AWS

AWS – Partner Program holds tiers of Certifications and partner levels. This can be a long-term goal.

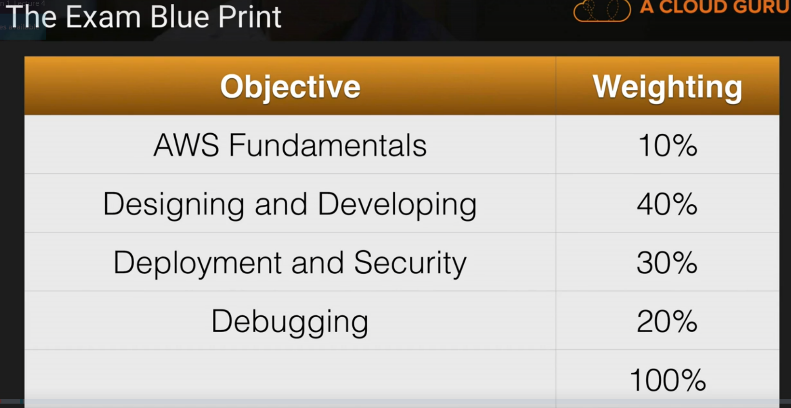
Entry Level Certification – Certified Practitioner (newest, came out in Reinvent 2017) – aimed at nontechnical and beginners path

Under Associate Tier – Certified Cloud Practitioner – Check this out.

In order to get the Devops Professional Ceritificate I need to complete Certified Developer Associate or Certified Sysops Administrator Associate exam.



There is an overlap of Knowledge for Certified Developer Associate exam and the Certified Solutions Architect Associate exam.

Questions and Pass Mark move around based on a bell-curve of everyone’s scores. 80 minutes to complete. $20 for practice. $150 for exam.

A Region is a geographical area. Each region consists of 2 or more availability zones. Availability Zone is simply a Data Center.

Edge Locations are endpoints for AWS which are used for caching content. Typically, this consists of CloudFront, Amazon’s Content Delivery Network (CDN). So, if someone were to host pics or videos in London and someone in Australia wanted to view them. They would download to an Australian Edge Location and be cached there so if anyone else wanted to view them it would be ready.

Again, I need to understand the differences between a Region, an Availability Zone, and an Edge Location.

A Region is a physical location in the world which consists of 2 or more Availability Zones (AZ).

An AZ is one or more data centers, each with redundant power, networking and connectivity, housed in separate facilities.

Edge Locations are endpoints for AWS which are used for caching content. Typically, this consists of CloudFront, Amazon’s CDN.

Compute –

EC2 – Elastic Compute Cloud. Virtual Machines in AWS Platform.

EC2 Container Service – Where you run and manage Dockett containers at scale.

Elastic Beanstalk – Upload code, it will then handle settings such as Load Balancers, Scaling groups, or two instances, etc. So, all the developers should just focus on is their code.

Lambda – Lambda is code that you upload to the cloud and then you control when it executes. You don’t have to worry about any underlying physical or virtual machines. There is literally no operating system or anything to manage.

Lightsail – Amazon’s VPN service. For someone who doesn’t want to know any of the intricacies of AWS. It will just give you a server and a static IP address that you can use. It will give you RDP access for windows or SSH access for Linux. Then it will provide you with a console to manage everything with.

Batch – Not in any of the certification exams. You would use this to preform batch computing in the cloud.

Storage –

Simple Storage Service (S3) – You have Buckets, and you upload your files into buckets that are in the cloud.

Elastic File System (EFS) – Network attached storage so we can go in and store on any FS volume and mount that to multiple virtual machines.

Glacier – Data archival. You can basically archive all your data. Perhaps you don’t need your data all the time, or you want to check it every year, you can store it with Glacier for very very cheap.

Snowball – A way to bring in large amounts of data into the AWS data center. Instead of broadband or WI-FI, you can write it to a disc, it will then be imported manually.

Storage Gateway – Virtual Appliances or machines that you install in your datacenter and it replicates data back to S3.

Databases –

RDS – things like MySQL, Aurora, Oracle, any relational database

DynamoDB – for Non-Relational Databases

Elasticache – A way of caching common queried things from the databases. It’s just a caching service.

RedShift – For data warehousing or business intelligence. This is where you will be preforming complex queries.

Migration –

AWS Migration Hub – Tracking service that allows you to track your applications as you migrate them to AWS. It integrates with other services within the migration framework.

Application Discovery Service – An automated set of tools that detects what applications you have and their dependencies. For example, if you have a program but it has a dependency of SQL Server, this will let you know what you need to ensure it works.

Database Migration Service – Easy way to migrate your databases from on premise to AWS.

Server Migration Service – Helps you migrate your virtual and physical servers into the AWS Cloud.

Snowball – Migrating large amounts of data, we are talking Terabytes.

Networking and Content Delivery –

VPC – Stands for Virtual Private Cloud. Think of it as a Virtual Data Center. You can configure things like the firewall, availability zones, network side address ranges, Network ACL, Route tables, etc.

CloudFront - Amazon’s Content Delivery Network. Things like Media files, video files, it stores the content closer to the Users.

Route 53 – Amazon’s DNS service. It is like an old school telephone book. If you look a cloud, it will give an IP Address.

API Gateway – A way of creating your own API’s for your other services to talk to.

Direct Connect – A way of running a dedicated line from your corporate head office directly into Amazon. It will directly connect into your PC.

Developer Tools –

CodeStar – Way of getting group of developers to work together. Collaborating with other developers. Project managing your code. Continuous delivery tool chain.

CodeCommit – Source Control Service. Place to store your code. Store private git repositories.

CodeBuild – Will compile that code for you or run tests against it and then it will produce software packages that are ready to deploy.

CodeDeploy – Automated deployment services.

CodePipeline – Continuous delivery service. Can see model and visualize the steps needed to automate the steps needed to release the software.

X-Ray – Used to debug and analyze applications. Can find root causes of issues.

Cloud9 – IDE Environment. A place where you can go to develop your code. Can develop in your web browser.

Monitoring Tools –

Cloud Watch – It is a monitoring service. SysOps Admin exam heavy.

CloudFormation – Way of scripting infrastructure. Before you would need to buy servers, firewalls, load balancers, etc. They had to be delivered, racked and stacked. This is all in code now, and can be deployed from a template. It can be reused and deploy other things later. Turning your infrastructure into code.

