s3,rds,iam,cognito,apm gateways,cloud formation template

Machine generated alternative text:
• Deployment: CICD, Beanstalk, Serverless 
• Security: each service deep-dive + dedicated section 
• Development with AWS Services: Serverless, API, SDK & CLI 
• Refactoring: Understand all the AWS services for the best migration 
• Monitoring and Troubleshooting: CloudWatch, CloudTrail, X-Ray 

Machine generated alternative text:
What we'll learn in this course 
l(tD 
Amazon 
On Dyna moDB 
on EC2 
Syst •ms 
AWS Step 
Amazon API 
Aws 
Cognito 
x -Ray 
Dyna DB 
Amazon 
CIO udWa tch 

IAM: has a global view not region based

Identity and access management

User: physical

Group

Role: machine based

Policy: what user and role can do

NOTE: once we create IAM it will be across all region

Machine generated alternative text:
IAM 101 Brain Dump 
• One IAM User per PHYSICAL PERSON 
• One IAM Role per Application 
• IAM credentials should NEVER BE SHARED 
• Never, ever, ever, ever, write IAM credentials in code. EVER. 
• And even less, NEVER EVER EVER COMMIT YOUR IAM credentials 
• Never use the ROOT account except for initial setup. 
• Never use ROOT IAM Credentials 

Machine generated alternative text:
Welcome to Identity and Access Management 
Sigrvin '1k: 
IAM Resources 
Security Status 
Activate MFA on root 
Create individual IAM uWS 
use groups to asson perm—ons 
Apply an IAM password "bey 
Rotate your keys 
Feature Spotlight 
AWS O 
Additional Information 
"EtiCC 
&'tity 
Pdicy Sim_'lator 
IAN and 
aws 
I Dashboard 
Idmtity providers 
AccrX'nt settings 
keys 

Subnet define : in which AG you want ec2 instance

Machine generated alternative text:
SSH Summary Table 
SSH 
Mac 
Linux 
Windows 10 
Windows 10 
EC2 Instance 
Putty 
Connect 

Command To connect ec2 through ssh

EC2Tutorial.pem :----- key,value

C:\Users\saurakes\AppData\Local\Temp\msohtmlclip1\02\clip_image006.png

Machine generated alternative text:
Elastic IPS 
• When you stop and then start an EC2 instance, it can change its public 
• If you need to have a fixed public IP for your instance, you need an 
Elastic IP 
• An Elastic IP is a public IPv4 IP you own as long as you don't delete it 
• You can attach it t 
me 

Install apache on EC2

C:\Users\saurakes\AppData\Local\Temp\msohtmlclip1\02\clip_image006.png

Sudo su

Yum update -y

Intall httpd:----yum install -y httpd.x86\_64

To start service: systemctl start httpd.service

systemctl enable httpd.service

Curl localhost:80 ( note we will get page but want in webbrowser)

Add inbound rule to work:

Machine generated alternative text:
Edit inbound rules 
Type 
NOTE: Any edits made existim a 
to fu a vey brÉf rew 
SH from any-wh_ 
HTTP traffic for 
trut 
HTTP 

Machine generated alternative text:
ec2—userl# echo "Hello World" /var/www/htnl/index.html 
troot@ip-172-31—34—1ØØ echo "Hello World from $(hostname —f)" /var/w•w/html/index.html 
Iroot@ip-172-31-34-1øø hostname -f 
compute. internal 

NOTE:

EC2 UserData is script which automatically installed when we create ec2 instance

Machine generated alternative text:
Remember, EC2 User Data is automatically run 
onfig nsta 
ep 
a) 
Enable 
0) 
T2 unlimited 
Advanced Details 
0) 
Q Feedback e English (us) 
etails 
with the sudo command 
• C Create 
C) Protæt *inst 
O Enable CloudWatch 
•WI te.—cy_ 
C) Enable 
As text O As O 
yurt -y 
i rst* •y 
system:tl start httpc.ær.•ice 
era* 
• Hello 
Review L_mmh 
Next: Add Storage 

Machine generated alternative text:
0) 
As text O As O 
-y 
i rst* •y 
start service 

Machine generated alternative text:
Which host is right for me? 
• On demand: coming and staying in resort 
whenever we like, we pay the full price 
• Reserved: like planning ahead and if we plan to 
stay for a long time, we may get a good 
discount. 
• Spot instances: the hotel allows people to bid 
for the empty rooms and the highest bidder 
keeps the rooms. You can get kicked out at any 
time 
• Dedicated Hosts: We book an entire building 
of the resort 

Machine generated alternative text:
EC2 - Checklist 
• Know how to SSH into EC2 (and change .pem file permissions) 
• Know how to properly use security groups 
• Know the fundamental differences between private vs public vs elastic IP 
• Know how to use User Data to customize your instance at boot time 
• Know that you can build custom AMI to enhance your OS 
• EC2 instances are billed by the second and can be easily created and 
thrown away, welcome to the cloud! 

