
AWS Certified Security - Specialty

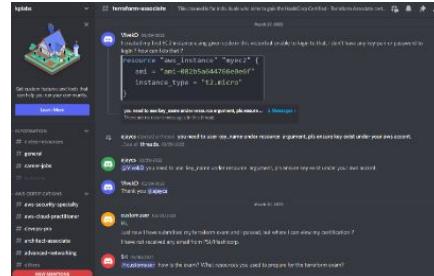
Instructed by Zeal Vora

Our Community

You can join our **Discord community** for any queries / discussions. You can also connect with other students going through the same course in Discord (Optional)

Discord Link: <http://kplabs.in/chat>

Group Page: #aws-security-specialty



Last Update Date

This PPT has been last updated on **8th May 2023**.

We regularly update the PPTs based on the course updates.

Check the PPT lecture to see the “Last Update Date” to verify if this is the latest PPT.

Case Study: Hacked Systems

Compromised servers are everywhere

My First Security Class

When I was learning Security during college times, our professor gave us Ubuntu CDs and asked us to install it in our computers.

After a few set of classes, he told us that the Ubuntu in that CD was infected with malicious scripts and all of our systems were compromised.

Lesson Learnt: Never Trust Packaged Software. Download Softwares from the Source.



Unknown Docker Images

Many developers directly use some random Docker Images that fulfills their use-cases.

This can also lead to security incidents within your organization.

The image displays three separate screenshots of the Docker Hub search results for the keyword "wordpress". Each screenshot shows a different Docker image entry:

- roelofr/wordpress**: This image is created by roelofr and was updated a year ago. It is described as "Wordpress with wp-cli" and is available for Linux and x86-64 architectures. It has 4.0K downloads and 0 stars.
- kevin808/wordpress-alpine-php-0.81**: This image is created by kevin808 and was updated a year ago. It is described as "Wordpress and wp-cli in a highly configurable, docker-friendly Ubuntu-box." and is available for Linux and x86-64 architectures. It has 10K+ downloads and 0 stars.
- funkygibbon/wordpress**: This image is created by funkgibbon and was updated 3 years ago. It is described as "Wordpress with wp-cli" and is available for Linux and x86-64 architectures. It has 3.4K downloads and 0 stars.

Use-Case: Hacked Server

Some time ago, I received an email from one of my friends requesting assistance related to security as their servers were hacked.

They came to know about it from 3rd party people and through various abuse complaints from the hosting provider.



Abuse Complaint - MegaRBL

My friend received an Abuse complaint from MegaRBL stating that his server IP is blacklisted.

Abuse Complaint

Please review the following abuse complaint and provide us with a resolution:

Hello Abuse Desk,

This is an automated message from MegaRBL.net to advise you that the IP below has been added to rbl.megarbl.net:

IP address : 128.199.252.161

Problem: Spam emitters

You can find more information at the URL:

<https://www.megarbl.net/check/128.199.252.161>

The removal procedure is also explained on this page.

Thank you for your help.

Best regards,

MegaRBL.net Report Desk

Investigation into the Compromise

Postfix was installed and thousands of spam emails were being sent.

| root@mydreams:/var/spool/postfix/maildrop 162x42 | | | | | | | | | | | |
|--|-------------|--------------|--------------|-------------|--------------|-------------|--------------|-------------|--|--|--|
| 36043117DA7 | 6257910D88 | 6F30A10CE58 | 8B8BC1CCD69 | 9840417D30F | A4EC918992C | B190017B042 | BE60916ED8D | DAA4E359E6 | | | |
| 360441A6193 | 6257A30951 | 6F30B1795E3 | 8B8BE16BAF6 | 984041C793 | A4EC918E009 | B1907DCDB7 | BE609172093 | DAA4F1D769E | | | |
| 3604515EB55 | 6257B1A4570 | 6F3101D4BCB | 8B8C016F73B | 984061C38A6 | A4ECB19DF57 | B1908993AA | BE6093B38A | DAA50198037 | | | |
| 3604723AEE | 6257E197BLE | 6F310236C7 | 8B8C4157BCA | 984091ADFB1 | A4ECC157A0 | B1909FEFF | BE60B12A07 | DAA501CE9F4 | | | |
| 36048180BAE | 6257F116E9E | 6F311106937 | 8B8C533EB2 | 9840C114A49 | A4ECC1650C5 | B190A15F972 | BE60DDF0E | DAA511A9A3A | | | |
| 3604917FC32 | 6257F165C43 | 6F31114A8F | 8B8C5B8829 | 9840C1A2A3A | A4EC01BBDB87 | B190A160917 | BE60F16636A | DAA5419E531 | | | |
| 360493E5B9 | 625801BB1D1 | 6F3111C552D | 8B8C7171959 | 9840D1246C | A4EC0D90E4 | B190AFE2C | BE6141987A | DAA5516266F | | | |
| 3604AFB98 | 62581171E46 | 6F3112DA48 | 8B8CE143D3 | 9840D1BD870 | A4ED031C7145 | B190B1ABE73 | BE6151A4DE0 | DAA561A863C | | | |
| 3604B105918 | 625811B3888 | 6F31217D9F8 | 8B8D01202D | 9840D1D06E1 | A4ED326C1A | B190D233C2 | BE61815ACEE | DAA57186FA1 | | | |
| 3604B2B894 | 625822C914 | 6F314119C6 | 8B8D01B4FB8 | 9840E161FB | A4ED626CBF | B190E3BB98 | BE61917E1A1B | DAA59DC2C | | | |
| 3604BD7D5 | 625831AE769 | 6F315163B8E | 8B8D1114FE | 9840E1738A8 | A4ED0810A0FF | B19101AE889 | BE61A38189 | DAA5BADD1B | | | |
| 3604F1581AE | 625831D1D5C | 6F3181AD966 | 8B8D3164AAD | 9840E1BEC04 | A4ED8181AB9 | B19111084D | BE61B10E0A4 | DAA5B1A6754 | | | |
| 3604F1625AF | 62583C53D | 6F3182A068 | 8B8D041BD599 | 9840F1A75B | A4ED932B9D | B191110D8D | BE61C1638CC | DAA5B1A9951 | | | |
| 3604F1AF10 | 62584165540 | 6F3191CA8ED | 8B8D5164B4E | 984111A5E60 | A4EDB16E245 | B1913CC34 | BE61C8EEA5 | DAA5C18C036 | | | |
| 360501C08BE | 6258418E99A | 6F31A176F9F | 8B8D5190AEE | 984131A906D | A4EDC1E0DBB | B19141A4832 | BE61E10CE16 | DAA5C1CE1CC | | | |
| 360511138D9 | 625841CB170 | 6F31A186F38 | 8B8D536F90 | 9841424FDA | A4EDDFC711 | B1916105499 | BE61E1D4D69 | DAA5F165F7D | | | |
| 360511660B3 | 6258514E48 | 6F31LBBAA23D | 8B8D610B0E | 984143E164 | A4EE01A123B | B191A1CED70 | BE61F15D9EA | DAA612F8E2 | | | |
| 360512BCE7 | 6258518B74D | 6F31D1ADCCC | 8B8D61B7C07 | 9841510B474 | A4EE01C800C | B191B1137CF | BE61FEEE1 | DAA641B0B91 | | | |
| 3605219716D | 6258610E27F | 6F31D1D0D66 | 8B8D8167F69 | 9841515F4A5 | A4EE2193E96 | B191C197391 | BE6201673E8 | DAA641C4D2F | | | |
| 360523D681 | 625861B67FE | 6F31E113BA5 | 8B8D91B11E1 | 9841517A585 | A4EE41680FF | B191C1A7621 | BE62311C08C | DAA642B6AE | | | |
| 360531156A7 | 625871A157A | 6F31F2F38B | 8B8DA1A3DF3 | 98416178374 | A4EE41CCE3B | B191D1C8F25 | BE6241162B3 | DAA6611923 | | | |
| 360531C783E | 625881C2053 | 6F3241E26A | 8B8DA3C478 | 984171B91B | A4EE5186C69 | B191F172B28 | BE6241B9C91 | DAA66171C6D | | | |
| 36054158998 | 625891L73C7 | 6F32528307 | 8B8DC10F838 | 984171D4C9B | A4EE619A863 | B192119663 | BE6241CE430 | DAA661C11F8 | | | |
| 360561589CB | 6258A16D259 | 6F326186D6C | 8B8DC1984CD | 98417323AC | A4EE716210C | B192419685B | BE62810C80B | DAA6716B488 | | | |
| 36057182623 | 6258A1D5CFC | 6F3271870A1 | 8B8DC31EA7 | 9841A1B107D | A4EE71CA107 | B1928303AB | BE6291CBDC3 | DAA671C2031 | | | |
| 3605817FF28 | 6258C15EF21 | 6F3282C7D2 | 8B8DD25874 | 9841B176EC4 | A4EE8195862 | B1929328AF | BE62A1A2EA1 | DAA68139939 | | | |

What was happening?

```
[root@mydreams maildrop]# cat test
T[1484191825 403090A]Rewrite_context=localF[ApacheS(angel_harding@example.comMN]To: madtrick66200@msn.comN=Subject: Artificial intelligence conquering the stock m
arket!N@X-PHP-Originating-Script: 48:general34.php(1950) : eval()'d codeN>Date: Thu, 12 Jan 2017 03:30:25 +0000N>From: Angel Harding <angel_harding@myclass.example.com>X-Priority: 3N[IME-Version: 1.0N$Content-Type: multipart/alternative;N/          boundary="b1_c7c33fb90c77e5578f86693d40956ea0"NNContent-Transfer-Encoding: 8bitNN%--b1_c7c33fb90c77e5578f86693d40956ea0N'Content-Type: text/plain; charset=utf-8N[Content-Transfer-Encoding: 8bitNN,Attention! This letter can change your life!NN[NN
A group of German mathematicians invented the smart program which trading on the exchange, brings great profit and never wrongs, and it making purchases only in a 100% profit.NN[While about it do not know others, while it is available and it's not blacked out, use your chance and turn your life into a dream! [ http://ampropertyinc.com/system.php?k=78&36ozS=hqNKxQHqLqCtceRXiwz&Dtf=BGC&2oy=VY4 ] More information is here.NNN%- -b1_c7c33fb90c77e5578f86693d40956ea0N&Content-Type: text/html; charset=utf-8N[Content-Transfer-Encoding: 8bitNN[html>NN[body>N[NN[Attention! This letter can change your life!<br>N[<br>NN[ group of German mathematicians invented the smart program which trading on the exchange, brings great profit and never wrongs, and it making purchases only in a 100% profit.<br>N[<br>NN[While about it do not know others, while it is available and it's not blacked out, use your chance and turn your life into a dream! <a href="http://ampropertyinc.com/system.php?k=78&36ozS=hqNKxQHqLqCtceRXiwz&Dtf=BGC&2oy=VY4">More information is here.</a><br>N</body>N</html>NNNN'--b1_c7c33fb90c77e5578f86693d40956ea0--NXR#madtrick66200@msn.com
```

What After Server is Compromised?

When a server is compromised, depending on the goal of an attacker, multiple approaches are commonly used about the future steps.



Attacker

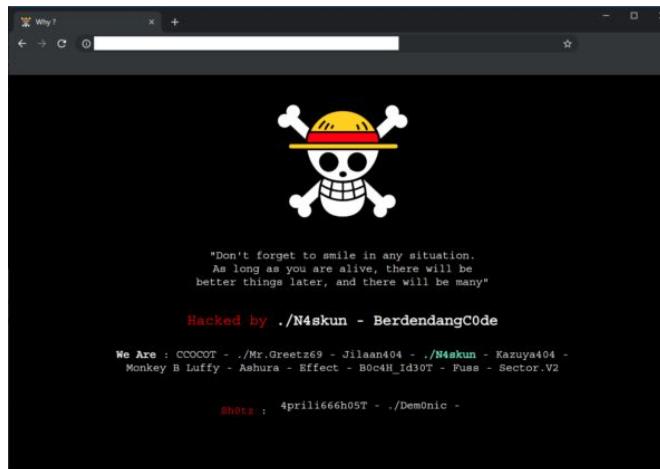
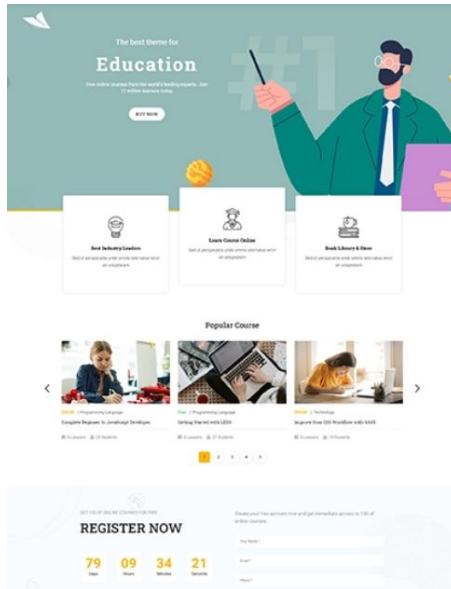
You are mine, now!



Random Server

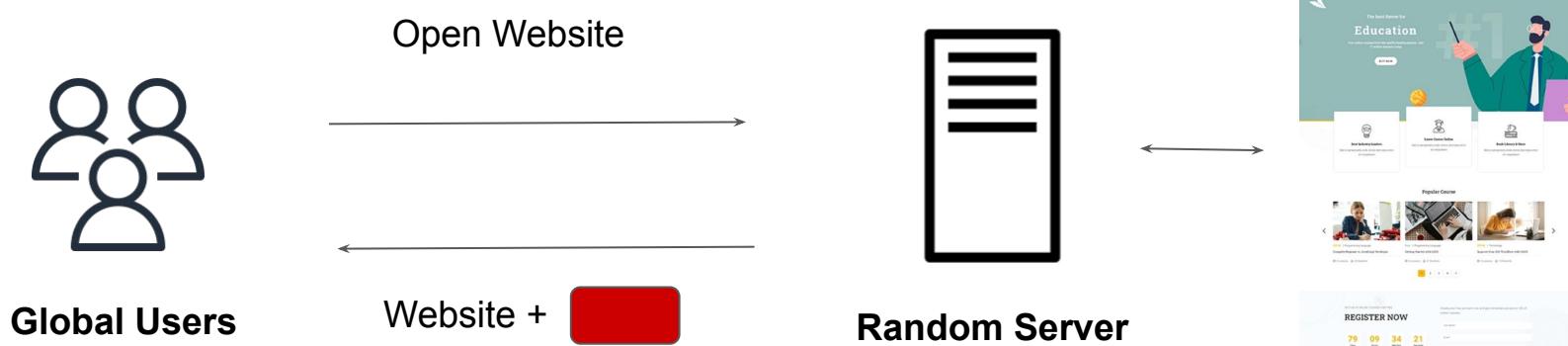
Common Pattern 1 - Defacing Website

Original website is replaced with an attacker's landing page to spread a message.



