Show Submission Credentials

# P0. Cloud Best Practices Best practices to follow on Cloud Platforms such as AWS, Azure, and GCP

- ✔ Cloud Best Practices
- ✔ Amazon Web Services
- ✔ Microsoft Azure
- ✔ Google Cloud Platform

Cloud Best Practices

## Cloud Best Practices

AWS, Azure, and Google Cloud Platform (GCP) are large-scale, shared cloud resources that are used by millions of users around the world. This differs significantly from the computing resources that you have been using elsewhere.

We will be covering the best practices followed when adopting the cloud, they apply to different cloud platforms and will help you better manage your resources throughout this course.

### Tagging Your Resources

Tags enable you to categorize your resources in different ways, for example, by purpose, owner, or environment. A tag is a key-value pair that users can add to the cloud resource which in itself doesn't have any semantic meaning, but acts as a metadata that external applications could use. They are interpreted strictly as a string of characters by the Cloud Service Providers (CSP). Tagging can be utilized to review past resource needs as well as in

making future budget projections. Tagging is a practice adopted by all cloud users and it is one of the learning objectives in our course. Therefore, you are recommended to tag your resources in each project.

## Managing Costs

Learners must use the cloud resources judiciously. Project modules have cost suggestions (budgets) which learners should follow to the letter and spirit. Learners will be held accountable for excessive usage of cloud resources. Learners will be expected to monitor their CSP usage and will be responsible for terminating their resources upon the completion of a project module.

## Protecting Cloud Credentials

Bots are scanning publicly available files for cloud credentials, aiming at compromising your account and launch as many resources for crypto mining, DDOS, etc.

You should never put any of your credentials in files on public Github, Dropbox, Google Drive, etc.

In this course, you will make use of the APIs of AWS, GCP or Azure for your projects. Make sure that you do **NOT** submit your code with such credentials in it.

Amazon Web Services

# Amazon Web Services

## Working with IAM Users

AWS strongly suggests against using the AWS account root user (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html) for everyday usage. Instead, AWS recommends that you follow the best practice of creating an IAM user that has the minimum set of permissions required. To get started with this process you may refer to the following references:

1. The AWS Intro primer
2. Creating Your First IAM Admin User and Group (https://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started_create-admin-group.html)
3. AWS IAM Users (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html)

## Tagging Your Amazon EC2 Resources

To help you manage your instances, images, and other Amazon EC2 resources, you can optionally assign your own metadata to each resource in the form of tags. Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it. Each tag consists of a key and an optional value, both of which you define.

**Adding tags while launching an EC2 instance:**

1. Follow the usual steps of Launching an EC2 instance, ie, on your EC2 dashboard click on **Launch Instance** and then:
    - Choose an AMI
    - Select an Instance Type
    - Configure Instance Details
    - Add Storage
2. Step 5 in the Launch Instance page is "Add Tags". Enter the Key and Value into it respectively for the tags that you have been instructed to add and even those that you wish to add.
3. Continue with Configuring your Security Group and later clicking on launching the instance.

**Updating tags for the active instances:**

1. In your EC2 Instances (https://console.aws.amazon.com/ec2/v2/home) page, select the VM whose tags you want to update.
2. You should see a *Tags* tab, select that.
3. Click on *Manage Tags* to create new tags or update existing ones.

**Special step for spot instances:**

When you Request Spot Instances you follow the same steps of configuring the instance and adding tags to it from the Spot Requests (https://console.aws.amazon.com/ec2sp/v1/spot/home) page. On completing the request, the tags are not automatically added to the instance that is spawned for this Spot request. Therefore, after placing the spot request, you should visit the EC2 Instances (https://console.aws.amazon.com/ec2/v2/home) page and wait for the instance to spawn. As soon as you see an entry for the new VM, follow the instructions given in "Updating tags for the active instances".

Tags don't have any semantic meaning to AWS and are interpreted strictly as a string of characters. Also, tags are not automatically assigned to your resources. You can use these tags to check your expenses per tag by visiting the Cost Explorer (https://console.aws.amazon.com/cost-reports/home) and filtering by Tag.

**Note:** All the tag keys and values are **case sensitive**. Each project in this course will require you to use special tags. Please make sure that you use the tags correctly.

