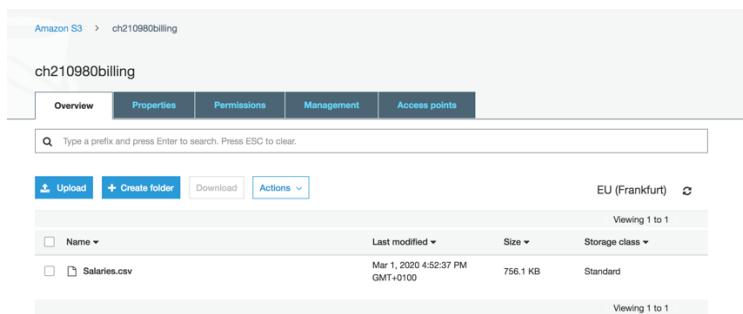
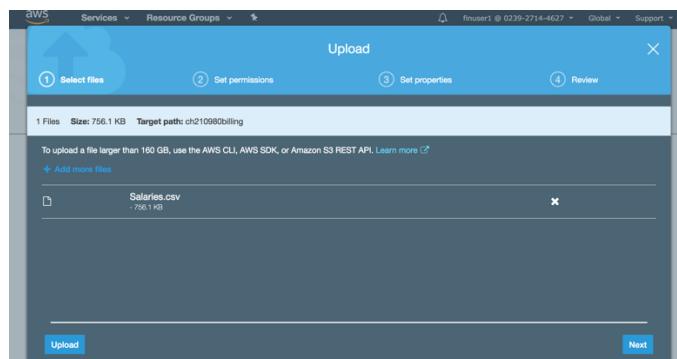
The screenshots show the AWS IAM console. The top one shows the "Groups" page under "Access management". A context menu is open over the "Delete Group" option for the "FinanceGroup". The bottom one shows the "Users" page under "Access management". A context menu is open over the "Delete user" option for the "finuser1" user. Both pages have a sidebar with links for Identity and Access Management (IAM), Dashboard, Access management (Groups, Users, Roles, Policies, Identity providers, Account settings), and a search bar.

## II. S3 bucket policy

Create an S3 bucket named ch210980billing within the console.



Upload the file salaries.csv into the bucket.



Create a bucket policy so that only User1 can read the contents.

Select the Permissions tab

Block public access (bucket settings)  
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. 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 and its access points. 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  
On

Block public access to buckets and objects granted through new access control lists (ACLS)  
On

Edit

The AWS Policy Generator wizard helps in creating policies controlling AWS resources. Select S3 Bucket Policy as Policy Type. The effect should be a Deny, because we would like to block access to the S3 bucket.

#### AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see [key concepts in Using AWS Identity and Access Management](#). Here are [sample policies](#).

#### Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Select Type of Policy  S3 Bucket Policy

#### Step 2: Add Statement(s)

A statement is the formal description of a single permission. See [a description of elements](#) that you can use in statements.

Effect  Allow  Deny

Principal

AWS Service   All Services (\*)

Actions   All Actions (\*)

Amazon Resource Name (ARN)   
ARN should follow the following format: arn:aws:s3:::<bucket\_name>/<key\_name>. Use a comma to separate multiple values.

Add Conditions (Optional)

The Policy Generator produces a JSON file which needs to be amended in the Resource section and the AWS section. In this case ituser1 is prohibited from gaining access to the S3 billing bucket because it contains information on salaries.

```
{ "Id": "Policy1583077539435", "Version": "2012-10-17", "Statement": [ { "Sid": "S1", "Action": "s3:*", "Effect": "Deny", "Resource": "arn:aws:s3:::ch210980billing", "Principal": { "AWS": "arn:aws:iam::023927144627:user/ituser1" } } ] }
```

This AWS Policy Generator is provided for informational purposes only. You are responsible for your use of Amazon Web Services features and services that you enable through this generator.

Close

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.  
An [amazon.com](#) company

The screenshot shows the AWS IAM Policy Generator interface. At the top, there's a text area with the message: "The block public access settings turned on for this bucket prevent granting public access." Below this is a code editor containing a JSON policy document:

```

1 {
2   "Id": "Policy1583077539435",
3   "Version": "2012-10-17",
4   "Statement": [
5     {
6       "Sid": "Stmt1583077535920",
7       "Action": "s3:*",
8       "Effect": "Deny",
9       "Resource": "arn:aws:s3:::ch210980billing",
10      "Principal": [
11        "*"
12      ]
13    }
14  ]
15 }
16 }
17 }

```

At the bottom of the page, there are links for "Documentation" and "Policy generator".

When logging onto the console as the ituser1 and trying to access the S3 bucket ch210980billing, an error message occurs and I am blocked from accessing the resource.

The screenshot shows the AWS S3 Buckets list. On the left sidebar, there are links for "Buckets", "Batch operations", "Access analyzer for S3", "Block public access (account settings)", and "Feature spotlight". The main area displays the "S3 buckets" section with a search bar and a dropdown for "All access types". It shows two buckets:

Bucket name	Access	Region	Date created
ch210980billing	Error	EU (Frankfurt)	Mar 1, 2020 4:38:54 PM GMT+0100
cm210980test	Bucket and objects not public	EU (Frankfurt)	Mar 1, 2020 4:39:32 PM GMT+0100

The screenshot shows the details page for the S3 bucket "ch210980billing". The top navigation bar includes "Console Home", "Amazon S3", and the bucket name. The main content area has tabs for "Overview", "Properties", "Permissions", "Management", and "Access points". The "Properties" tab is selected. A red-bordered box highlights an "Error" message: "Access Denied". Below it is a search bar with the placeholder "Type a prefix and press Enter to search. Press ESC to clear." At the bottom, there are buttons for "Upload", "Create folder", "Download", and "Actions". The region is listed as "EU (Frankfurt)".