Common Pattern 2 - Malicious Attachment

The website code is modified so that when someone visits it, automatically a file gets downloaded to the browser (a malware file)



Common Pattern 3 - Encryption

All the files are encrypted by an attacker. Ransom is asked to decrypt the files.



Meat supplier JBS paid ransomware hackers \$11 million

PUBLISHED WED, JUN 9 2021 7:43 PM EDT | UPDATED WED, JUN 9 2021 8:42 PM EDT

NBC NEWS | Kevin Collier

SHARE [f](#) [t](#) [in](#) [e](#)



TRENDING NOW



A toxic culture and 'race to the bottom': Pilots open up on why air travel is in chaos



Here's the average salary Americans need to feel 'financially healthy' at every age



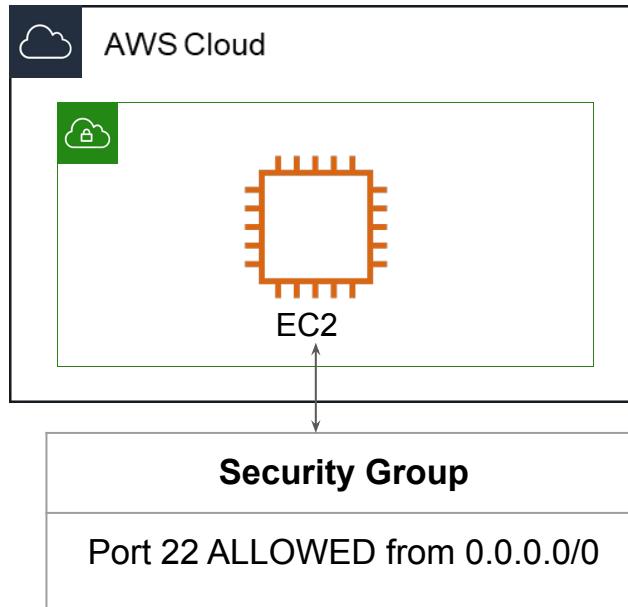
Mortgage rates fall

Common Shortcomings for Compromise.

- Improper firewall configuration.
- Lack of Web Application Firewall.
- Server Hardening is a must.
- File Integrity Monitoring should always be there.
- Vulnerability Assessment
- Patch Management
- Always scan code with Web Application Scanner.
- Monitor for sudden open ports and logs.

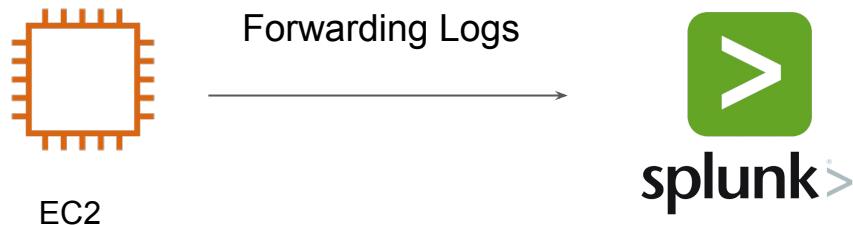
Simple Setup for Curiosity

A simple EC2 with open security group can teach you many things.



Our Setup

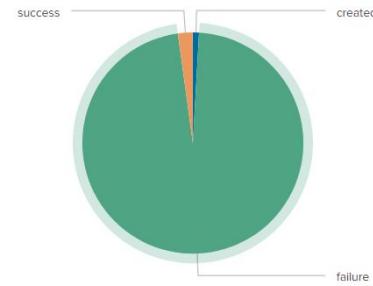
1. Single EC2 instance running for 24 hours.
2. Port 22 is open for 0.0.0.0/0
3. Instance connected to Splunk for Log Management.



Results



616 failed attempts



96% failure rate



Bruteforce from
across the world.

AWS Abuse Reports

Stay within Acceptable Use Policy

Acceptable Usage Policy

Acceptable usage policy or fair use policy is a set of rules applied by the owner to the service user.

Acceptable Use Policy for Rental Apartments:

- No Loud Music
- No Pet Animals.
- No Plants



AWS Acceptable Use Policy

You may not use, or facilitate or allow others to use, the Services or the AWS Site:

- for any illegal or fraudulent activity;
- to violate the rights of others;
- to violate the security, integrity, or availability of any user, networks
- to threaten, or actively encourage violence, terrorism, or other serious harm

What is Abuse Report ?

AWS sends abuse report to customers when their AWS resources are being used for abusive purposes.



Hello,

We've received a report(s) that your AWS resource(s)

AWS ID: 143259556828 Region: ap-south-1 EC2 Instance Id: i-0a336b1d6gfa5f

has been implicated in activity that resembles a Denial of Service attack against remote hosts; please review the information provided below about the activity.

Please take action to stop the reported activity and reply directly to this email with details of the corrective actions you have taken. If you do not consider the activity described in these reports to be abusive, please reply to this email with details of your use case.

If you're unaware of this activity, it's possible that your environment has been compromised by an external attacker, or a vulnerability is allowing your machine to be used in a way that it was not intended.

Who raises abuse complaint ?

Abuse Complaint can directly be filed by clients who are getting affected.

If you are receiving some suspected unknown traffic from AWS resource, you can file Abuse complaint in the “Report Amazon AWS Abuse Form”.

Report Amazon AWS abuse

Do you have an existing AWS account? Make sure your request is associated with your account by clicking the button below to reach us via the Support Console.

[Sign in and submit AWS support request](#)

Please complete the form below to report suspected abuse of Amazon AWS resources.

Please provide information as completely and accurately as possible. Amazon AWS is a dynamic environment where customers launch and terminate many services over the course of a few hours. This means that customers may occupy the same host or service at different times of the same day. Therefore, it is critical that you identify the IP address(es), date, exact time (accurate to within 1 minute), and time zone in order for us to accurately identify the reported resource.

Details of reported abuse

We will use the information that you provide in this form to investigate and attempt to resolve the incident you have reported. We might share your information if it is necessary for the investigation of your report.

Source IP address

The source IP address of the reported abuse

Destination IP addresses - optional

The destination IP address(es) of the reported abuse

Use commas to separate multiple IP addresses

Destination ports and protocols - optional

22/TCP

Responding to AWS Abuse Reports

If you receive an abuse notice from AWS, do the following:

1. Review the abuse notice to see what content or activity was reported. Logs that implicate abuse are included along with the abuse report, as provided by the reporter.
2. Reply directly to the abuse report and explain how you're preventing the abusive activity from recurring in the future.

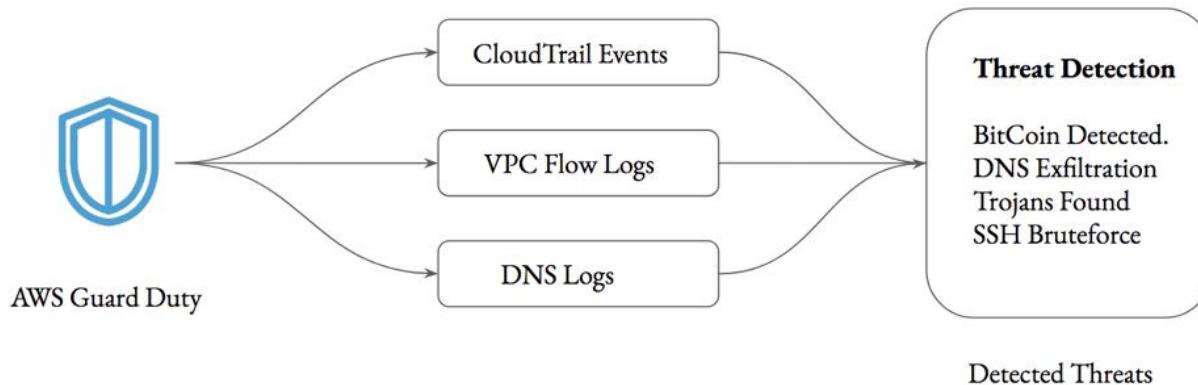
If you don't respond to an abuse notice within 24 hours, AWS might block your resources or suspend your AWS account.

AWS GuardDuty

Let's start Rolling !

Understanding GuardDuty

AWS Guard Duty is a threat intelligence service by AWS which monitors for malicious behavior to help customers protect their AWS workloads.



GuardDuty Findings

Findings 

Showing 67 of 67   

| <input type="checkbox"/> | Finding type | Resource | Last seen | Account ID | Co... |
|--------------------------|--|-----------------------------------|--------------|--------------|-------|
| <input type="checkbox"/> |  [SAMPLE] UnauthorizedAccess:EC2/RDPBruteForce | Instance: i-99999999 | 2 months ago | 101586075... | 1 |
| <input type="checkbox"/> |  [SAMPLE] Trojan:EC2/PhishingDomainRequest!DNS | Instance: i-99999999 | 2 months ago | 101586075... | 1 |
| <input type="checkbox"/> |  [SAMPLE] CryptoCurrency:EC2/BitcoinTool.B!DNS | Instance: i-99999999 | 2 months ago | 101586075... | 1 |
| <input type="checkbox"/> |  [SAMPLE] Trojan:EC2/BlackholeTraffic!DNS | Instance: i-99999999 | 2 months ago | 101586075... | 1 |
| <input type="checkbox"/> |  [SAMPLE] UnauthorizedAccess:EC2/SSHBruteForce | Instance: i-99999999 | 2 months ago | 101586075... | 1 |
| <input type="checkbox"/> |  [SAMPLE] UnauthorizedAccess:EC2/TorIPCaller | Instance: i-99999999 | 2 months ago | 101586075... | 1 |
| <input type="checkbox"/> |  [SAMPLE] UnauthorizedAccess:IAMUser/MaliciousIPCaller | AccessKey: GeneratedFindingAccess | 2 months ago | 101586075... | 1 |
| <input type="checkbox"/> |  [SAMPLE] Recon:EC2/Portscan | Instance: i-99999999 | 2 months ago | 101586075... | 1 |
| <input type="checkbox"/> |  [SAMPLE] UnauthorizedAccess:EC2/MaliciousIPCaller.C... | Instance: i-99999999 | 2 months ago | 101586075... | 1 |

Important Pointers

Guard Duty will only monitor the Route53 for DNS Logs.

Lot of organizations makes use of Active Directory DNS. The logs from these servers will not be monitored.

Relax and Have a Meme Before Proceeding



Whitelisting Alerts on GuardDuty

Security Angle



Handling GuardDuty Alerts

Amazon GuardDuty can generate a wide variety of alerts.

Some of these might be true but you might want to ignore them.

Example:

There is a central Security server that performs port-scans as part of penetration testing on all the production servers.

This can lead to GuardDuty alerts like port scans or brute force being triggered.

Managing Trusted IP Lists

AWS GuardDuty allows customers to add their own “Trusted IP” list.

GuardDuty does not generate findings for IP addresses on trusted IP lists.

Example Trusted IP List:

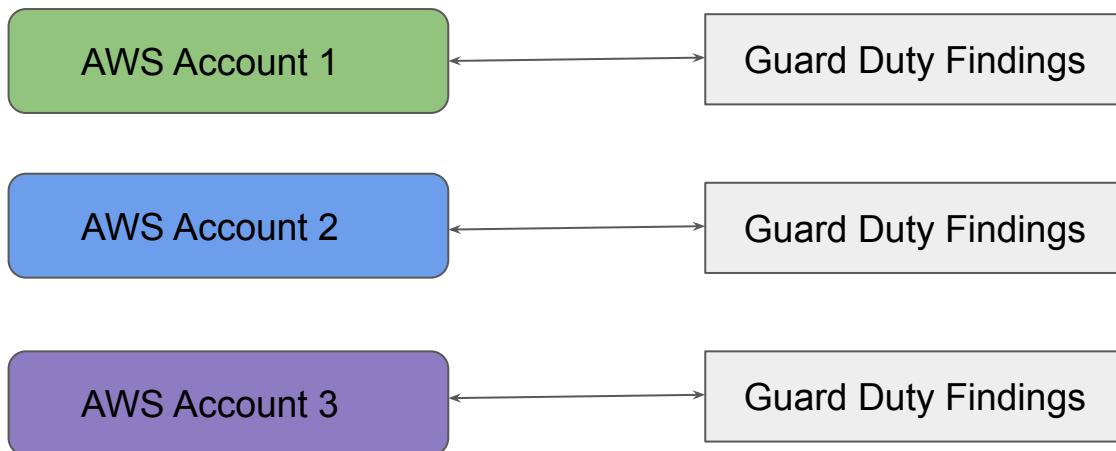
116.75.25.50/32

Managing GuardDuty Findings Centrally

Multiple AWS Accounts

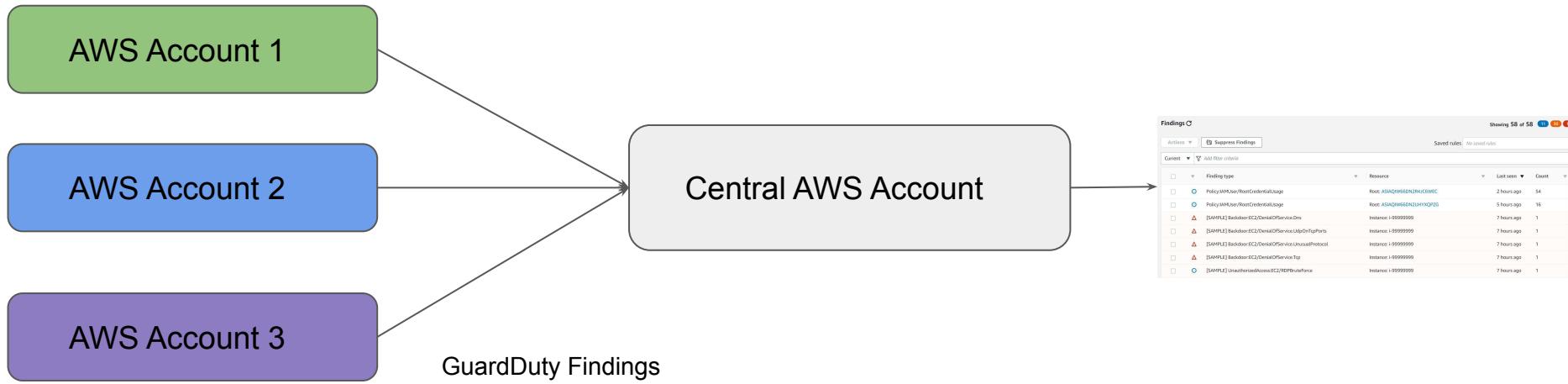
Understanding the Challenge

- Enabling GuardDuty across all AWS account is recommended.
- Checking findings across individual account is troublesome.



