# Cloud Transformation

Getting Started

# CraigKeenan.Info: Lesson and Lab Guide

# Lesson Primer

## Cloud Transformation - What and Why?

What are we learning?

Hopefully, you are reading this to learn about Amazon Web Services (AWS) and Cloud Computing.

Why learn AWS?

- If you are employed or intend to be employed in the Information Technology (IT) field, Cloud Computing is quickly becoming the road map to the future. Its benefits include ease of use, secure, scalable, reliable, flexible and cost-effective. AWS is empowering businesses, and developers to focus on growing their businesses, not their IT budgets.
- If you know nothing about IT, Great! We'll teach you, step-by-step, how to leverage Cloud Computing. In a few lessons, we will build a scalable WordPress website, and that is only the beginning.
- Most important with AWS, you can sign up for a 12-Month Free Tier Account. Free is a great price!

## Who is the intended audience?

These lessons are intended for everyone. Like AWS, we want to share with you for Free. We will provide you reading material, hands-on labs, and HINTs. You can gain experience at your own pace as you follow these lessons. We do have to make some basic assumptions. You are approximately 18 years old (AWS offers certifications. More on this in a minute). You have proficient reading/writing comprehension skills. You have access to a personal computer with Internet Access. You have a smart phone that supports applications. Because we want to speak to a broad audience we will assume little to no IT background.

## Lesson/Lab Format

We will begin each lesson with a brief overview (primer). The next section, and bulk of the material, is hands on labs. You will require an AWS account for the lab. We will provide a lab overview, explaining the goal of the experiment. We will conclude all lessons by providing a technical deep-dive (Knowledge Base), a lesson summary, and appendix if needed for supplemental information.

We will cover a massive amount of material. AWS offers nearly 1000 services. Each service has its own required knowledge. We ask that at the beginning you accept that we cannot provide detailed explanation for all topics. The intention is to chunk up the material into small manageable chunks, and let you digest it versus overloading you with information.

In an effort to provide a comprehensive set of procedures, we strive to present related operations. For example, if we create an IAM User, then we provide steps to delete the IAM user. Often times we want you to create, modify, delete some resource a few times to practice and learn. In other cases, we are just pointing out the steps and commands. To guide you, we have highlighted the steps we want you to perform.

## Teaching Method

We believe that experience is the best teacher. Therefore our lessons are lab driven. We do provide you with an extensive amount of reading material. You can read the lessons at your own pace, before, during or after the lab. Our observations with our own Cloud Transformation was that we really started learning, not from what we had read, but from what we had done.

These lessons and labs have been designed to get you working with those services, to build a procedure repository you can reference, and identify where you can locate the vendor documentation for additional

support. Most importantly, we want you to do, not listen or read. Practice, make mistakes, be confused, and let the learning begin.

## Training Material

The definitive source for knowledge is the respective vendors, their documentation and customer support services. Most of the information, including procedures, are taken directly from vendor documentation. Every section begins with a URL link to the respective documentation. The challenge is that there is a large amount of documentation. There are literally dozens of guides and thousands of pages of material. This is where we add our value. We will structure and filter that information, and present it to you in small pieces. At the same time, we reference the source material. By leveraging the original documents, we maintain a consistent look and feel as you switch between this document and the source. For the labs, we highlight in yellow any activity you must perform, and highlight in grey any data/information you must provide.

## What is expected of our Students?

We expect and hope that our students want to learn AWS Cloud Computing services. Please read the material carefully. You can perform most labs within Free Tier. However, you **MUST** clean up after each lab, and not leave services and resources running when they are not needed. If you do, you will be billed for those services and resources. We will identify when a lab will incur charges, typically we can do all the labs for a few dollars in one month. You can decide only to read the section of the lab, and not incur any costs.

When you read the Knowledge Base and Summary sections, is your choice. We have ordered it lab first, then provide you a technical review and summary. You can read this material before doing the labs, if you prefer. Our recommendation is you try the labs first, read the material, then if needed go back and perform the labs again until you are comfortable with the material.

## Creating a Sharing Economy in the Cloud Transformation

If you have heard of Uber, then you are familiar with the concept of "Sharing Economy". It is an umbrella term often used to describe social and economic activity. It grew out of the open-source community to refer to peer-to-peer based sharing of good and services. We are trying to extend that activity to Cloud Transformation.

