kontikilabsInternal Documentation

Release 0.1

Tanya Thakur

Jan 04, 2018

Contents

This is a guide for writing consistent and pleasing code. The guide rules out the important commenting structure to be followed by the Kontiki Labs engineering team.

CHAPTER 1

The Standard Code Writing & Commenting Format

1.1 Create a New File

Whenever you create a new file, the first line of the file should start with a comment dedicated to the file. The comment structure should be like

```
/*****************************************************************
// @desc             : A short description of the file
// @author           : The name of the developer creating the file
// @files_required   : Name the required system files
// @requested_modules: Name the module dependencies, if any
// @created_date     : Time and date when the file is created.
*****************************************************************/
```

1.2 Functions

It is important that we **write meaningful function names**, following the *lowerCamelCase* naming convention.

Before you start writing the method, you should include a comment stating its purpose. Remember, to indicate the data type for a `@param` or `@return` tag, put the data type in {} brackets

```
/*****************************************************************
// @desc    : A short description of the function
// @param   : {data_type_1} paramName1, {data_type_2} paramName2
// @return  : {data_type}
*****************************************************************/
```

Example

```
function processOrder (pdt, x) {      # Note spaces before, after function_name &␣
↪parenthesis
        const MAX_ITEMS = 10;         # maximum number of packets
```

```
        const MASK = 0x1F;          # mask bit TCP
        return true;
}

Avoid obvious comments such as:
-------------------------------------------------------------------------------------------
↪-----------------------------------------------------------------
if (a == 5)       // a equals 5
counter = 0;      // setting the counter to zero

Try to write comments that explain higher level mechanisms or clarify difficult␣
↪segments of your code. Do not use comments to restate trivial things.
```

1.3 Variables

Variables names should use *lowerCamelCase*. They should also be descriptive. Single character variables and uncommon abbreviations should generally be avoided

```
var stringMatches = item.match(/ID_([^\n]+)=([^\n]+)/);  # Execute a regex : Add a␣
↪comment to a global variable
-------------------------------------------------------------------------------------------
↪-----------------------------------------------------------------
var numberCount = 0;   # The local variables need not to be described each time.␣
↪Don't wastes your time writing needless comments.
```

1.4 Special Tags

When working on code as a team, adopt a consistent set of tags to communicate among programmers. For example, use a **TODO:** tag to indicate a section of code that requires additional work

```
function estimate (x, y) {
    // TODO: implement the calculations
    return 0;
}
```

Few special tags are

```
-------------------------------------------------------------
| BUG    - a known bug that should be corrected.            |
-------------------------------------------------------------
| FIXME  - should be corrected.                             |
-------------------------------------------------------------
| HACK   - a workaround.                                    |
-------------------------------------------------------------
| TODO   - something to be done.                            |
-------------------------------------------------------------
| UNDONE - a reversal or "roll back" of previous code.      |
-------------------------------------------------------------
| UX     - user experience, notice about non-trivial code.|
-------------------------------------------------------------
```

1.5 End of the File

Signal the end of any file with the comment structure as below

```
/*****************************************************************
// EOF : File_Name (Signal the end of a file)
/*****************************************************************
```

1.6 Committing the Code

Follow the below guidelines while pushing the code to the GIT repository:

- Always create a README.md file using the Markdown Language format.
- While pushing the code to the repo, add a valid description of the work you have done.
- Commit code in batches, please avoid small code commits.

CHAPTER 2

Get started with Docker

Docker is an open platform for developers and sysadmins to build, ship, and run distributed applications, whether on laptops, data center VMs, or the cloud.

Follow the guide below to know all the important docker commands.

2.1 Get started with Docker

2.1.1 Install Docker

Docker is available on multiple platforms. Check the following link to choose the best installation path for you:

- Docker for Mac (macOS)
- Docker for Windows (Microsoft Windows 10)

If the above does not fulfil your requirements follow the link here .