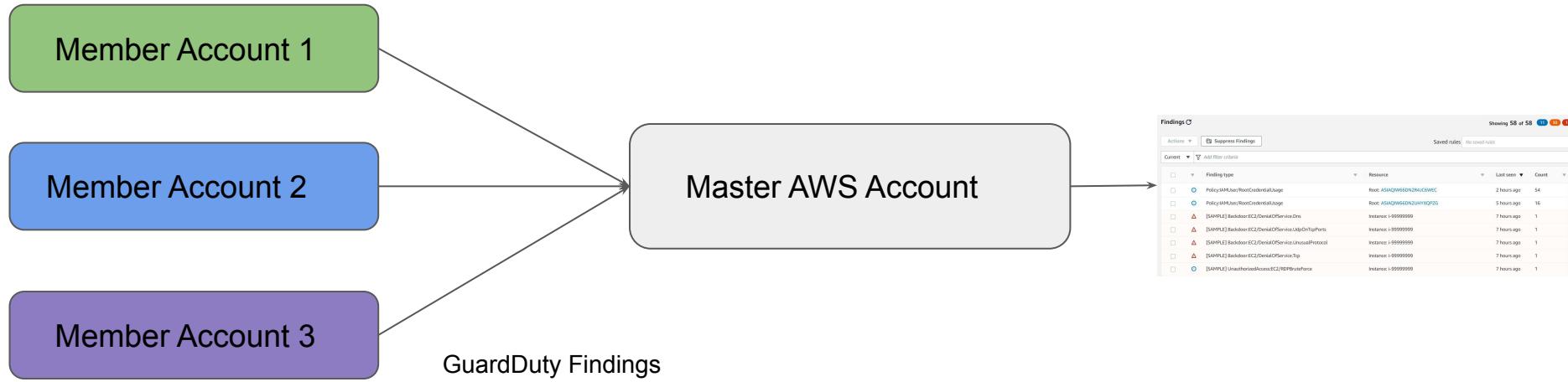
Central Architecture

In this architecture, the Guard Duty findings from all the AWS Accounts will be sent to the Central AWS account.



Right Terminology

In this architecture, the Guard Duty findings from all the AWS Accounts will be sent to the Central AWS account.



Incident Response

Let's Fix what is broken!

What is an incident ?

A security incident is any attempted or actual **unauthorized access**, use, disclosure, modification, or destruction of information.

Example: S3 Bucket with Sensitive Data has Public Read Access.



Global Users



Sensitive S3 Bucket

What is Incident Response ?

Incident Response is an organized approach to address and manage the aftermath of a security incident in an organization.

The goal is to handle the situation in a way that limits damage, reduces recovery time and the costs.



Security Admin

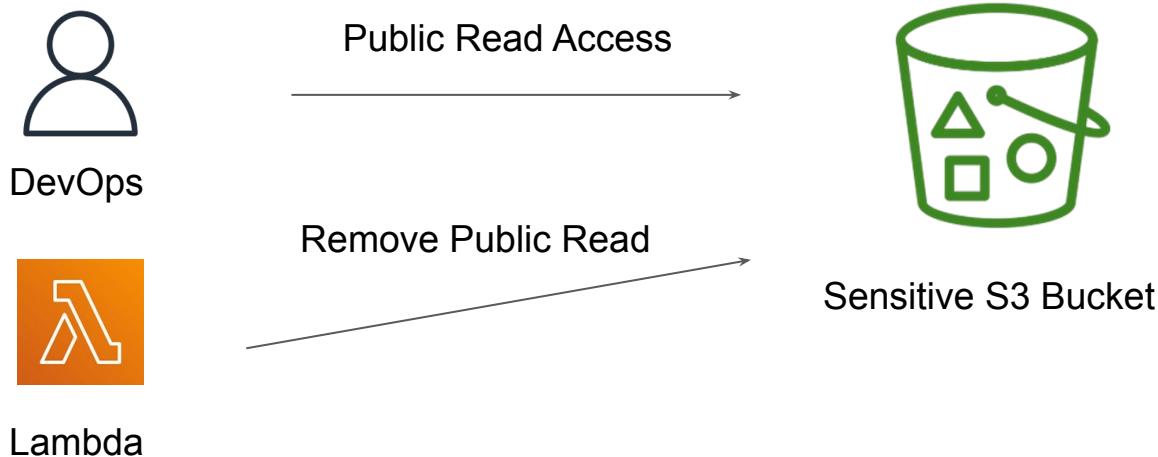
Block Public Read Access



Sensitive S3 Bucket

Event Driven Security

With an event-driven response system, a detective mechanism triggers a responsive mechanism to automatically remediate the event.



Prevention is the Best Cure

Preventive controls protect your workloads and mitigate threats and vulnerabilities.

AWS Provides multiple controls that can prevent threats within your organization.



WAF



IAM



Network Firewall



KMS

Tools for Preventive Controls

Detective Controls

Detective controls provide full visibility and transparency over the operation of your deployments in AWS.



CloudTrail



CloudWatch



Inspector



Detective

Tools for Detective Controls

Incident Response - Use Cases

Let's start Rolling !

Two primary use-cases

You should be aware of step by step approach for incident response for two use-cases

i) Exposed AWS Access & Secret Keys

ii) Compromised EC2 instances

Exposed Access Keys

Incident Response

How to deal with it ?

Exposed AWS Access keys is one of the very common use-cases that you will find across many of the organizations.

There are certain steps which AWS recommends in such scenario:

- i) Determine the access associated with those keys.
- ii) Invalidating the credentials.
- iii) Invalidating any temporary credentials issued with the exposed keys.
- iv) Restore the access with new credentials.
- v) Review your AWS account.

Pointer 1

Determine the access associated with those keys.

Depending on the permissions associated with those exposed keys, it will help you choose the steps that needs to be taken and in which order.

- i) Exposed keys has read and write access to the very sensitive data.
- ii) Exposed keys has read access to a public S3 bucket.

Pointer 2

Invalidating the credentials.

When we disable or delete the credentials, any application using them might be affected.

Ideally, disabling credentials is recommended instead of deleting because disabled credentials can be enabled back instead of any major production outages.

Pointer 3

Invalidating any temporary credentials that might have been issued with exposed keys

Temporary credentials can be generated from the access/secret keys.

These credentials can have lifetime from 15 minutes to 36 hours.

Ideally, disabling credentials is recommended instead of deleting because disabled credentials can be enabled back instead of any major production outages.

Pointer 4

Restore the access with new credentials

Because access keys were disabled / deleted in previous steps, consider following options to restore the access:

- i) Consider creating a new pair of access/secret keys.
- ii) Instead of using long term keys, consider using IAM roles or federation.

Pointer 5

Review your AWS account

Review all the available S3 bucket as well as CloudTrail logs to see on what actions might had been performed on your AWS resources.

You might want to restore data from a backup that was made before the credentials were exposed.

Compromised EC2 Instance

Incident Response

How to deal with it ?

Compromised EC2 instance is again, one of the very common use-cases that you will find across many of the organizations.

There are certain recommended steps in such scenario:

- i) Lock the instance down
- ii) Take the EBS Snapshot
- iii) Memory Dump
- iv) Perform Forensic Analysis
- v) Terminate the instance

Pointer 1

Lock the instance down

In this step, we isolate the EC2 instance so that it cannot contact the outside world.

Only access to the EC2 instance should be for forensic purposes.

Automation is a key here

Pointer 2 and 3

EBS Snapshot & Memory Dump

EBS Snapshot will help ensure that all the files in the server will be snapshotted.

Memory Dump ensures that all the processes running in memory are being dumped.

Pointer 4 and 5

Perform Forensics and Terminate the Instance

Once you have the EBS snapshot as well as memory dump, it should be a good base for performing forensics.

Once forensics are done and RCA is released, we can go ahead and terminate the EC2 instance.

Important Pointer

Exam Essentials

You are not expected to know on how to perform forensics of memory dump aspects.

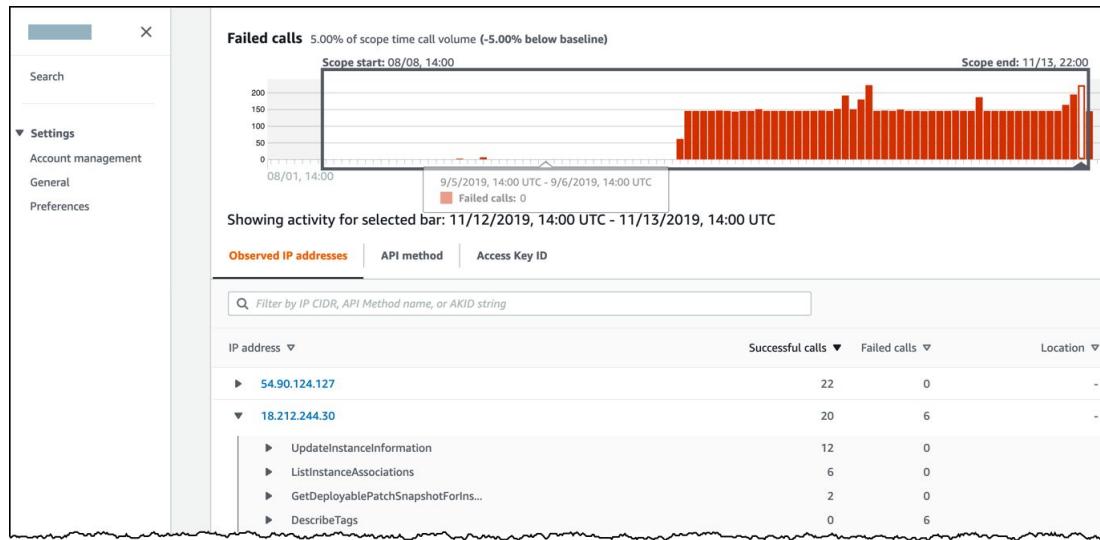
All that is needed for exam, is to know the step by step approach to deal with in such scenario.

Amazon Detective

Threat Detection Service

Basics of Amazon Detective

Amazon Detective makes it easy to investigate, analyze, and quickly identify the root cause of potential security issues or suspicious activities.



Important Note

Amazon Detective is a [threat detection service](#) that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads.

Amazon Detective enables you to analyze and visualize security data from your AWS CloudTrail logs, VPC Flow logs, and Amazon GuardDuty findings.

Amazon Detective pricing is based on the volume of data ingested from AWS CloudTrail logs, Amazon VPC Flow Logs, and Amazon GuardDuty findings. You are charged per Gigabyte (GB) ingested per account/region/month

Incident Response in Cloud

Let's Fix what is broken!

What is it all about ?

AWS provides various visibility, security and automation controls that can help us overall in the incident response process.

When we use cloud, many of the things related to proactively detection, reaction, recovery can be easier in much more faster and cost effective way.

With help of various tools like AWS Config, CloudTrail, Guard Duty, Cloudwatch and many more, we can easily track, monitor, analyze security related events.

What is it all about ?

When an incident occurs, it is important that one manages that incident properly by following your incident response plan.

Incident Response plan has several steps:

- Preparation
- Detection
- Containment
- Investigation
- Recovery
- Lessons Learned

Preparation Phase

This is one of the very important phase of the incident response plan.

We need to make sure controls are in-place that will help us in detection of anomalies within the infrastructure.

Sample steps during this phase:

- Ensure logging is enabled with help of CloudTrail, VPC Flow Logs, EC2 instances.
- Using AWS organizations to separate accounts to reduce the blast surface.

Detection Phase

If you don't know if something is going wrong, you will not be able to respond to it.

Use behavioural based rules by identifying or detecting breaches

Sample steps during this phase:



- Lots of AWS console sign-in failures in past one hour.
- If a user is logging in at 3 AM in morning and launching new servers.

Containment Phase

Once we have identified that incident has occurred, prefer to use some kind of automation to help you contain the resource.

Use AWS CLI or SDK's for quick containment using the predefined security groups.

Sample steps during this phase:

If you have identified one server is infected with malware, quickly run predefined AWS CLI command that attach restrictive security group (ingress/egress) and remove earlier security group.

Investigation Phase

Once the server is isolated, determine and analyze logs as well as timelines.

Sample steps during this phase:

Use CloudWatch logs to determine what occurred inside the server.

Use AWS Config to see infrastructure timeline to see if anything was changed.



Recovery Phase

- In this stage, restoration process begins to recovery things back to the original state.
- Automation plays major role here to make things faster.

Sample steps during this phase:

- Use pre-built AMI for the application to launch fresh new app server.