### III. Modify EC2 security settings

Start the Linux virtual machine MyLinuxVM1 within the EC2 dashboard.

The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with 'INSTANCES' expanded, showing 'Instances' and other options like 'Instance Types' and 'Launch Templates'. The main area displays three instances: MyLinuxVM1 (running), MyLinuxVM2 (stopped), and WindowsVM (stopped). A context menu is open over MyLinuxVM1, listing actions: Connect, Get Windows Password, Create Template From Instance, Launch More Like This, Instance State (with 'Start' highlighted), Instance Settings, Image, Networking, CloudWatch Monitoring, and Terminate. Below the instance list, a detailed view for MyLinuxVM1 shows its instance ID (i-01f90f8dc091d7704), state (stopped), type (t2.micro), and various network and security details.

This screenshot shows the same EC2 dashboard interface. The 'INSTANCES' section is expanded, and the 'Instances' tab is selected. The table lists three instances: MyLinuxVM1 (running), MyLinuxVM2 (stopped), and WindowsVM (stopped). Below the table, a detailed view for MyLinuxVM1 is shown, mirroring the information from the previous screenshot but with slightly different visual styling.

Try to ping the VM using the Terminal window on my Mac.  
ping IP address

A screenshot of a Mac OS X terminal window titled 'Christina — ping 18.184.154.138 — 80x24'. The user has run the command 'ping 18.184.154.138'. The terminal output shows the following:

```
Last login: Sun Mar  1 17:15:48 on ttys000
(base) Christinas-MacBook-Pro:~ Christina$ ping 18.184.154.138
PING 18.184.154.138 (18.184.154.138): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
```

Ping doesn't allow to connect to the VM by default.

Amend the security settings to allow ping and launch the wizard.

Security groups [launch-wizard-1. view inbound rules. view outbound rules](#)

Scheduled events [No scheduled events](#)

The screenshot shows the AWS EC2 Security Groups page. On the left, there's a sidebar with links like 'New EC2 Experience', 'EC2 Dashboard', 'Events', 'Tags', 'Reports', 'Limits', 'INSTANCES', 'Instances', 'Instance Types', 'Launch Templates', and 'Create Document'. The main area has a search bar with 'Group ID : sg-0a143b9d239d61f7a' and a table with one row:

Name	Group ID	Group Name	VPC ID	Owner
sg-0a143b9d239d61f7a	launch-wizard-1	vpc-72cb0918	023927144627	lau

Below this, there's a detailed view for 'Security Group: sg-0a143b9d239d61f7a'. It shows tabs for 'Description', 'Inbound' (which is selected), 'Outbound', and 'Tags'. Under 'Edit', there's a table with one rule:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	

Edit inbound rules through adding a new rule.

The screenshot shows the 'Edit inbound rules' dialog box. It has fields for 'Type' (SSH), 'Protocol' (TCP), 'Port Range' (22), 'Source' (Custom, 0.0.0.0/0), and 'Description' (e.g. SSH for Admin Desktop). A note at the bottom says: 'NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.' At the bottom right are 'Cancel' and 'Save' buttons.

## Edit inbound rules

This rule should allow connecting from my IP address to the VM using ping.

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
All ICMP - IPv4	ICMP	0 - 65535	My IP 193.80.81.122/32	e.g. SSH for Admin Desktop

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

[Cancel](#) [Save](#)

Overview of security settings of MyLinuxVM1.

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	
All ICMP - IPv4	All	N/A	193.80.81.122/32	

Ping is now enabled with my IP address.

```
Christina — ping 18.184.154.138 — 80x24
PING 18.184.154.138 (18.184.154.138): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
Request timeout for icmp_seq 8
^C
--- 18.184.154.138 ping statistics ---
10 packets transmitted, 0 packets received, 100.0% packet loss
(base) Christina-MacBook-Pro:~ Christina$ ping 18.184.154.138
PING 18.184.154.138 (18.184.154.138): 56 data bytes
64 bytes from 18.184.154.138: icmp_seq=0 ttl=244 time=34.979 ms
64 bytes from 18.184.154.138: icmp_seq=1 ttl=244 time=36.365 ms
64 bytes from 18.184.154.138: icmp_seq=2 ttl=244 time=35.241 ms
64 bytes from 18.184.154.138: icmp_seq=3 ttl=244 time=35.629 ms
64 bytes from 18.184.154.138: icmp_seq=4 ttl=244 time=35.226 ms
64 bytes from 18.184.154.138: icmp_seq=5 ttl=244 time=34.116 ms
64 bytes from 18.184.154.138: icmp_seq=6 ttl=244 time=34.609 ms
64 bytes from 18.184.154.138: icmp_seq=7 ttl=244 time=34.683 ms
```

Once the previously generated permission is removed, ping is disabled again.

```
--- 18.184.154.138 ping statistics ---
20 packets transmitted, 20 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 33.297/34.891/36.365/0.680 ms
(base) Christina-MacBook-Pro:~ Christina$ ping 18.184.154.138
PING 18.184.154.138 (18.184.154.138): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
```