ELB: EC2 load balancer

Machine generated alternative text:
Application Load Balancer (v2) 
I-ITTP Based Traffic 
0 
EC2 
Instance 
EC2 
Instance 
EC2 
Instance 
EC2 
Instance 
HTTP 
HTTp 
www 
www 
Route /user 
External 
Application 
Load Balancer 
(v2) 
Route /search 

Machine generated alternative text:
ASGs have the following attributes 
• A launch configuration 
• AMI + Instance Type 
• EC2 User Data 
• EBSVolumes 
• Security Groups 
• SSH Key Pair 
• Min Size / Max Size / Initial Capacity 
• Network + Subnets Information 
• Load Balancer Information 
• Scaling Policies 

Route 53 is use to managed DNS

Machine generated alternative text:
Route 53 - 
Web Browser 
Diagram for A Record 
.coff, 
ON domain 
. I I oapp. 
R e quest 'Ott?. 
o 
omain. corn 
Response 
Route 53 
Application Server 
IP: 32.45.67.85 

Machine generated alternative text:
AVVS RDS Overview 
• RDS stands for Relational Database Service 
• It's a managed DB service for DB use SQL as a query language. 
• It allows you to create databases in the cloud that are managed by AWS 
• Postgres 
• Oracle 
• MySQL 
• MariaDB 
• Oracle 
• Microsoft SQL Server 
• Aurora (AWS Proprietary database) 

Machine generated alternative text:
RDS Security 
• RDS databases are usually deployed within a private subnet, not in a 
public one 
• RDS Security works by leveraging security groups (the same concept as 
for EC2 instances) — it controls who can communicate with RDS 
• IAM policies help control who can manage AWS RDS 
• Traditional Username and Password can be used to login to the 
database 
• IAM users can now be used too (for MySQL / Aurora — NEW!) 

Machine generated alternative text:
AWS ElastiCache Overview 
• The same way RDS is to get managed Relational Databases... 
• ElastiCache is to get managed Redis or Memcached 
• Caches are in-memory databases wi 
ally high performance, low latency 
• Helps reduce load off of datab f rea intensive workloads 
• Helps make your application st el 
• Write Scaling using sharding 
• Read Scaling using Read Replicas 
• Multi AZ with Failover Capability 
• AWS takes care of OS maintenance / patching, optimizations, setup, 
configuration, monitoring, failure recovery and backups 

Machine generated alternative text:
AVMS VPC 
• Within a Region, you're able to create 
VPCs (Virtual Private Cloud) 
• Each VPC contains subnets (networks) 
• Each subnet must be mapped ap 
• It's common to have a public ub 
(public IP) 
• It's common to have a private su 
(private IP) 
• It's common to have many subnets per 
vpc 
public 
subnet 
public 
subnet 
public 
subnet 
private 
subnet 
private 
subnet 
private 
subnet 

Machine generated alternative text:
AWS VPC 
vpc 
0 
0 
• Public Subnets usually contains: 
• Load Balancers 
• Static Websites 
Files 
• Public Authentication Layers 
• Private Subnets usually contai 
s: 
• Web application servers 
• Databases 
public 
subnet 
public 
subnet 
public 
subnet 
private 
subnet 
private 
subnet 
private 
subnet 

Machine generated alternative text:
Typical architecture 
Web App 3-tier 
Private Subnet 
Public Subnet 
Elastic Load 
Balancing 
Route 53 
Scali 
VS Certified Developer O Stephane Maarek 
Data / Private Subnet 
ElastiCache 
RDS 
RUS 

Machine generated alternative text:
AWS S3 Overview - Buckets 
• Amazon S3 allows people to store objects (files) in "buckets" (directories) 
• Buckets must have a globally unique name 
• Buckets are defined at there n I 
• Naming convention 
No uppercase 
• 
• No underscore 
• 3-63 characters long 
Not an IP 
Must start with lowercase letter or number 
• 

Machine generated alternative text:
S3 Encryption for Objects 
• There are 4 methods of encrypting objects in S3 
• SSE-S3: encrypts S3 objects using keys handled & managed by AWS 
• SSE-KMS: leverage AWS Key Management Service to manage encryption keys 
• SSE-C: when you want to manage your own encryption keys 
• Client Side Encryption 

Bucket policy

Machine generated alternative text:
S3 Websites 
• S3 can host static websites and have them accessible on the www 
• The website URL will be: 
• Kbucket-nam&.s3-website-KAW 
• OR 
• •ucket-nam& .s3-website.« 
ionhamazonaws.com 
n .amazonaws.cop 