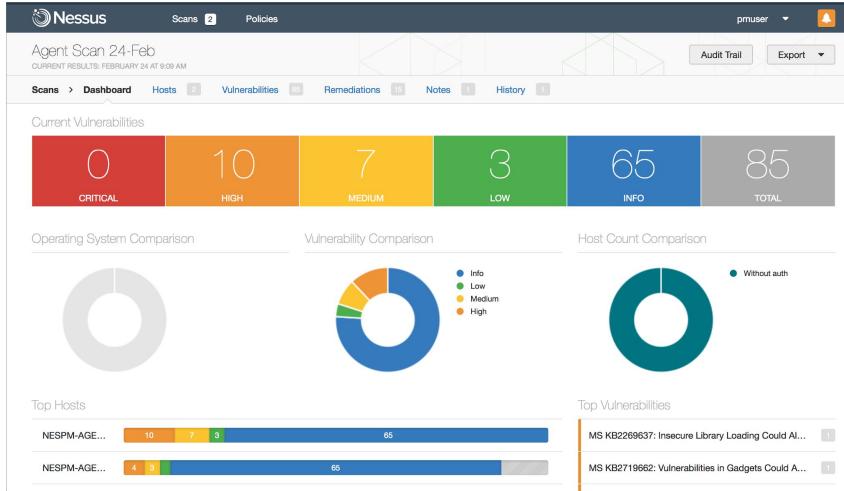


Penetration Testing in AWS

Understand before you pentest

Understanding Vulnerability Scanning

Vulnerability Scanning generally refers to scanning of a system to find known weakness.



Understanding Penetration Testing

Penetration Tests often refers to running exploits against a given system with intention to compromise.

```
root@kali:~# msfconsole
[-] Failed to connect to the database: could not connect to server: Connection refused
      Is the server running on host "localhost" (::1) and accepting
      TCP/IP connections on port 5432?
could not connect to server: Connection refused
      Is the server running on host "localhost" (127.0.0.1) and accepting
      TCP/IP connections on port 5432?

          dBBBBBBBb  dBPP  dBBBBBBP  dBBBBBBb  .
          dB' dB' dB'  dBPP  dB'P  BB   BP
          dB' dB' dB'  dBPP  dB'P  BB   BP
          dB' dB' dB'  dBPP  dB'P  BB   BP

          dBBBBBP  dBBBBBb  dB'P  dBBBBBP  dB'P  dBBBBBBB
          dB'P  dBBBB' dB'P  dB' .BP  dB'P  dB'P
          dB'P  dB'P  dB'P  dB' .BP  dB'P  dB'P
          dB'P  dB'P  dB'P  dB' .BP  dB'P  dB'P

          o
          To boldly go where no
              shell has gone before

          =[ metasploit v4.17.3-dev
+ -- --=[ 1795 exploits - 1019 auxiliary - 310 post
+ -- --=[ 538 payloads - 41 encoders - 10 nops
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
msf > [
```



Getting Started

Earlier it was **mandatory** to submit an “AWS Vulnerability / Penetration Testing Request Form” to request the authorization for pentest to or from the AWS workloads.

AWS has now removed the clause and customers can go ahead and carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 services.

Allowed Services

Following are the supported services where prior approval is not needed.

- Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers
- Amazon RDS
- Amazon CloudFront
- Amazon Aurora
- Amazon API Gateways
- AWS Lambda and Lambda Edge functions
- Amazon Lightsail resources
- Amazon Elastic Beanstalk environments

Do note that these lists are constantly updated by AWS.

Additional Important Pointers

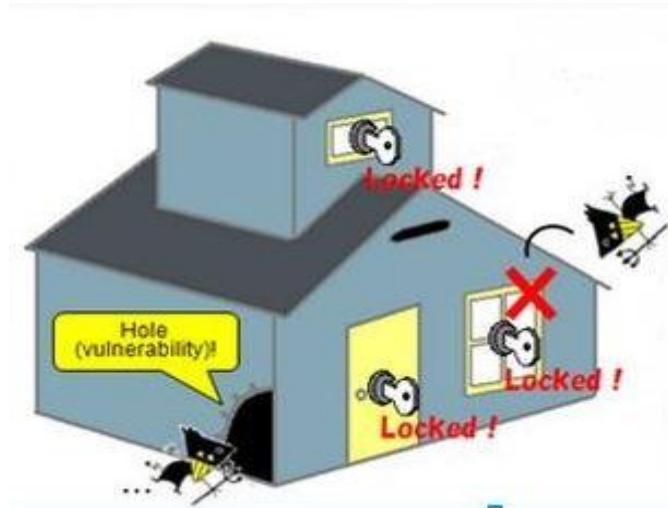
It is recommended to exclude following EC2 instance types to minimize potential disruption to your environment

- T3.nano
- T2.nano
- T1.micro
- M1.small

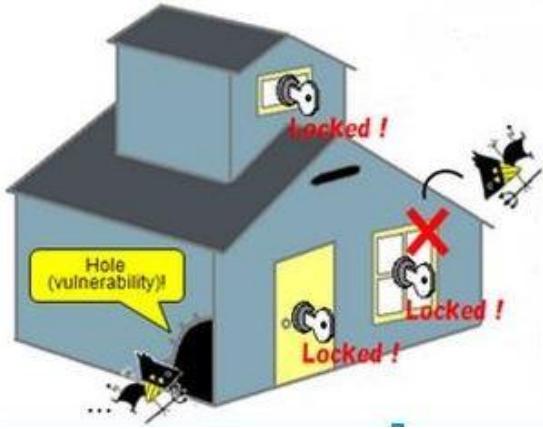
Vulnerability, Exploit, Payload

Ethical Hacking Terminology

The simple house terminology



The Answers

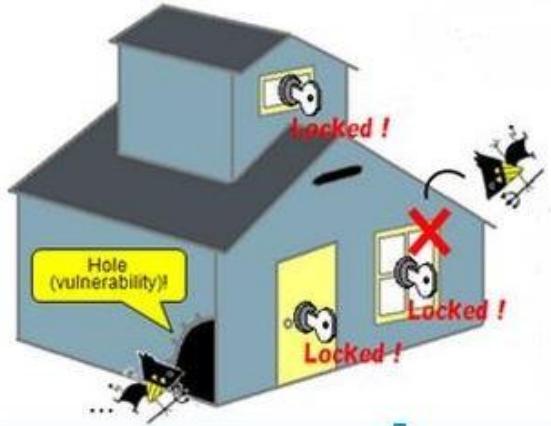


Vulnerability :- Hole on the Side of the House

Exploit :- The Robber

Payload :- What Robber does inside the house

Security Terminology



Vulnerability :- Bad Software Code

Exploit :- Program that exploits code to get inside.

Payload :- Stealing Data, Ransomwares etc.

Scan Result of Vulnerability Scanners

Internal Scan
CURRENT RESULTS: TODAY AT 9:55 PM

Configure Audit Trail Launch Export

Hosts > 127.0.0.1 > Vulnerabilities 164

| <input type="checkbox"/> | Severity ▲ | Plugin Name | Plugin Family | Count |
|--------------------------|------------|--|------------------------------|-------|
| <input type="checkbox"/> | Critical | Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : firefox regression (USN-3216-2) | Ubuntu Local Security Checks | 1 |
| <input type="checkbox"/> | Critical | Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : icu vulnerabilities (USN-3227-1) | Ubuntu Local Security Checks | 1 |
| <input type="checkbox"/> | Critical | Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : libxml2 vulnerabilities (USN-3235-1) | Ubuntu Local Security Checks | 1 |
| <input type="checkbox"/> | Critical | Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : python2.7, python3.2, python3.4, python3.5 vulnerabilities (USN-3134-1) (httpoxy) | Ubuntu Local Security Checks | 1 |
| <input type="checkbox"/> | High | PostgreSQL Default Unpassworded Account | Databases | 1 |
| <input type="checkbox"/> | High | Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : nspr vulnerability (USN-3028-1) | Ubuntu Local Security Checks | 1 |
| <input type="checkbox"/> | High | Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : nss vulnerability (USN-3029-1) | Ubuntu Local Security Checks | 1 |
| <input type="checkbox"/> | High | Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : thunderbird vulnerabilities (USN-3023-1) | Ubuntu Local Security Checks | 1 |
| <input type="checkbox"/> | High | Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : pidgin vulnerabilities (USN-3031-1) | Ubuntu Local Security Checks | 1 |

CVE & CVSS

Vulnerability Dictionary

Understanding CVE

- **CVE** stands for Common Vulnerabilities & Exposure.
- CVE are like dictionary of publicly known information security vulnerabilities.
- Primary source for CVE is “National Vulnerability Database” managed by NIST.

| CVE-ID | |
|--|--|
| CVE-2014-3556 | Learn more at National Vulnerability Database (NVD) |
| • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings | |
| Description | |
| The STARTTLS implementation in mail/ngx_mail_smtp_handler.c in the SMTP proxy in nginx 1.5.x and 1.6.x before 1.6.1 and 1.7.x before 1.7.4 does not properly restrict I/O buffering, which allows man-in-the-middle attackers to insert commands into encrypted SMTP sessions by sending a cleartext command that is processed after TLS is in place, related to a “plaintext command injection” attack, a similar issue to CVE-2011-0411. | |
| References | |
| Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete. | |
| • MLIST [nginx-announce] 20140805 nginx security advisory (CVE-2014-3556) • URL http://mailman.nginx.org/pipermail/nginx-announce/2014/000144.html • CONFIRM http://nginx.org/download/patch_2014_starttls.patch • CONFIRM https://bugzilla.redhat.com/show_bug.cgi?id=1126891 • HP-IPSOV03227 • URL http://marc.info/?l=bugtraq&m=142103967620073&w=2 | |
| Date Entry Created | |
| 20140514 | Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE. |
| Phase (Legacy) | |
| Assigned (20140514) | |
| Votes (Legacy) | |
| Comments (Legacy) | |
| Proposed (Legacy) | |
| N/A | |

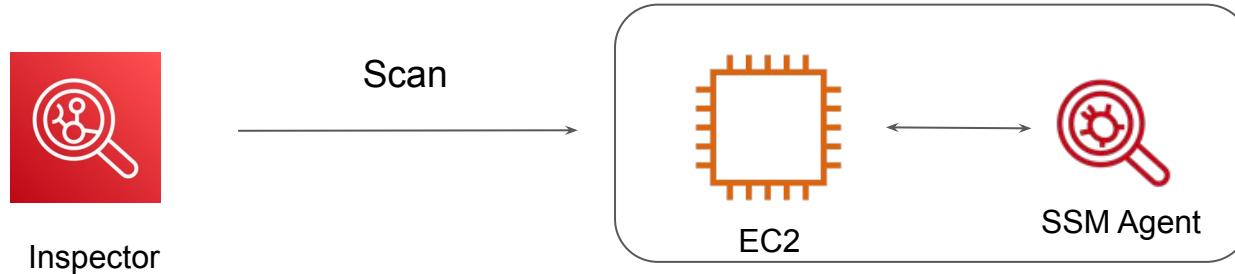
AWS Inspector

Vulnerability Scanner

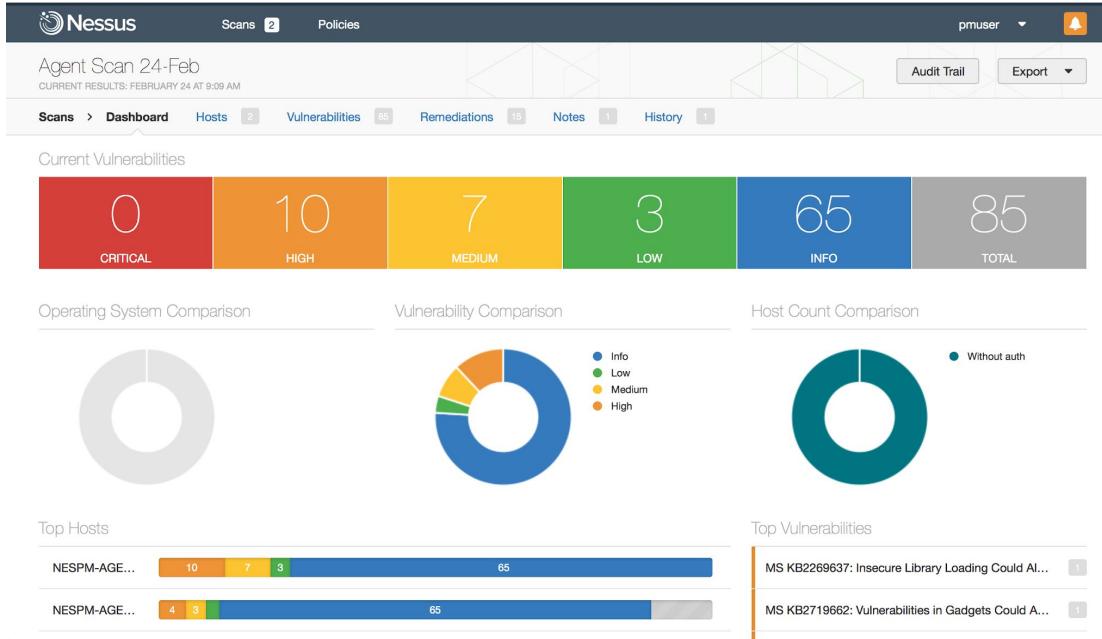
Basics of AWS Inspector

AWS Inspector is similar to a vulnerability scanner which will scan the system for specific vulnerabilities and provide the results.

It relies on the agent installed on the server to scan the server.

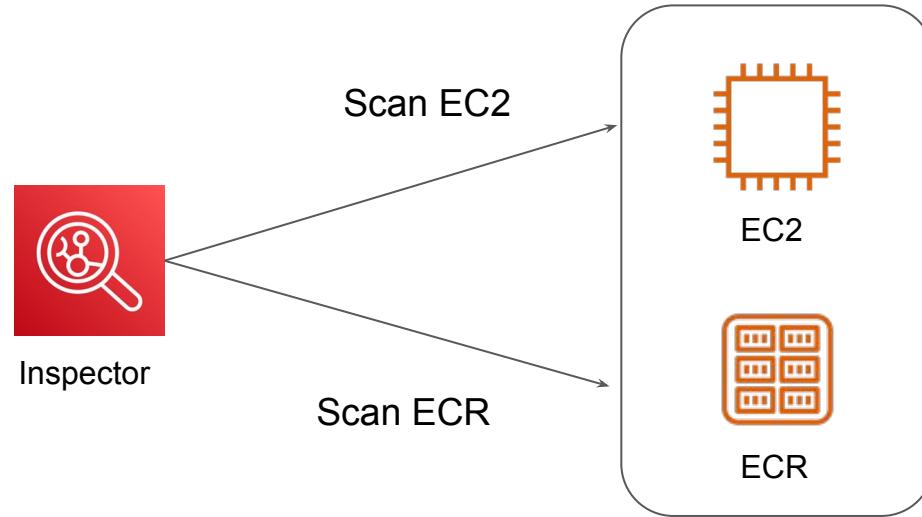


Similar to Nessus



Supported Scans

Amazon Inspector gives you the flexibility to enable either EC2 scanning or ECR container image scanning, or both.