CloudTrail – Logs every change in your AWS environment. On by default but only logs one week and then deletes.

Config – Monitors the configuration of your entire AWS environment and can see what your system was doing at any given time.

OpsWork – Similar to elastic beanstalk. Way of automating environments.

Service Catalog – Manage a catalog of IT services that are proof use for AWS. Can be virtual machines, databases, etc. Used for basically governance and compliance requirements. Not in any exam.

Systems Manager – Interface for managing AWS resources. Used for EC2. Can be used to roll out patches across instances. Can group resources into smaller groups.

Trusted Advisor – Will give you advice across multiple different disciplines and security. It will tell you if you have left your ports open, if you are not using your AWS Service as much as you can. Can tell you how to save money using AWS. Think of it as an advisor or friend that you trust.

Managed Services – If you don’t want to worry about your EC2 instances or any of your auto scaling, this can help you out.

Media Services –

Elastic Transcoder – Takes the video which was recorded and resizes it to look good on an Android Device, an iPhone, iPad, etc.

MediaConvert – file based video transcoding service. Allows you to create video for broadband delivery.

MediaLive – Live video processing service. Creates high quality video stream for you to deliver.

MediaPackage – Prepares and protects videos for delivery over the internet.

MediaStore – Storage service that’s optimized for media.

MediaTailor - Allows you to do targeted advertising into video streams.

Machine Learning –

SageMaker – Makes it easy for developers to use deep learning when basically coding for their environments.

Comprehend – Sentiment analysis around data. Tells you whether people are saying good or bad things about your product.

DeepLens – Artificially aware camera. The camera can figure out what it’s looking at.

Lex – What powers the amazon Alexa service. Artificial intelligence way for you to chat with your customer.

Machine Learning – Can analyze data set, give it results and then it will detect an outcome based off the data. Similar to recommended products.

Polly – Takes text and turns it into speech. Very human, can choose languages and accents. Can change text to MP3.

Rekognition – Video and Images, you can upload it and the recognition will tell you what it is with a certain accuracy.

Amazon Translate – Machine translation services. Like google translate, can translate one language into another.

Amazon Transcribe – Way to translate captions and take text into captions.

Analytics –

Athena – Allows you to run SQL queries against things in your S3 buckets. You can actually run SQL to go into objects and determine things. For instance, you have Excel in your S3 bucket and want to know all your employees. You can run a query to determine all of them from the spreadsheet.

EMR – Has a bunch of different servers and chops your data up for analysis.

CloudSearch/ElasticSearch Service – Basic search services for AWS.

Kinesis – Way of ingesting large amounts of data into AWS. Things like social media feeds, etc. Maybe it’s a bunch of tweets or hashtags relative to your company.

Kinesis Video Streams – If you have a large amount of people viewing your video, this allows you to ingest this and then run a bunch of processing against it.

QuickSight – Amazon’s business intelligence tool. Not in any exams yet.

Data Pipeline – Way of moving your data between different AWS Services.

Glue – Used for extract, transform and then load. You can change an item into a different one and then reload it.

Security & Identity & Compliance –

IAM –

Cognito – Way of performing device authentication. Using facebook, gmail, twitter, etc.

GuardDuty – Monitors for malicious activities on your AWS account.

Inspector – Agent that you install to run tests on your machine. Can run tests to check for vulnerabilities and generate severities report.

Macie – Scan S3 buckets and look for things that have identifiable information.

Certificate Manager – Way of managing your SSL certificates.

CloudHSM – Dedicated bits of hardware, used to store keys. Private and public keys. Can store other encryption keys. Real hands on security and key experience.

Directory Service – way of integrating your Microsoft active directory services with AWS services.

WAF – Web application firewall and stops malicious scripting. Things like sql injection or cross-site scripting. Checks and says “What is this user doing? Is this malicious? Do I want to stop them?”

Shield – DDOS Mitigation. Can prevent DDOS.

Artifact – On-Demand access to download AWS compliant reports. Downloading and inspecting Amazon documentation.

Mobile Services –

Mobile Hub – Management console. Sets up your AWS services.

Pinpoint – Way of using targeted push notifications.

AWS AppSync – Automatically updates the data in web and mobile applications in real time. Also updates data for offline users as soon as they reconnect.

Device Farm – Way of testing apps on real devices.

Mobile Analytics – Analytics service for mobiles.

AR/VR -

Sumerian – In Demo. First language ever written down for VR. Common set of tools that we can use to make these environments. Can be used for augmented and 3-d too. Don’t need to code.

Read Ready Player One

Application Integration

Step Functions – Way of managing your different Lambda functions and the different steps to go through it.

Amazon MQ – way of doing message queues.

SNS – Notification Service. Example, if our bill goes over $10, let me know.

SQS – Way of decoupling your infrastructure. Can hold requests while your EC2 instances are polling the rest.

SWF – Every time you order a package online it basically creates a simple workflow job. Simple workflow can have human beings in it. Like we said if someone orders something online, another person must go and put a label on it in a warehouse. That can be a step in their simple work flow.

Customer Engagement –

Connect – Contact center as a service. Think of it like having your own call center in the cloud. Can configure service configuration, dynamic, personal or natural customer engagement.

Simple Email Service – Great way of sending large amounts of email. Great deliverability and highly customizable.

Business Productivity –

Alexa For Business – Does many things. Can dial into a meeting room, can inform IT that printer is broken, can reorder Ink.

Chime – Like google Hangouts, video conferencing.

Work Docs – Dropbox for AWS.

WorkMail – Amazon’s version of Office 365.

Desktop & App Streaming –

Workspaces – VDI Solution

AppStream 2.0 – Way to stream the applications. The application itself is running in the cloud.

Internet of Things –

iOT – Way of having thousands of devices sending data.

iOT Device Management – Way to manage all the data coming back from iOT.

Amazon FreeRTOS – Operating System for Micro controllers

Greengrass – software that lets you run local compute messaging data caching sync and to machine learning interface capabilities for connected devices in a secure way.