Machine generated alternative text:
S3 CORS 
• If you request data from another S3 bucket, you need to enable CORS 
• Cross Origin Resource Sharing allows you to limit the number of 
websites that can request your fil 
S3 (and limit your costs) 
• It's a popular exam question 
mybucket 
Client 
GET coffee-jpg 
ORIG I N : http://mybucket.s3-website.eu-west-3.a mazonaws.com/ 
Access-Control-Allow-Origin: cdomain» 
myimagebucket 

Machine generated alternative text:
AWS S3 - Consistency Model 
• Read after write consistency for PUTS of new objects 
• As soon as an object is written, we can retrieve it 
ex: (PUT 200 GET 200) 
• This is true, except if we did a GET before to see if the object existed 
ex: (GET 404 PUT 200 GET 404) - eventually consistent 
• Eventual Consistency for DELETES and PUTS of existing objects 
• If we read an object after updating, we might get the older version 
ex: (PUT 200 PUT 200 GET 200 (might be older version)) 
• If we delete an object, we might still be able to retrieve it for a short time 
ex: (DELETE 200 GET 200) 

Machine generated alternative text:
Section Introduction 
• So far, we've interacts with services manually and they exposed standard 
information for clients: 
• EC2 exposes a standard Linux machine we can use any way we want 
• RDS exposes a standard databas 
• ElastiCache exposes a cache U 
• ASG / ELB are automated and e 
connect to using a URL 
nnect to using a URL 
h to program against them 
• Route53 was setup manual 
• Developing against AWS has two components: 
• How to perform interactions with AWS without using the Online Console? 
• How to interact with AWS Proprietary services? (S3, DynamoDB, etc... ) 

Aws s3 ls ( cli command) (read in google)

Machine generated alternative text:
awS s3 CP s3://thebucketofstephane/coffee. jpg coff 
download: s3: //thebucketofstephane/coffee.jpg to ./coffee. jpg 
11 
total 360 
1 stephanemaarek staff 1.7K 19 Sep 14:47 EC2Tutoria 
1 stephanemaarek staff 1.01 21 Sep 14:13 coffee. jpg 
—rw—r— r— 
EC2Tutorial.pem coffee. jpg 
aws s3 mb s3://dsoifjsoiucner 
make bucket: dsoifjsoiucner 
aws s3 Is 
11: 16:52 dsoifjsoiucner 
-ø9— 1 14:5ø:16 thebucketofstephane 
—dli—øg— 1 13:42:17 theotherbucketofstephane 
aws s3 rb s3://dsoifjsoiucner 
remove_bucket: dsoifj 
2ø18-ø9-21 thebucketofstephane 
2ø18-ø9-21 13:42:17 theotherbucketofstephane 

NOTE: if we attached iam to s3 then we can access it from cli

Aws policy simulator

**dry**-**run** is an optional boolean flag that doesn't take a value. ... OPTIONS --**dry**-**run** | --no-**dry**-**run** (boolean) Checks whether you have the required permissions for the action, without actually making the request, and provides an error response.

Machine generated alternative text:
Continuous Integration 
Developers push the code to a code 
repository often (GitHub / CodeCommit / 
Bitbucket / etc... ) 
• A testing / build server checks the code as 
soon as It's pushed (CodeBuild / Jen 
/ etc...) 
• The developer gets feedback abo th 
tests and checks that have passed ail 
Find bugs early, fix bugs 
• 
Deliver faster as the code is tested 
• 
Deploy often 
• 
Push code 
often 
Code 
Repository 
Tell developer 
sults of build 
Build Server 
Get code 
build & test 

Machine generated alternative text:
Continuous Delivery 
• Ensure that the software can be released 
reliably whenever needed. 
• Ensures deployments happen often and 
are quick 
• Shift away from "one release every 3 
months" to "5 releases a day" 
• That usually means automated deployment 
• CodeDeploy 
• Jenkins CD 
• Spinnaker 
• Etc... 
o 
o 
Push code 
often 
Get code 
build & test 
Deploy every 
passing build 
Application 
Server VI 
Application 
Server v2 
Code 
Repository 
Build Server 
Deployment 
Server 
Application 
Server VI 
Application 
Server v2 
Application 
Server VI 
Application 
Server v2 

Machine generated alternative text:
Technology Stack for CICD 
Deploy 
Provision 
Code 
CodeCommit 
GitHub 
or Yd party 
code repository 
Build 
Test 
AWS Elastic Beanstalk 
User Managed 
EC2 Instances 
AWS CodeDeploy 
Fleet 
(CloudFormation) 
AWS CodeBuild 
Jenkins Cl 
Or 3rd party Cl servers 