2.1.2 Create & Execute the Dockerfile

Docker automatically build images by reading the instructions you provide in the `Dockerfile`. A `Dockerfile` is a text document that contains all the command a user could call on the command line to assemble an image.

The `Dockerfile` must start with the `FROM` instruction. Below is an example of a `Dockerfile`

```
# base image
FROM ubuntu:latest

# clean and update sources
RUN apt-get clean && apt-get update

# install basic apps
RUN apt-get install -qy nano
```

```
# install Python and modules
RUN apt-get install -qy python3
RUN apt-get install -qy python3-psycopg2
```

Follow this link to know more about creating a `Dockerfile`.

- To login into your account

```
$ docker login
```

- Executing the `Dockerfile` commands

```
To directly execute the file command use:
$ docker build . (With this command <none> repo is created. To avoid this use the␣
↪next command)
Sending build context to Docker daemon 5.51 MB
...

You can specify the name of the repository with:
$ docker build -t your_name .
```

2.1.3 View all the Images

- To view all the top level images run

```
$ docker images

The output:

REPOSITORY    TAG       IMAGE ID       CREATED          SIZE
--------------------------------------------------------------
your_name     latest    d6e415a70abf   8 seconds ago    210MB
ubuntu        latest    747cb2d60bbe   2 weeks ago      122MB
```

The above output states that the repository `ubuntu` is the base image, because of the `FROM ubuntu:latest` command in the Dockerfile.

The `your_name` image is the combination of all the packages mentioned in the Dockerfile.

- To delete the images

```
$ docker rmi image_id
```

2.1.4 Containers

Docker containers ensures that the software will behave the same way, regardless of where it is deployed, because its runtime environment is ruthlessly consistent.

- To create a container in your image use

```
$ docker run -ti image_name

Where :
        -       t : gives us the terminal
        -       I : allows us to interact with the terminal
```

```
Output - root : root@contaner_id:/#
```

- To exit from the container

```
root : root@contaner_id:/# exit
```

- To Check all containers in your image

```
To list all the containers:
$ docker ps -a

To check the running container:
$ docker ps
```

- To delete the container

```
$ docker rm contaner_id
```

2.1.5 Image to Docker Cloud

- Search command to find suitable image

```
$ docker search image_name
```

Below is a screenshot for : `docker search ubuntu`

```
Tanyas-MacBook-Air:~ tanya$ docker search ubuntu
NAME                                                DESCRIPTION                                     STARS               OFFICIAL            AUTOMATED
ubuntu                                              Ubuntu is a Debian-based Linux operating s...   6714                [OK]
dorowu/ubuntu-desktop-lxde-vnc                      Ubuntu with openssh-server and NoVNC            139                                     [OK]
rastasheep/ubuntu-sshd                              Dockerized SSH service, built on top of of...   113                                     [OK]
ansible/ubuntu14.04-ansible                         Ubuntu 14.04 LTS with ansible                   87                                      [OK]
ubuntu-upstart                                      Upstart is an event-based replacement for ...   80                  [OK]
neurodebian                                         NeuroDebian provides neuroscience research...   40                  [OK]
ubuntu-debootstrap                                  debootstrap --variant=minbase --components...   31                  [OK]
nuagebec/ubuntu                                     Simple always updated Ubuntu docker images...   22                                      [OK]
tutum/ubuntu                                        Simple Ubuntu docker images with SSH access     19
1and1internet/ubuntu-16-nginx-php-phpmyadmin-mysql-5   ubuntu-16-nginx-php-phpmyadmin-mysql-5          16                                      [OK]
ppc64le/ubuntu                                      Ubuntu is a Debian-based Linux operating s...   11
aarch64/ubuntu                                      Ubuntu is a Debian-based Linux operating s...   9
i386/ubuntu                                         Ubuntu is a Debian-based Linux operating s...   8
darksheer/ubuntu                                    Base Ubuntu Image -- Updated hourly             3                                       [OK]
codenvy/ubuntu_jdk8                                 Ubuntu, JDK8, Maven 3, git, curl, nmap, mc...   3                                       [OK]
1and1internet/ubuntu-16-nginx-php-5.6-wordpress-4   ubuntu-16-nginx-php-5.6-wordpress-4             2                                       [OK]
1and1internet/ubuntu-16-apache-php-7.0              ubuntu-16-apache-php-7.0                        1                                       [OK]
pivotaldata/ubuntu-gpdb-dev                         Ubuntu images for GPDB development              0
pivotaldata/ubuntu                                  A quick freshening-up of the base Ubuntu d...   0
1and1internet/ubuntu-16-healthcheck                 ubuntu-16-healthcheck                           0                                       [OK]
thatsamguy/ubuntu-build-image                       Docker webapp build images based on Ubuntu      0
1and1internet/ubuntu-16-sshd                        ubuntu-16-sshd                                  0                                       [OK]
ossobv/ubuntu                                       Custom ubuntu image from scratch (based on...   0
defensative/socat-ubuntu                                                                            0                                       [OK]
smartentry/ubuntu                                   ubuntu with smartentry                          0                                       [OK]
Tanyas-MacBook-Air:~ tanya$
```