Game Development –

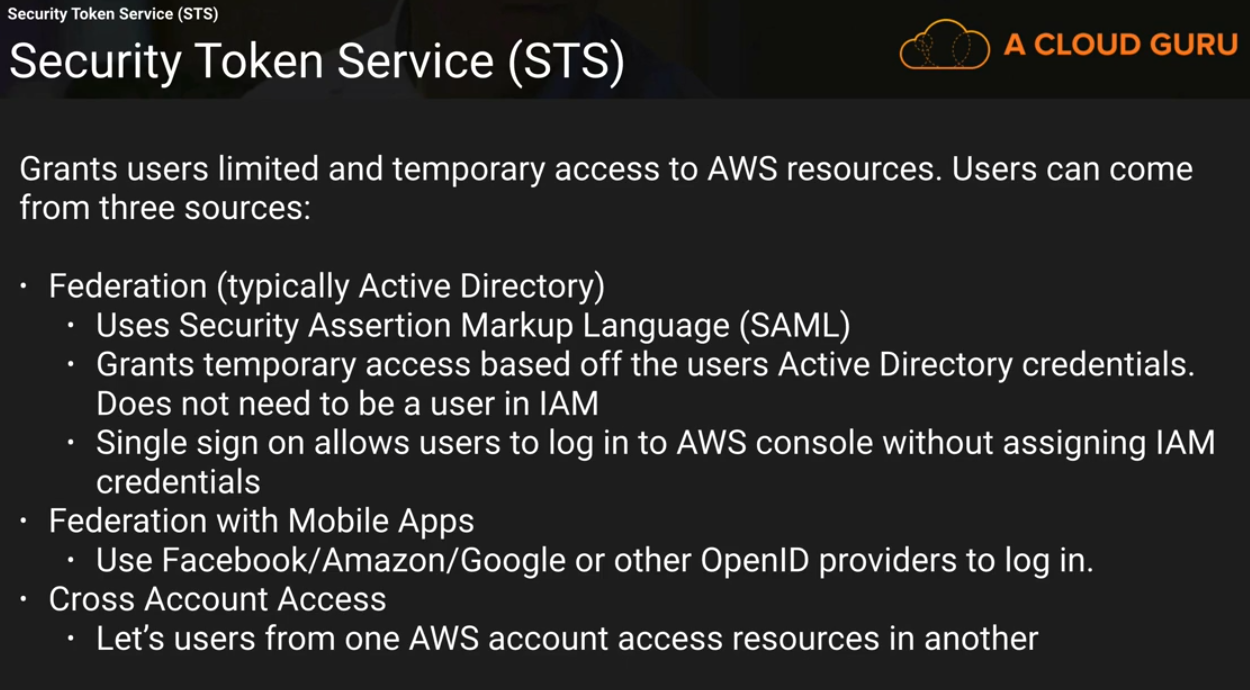
GameLift – Service to help you develop games.

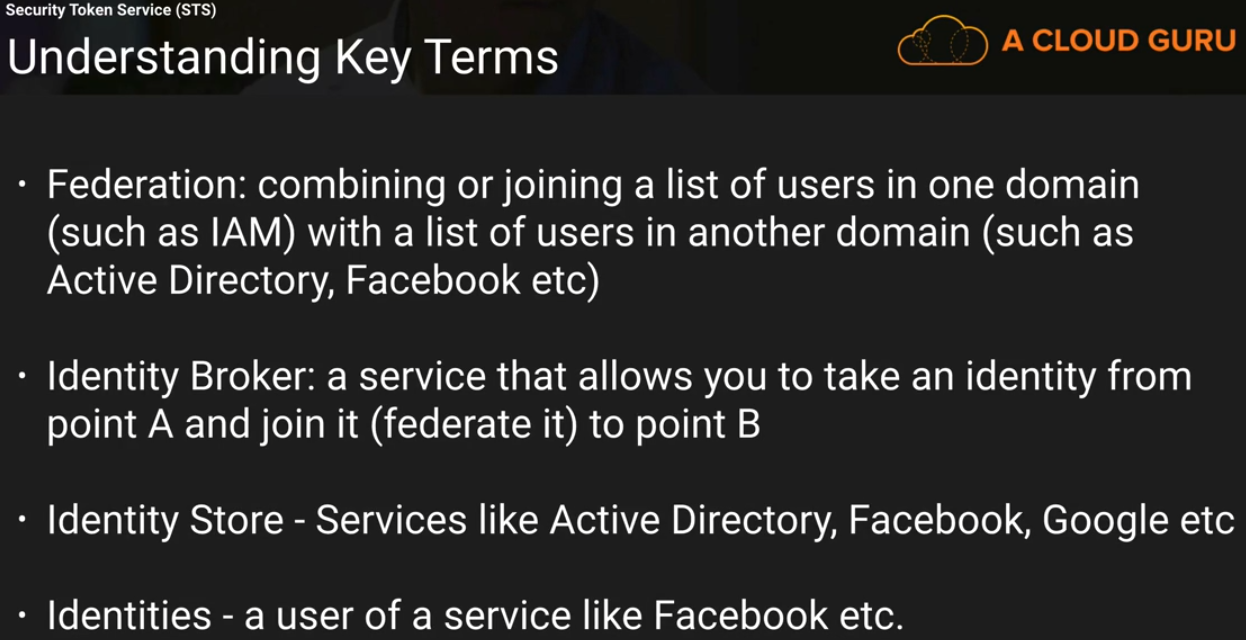
Identity Access Management 101 (IAM) –

IAM Allows you to manage users and their level of access to the AWS Console. It is important to understand IAM and how it works for administrating a company’s AWS account in real life.

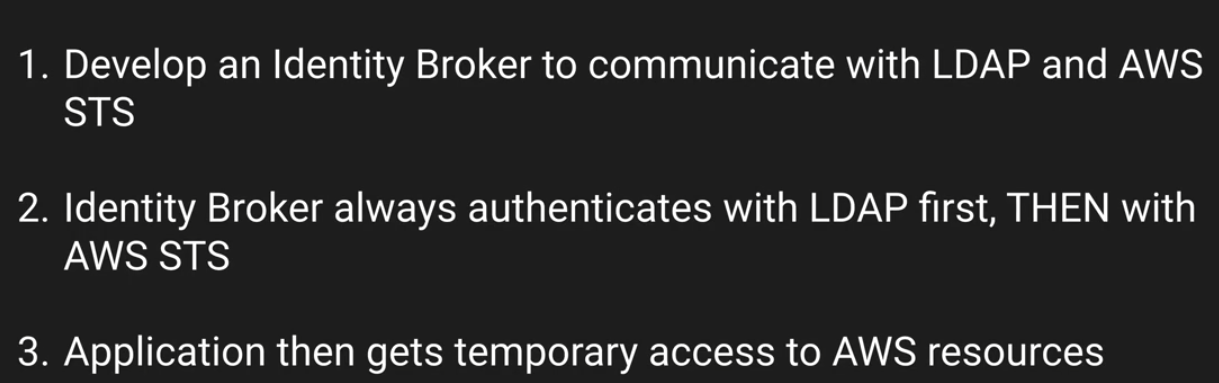


Security Token Service (STS)