Relax and Have a Meme Before Proceeding

When someone says
you look nice and it
makes you feel nice.

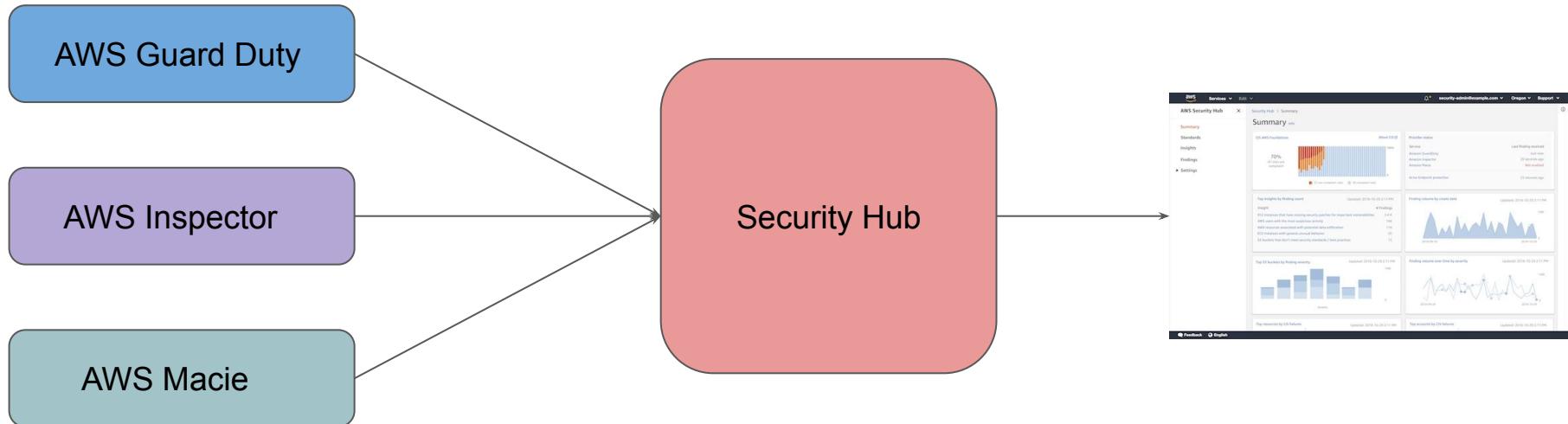


Security Hub

Centralized Security Hub

Overview of Security Hub

AWS Security Hub gives you a comprehensive view of your high-priority security alerts and compliance status across AWS accounts.



Supported Compliance Standard

AWS Security Hub also has ability to generate its own findings by running automated and continuous checks against the rules in a set of supported security standards.

Following Standards are supported:

- CIS AWS Foundation
- PCI DSS



| Standard | Passed | Failed | Score ▲ |
|--------------------------------------|--------|--------|---------|
| CIS AWS Foundations Benchmark v1.2.0 | 12 | 30 | 29% |
| PCI DSS v3.2.1 | 22 | 9 | 69% |

Web Application Firewall

Next generation firewalls

Getting started

We all know about Firewalls and in some way might have worked as well.

Firewall works on the Layer 3 and Layer 4 of the OSI model.

Main aim of firewall: Block malicious and unauthorized traffic.

However what about malicious traffic like SQL Injection attacks, XSS and many more ?

Introducing WAF

A Web Application Firewall is an application level firewall for HTTP applications.

It applies set of rules for the HTTP based conversations.

WAF generally are deployed to protect against attacks targeted towards application, specifically the ones defined in the OWASP Top 10 metrics.



WAF Vendors

There are lot of ways in which you can implement WAF and various vendors as well.

Naxsi and Modsecurity are some of the famous open sources ones.

Signal Sciences, Akamai, AWS WAF are some of the commercial vendors that offer WAF related functionalities.



AWS WAF

Protection against Layer 7 Attacks

Understanding AWS WAF Concepts

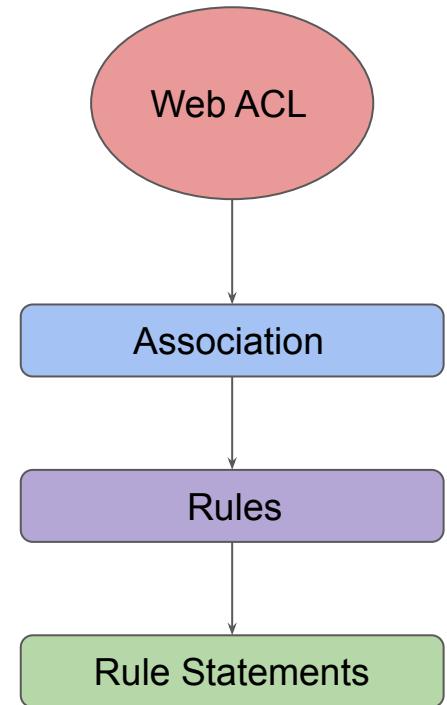
I live in a place A in Bangalore and want to meet my friend living in place B in Bangalore.

Rule Statement: If traffic is less on the roads?
Are there any Uber / OLA available?

Rules: If traffic is less AND uber ola available then yes or no

WebACL: Container for all the things + default action.

Association: Zeal



Rule Statements

Rule Statements define basic characteristics that would be analyzed within a web request.

These can be custom-defined or you can use ready-made ones from AWS and marketplace.

1. Block all the requests which are coming from out of India.
2. Block request which has a URI Path of /admin

You can even build custom condition based on:

Headers, HTTP Method, Query Strings, URI Path, Geo-Location, Body.

Rules in WAF

We can combine multiple statements into rules to precisely target requests.

WAF provides two primary rule types: **Regular Rule & Rate-Based rule**

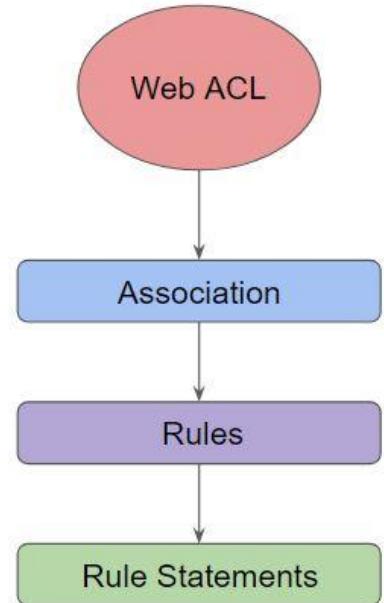
Let's look into sample regular rule:

1. If a request comes from 172.30.0.50
2. Request has SQL-like code

Rules with multiple statements can be AND, OR, NOT

Rate-Based rule = Regular Rule + Rate limiting feature

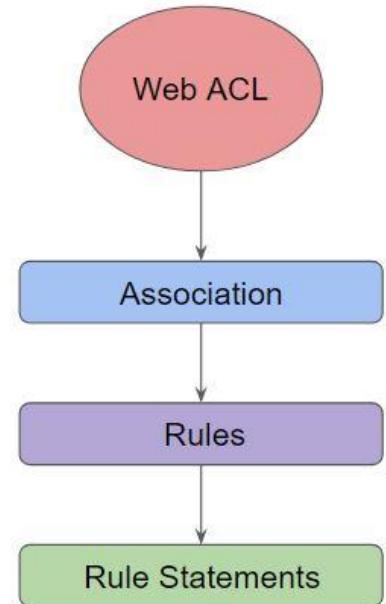
1. If a request comes from 172.30.0.50
2. If requests exceeds 1000 request in 10 minutes



Web ACL in WAF

Web ACL is a centralized place that contains the rules, rule statements and associated configuration.

It is used to define the protection strategy.

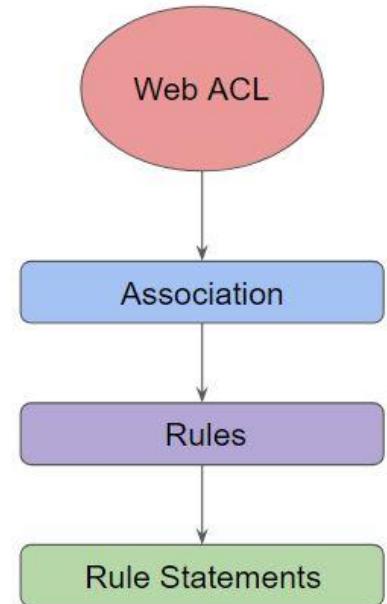


Association in WAF

Association defines to which entity WAF is associated to.

WAF cannot be associated with EC2 instances directly.

Support Association: ALB and CloudFront, API Gateway



Important Pointers

Rule Groups can be configured which has multiple rules that can be used across multiple Web ACLs.

Customers can decide to use ready-made AWS-Managed rules or even rules from AWS Marketplace.

Every Rule has a priority. If a request matches Priority 0 rule, none of the other rules will inspect the request

Pricing Aspect:

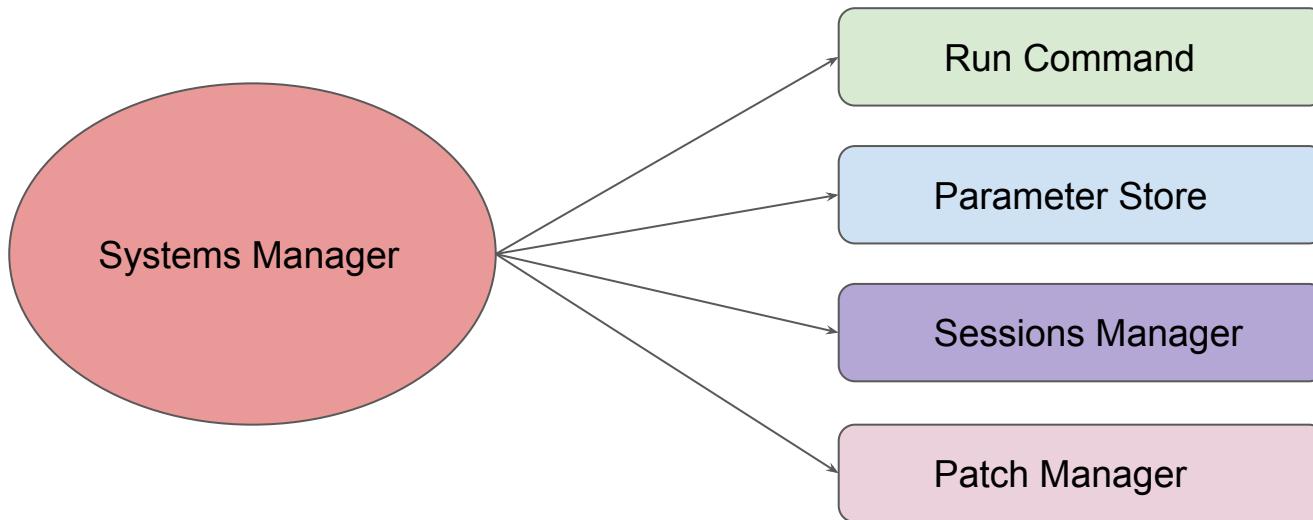
Web-ACL (\$5 per month), Rule (\$1 per month), Requests (\$0.60 / 1 million)

AWS Systems Manager

Interesting Set of Services

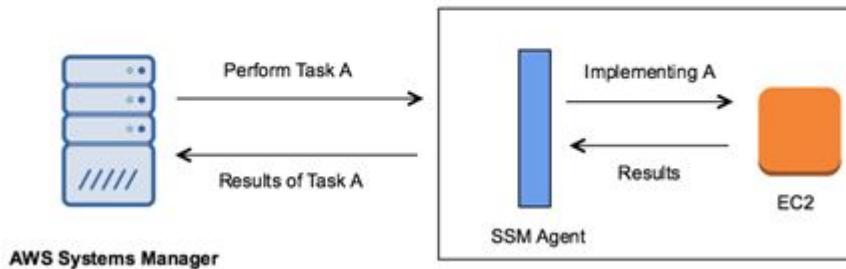
Overview of Systems Manager

AWS Systems Manager is a group of services which allows customers to have a better visibility and control of the infrastructure.



High Level Overview

The basic idea behind the " Systems Manager" is that there will be an SSM agent installed in the EC2 instances, and the customer can provide specific tasks to the installed agent from the systems manager console.

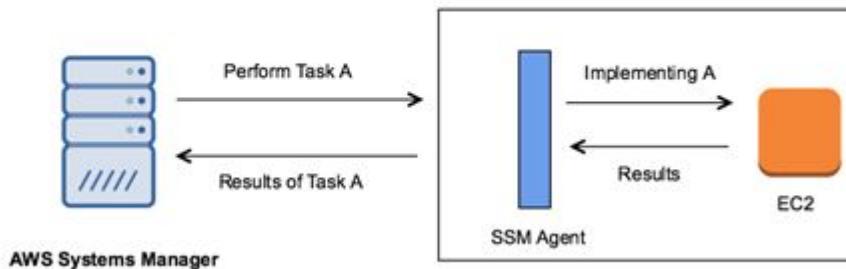


Configuring SSM Agent

Systems Manager Agent

High Level Overview

The basic idea behind the " Systems Manager" is that there will be an SSM agent installed in the EC2 instances, and the customer can provide specific tasks to the installed agent from the systems manager console.



Overview of the SSM Agent

AWS Systems Manager Agent (SSM Agent) is Amazon software that can be installed and configured on an Amazon EC2 instance, an on-premises server, or a virtual machine (VM).

SSM Agent is preinstalled, by default, on the following Amazon Machine Images (AMIs):

- Amazon Linux
- Amazon Linux 2
- Ubuntu Server 16.04, 18.04, and 20.04
- Amazon Linux 2 ECS-Optimized Base AMIs

Required Permissions

By default, AWS Systems Manager doesn't have permission to perform actions on your instances

You need to attach IAM role with [AmazonSSMManagedInstanceCore](#) policy to allow an instance to use Systems Manager service core functionality.