- To pull the image

```
$ docker pull username/repo_name:tag_Name
```

- To commit the image

```
$ docker tag IMAGE_ID username/repo_name:tag_Name
```

- To push the image

```
$ docker push username/repo_name:tag_Name
```

CHAPTER 3

Server Security With AWS

Server Security should be of highest priority for any developer. Therefore in order to maintain a secure environment it is important to understand the **Amazon Web Service (AWS).**

AWS allows customers to experiment while keeping security its utmost priority.

3.1 Server Security With AWS

3.1.1 Elasticsearch Services (Amazon ES)

Amazon ES is an open-source search engine. We will access the Amazon ES Service via the Amazon ES console which can create, configure, and monitor your domains and upload data.

Click on the Elasticsearch Service from the list of AWS service displayed. The next action displays the list of existing Elasticsearch domains.

On selecting the desired Domain, the domain configurations which have already been set are displayed. Let us see how you can manage the domain security from here.

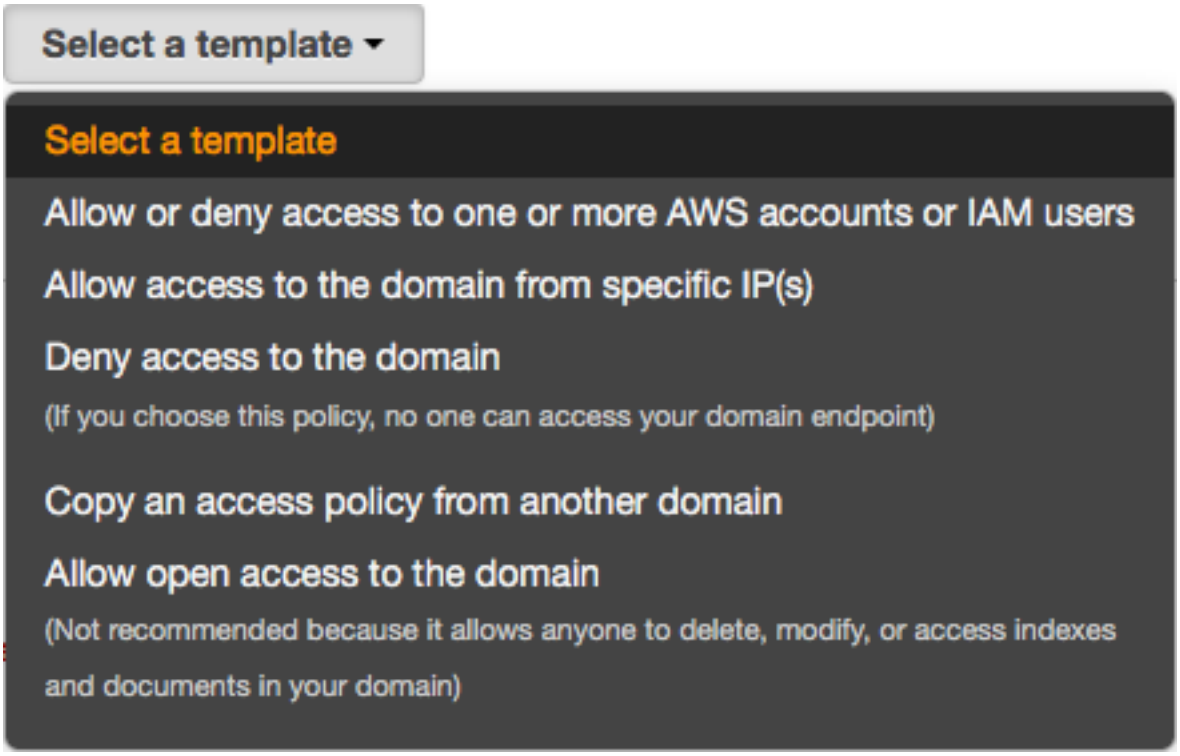
Configure Cluster

Amazon ES EndPoints

A domain search endpoint for uploading data and submitting search requests. Using this, you can access the configuration API and have domain-specific endpoints for accessing the search API.

Modify the access policy

This section lets you allow or block access to your selected domain. You can directly edit the access policy from *'Add or edit the access policy'* or you can opt for any one of the policy templates from the *'Select a template'* dropdown list as displayed below.



Access Policies	Description
Allow or deny access to one or more AWS accounts or IAM users	Allow or deny access to one or more AWS accounts or IAM users
Allow open access to the domain	This policy is not recommended because it allows anyone to delete, modify, or access indexes and documents in your domain. It is intended only as a convenience for testing. Don't load sensitive data to a domain that has these settings.
Deny access to the domain	This policy allows access only through the Amazon ES console or or by the owner of the AWS account who created the domain.
Allow access to the domain from specific IP(s)	This policy is used to restrict anonymous access to a specific IP address. It also allows us to add multiple IP addresses The activation process takes 10-15 mins
Copy access policy from another domain	This policy provides a convenient way to import an existing access policy from another domain.