Remember below for exam:



Active Directory Federation

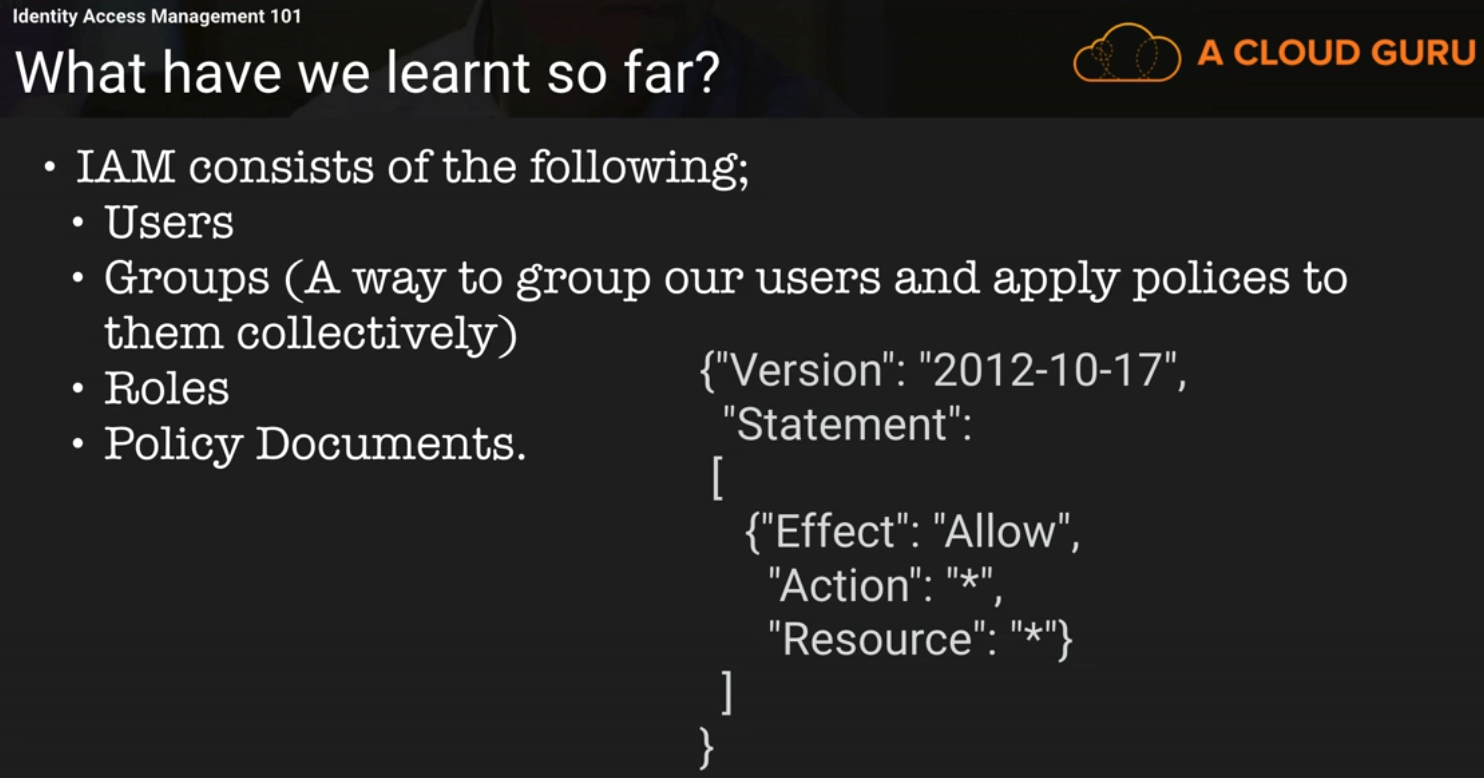
You can authenticate with Active Directory. It is by using SAML.

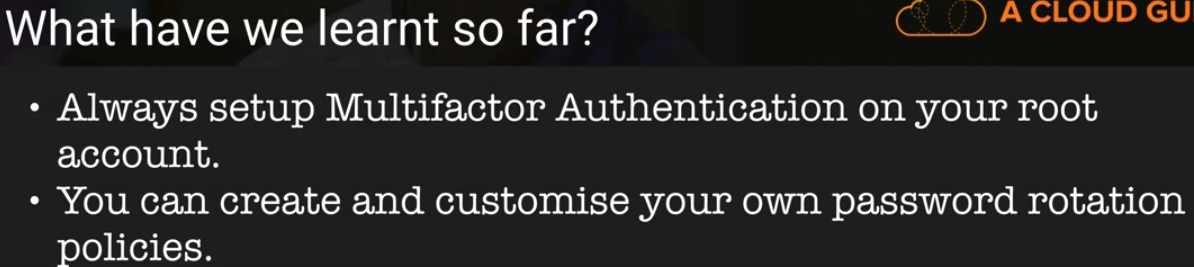
You always authenticate against Active Directory first and then you will be assigned a temporary security credential.