Systems Manager - Sessions Manager

Interesting Set of Services

Overview of Sessions Manager

Sessions Manager allows customers to connect to the instances through an interactive one-click browser-based shell or through the AWS CLI.



Difference Between EC2 Connect & Sessions Manager

| | EC2 Connect | Sessions Manager |
|---------------------|--------------------|-------------------------|
| IAM Role for EC2 | Not Required | Required |
| Security Group (22) | Required | Not Required |
| Public IP | Required | Not Required |

Benefits of Sessions Manager

Some of the notable benefits of Sessions Manager are as follows:

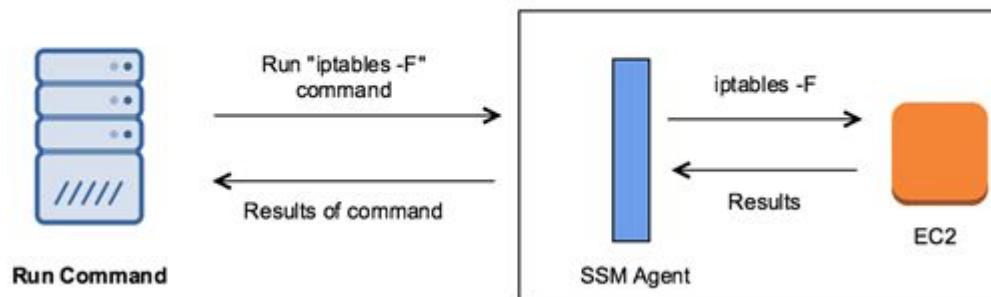
- Centralized Access Control using IAM Policies
- No Inbound Ports Needs to be Open
- Logging and auditing session activity
- One-click access to instances from the console and CLI
- No need of VPN to connect to instances.

Systems Manager - Run Command

Running Commands Remotely

Overview of Run Command

Run Command, as the name suggests allows us to run specific commands in the instances where SSM agent is installed.



Document Feature

Run Command provides much more granular features because of its “command document” feature.

There are various command document available that can perform certain ready-made actions.

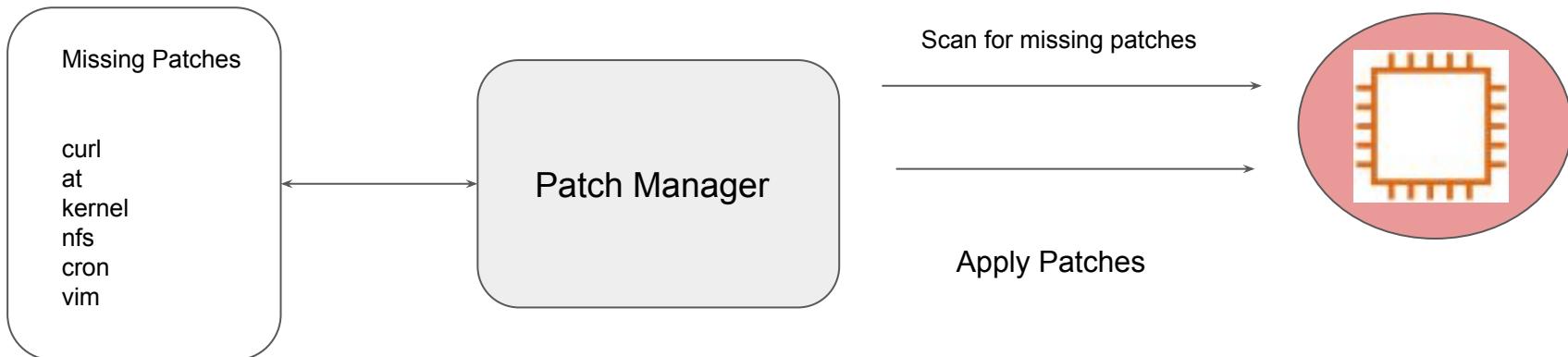
- AWS-RunAnsiblePlaybook
- AWS-ConfigureDocker
- AWS-InstallMissingWindowsUpdates
- AWS-RunShellScript

Systems Manager - Patch Manager

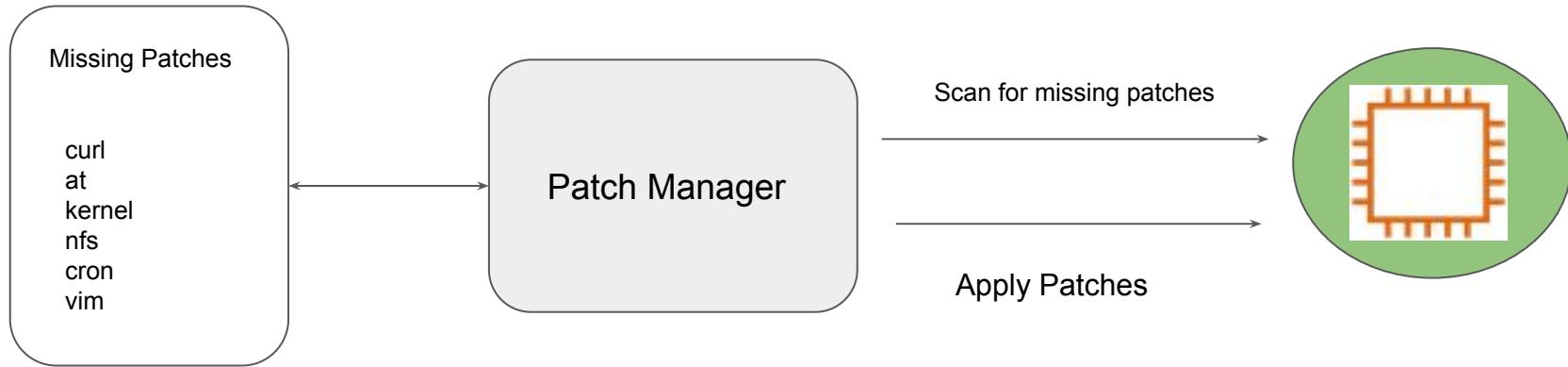
Interesting Set of Services

Overview of Patch Manager

Patch Manager automates the process of patching managed instances with both security related and other types of updates.



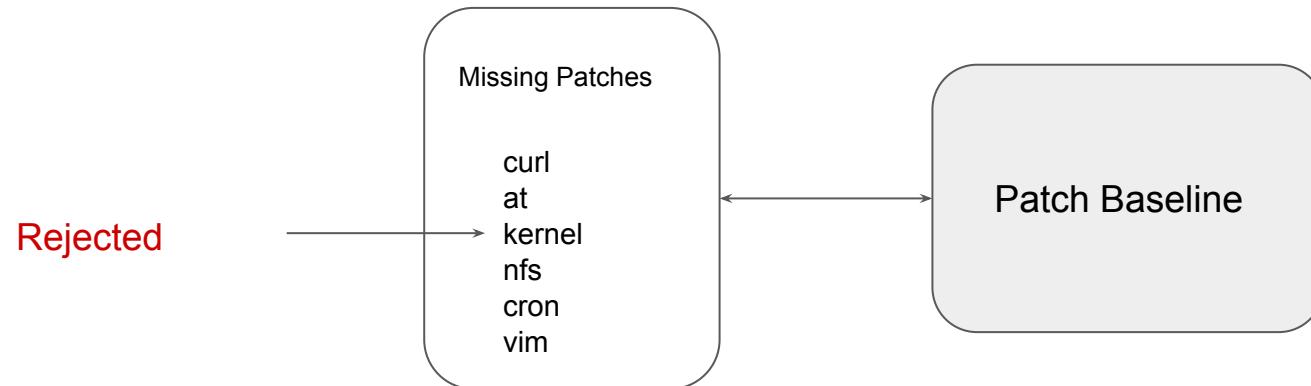
After Patching



Patch Baseline

Patch Baseline service determines the list of missing patches that need to be installed in the EC2 instance.

A patch baseline defines which patches are approved for installation on your instances. You can specify approved or rejected patches one by one.



Maintenance Window

Maintenance Window provides a mechanism for scheduling a particular activity on the specific target.

Example: Perform Patching activity at 2 AM in the morning.



SSM - Automation

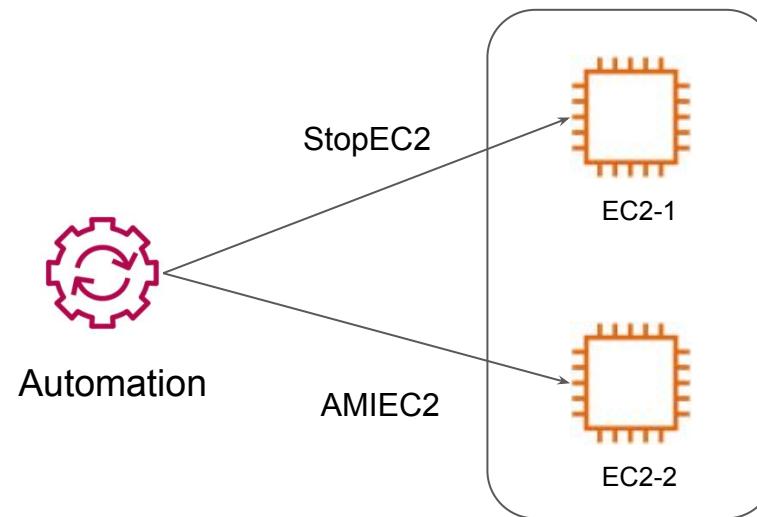
Automate Everything

Overview of SSM Automation

Automation, a capability of AWS Systems Manager, simplifies common maintenance and deployment tasks Amazon EC2 instances and other AWS resources.

Example Automation Tasks:

- Attach IAM to EC2 Instances
- Create AMI of Instances
- Perform Patching Activities



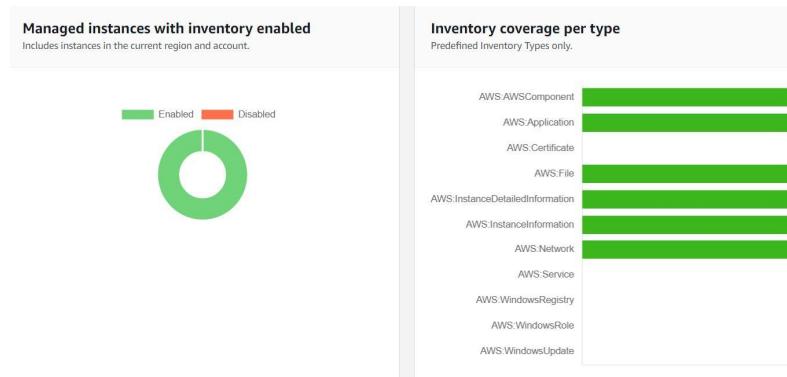
SSM - Inventory

Automate Everything

Overview of SSM Inventory

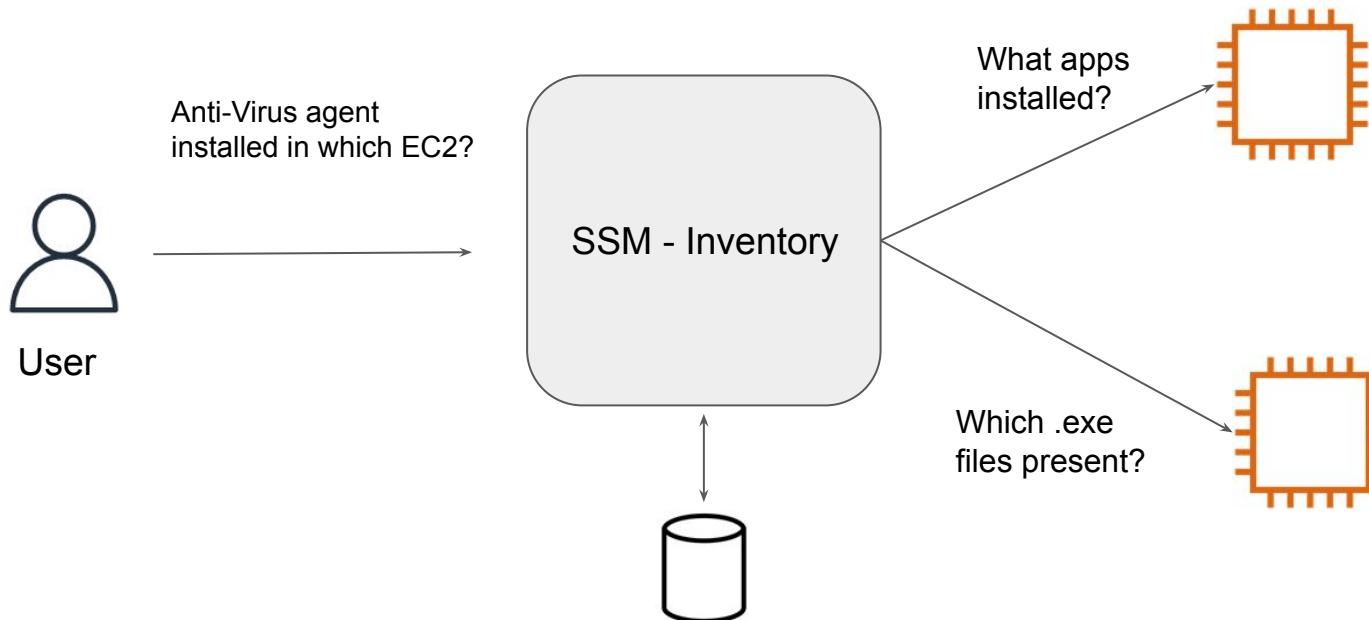
AWS Systems Manager Inventory provides visibility into your Amazon EC2 and on-premises computing environment.

It can capture various informations like Application Names, Files, Network Configuration, Instance Details, Windows Registry and others.