Our theory is simple. We invested dozens of hours to create notes and procedures to assist us in learning AWS. We believe it was a great aid in our own learning. As far as we are concerned, it was time/money well spent. But we can exponential increase the scope of that learning by sharing freely with others. Now you can follow a similar path without having to invest the time to write the notes and procedures. This allows you to dedicate that time to other important activities. Imagine if we extended that time savings by a few million people. That's hundreds of millions of hours of saved labor. We can accomplish more as team than as individuals.

## Additional Training

If you are interested in lecture style lessons and video demonstration of the labs, Acloud.Guru offers great courses at a reasonable price. They offer a Solutions Architect Associate course for $29. We used it and were very happy with the results. They do NOT provide written notes or procedures. We can assist you there.

## A Final Word about Certifications

Things change very quickly in the technology world. Will Amazon Web Services be relevant in the future? Hard to say. In 2015, AWS did approximately $6.5 billion in revenue. In 2016, they did nearly $13 billion. They offer both Associate and Profession level certifications on a few separate tracks (Solutions Architect, DevOps, and SysOps). One of 2016's most desired certifications was the Solutions Architect with an average salary of $125K.

We can't promise you'll get the certification or the salary, but we can do our best you give you a solid foundation, knowledge base, and shared procedures. The rest is up to you!

We strive to create lessons and procedures that are consistent, repeatable and still flexible. It's a fine balance to provide the needed information without being so verbose it becomes a lecture. Backing every lab and lessons is the link to the vendor's documentation. Remember, we have filtered it down for you. Please feel free to explore the links to the vendor. Its many pages of great information. It is there as a reference. If you choose to follow every link, you'll spend dozens of hours reading. We are not suggestion you read every link, but reference those where you are unsure of the information as we have provided it to you. We will be straight forth with you from the beginning, you will HAVE to do a lot of reading. It's just a lot of material. The trick is to identify the Key Understanding required to pass the certifications.

**HINT** Compare the number of pages in each Knowledge Base to the number of pages in the lesson summary.

# Before you begin

Before you begin your Cloud Transformation, you will need to have think about a few things. Two topics you should have considered are which Identity you will use, and what will be your Domain Name.

## Choose your Identity

AWS Account – It is recommended you setup an account using an appropriate name, and isolated from your other Social Media identities. A good example would be your full name and possible Month/Day of your birth to ensure account name is unique. Keep in mind you may eventually want to share your account with others.

## Choose your Domain

Domain Name – While not strictly necessary, it is recommended that you establish a domain name, and register that domain with a Domain Registrar (i.e. GoDaddy, AWS). There are several labs that will utilize AWS Route 53 for DNS, and while you can follow along, it is recommended you create your own domain. You don't have to do it now, as we will do in a later lesson, but give some thought to a name for your domain.

## Lab Overview

Throughout all lessons, we will be acting as if we are an individual who is looking to get started with Amazon Web Services Cloud Computing. Fortunately, we have a friend who is a Cloud Guru, and this friend has agreed to guide us through the process. Our goal is to build a web site for our product/service. It can be anything we want it to be. For teaching purposes, we'll call our experiment OurAmazonWebServices (**OAWS**).

Note: When you see an example using **oaws** or **ouraws** in the name, you must replace with a name unique to your environment.

Before we get started building our web site, or deploying any applications, we will need to setup an account. While we are setting up the account, we will also enable billing notifications. Unfortunately, we are operating on a minimal budget (less than $1/month). That's OK, some really big accomplishments have started as really small ideas.

# Getting Started - Lab Overview

## Account Setup

- ☐ Create Google Account
- ☐ Create AWS Account
- ☐ Login to AWS Management Console
- ☐ Create a Budget
- ☐ Create a Billing Alarm

## Identity and Access Management

- ☐ Customize IAM User Sign-In Link
- ☐ Create IAM Group
- ☐ Create IAM User
- ☐ Add/Remove Users in an IAM Group
- ☐ Login to AWS Management Console using IAM Users Sign-In link
- ☐ Login to AWS Management Console as Root Account using MFA
- ☐ Delete IAM User
- ☐ Delete IAM Group

## Cleanup!

- ☐ Created a Billing Alarm!
- ☐ Enable MFA on Root Account
- ☐ Created Administrator Privilege Group and User(s)

# Lab - Getting Started!

## Account Setup

### Create Google Account

URL Link: https://accounts.google.com/signup

It's free to create a Google Account. You can use the username and password for your Google Account to sign in to Gmail and other Google products like YouTube, Google Play and Google Drive.