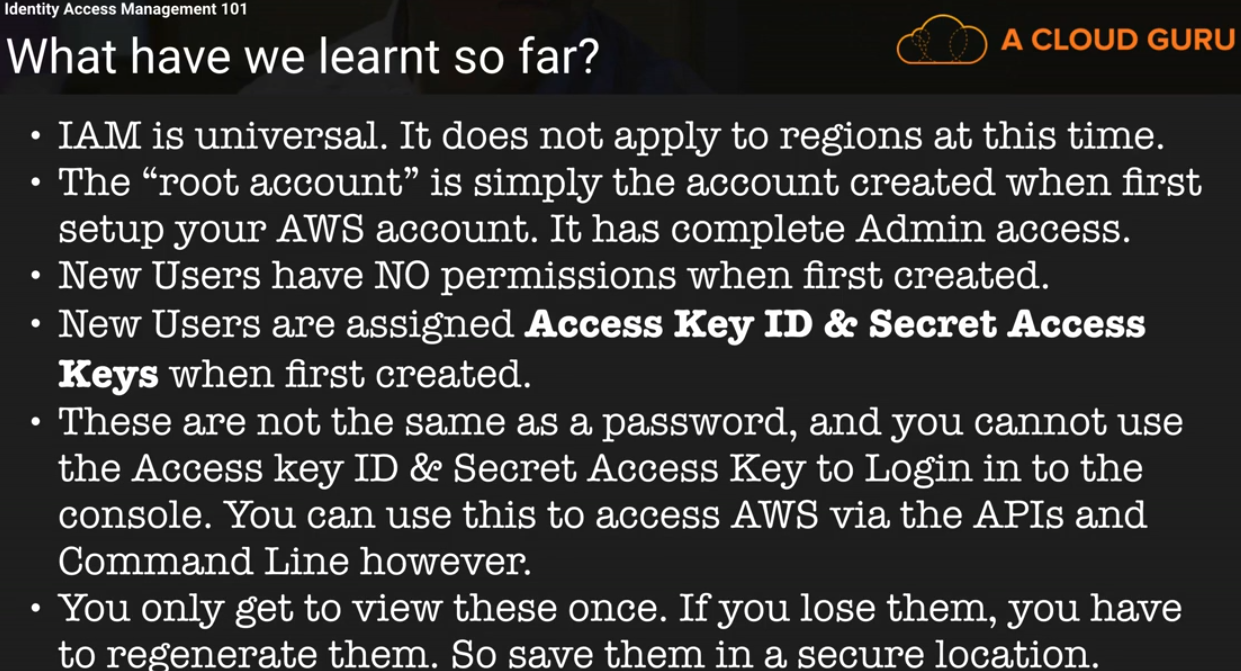
Web Identity Federation

Need to know that you can authenticate using things like Facebook, LinkedIn, Google. To set it up uses a fair amount of coding.

You do not need to know how to do it programmatically. You need to understand the process, you authenticate and get temporary security credentials. You call the AssumeRoleWithWebIdentity and you can access your resources.



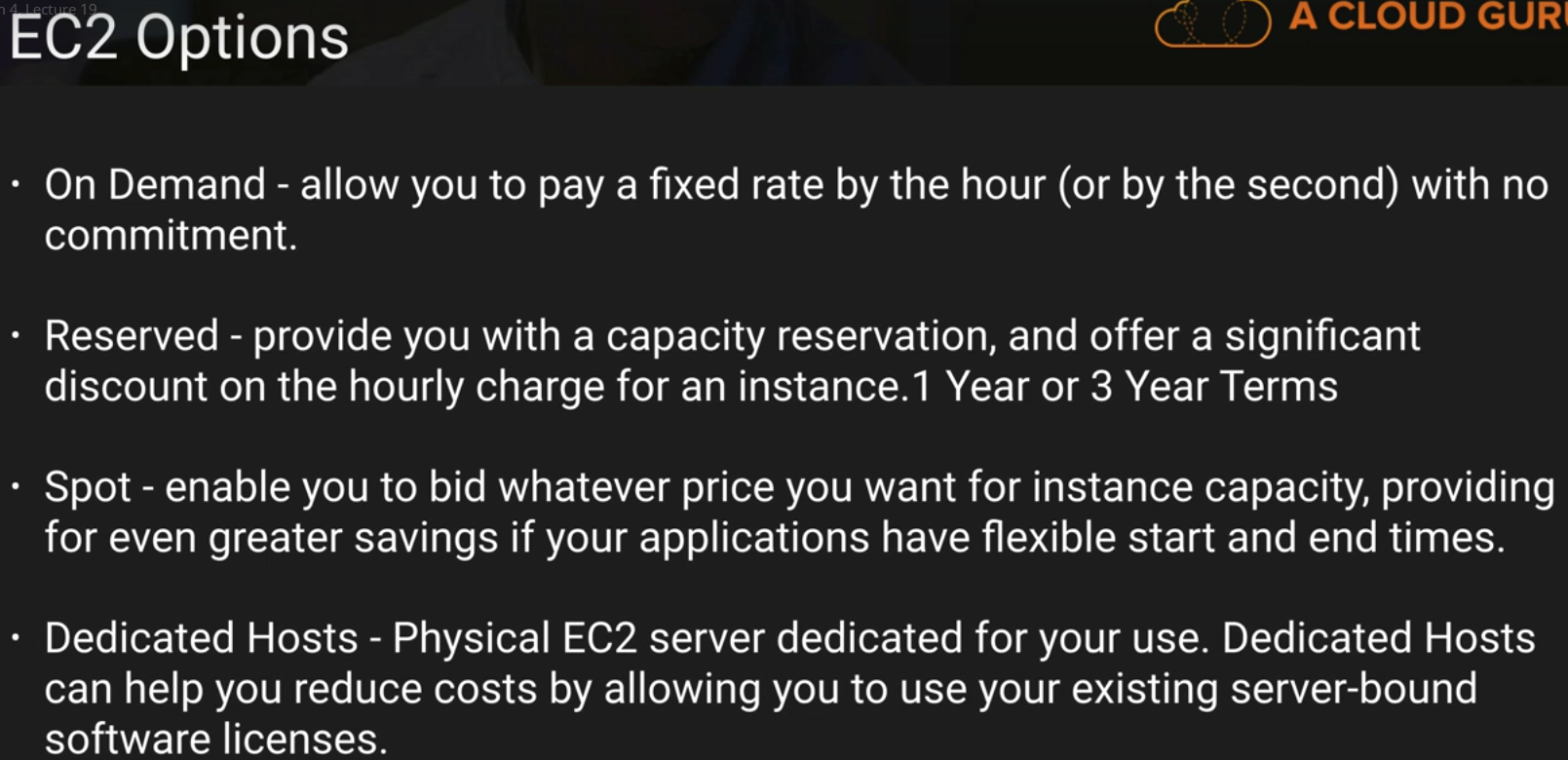




EC2 101 – Elastic Compute Cloud

EC2 is a web service that provides resizable compute capacity in the cloud. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change.