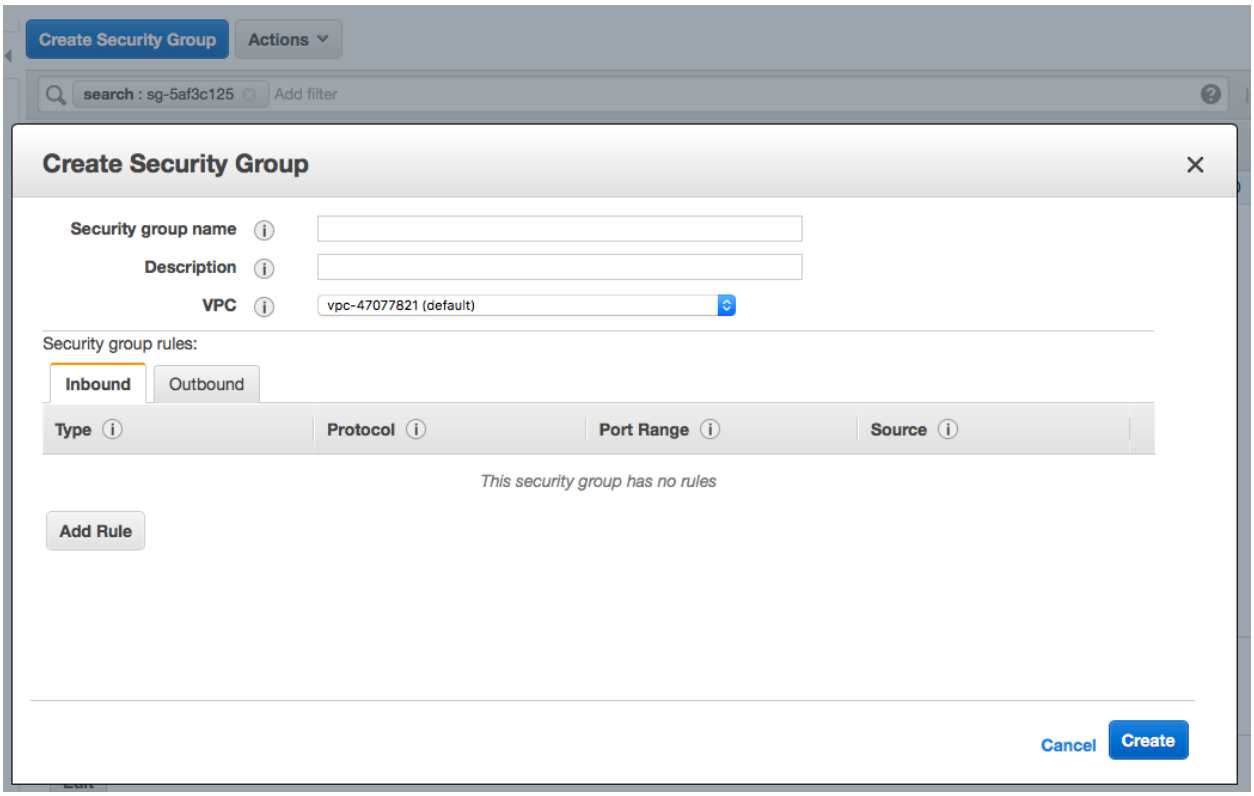
3.1.2 Amazon Elastic Compute Cloud (Amazon EC2)

Amazon EC2 provides scalable computing capacity in the AWS cloud. You can use Amazon EC2 to launch as many, or as few virtual servers as you need, configure security and networking, and manage storage.

Select 'Running Instances' from the Amazon EC2 resources. The running instance displays a list of already created servers. Each instance can be assigned a particular security group.

Security Group

A virtual firewall that controls the traffic for one or more instances. Whenever an instance is launched, it is important that at least one security group is assigned to the instance for reliability. You can create a security group from the below screen which appears on clicking on the existing security group or while creating a server.



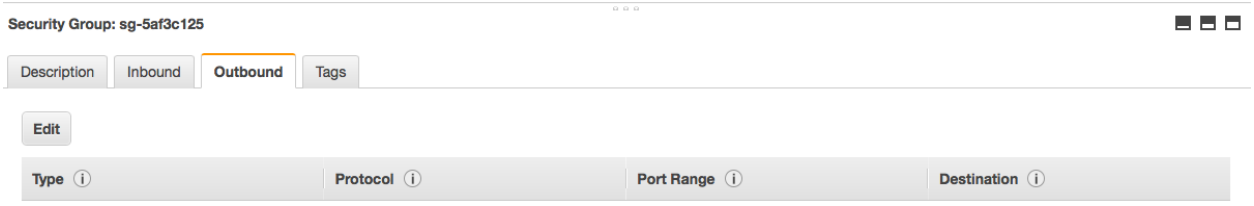
Security Group Rules

Outbound: Protects against outgoing traffic from the enterprise network.By default, all the outbound traffic is allowed.

Protocol type	Port number	Destination IP
All	All	0.0.0.0/0

Inbound: Protects the network against incoming traffic from the internet. You can set the inbound rules as:

Protocol type	Port number	Destination IP
TCP	22 (SSH)	203.0.113.1/32
TCP	80 (HTTP)	0.0.0.0/0
ICMP	All	0.0.0.0/0



3.1.3 Amazon Simple Storage Service (S3)

Storage space for images, videos and anything which needs a link format to be displayed publicly.

Create bucket and select it from the list of buckets displayed and go to the permissions tab to manage the control.