1. Visit the Google Account creation page (https://accounts.google.com/signup)
2. Follow the step on screen to complete your account setup.
3. After you've created you Google Account, you can use it to sign in to Gmail on your computer, phone or tablet.

**Note**: After account creation, you may be prompted to verify your account by sending validation code to your mobile to complete account setup.

### Creating an Amazon Web Services Account

URL Link: http://aws.amazon.com

When you create an account, AWS automatically signs up the account for all services. You are charged only for the services you use.
The AWS Free Tier enables you to gain free, hands-on experience with the AWS platform, products, and services.

**To create an AWS account**

1. Go to http://aws.amazon.com, and click Create an AWS Account.
2. Follow the on-screen instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a PIN using the phone keypad.

**Note**: Use the google account you created for Amazon Web Service Account.

During setup you will be prompted to provide a credit card.

You will only be billed for services you use.

We will be using Free Tier services wherever possible

When asked to choose a support plan. Choose Basic.

### The Root Account Sign-in Page

URL Link: URL Link: http://docs.aws.amazon.com/IAM/latest/UserGuide/console.html

When users sign in to your AWS account, they sign in via the account sign-in page.

If you want to sign in to the console using your AWS root account credentials instead of IAM user credentials, go to the account sign-in page and then click Sign in using root account credentials. The Amazon Web Services sign-in page appears that you can use to sign in with your AWS root account credentials.

**You can sign in to the AWS Management Console using your root AWS account credentials at:**

https://console.aws.amazon.com/console/home.

## Create a Budget

URL Link: http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/budgets-create.html

A budget is a way to plan your usage and your costs (also known as spend data), and to track how close your usage and costs are to exceeding your budgeted amount. Budgets provide you with a quick way to see your usage-to-date and current estimated charges from AWS, and to see how much your predicted usage accrues in charges by the end of the month.

You can create budgets to track your usage and costs.

**To create a budget**

1. Sign in to the AWS Management Console and open the Billing and Cost Management console at https://console.aws.amazon.com/billing/home#/.
2. On the navigation pane, choose **Budgets**.
3. At the top of the page, choose **Create Budget**.
4. Under **Budget details**, for **Name**, type the name of your budget.
   Your budget name must be unique within your account, and can use A-Z, a-z, spaces, and the following characters: _.:/=+-%@
   **(Ex. MonthlyBudget)**
5. For **Select cost or usage**, choose **cost**.
6. For **Period**, choose how often you want the budget to reset the actual and forecasted spend. Choose **Monthly**.
7. (Optional) For **Start date**, budget defaults to the first date of the current month.
8. For **Budgeted Amount**, enter the total amount that you want to use or spend for this budget period.
   (Ex. $1)
   (Optional) Under **Notifications**, define the notifications that you want this budget to have. If you do not want notifications, leave the **Notifications** fields blank.
9. For **Notify me when**, choose actual cost (**Actual).**
10. For **usage is**, choose the comparison operator that you want your budget to use.
    (Ex. greater than)
11. For **% of budgeted usage**, type the percentage of the budget that you want to be notified at.
    (Ex. 50%)
12. (Optional) For **Email contacts**, type the email addresses that you want the notifications to be sent to. Separate multiple email addresses with a comma. A notification can have up to ten email addresses.
    (Ex. username@gmail.com)
13. Choose **Create**.

## Creating a Billing Alarm

URL Link: http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/free-tier-alarms.html

**Creating a Billing Alarm**

Even if you're careful to stay within the free tier, it's a good idea to create a billing alarm to notify you if you exceed the limits of the free tier.
After you complete this procedure, you'll receive an email as soon as your account's usage exceeds the free tier limits.

**Create a Billing Alarm to Notify You if Your Usage Exceeds the Free Tier**

To create a billing alarm, you must first enable billing alerts. The following procedure explains how.

**To enable billing alerts**

Before you create a billing alarm, you must enable billing alerts. You need to do this only once. After you enable billing alerts, you can't turn them off.

1. Sign in to the AWS Management Console and open the Billing and Cost Management console at https://console.aws.amazon.com/billing/home#/.
2. On the navigation pane, choose **Preferences**.
3. Select the **Receive Billing Alerts** check box.
4. Choose **Save preferences**.

Once you have enabled billing alerts, you can create a CloudWatch billing alarm.