Amazon EC2 changes the economics of computing by allowing you to pay only for the capacity that you actually use. Amazon EC2 provides developers the tools to build failure resilient applications and isolate themselves from common failure scenarios.



On Demand –

* Users that want the low cost and flexibility of Amazon EC2 without any up-front payment or long-term commitment
* Applications with short term, spiky, or unpredictable workloads that cannot be interrupted.
* Applications being developed or tested on Amazon EC2 for the first time.

Reserved –

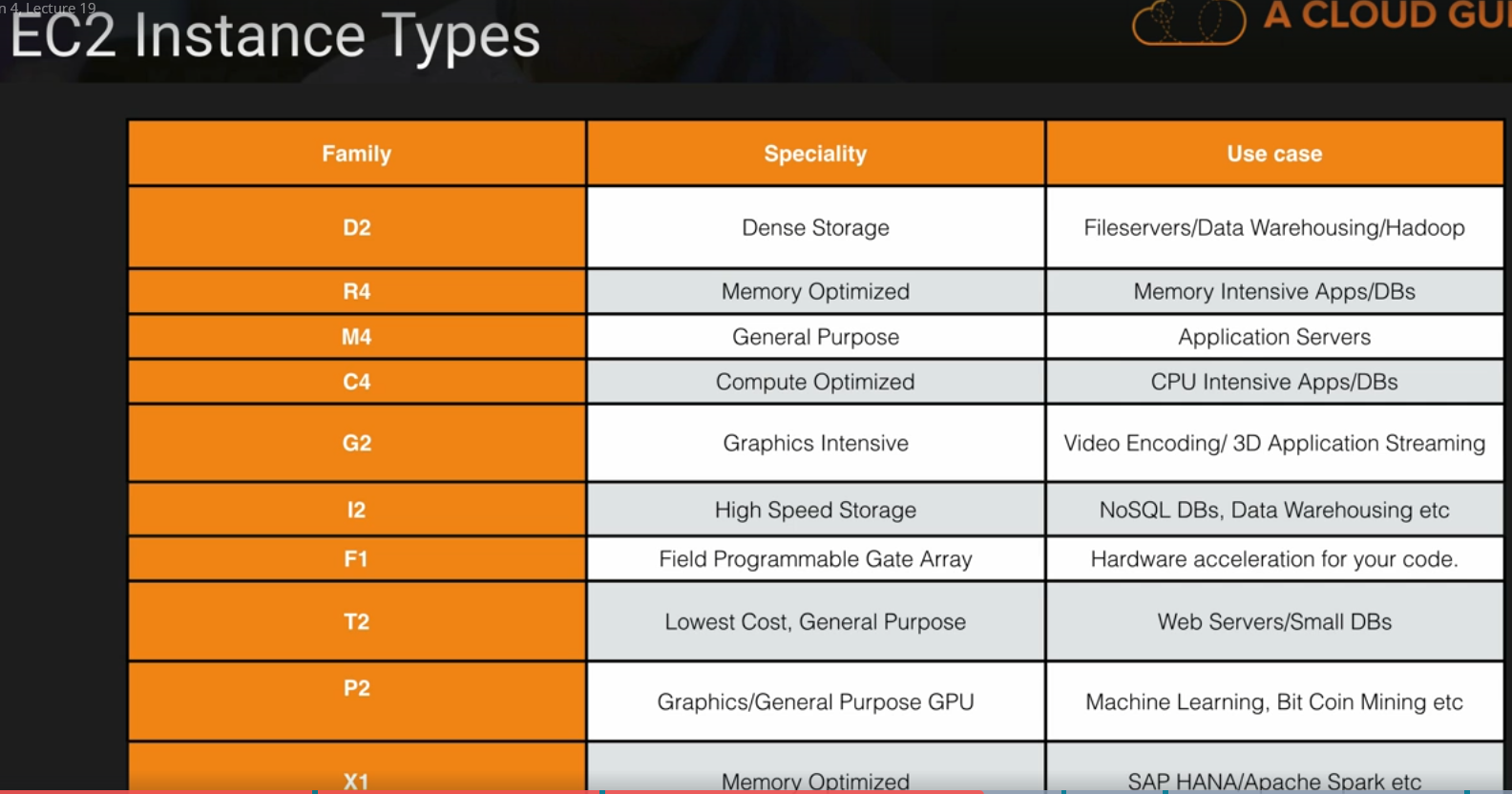
* Applications with steady state or predictable usage.
* Applications that require reserved capacity.
* Users able to make upfront payments to reduce their total computing costs even further.
  + Standard RI’s (Up to 75% off on demand)
  + Convertible RI’s (Up to 54% off on demand) capability to change the attributes of the RI as long as the exchange results in the creation of *Reserved Instances* of equal or greater value.
  + Scheduled RI’s available to launch within the time windows you reserve. This option allows you to match your capacity reservation to a predictable recurring schedule that only requires a fraction of a day, a week, or a month.