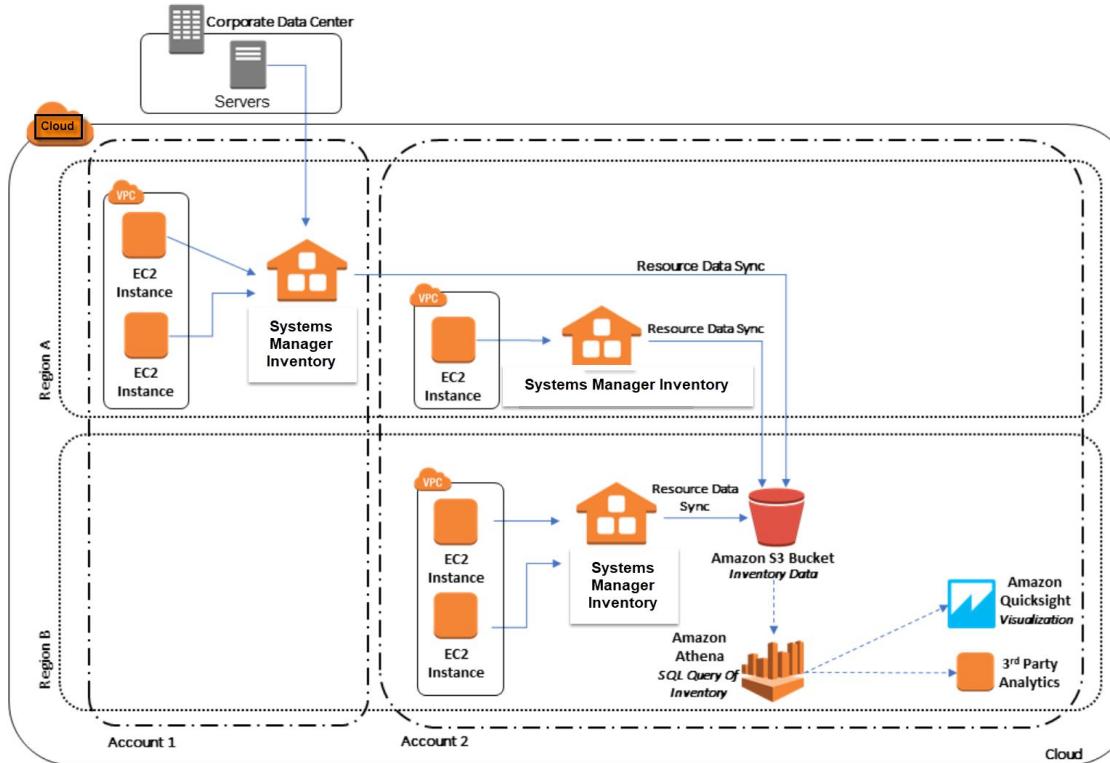


Overview of SSM Inventory

Administrator can run various queries to search for specific data based on the use-case.



Centralized Architecture



Unified CloudWatch Agent

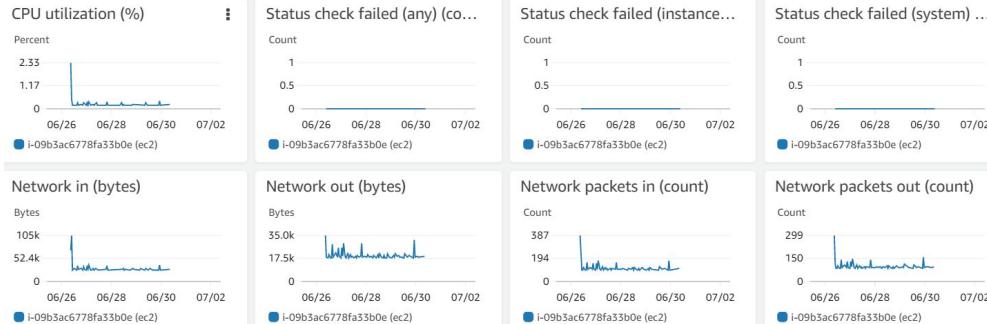
Metrics and Logs

Default CloudWatch Metrics

When we launch an EC2 instance in AWS, there are certain metrics that are captured by default.

Some of these include:

- CPU Utilization
- Network Related
- Disk Related

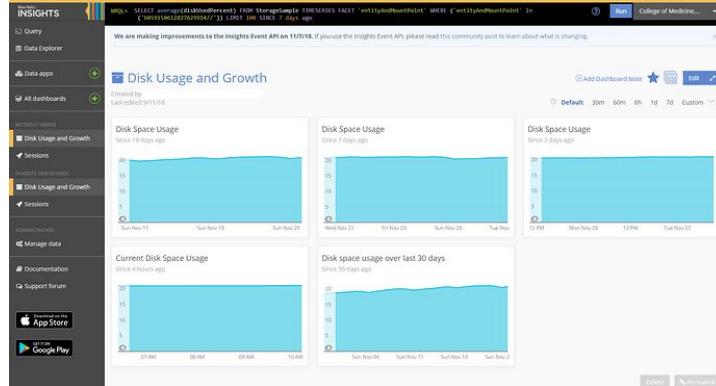


Challenge 1 -More Metrics Are Needed

There are various important metrics that needs to be collected in addition to the default ones.

Some of these include:

- Memory Metrics
- Disk Usage Metrics
- Netstat related.

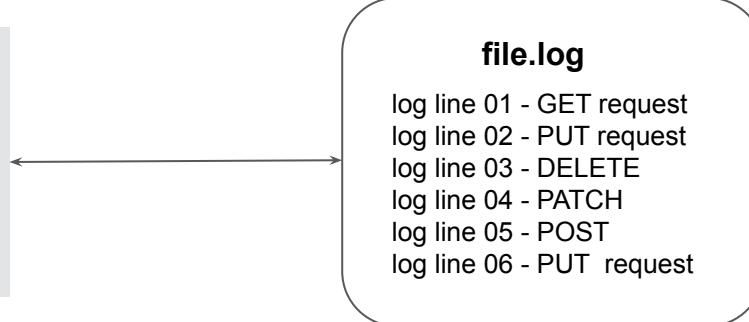


Challenge 2 - Log Monitoring

A server can contain a lot of log files, from system logs to the application logs.

During debugging, it is important to have log files at hand.

This means in default case; you need to give access to the server to an individual who wants to debug.

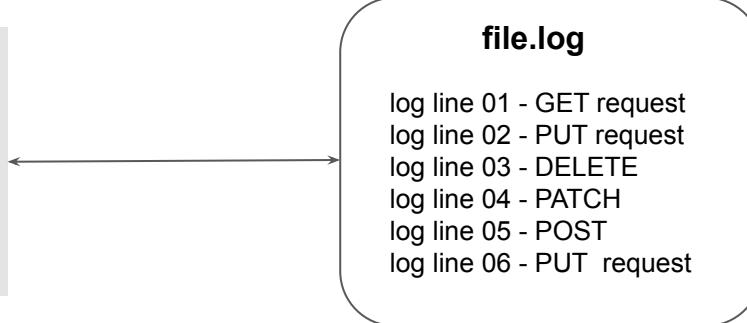


Disadvantage of the Approach

Access must be given to the server to the developers.

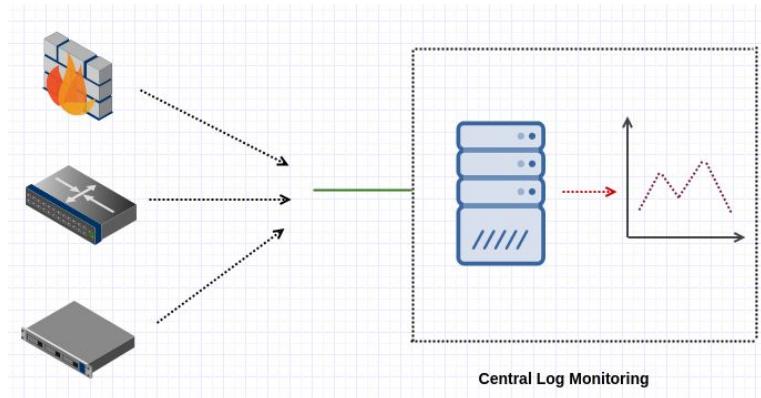
If the server gets terminated, the logs are lost.

No way to set up an alarm on certain conditions or create complex filters.



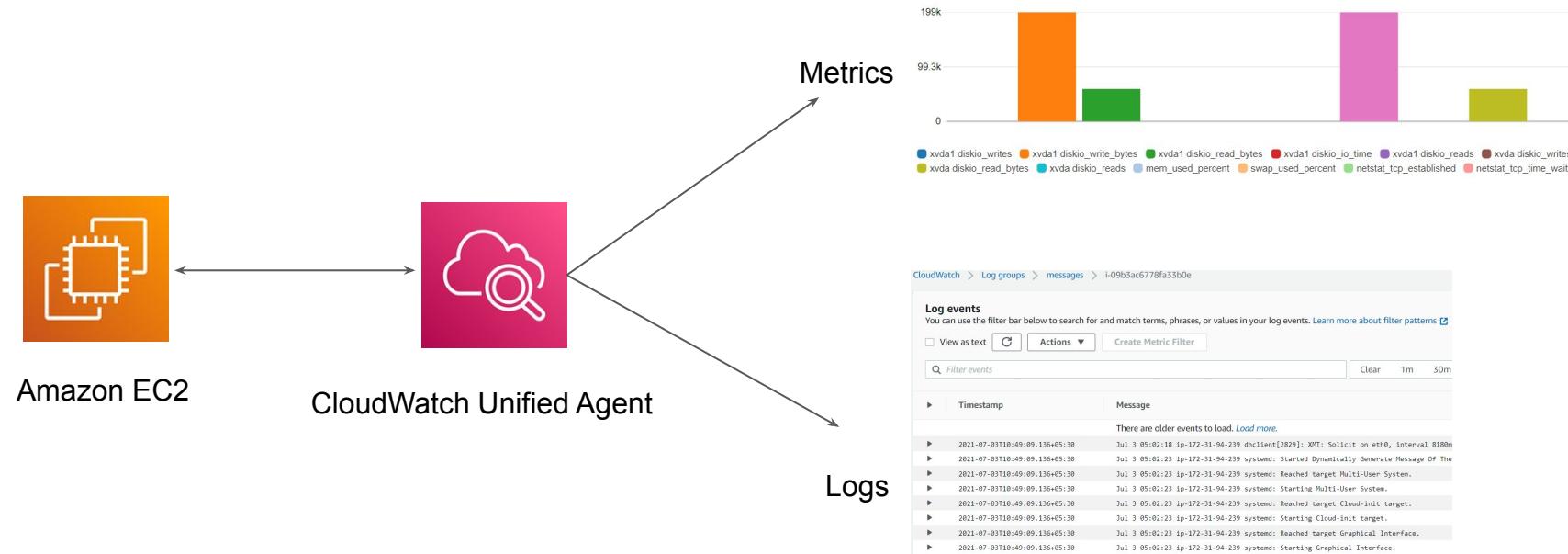
Better Way

- We create a Central Log Server.
- We push the log files from individual systems to Central Log Server.



Introducing Unified CloudWatch Agent

Unified CloudWatch Agent allows customers to capture both the internal system level metrics as well as logs collection.



How-To Steps

1. Create a IAM Role with CloudWatchAgentServer policy.
2. Create EC2 using IAM Role.
3. Install CloudWatch Agent.
4. Run CloudWatch Agent Configuration Wizard
5. Start Unified CloudWatch Agent.

Relax and Have a Meme Before Proceeding

When you're the only one who
can pass the helicopter mission
in GTA Vice City and your friend
call you to pass it for him