**To create a billing alarm**

1. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
2. If necessary, change the region on the navigation bar to US East (N. Virginia). The billing metric data is stored in this region, even for resources in other regions.
3. On the navigation pane, under **Alarms**, choose **Billing**.
4. Choose **Create Alarm**.
5. Define the alarm as follows.

a. If you want the alarm to trigger as soon as you go over the free tier, set **When my total AWS charges for the month exceed** to $.01.
b. Choose the **New list** link next to the **send a notification to** box.
c. When prompted, enter your email address.
d. Choose **Create Alarm**.

## Identity & Access Management (IAM)

### Customize IAM User Sign-in Link

URL Link: http://docs.aws.amazon.com/IAM/latest/UserGuide/console.html

Users who want to use the AWS Management Console must sign in to your AWS account through a sign-in page that's specific to your account. You provide your users with the URL they need to access the sign-in page. You can find the URL for your account sign-in on the dashboard of the IAM console.

If you want the URL for your sign-in page to contain your company name (or other friendly identifier) instead of your AWS account ID, you can create an alias for your AWS account ID.

**To create or remove an account alias**

1. Sign in to the IAM console at https://console.aws.amazon.com/iam/.
2. On the navigation pane, select **Dashboard**.
3. Find the **IAM users sign-in link**, and click **Customize** to the right of the link.
4. Type the name you want to use for your alias, then click **Yes, Create**.
5. To remove the alias, click **Customize**, and then click **Yes, Delete**. The sign-in URL reverts to using your AWS account ID.
   Recommendation is replace account number and use your Domain Name
   (Ex. https://ouraws.signin.aws.amazon.com/console)

### Create IAM Group

URL Link: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups_create.html

To set up a group, you need to create the group, give it permissions based on the type of work that you expect the users in the group to do, and then add users to the group.

**To create an IAM group and attach policies (AWS Management Console)**

1. Sign in to the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, click **Groups** and then click **Create New Group**.
3. In the **Group Name** box, type the name of the group and then click **Next Step**.

   **Important** Group names must be unique within an account. They are not distinguished by case, for example, you cannot create groups named both "ADMINS" and "admins".

   (Ex. oawsAdminGroup)
4. In the list of policies, select the check box for each policy that you want to apply to all members of the group. Then click **Next Step**.
5. Click **Create Group**.

## Create IAM User (Console)

URL Link: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_create.html

**Creating an IAM User in Your AWS Account**

You can create one or more IAM users in your AWS account. You might create an IAM user when someone joins your organization, or when you have a new application that needs to make API calls to AWS.

**Creating IAM Users (Console)**

**To create one or more IAM users from the AWS Management Console**

1. Sign in to the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose **Users** and then choose **Add user**.
3. Type the user name for the new user.

   (Ex. oawsAdmin)
4. Select the type of access this set of users will have. You can select programmatic access to the APIs, AWS CLI, and Tools for Windows PowerShell, access to the AWS Management Console, or both.

   Select **AWS Management Console access**

   (Optional) We recommend that you choose **Require password reset** to ensure that users are forced to change their password the first time they sign in.
5. Choose **Next: Permissions**.
6. On the **Set permissions** page, specify how you want to assign permissions to this set of new users. Choose the following option:

   **Add user to group**.
7. Choose **Next: Review** to see all of the choices you made up to this point. When you are ready to proceed, choose **Create user**.
8. Provide each user with his or her credentials. On the final page you can choose **Send email** next to each user. Your local mail client opens with a draft that you can customize and send. The email template includes the following details to each user:
   a. User name
   b. URL to the account sign-in web page. Use the following example, substituting the correct account ID number or account alias: https://*AWS-account-ID or alias*.signin.aws.amazon.com/console

**Important** The user's password is **not** included in the generated email. You must provide them to the customer in a way that complies with your organization's security guidelines.

## Adding and Removing Users in an IAM Group

URL Link: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups_manage_add-remove-users.html

At any time, you can add users to or remove users from an IAM group. This is useful as people enter and leave your organization.

### To add a user to an IAM group

1. AWS Management Console: In the navigation pane, choose **Groups** and then choose the name of the group.
2. Choose the **Users** tab and then choose **Add Users to Group**.
3. Select the users you want to add and then choose **Add Users to Group**.

### To remove a user from an IAM group

1. AWS Management Console: In the navigation pane, choose Groups and then choose the name of the group.
2. Choose the Users tab and then choose Remove Users from Group.
3. Select the users you want to add and then choose Remove Users from Group.