Spot –

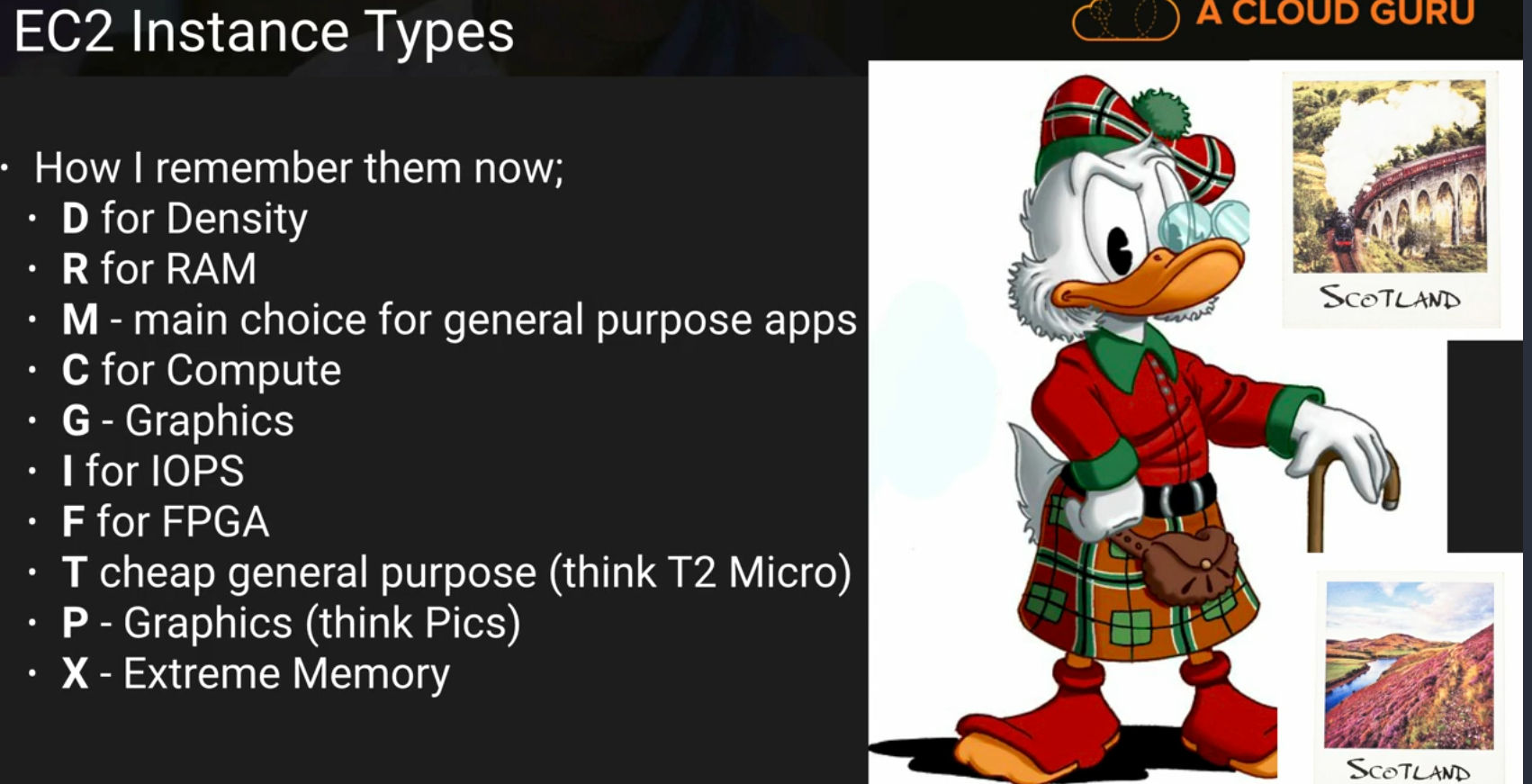
* Applications that have flexible start and end times.
* Applications that are only feasible at very low compute prices.
* Users with urgent computing needs for large amount of additional capacity.

Dedicated Hosts-

* Useful for regulatory requirements that may not support multi-tenant virtualization.
* Great for licensing which does not support multi-tenancy or cloud deployments.
* Can be purchased On-Demand (hourly).
* Can be purchased as a Reservation for up to 70% off the On-Demand price.



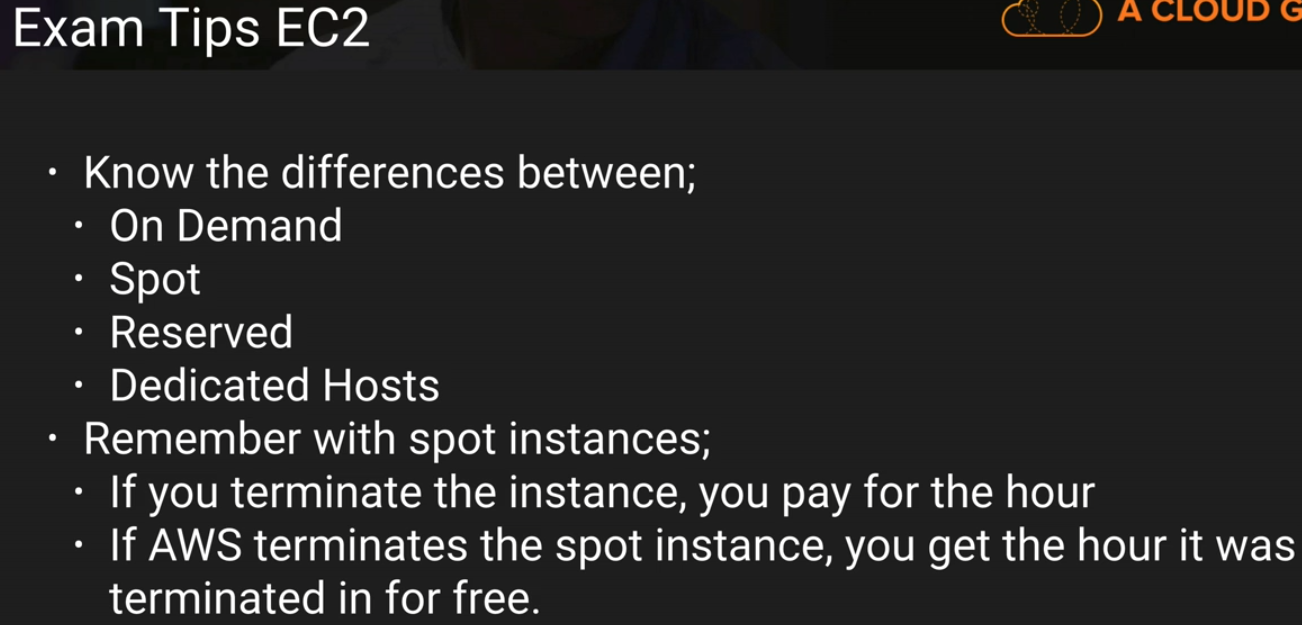
Dr Mc GIFT PX – way to remember the different types of EC2 Instance Types