Bucket Policy Tab

Opt for the *'policy generator'* option, present below the text area to set the bucket policies. Policy generator is a tool that enables you to create policies that control access to AWS products and resources.

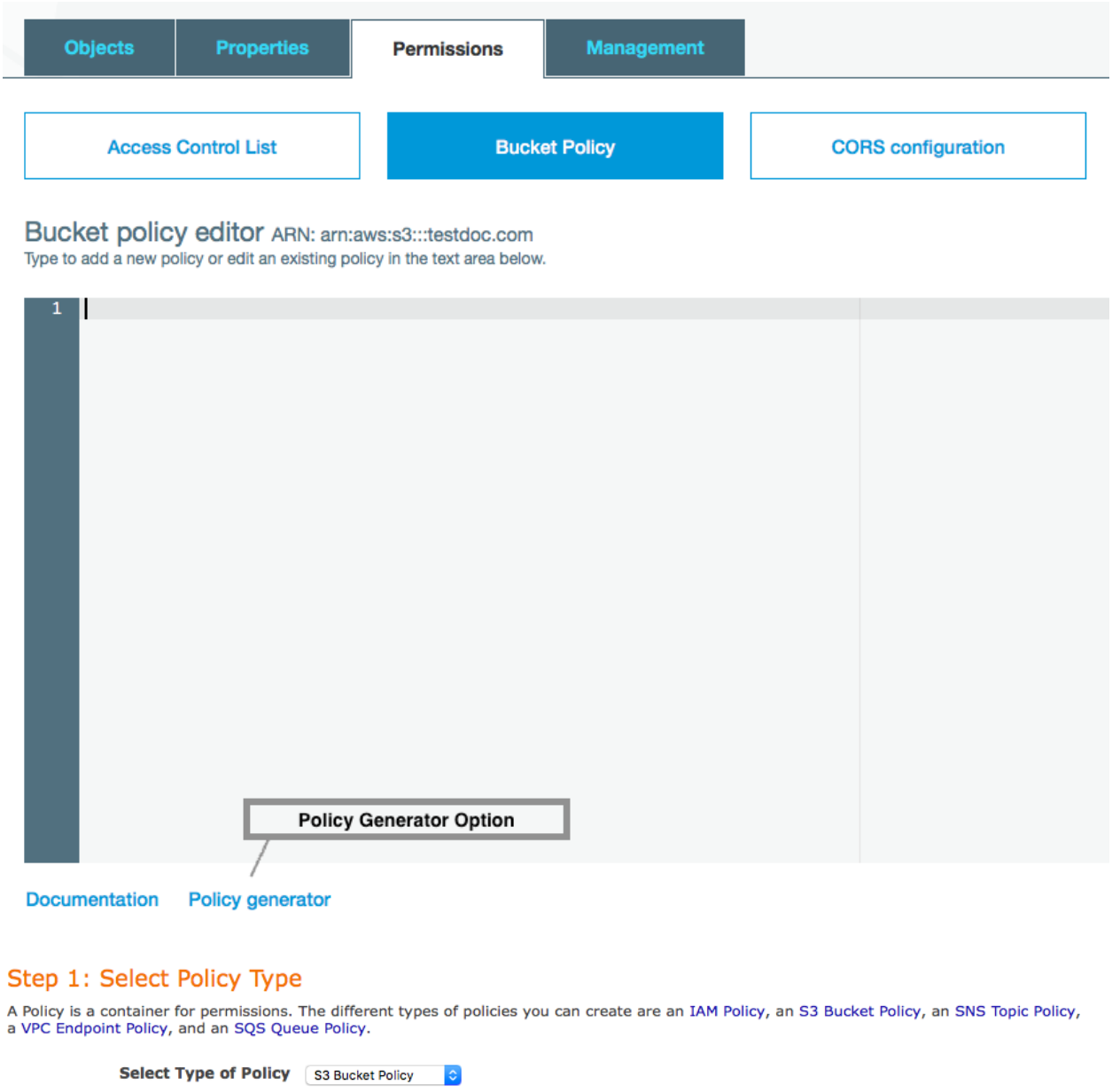
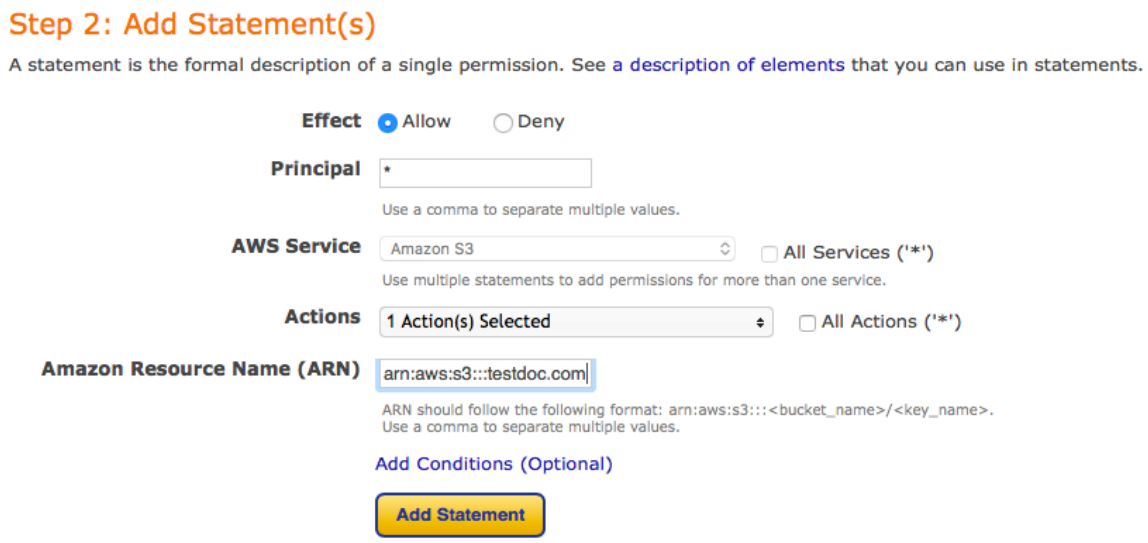