## Setting an Account Password Policy for IAM Users

URL Link: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

**Setting an Account Password Policy for IAM Users**

You can set a password policy on your AWS account to specify complexity requirements and mandatory rotation periods for your IAM users' passwords. You can use a password policy to do these things:

- Set a minimum password length.
- Require specific character types, including uppercase letters, lowercase letters, numbers, and non-alphanumeric characters. Passwords are case sensitive.
- Allow all IAM users to change their own passwords.
- Require IAM users to change their password after a specified period of time (enable password expiration).
- Prevent IAM users from reusing previous passwords.
- Force IAM users to contact an account administrator when the user has allowed his or her password to expire.

**Setting a Password Policy (AWS Management Console)**

You can use the AWS Management Console to create, change, or delete a password policy. As part of managing the password policy, you can let all users manage their own passwords.

**To create or change a password policy**

1. Sign in to the IAM console at https://console.aws.amazon.com/iam/
2. In the navigation pane, click Account Settings.
3. In the Password Policy section, select the options you want to apply to your password policy.
4. Click Apply Password Policy.

**To delete a password policy**

1. Sign in to the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, click Account Settings, and then in the Password Policy section, click Delete Password Policy.

## Activate MFA on Root Account

URL Link: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html#enable-virt-mfa-for-root

**Activate MFA on the Root User**
Another security best practice is to always enable multi-factor authentication (MFA) on any user that can perform sensitive operations in your account.

**Enable a virtual MFA device for your AWS root account (AWS Management Console)**
You can use IAM in the AWS Management Console to configure and enable a virtual MFA device for your AWS root account.
**Important**
To manage MFA devices for the AWS account, you must be signed in to AWS using your root account credentials. You cannot manage MFA devices for the root account using other credentials.
**Note**: Google Authenticator is most common Virtual MFA Device. Available for free for iPhone and Android

**To configure and enable a virtual MFA device for use with your root account**

1. Sign in to the IAM console at https://console.aws.amazon.com/iam/.
2. Do one of the following:
   - Option 1: Choose **Dashboard**, and under **Security Status**, expand **Activate MFA on your root account**.
   - Option 2: On the right side of the navigation bar, choose your account name, and choose **Security Credentials**. If necessary, choose **Continue to Security Credentials**. Then expand the **Multi-Factor Authentication (MFA)** section on the page.
3. Choose **Manage MFA** or **Activate MFA**, depending on which option you chose in the preceding step.
4. In the wizard, choose **A virtual MFA device** and then choose **Next Step**.
5. Confirm that a virtual MFA application is installed on the device, and then choose **Next Step**.
   IAM generates and displays configuration information for the virtual MFA device, including a QR code graphic. The graphic is a representation of the secret configuration key that is available for manual entry on devices that do not support QR codes.
6. With the **Manage MFA Device** wizard still open, open the virtual MFA application on the device.
7. If the virtual MFA software supports multiple accounts (multiple virtual MFA devices), then choose the option to create a new account (a new virtual device).
8. The easiest way to configure the application is to use the application to scan the QR code. If you cannot scan the code, you can type the configuration information manually.
   - To use the QR code to configure the virtual MFA device, follow the app instructions for scanning the code. For example, you might need to tap the camera icon or tap a command like Scan account barcode, and then use the device's camera to scan the QR code.
   - If you cannot scan the code, type the configuration information manually by typing the **Secret Configuration Key** value into the application. For example, to do this in the AWS Virtual MFA application, choose **Manually add account**, and then type the secret configuration key and choose **Create**.

   **Important** Make a secure backup of the QR code or secret configuration key, or make sure that you enable multiple virtual MFA devices for your account. If the virtual MFA device is unavailable (for example, if you lose the smartphone where the virtual MFA device is hosted), you will not be able to sign in to your account and you will have to contact customer service to remove MFA protection for the account.

9. In the **Manage MFA Device** wizard, in the **Authentication Code 1** box, enter the six-digit number that's currently displayed by the MFA device. Wait up to 30 seconds for the device to generate a new number, and then type the new six-digit number into the **Authentication Code 2** box.
10. Choose **Next Step**, and then choose **Finish**.

The device is ready for use with AWS.

## Login to AWS Management Console using IAM Users Sign-In Link

URL Link: http://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started_how-users-sign-in.html

After you create IAM users and passwords for each, users can sign in to the AWS Management Console for your AWS account with a special URL.

You can find the sign-in URL for an account on the IAM console dashboard.