# Pricing Calculators for Cost Estimation

AWS has the AWS Pricing Calculator (https://calculator.aws/#/) in which you could specify the AWS resources you would be using (such as EC2, S3, etc.) and AWS will calculate the Estimated Monthly Bill for the specified resources. AWS uses their regulated cost for providing an estimate, pricing for spot instances is not used in this estimate.

## Spot Instances

Spot instances in AWS offer significant cost savings to regular on-demand instances, especially for more powerful instance types. Students should use spot instances whenever possible, except for services that need to be kept alive for instructor assessment. Using spot instances for long-running, mission-critical tasks is not recommended as your instances could be terminated due to price fluctuations.

# Protecting Cloud Credentials

**Periodically Clearing up Old Certificates**

Certificates in the form of Key Pairs, PEM file that is used for authentication should be cleared up periodically. These files in the wrong hands could provide access to malicious users which could affect your setup deployed on the cloud.

**AWS Access Keys in code**

Amazon provides APIs via their Software Development Kits which enable you to access AWS services from your preferred programming language. To successfully send requests to AWS APIs, you need to have a valid set of security credentials called access keys. These access keys have two parts, Access key ID and Secret access key.

Access keys are primarily used by AWS for two purposes:

- Check who sent the API request.
- Determine if that user is allowed to do what they're asking to do.

Hence, the access keys are required to be present in your API calls but its cleartext presence in the code will make it visible to everyone who has access to your source code. They can use these keys in their application to impersonate you for getting access to the AWS and may cause harm to your Cloud setup.

To avoid using access keys in cleartext in your code, one approach would be to fetch those access keys from the environment variables. In your code, you can get these keys using the language specific APIs ( `System.getenv` in Java and `os.environ` in Python). When this code goes into the hands of other users, they won't be able to see the keys, and the code wouldn't run as their machine's environment variables do not have the access keys defined.

Microsoft Azure

# Microsoft Azure

## Tagging your Azure Resources

Similar to Tags in AWS and Labels in GCP, Azure uses the term Tags for all resources. Every resource that we create on Azure has an option to add tags in that resource's page.

After adding the required tags on your respective resources, you can look up for resources based on the tags. To see that, go to Console Menu -> Click on More services -> Enter "Tags" in the filter that shows up and click on the Tags you wish to see.

For more information, please visit Using tags to organize your Azure resources (https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags).

## Pricing Calculator on Azure

Microsoft Azure provides a Pricing Calculator (https://azure.microsoft.com/en-us/pricing/calculator/). Click on "+Add Items" to add the resources you plan to use and it will show you the estimate for all the resources added on the right hand side.

## Billing Alerts for Microsoft Azure Subscriptions

Azure also provides a billing alert service. In this course, you will be given an Azure coupon. The billing alert service will be immensely helpful to send out warnings when you exceed a threshold. To enable billing alerts, follow the instructions to Set up billing alerts for your Microsoft Azure subscriptions (https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/cost-mgt-alerts-monitor-usage-spending).

Google Cloud Platform

# Google Cloud Platform

## Tagging Your Google Compute Instances

A GCP label is a key-value pair that helps you group related or associated resources on Google Cloud. A common use of labels is for cost accounting or budgeting. You can create GCP budget alerts (https://cloud.google.com/billing/docs/how-to/budgets) to monitor the cost, and use labels to break down the cost.

# Price Calculators for Cost Estimation

GCP has Google Cloud Platform Pricing Calculator (https://cloud.google.com/products/calculator/) using which you could specify the GCP resources and services you would be using. Fill in the form and GCP will calculate the Estimated Total Cost for the resources you will be using.

# Budgets and Alerts

GCP can help you with project planning and controlling costs. You can set a budget which lets you track how your spend is growing towards that amount.

You can apply a budget to either a billing account or a project, and you can set the budget at a specific amount or match it to the previous month's spend. You can also create alerts to notify billing administrators when spending exceeds a percentage of your budget.

To create a budget:

1. Go to the Google Cloud Platform (https://console.cloud.google.com) page
2. Click on the console menu (which lists the products & services on the top left) and go to the Billing (https://console.cloud.google.com/billing/) page.
3. Choose Budgets & alerts and click on Create Budget.
4. In the Create budget page:
    - Give a budget name
    - Choose if you wish to apply this budget for the entire billing account or a specific project
    - Specify a budget amount
    - You can specify various budget to alert (ie at various percentages).
5. Click on Save and you should see the budget in the index page.