Fig. 3.1: Choose the 'S3 Bucket Policy' from the drop down.



Option	Description
Effect	Specifies whether the statement will result in allow or an explicit deny.
Principle	Specify the user (IAM user, federated user, or assumed-role user), AWS account, AWS service, or other principal entity that is allowed or denied access to a resource. We use * to give every one access.
Actions	Describes the specific action or actions that will be allowed or denied.
ARN	Amazon Resource Name (ARN) condition operators let you construct condition elements that restrict access based on comparing a key to an ARN.

How to copy ARN and use it?

- Go to the bucket list and click on your desired bucket row.
- A popup will appear on your right side allowing you to copy the 'Bucket ARN'
- Add '/<key_name>' at the end of 'arn:aws:s3:::<bucket_name>'. We use '*' to give access to all uploaded files.
- Use the file name, if you want a particular file to be exposed publicly and use comma to separate the names.

Click on '*Add statement'* after completing the 2 steps. You will then be asked to confirm the statement. Next proceed with the '*Generate policy*' button that gives you policy JSON document. Paste the JSON on policy generator text area under the '*Bucket Policy*' tab of Amazon S3.

CORS configuration Tab

Cross origin resource sharing defines a way for client web applications that are loaded in one domain to interact with resources in a different domain.

```
<!-- Sample policy -->
<CORSConfiguration>
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <MaxAgeSeconds>3000</MaxAgeSeconds>
        <AllowedHeader>Authorization</AllowedHeader>
    </CORSRule>
</CORSConfiguration>
```

All the above steps will help you secure our server. In order to get your AWS credentials, please contact Anurag Mishra, our Server Admin.