## Deleting an IAM User (AWS Management Console)

URL Link: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_manage.html

**To use the AWS Management Console to delete an IAM user**

1. Sign in to the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose **Users**, and then select the check box next to the user name that you want to delete, not the name or row itself.
3. For **User Actions** at the top of the page, choose **Delete User**.
4. In the confirmation dialog box, wait for the service last accessed data to load before you review the data. The dialog box shows when each of the selected users last accessed an AWS service. If you attempt to delete a user that has been active within the last 30 days, you must select an additional check box to confirm that you want to delete the active user. If you want to proceed, choose **Yes, Delete**.

## Deleting an IAM Group

URL Link: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups_manage_delete.html

**To delete an IAM group (AWS Management Console)**

1. Sign in to the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, select **Groups**.
3. In the list of groups, select the check box next to the name of the group to delete. You can use the **Filter** menu and the **Search** box to filter the list of policies.
4. Click **Group Actions**, then click **Delete Group**.
5. In the confirmation box, click **Yes, Delete**.

## Cleanup!

### Stop/Terminate All Unneeded Resources

There is no real cleanup of resources to perform after this lab. IAM Users and Groups are a free service.

We recommend, if you have time, repeat the labs several times. This is pretty basic stuff, but it will get advanced quickly.

Look around the AWS Management Console. There are dozens of services we have not touched on. Don't be preoccupied. We will get through it in a fun and easy way.

### Environment Configuration

At the end of this lab, your environment should be configured as follows:

**AWS Account Management**

1. MFA Activated on Root Account
2. Budget Created
3. Billing Alarm Created

**Identity and Access Management (IAM)**

4. Administrative IAM Group Created
5. Admin IAM User Created

   **HINT:** It is common in corporate and campus environment to provide usernames that are either:

   - Some combination of an individual's name (i.e. jdoe, john.doe, etc.)
   - A employee id or some other unique number (i.e. 123456)

   We recommend you keep it simple and create an IAM user with your full name, all lowercase, and optionally your birth month & date. (Year is neither necessary nor advised)
6. Admin IAM User added to IAM Admin Group

# Knowledge Base

## Cloud Computing

### What is Cloud Computing?

Cloud computing is the on-demand delivery of compute power, database storage, applications, and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing.

### Why use Cloud Computing?

Benefit from durable, scalable, utility computing at zero or near zero cost. The prime example is a Google Account. Multiple Cloud services (email, chat, screen share, etc.) for free.

### Cloud Computing Basics

Whether you are running applications that share photos to millions of mobile users or you're supporting the critical operations of your business, a cloud services platform provides rapid access to flexible and low cost IT resources.

### How Does Cloud Computing Work?

Cloud computing provides a simple way to access servers, storage, databases and a broad set of application services over the Internet. A Cloud services platform such as Amazon Web Services owns and maintains the network-connected hardware required for these application services, while you provision and use what you need via a web application.

### Six Advantages and Benefits of Cloud Computing

Trade capital expense for variable expense
Benefit from massive economies of scale
Stop guessing capacity
Increase speed and agility
Stop spending money on running and maintaining data centers
Go global in minutes

## Amazon Web Services (AWS)

### What is Amazon Web Services?

Amazon Web Services (AWS) is a secure cloud services platform, offering compute power, database storage, content delivery and other functionality to help businesses scale and grow.

### Why use Amazon Web Services?

Amazon Web Services offers 12 month AWS Free Tier term. Sign up and learn about AWS Services for free.

### Amazon Web Services Overview

AWS Account Root User

When you first create an Amazon Web Services account, you begin only with a single sign-in identity that has complete access to all AWS services and resources in the account.

Identity Access Management (IAM)

AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources

CloudWatch

Amazon CloudWatch provides a reliable, scalable, and flexible monitoring solution that you can start using within minutes. You no longer need to set up, manage, and scale your own monitoring systems and infrastructure.

## AWS Account Management

### The IAM Console and the Sign-in Page

URL Link: http://docs.aws.amazon.com/IAM/latest/UserGuide/console.html

The AWS Management Console provides a web-based way to administer AWS services. You can sign in to the console and create, list, and perform other tasks with AWS services for your account.
If you're the account owner, you can sign in to the console directly. If you've created IAM users in your account, assigned passwords to those users, and given the users permissions, they can sign in to the console using a URL that's specific to your account.

This section provides information about the IAM-enabled AWS Management Console sign-in page and explains how to create a unique sign-in URL for your account.