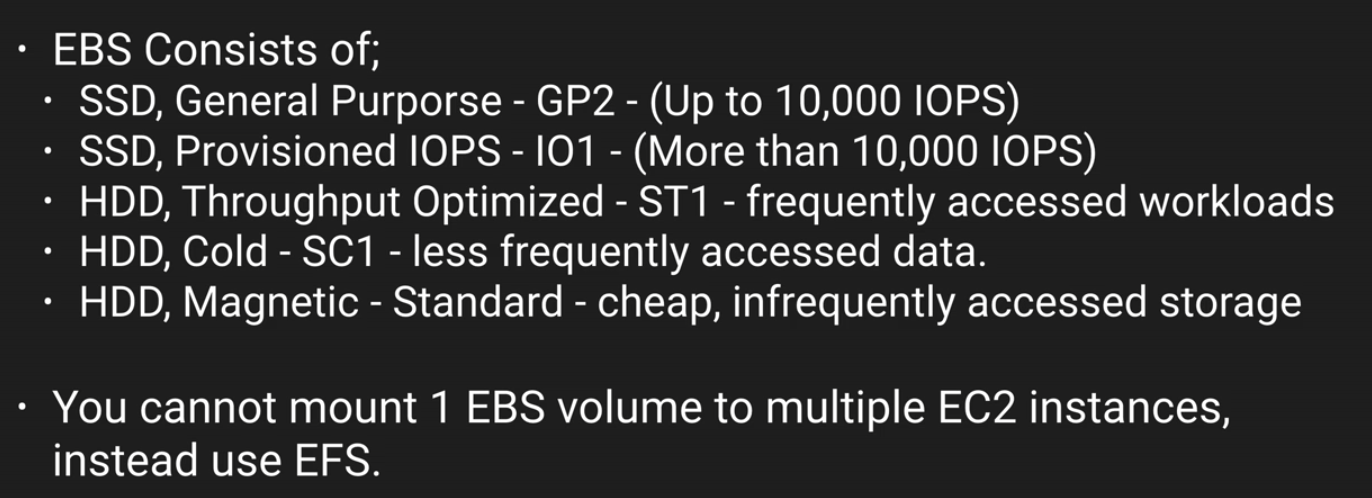


EBS – Allows you to create storage volumes and attach them to Amazon EC2 Instances. Once attached, you can create a file system on top of these volumes, run a database, or use them in any other way you would use a block device. Amazon EBS Volumes are placed in a specific Availability Zone, where they are automatically replicated to protect you from the failure of a single component.

EBS Volume Types:

* General Purpose SSD (GP2)
  + General Purpose, balances both price and performance.
  + Ratio of 3 IOPS per GB with up to 10,000 IOPS and the ability to burst up to 3000 IOPS for extended periods of time for volumes at 3334 GiB and above.
* Provisioned IOPS SSD (IO1)
  + Designed for I/O intensive applications such as large relational or NoSQL databases.
  + Use if you need more than 10,000 IOPS.
  + Can provision up to 20,000 IOPS per volume.
* Throughput Optimized HDD (ST1)
  + Big Data
  + Data Warehouses
  + Log Processing
  + Cannot be a boot volume
* Cold HDD (SC1)
  + Lowest Cost Storage for infrequently accessed workloads
  + File Server
  + Cannot be a boot volume
* Magnetic (Standard)
  + Lowest cost per gigabyte of all EBS volume types that is bootable. Magnetic volumes are ideal for workloads where data is accessed infrequently, and applications where the lowest storage cost is important.





Step 3 is the main setup page for Ec2



Does not look too bad.

1 Subnet = 1 Availability Zone

Advanced Details in Step 3 EC2 set up is where you can pass your bootstrap scripts

Putty for Windows

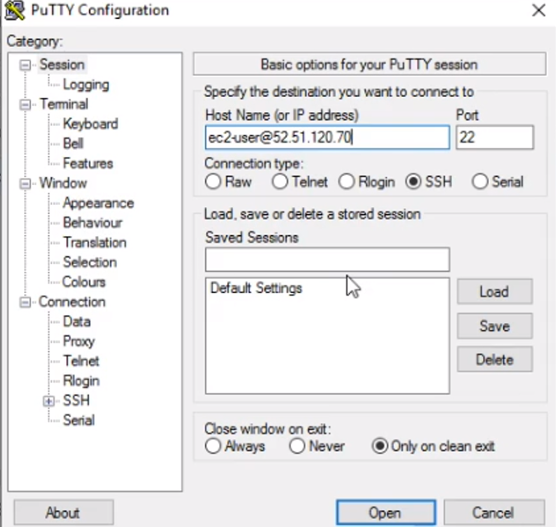
* Turns PEM files into PKK files

The first thing that I did was create a folder on the desktop that I can store the PEM file. I then use PuttyGen to load the Key. Change it to All files and then select the pem file. It will say its successfully importaed. Save Private Key!!!! You can set a passphrase if you want. I chose no since it’s just setting up for the first time. I say yes and then change it to all Files, use the SAME NAME and then save it as a .PPK. Save. I can see both of them now.

Next open up Putty.

Look at the Live EC2 Instance. Get the PUBLIC IP Address and go back to the Putty configuration.

I am just entering ec2-user@(pasted IP address from public ec2 Instance) in the Host Name Section.

Copy paste the full host-name into the Saved Sessions Field in the middle of the page.

Go to SSH and Auth -> Press browse and enter where the private key is.

Go to Session and press Save. Click on the ec2-user again and press Load.

Press Yes if it’s not in the registry, that’s fine.

SECURITY ISSUE – When you first get started, this tutorial is saying to give yourself root access by entering: sudo su. I need to make sure this is correct.

Once I am in I can enter: yum update -y which will update all the patches and security updates needed for the OS.

So in this tutorial: I’ve created my first EC2 Instance in the cloud, I’ve ssh’ed into it, I’ve applied security patches to it, I’ve turned it into a web server and I’ve made a web page that can be browsed anywhere in the world.

There 2 types of Status Checks:

* System Status Check – which makes sure that your System is reachable. If this is not working, there may be a Hardware problem.
* Instance Status Check – Makes sure that the instance can receive packets.

The initial Root Storage volume cannot be encrypted out the gate. They need to be provisioned and additional steps are required. You can encrypt the other ones that you add but not the first one.

Lab Summary –

* Termination Protection is turned off by default, you must turn it on.
* On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. (For the VM when you try and delete the VM, the virtual hard disk will be deleted by default when that gets deleted)
* EBS Root Volumes of your DEFAULT AMI’s cannot be encrypted. You can also use a third-party tool (such as bit locker etc.) to encrypt the root volume, or this can be done when creating AMI’s in the AWS console or using the API.
* Additional Volumes can be encrypted.

Security Groups

When you delete Security groups outbound rules, it does not mean that you can’t get results for someone pinging your page. If it is in inbound, whether it shows or not those rules apply for outbound as well. Anything allowed in is allowed out. Security groups are Stateful.