**The Root Account Sign-in Page**
When users sign in to your AWS account, they sign in via the account sign-in page. The AWS Management Console uses the account sign-in page by default.

If you want to sign in to the console using your AWS root account credentials instead of IAM user credentials, go to the account sign-in page and then click Sign in using root account credentials. The Amazon Web Services sign-in page appears that you can use to sign in with your AWS root account credentials.

**The User Sign-in Page**
Users who want to use the AWS Management Console must sign in to your AWS account through a sign-in page that's specific to your account. You provide your users with the URL they need to access the sign-in page. You can find the URL for your account sign-in on the dashboard of the IAM console.

Your unique account sign-in page URL is created automatically when you begin using IAM. You don't have to do anything to use this sign-in web page. https://My_AWS_Account_ID.signin.aws.amazon.com/console/

You can also customize the account sign-in URL for your account if you want the URL to contain your company name (or other friendly identifier) instead of your AWS account ID number.

> **Tip** To create a bookmark for your account sign-in page in your web browser, you should manually enter your account's sign-in URL in the bookmark entry. Don't use your web browser's "bookmark this page" feature because of redirects that obscure the sign-in URL.

### The Account Root User

URL Link: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html

When you first create an Amazon Web Services account, you begin only with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the root user and is accessed by signing-in with the email address and password you used to create the account.

**Important** We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the best practice of using the root user only to create your first IAM user and then securely lock away the root user credentials and use them to perform only a few account and service management tasks.

## Identity and Access Management (IAM)

### What Is IAM?

URL Link http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources for your users. You use IAM to control who can use your AWS resources (authentication) and what resources they can use and in what ways (authorization).

#### IAM Features

IAM gives you the following features:

**Shared access to your AWS account**

You can grant other people permission to administer and use resources in your AWS account without having to share your password or access key.

**Granular permissions**

You can grant different permissions to different people for different resources. For example, Full Access versus read-only access, or to access your billing information..

**Secure access to AWS resources for applications that run on Amazon EC2**

You can use IAM features to securely give applications that run on EC2 instances the credentials that they need in order to access other AWS resources.

**Integrated with many AWS services**

For a list of AWS services that work with IAM, see AWS Services That Work with IAM.

**Free to use**

AWS Identity and Access Management is a feature of your AWS account offered at no additional charge. You will be charged only for use of other AWS products by your IAM users

AWS Security Token Service is an included feature of your AWS account offered at no additional charge. You are charged only for the use of other AWS services that are accessed by your AWS STS temporary security credentials.

#### Accessing IAM

You can work with AWS Identity and Access Management in any of the following ways.

**AWS Management Console**

The console is a browser-based interface to manage IAM and AWS resources. For more information about accessing IAM through the console, see The IAM Console and the Sign-in Page.

**AWS Command Line Tools**

You can use the AWS command line tools to issue commands at your system's command line to perform IAM and AWS tasks; this can be faster and more convenient than using the console. The command line tools are also useful if you want to build scripts that perform AWS tasks.

**AWS SDKs**

AWS provides SDKs (software development kits) that consist of libraries and sample code for various programming languages and platforms (Java, Python, Ruby, .NET, iOS, Android, etc.). The SDKs provide a convenient way to create programmatic access to IAM and AWS.

**IAM HTTPS API**

You can access IAM and AWS programmatically by using the IAM HTTPS API, which lets you issue HTTPS requests directly to the service. When you use the HTTPS API, you must include code to digitally sign requests using your credentials.

## Identities (Users, Groups, and Roles)

URL Link: http://docs.aws.amazon.com/IAM/latest/UserGuide/id.html

This section describes IAM identities, which you create to provide authentication for people and processes in your AWS account. This section also describes IAM groups, which are collections of IAM users that you can manage as a unit. Identities represent the user, and can be authenticated and then authorized to perform actions in AWS.

**IAM Users**

An IAM user is an entity that you create in AWS. The IAM user represents the person or service who uses the IAM user to interact with AWS. A primary use for IAM users is to give people the ability to sign in to the AWS Management Console.

A user in AWS consists of a name, a password to sign into the AWS Management Console. When you create an IAM user, you grant it permissions by making it a member of a group that has appropriate permission policies attached (recommended), or by directly attaching policies to the user.

**IAM Groups**

An IAM group is a collection of IAM users. You can use groups to specify permissions for a collection of users, which can make those permissions easier to manage for those users.

Any user in that group automatically has the permissions that are assigned to the group. If a new user joins your organization and should have administrator privileges, you can assign the appropriate permissions by adding the user to that group. Similarly, if a person changes jobs in your organization, instead of editing that user's permissions, you can remove him or her from the old groups and add him or her to the appropriate new groups.

**The Account "Root" User**

When you first create an AWS account, you create an account (or "root") identity, which you use to sign in to AWS. You can sign in to the AWS Management Console as the root user—that is, the email address and password that you provide when you create the account. This combination of your email address and password is called your root account credentials.

When you sign in as the root user, you have complete, unrestricted access to all resources in your AWSaccount, including access to your billing information and the ability to change your password. This level of access is necessary when you initially set up the account. However, we recommend that you **don't** use root account credentials for everyday access. We especially recommend that you do not share your root account credentials with anyone, because doing so gives them unrestricted access to your account. It is not possible to restrict the permissions that are granted to the root account. Instead, we strongly recommend that you adhere to the best practice of using the root user only to create your first IAM user and then securely locking away the root user credentials.

## Using Multi-Factor Authentication (MFA) in AWS

URL Link http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html

For increased security, we recommend that you configure multi-factor authentication (MFA) to help protect your AWS resources. MFA adds extra security because it requires users to enter a unique authentication code from an approved authentication device or SMS text message when they access AWS websites or services.

- **Security token-based**. This type of MFA requires you to assign an MFA device (hardware or virtual) to the IAM user or the AWS root account. A virtual device is a software application running on a phone or other mobile device that emulates a physical device. Either way, the device generates a six digit numeric code based upon a time-synchronized one-time password algorithm. The user must enter a valid code from the device on a second web page during sign-in. Each MFA device assigned to a user must be unique; a user cannot enter a code from another user's device to authenticate.

No matter how the user receives the six digit numeric MFA code, the user enters it on a second page of the sign-in process for the AWS Management Console.

This section shows you how to configure MFA for your users and set them up to use token devices or SMS text messages. It also describes how to synchronize and deactivate existing token devices, and what to do when a device is lost or stops working.

**Note**

- When you enable MFA for the root account, it affects only the root account credentials. IAM users in the account are distinct identities with their own credentials, and each identity has its own MFA configuration.
- If you enable MFA on your AWS account (the root user) and also enable MFA on the associated Amazon.com account with the same email address, you will be prompted for two different MFA codes whenever you sign in as the root user.

# AWS Billing and Cost Management

## Managing Your Costs with Budgets

URL Link: http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/budgets-managing-costs.html

A budget is a way to plan your usage and your costs (also known as spend data), and to track how close your usage and costs are to exceeding your budgeted amount. Budgets use data from Cost Explorer to provide you with a quick way to see your usage-to-date and current estimated charges from AWS, and to see how much your predicted usage accrues in charges by the end of the month.
AWS updates your budget status several times a day. Budgets track your unblended costs, subscriptions, and refunds.

You can create budgets for different types of usage and different types of cost. For example, you can create a budget to see how many EC2 hours you have used, or how many GB you have stored in an S3 bucket. You can also create a budget to see how much you are spending on a particular service, or how often you call a particular API operation. Budgets use the same data filters as Cost Explorer.

**Note**

You can create up to 20,000 budgets per AWS payer account. Your first two active budgets are free of charge. Each additional active budget costs $0.02 per day.

You can also set up notifications that warn you if you go over your budgeted amount, or are forecast to go over your budgeted amount. Notifications can be sent to an Amazon SNS topic and to email addresses. When a

budget goes over the notification amount, AWS sends a notification to the SNS topic and email addresses that are associated with your budget notification.

# Lesson Summary

## AWS Account Management

### AWS Root Account

Amazon Web Services provides you with a Root Account when you sign up for your account. This account is typically the email you used when creating the account, along with a unique account number that gets created for you.

The account credentials provide unlimited access to your AWS resources.
This account controls access to billing information and services.
PROTECT the Root Account

- Enable MFA on Root Account
- Do not create programmatic security credentials (Access Key/Secret Access Key)

To help secure your account, follow an AWS best practice by creating and using AWS Identity and Access Management (IAM) users with limited permissions.

### Identity and Access Management - Initial Setup

You can customize the IAM Users sign-in link: (ex. https://<AWS-Account>.signin.aws.amazon.com/console)
Best practice is to perform the following activities

- Delete your root access keys
- Activate MFA on your root account
- Create individual IAM Users
- Use groups to assign permissions
- Apply an IAM password policy