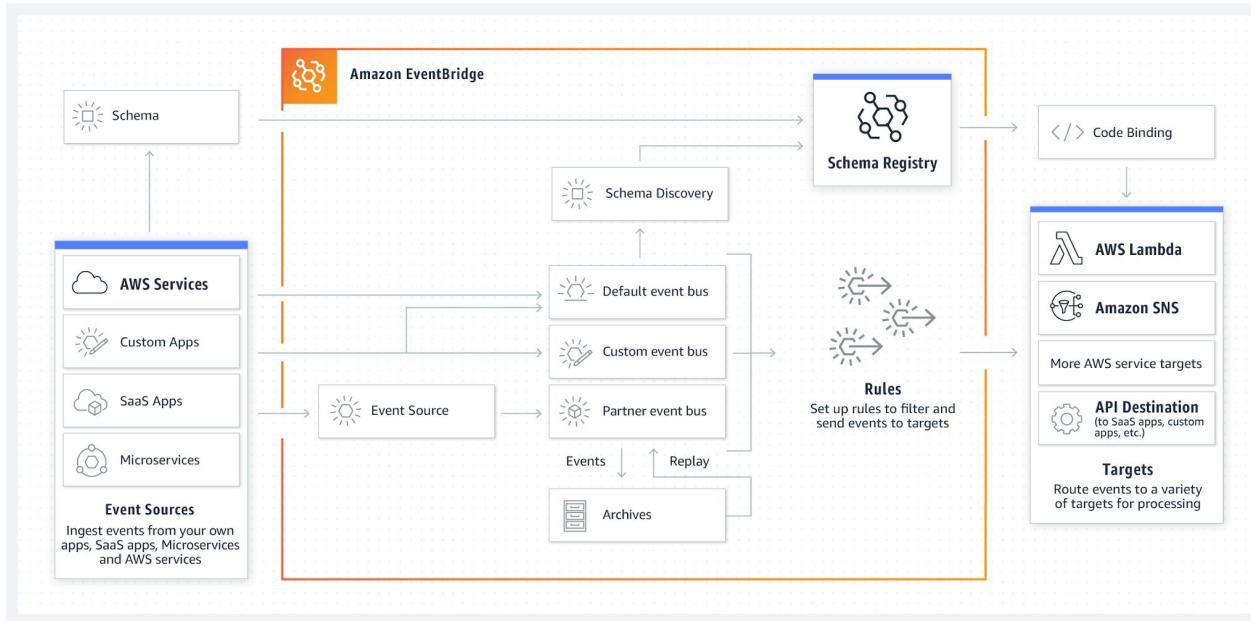


Amazon EventBridge

Connecting Services

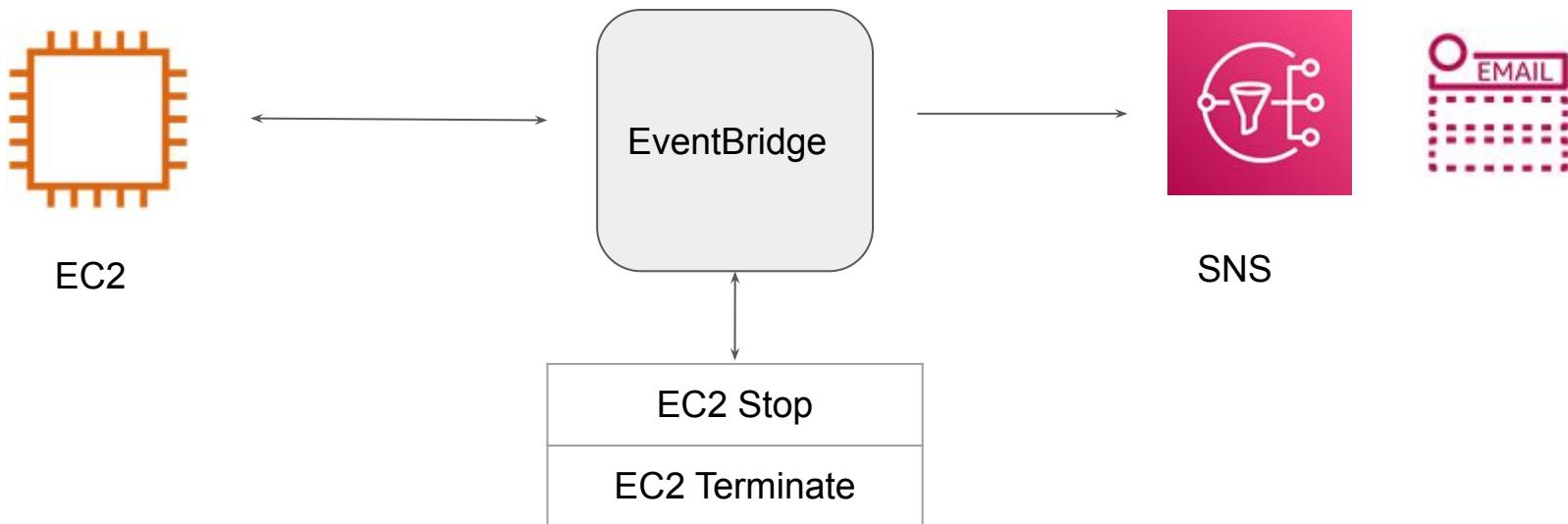
Overview of Amazon Event Bridge

EventBridge delivers a stream of real-time data from event sources to targets.



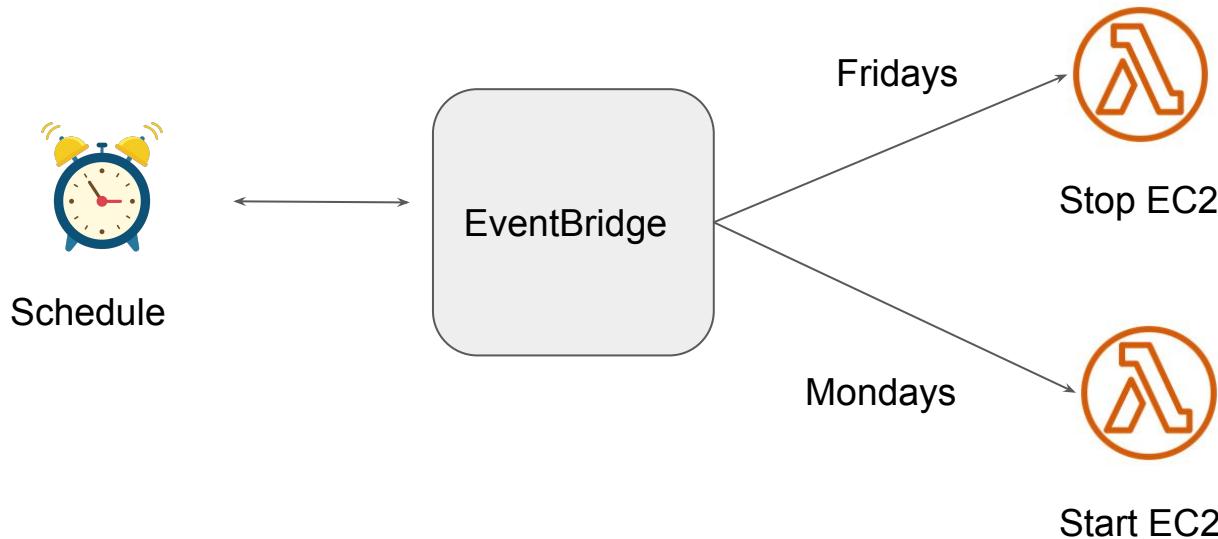
Use-Case 1: EC2 to SNS

Whenever a EC2 instance is stopped, Administrator should be notified.



Use-Case 2: Stop Dev EC2 Instances

Stop all DEV instances at 8PM on Fridays and Start at 9 AM on Mondays.

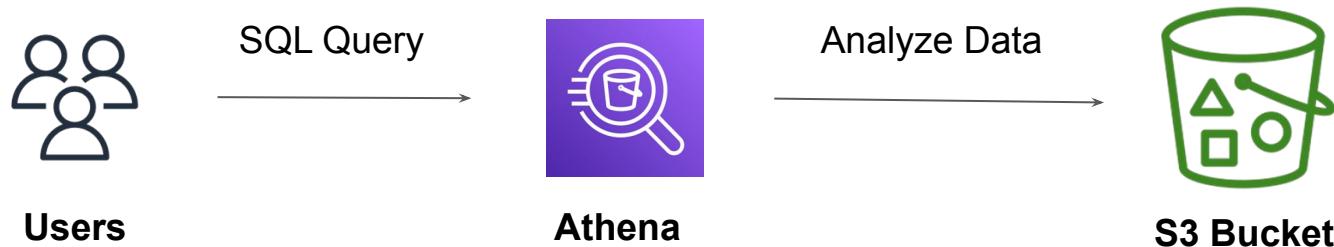


Amazon Athena

Query Logs from S3

Getting the basics right

Amazon Athena is service that allows us to analyze various log files from a data source using standard SQL



Approach Before Athena

You have CloudTrail logs in S3 and you want to see who has logged in, in the past 10 days.

- Create EC2 instances.
- Deploy monitoring stack like Splunk, ELK or others.
- Add the data source from S3 to import CloudTrail logs.
- Begin Analyzing.

AWS Config

Overview of Infrastructure Changes

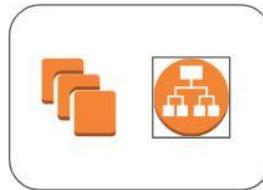
AWS Config - High Level Overview

AWS Config is primarily used to record the resource configuration changes over time.

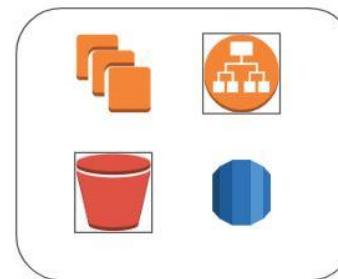
An EC2 instance was hosting website from past 90 days. Suddenly in last one week, there have been a lot of issues with the requests. What was changed?



Week 1



Week 2



Week 3

Audit and Compliance

AWS Config comes with large set of rules that can continuously monitor your AWS environment and report the findings.

| Noncompliant rules by noncompliant resource count | |
|--|---|
| Name | Compliance |
| RootAccountHardwareMFAEnabled-conformance-pack-zcx0hyuom | ⚠ 1 Noncompliant resource(s) |
| RootAccountMFAEnabled-conformance-pack-zcx0hyuom | ⚠ 1 Noncompliant resource(s) |
| IAMPasswordPolicy-conformance-pack-zcx0hyuom | ⚠ 1 Noncompliant resource(s) |
| approved-amis-by-id | ⚠ 1 Noncompliant resource(s) |
| cloudtrail-security-trail-enabled | ⚠ 1 Noncompliant resource(s) |

[View all noncompliant rules](#)

Conformance Packs

A conformance pack is a collection of AWS Config rules and remediation actions that can be easily deployed

The screenshot shows the 'Deploy conformance pack' wizard. The left sidebar lists three steps: Step 1 (Specify template), Step 2 (Specify conformance pack details), and Step 3 (Review and deploy). The main area is titled 'Step 1 Specify template'. It features a search bar with the placeholder 'Search' and a dropdown menu showing a list of pre-defined templates. The first item in the list is 'Operational Best Practices for Amazon S3', which is highlighted. Other items include 'Operational Best Practices for Asset Management', 'Operational Best Practices for BCP and DR', 'Operational Best Practices for BNM RMIT', 'Operational Best Practices for CCN ENS Low', 'Operational Best Practices for CCN ENS Medium', 'Operational Best Practices for CIS AWS v1_3 Level1', 'Operational Best Practices for CIS AWS v1_3 Level2', 'Operational Best Practices for CIS', 'Operational Best Practices for CMMC Level 1', 'Operational Best Practices for CMMC Level 2', 'Operational Best Practices for Compute Services', 'Operational Best Practices for Data Resiliency', and 'Operational Best Practices for Amazon S3'. To the right of the dropdown, there is descriptive text about AWS accounts and a note about creating your own template. At the bottom, a link to 'Conformance Pack Sample Templates' is provided, along with 'Cancel' and 'Next' buttons.

Pricing of AWS Config

You pay \$0.003 per configuration item recorded in your AWS account per AWS Region. A configuration item is recorded whenever a resource undergoes a configuration change or a relationship change.

Based on rule evaluation. A rule evaluation is recorded every time a resource is evaluated for compliance against an AWS Config rule.

You are charged per conformance pack evaluation in your AWS account per AWS Region based on the tier below.

AWS Config Aggregator



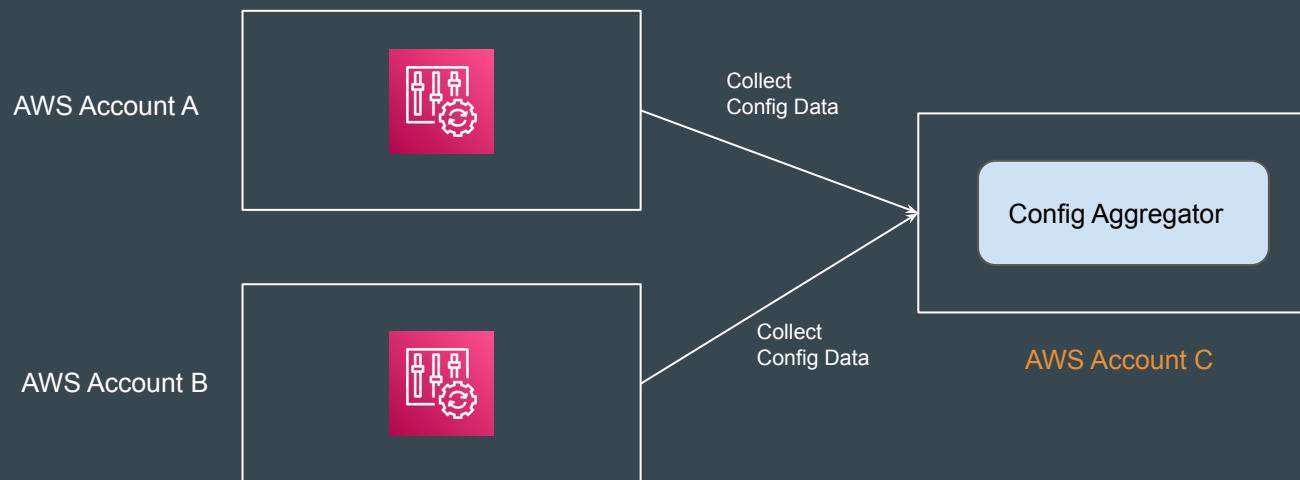
Understanding the Basics

An **aggregator** is an AWS Config resource type that collects AWS Config configuration and compliance data from the following:

1. Multiple accounts and multiple regions.
2. Single account and multiple regions.
3. An organization in AWS Organizations and all the accounts in that organization which have AWS Config enabled.

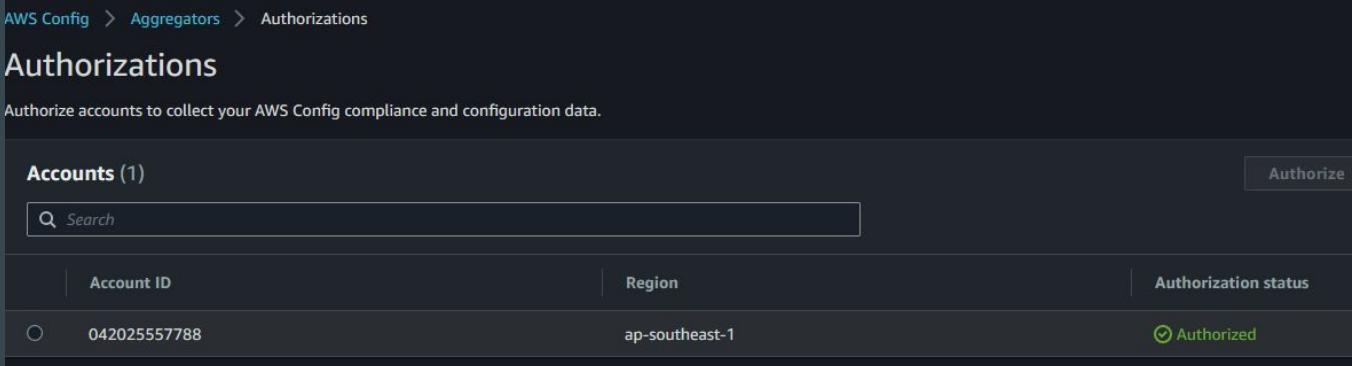
Understanding the Workflow

Config Aggregator can collect Config Data from multiple external accounts.



Important Step - Authorization

In the external accounts, you need to allow a specified aggregator account and Region to collect AWS Config configuration and compliance data from your current account.



The screenshot shows the AWS Config Authorizations page. The navigation bar at the top includes links for AWS Config, Aggregators, and Authorizations. The main title is "Authorizations" with the subtitle "Authorize accounts to collect your AWS Config compliance and configuration data." Below this, there is a section titled "Accounts (1)" with a search bar. A single account is listed in the table:

| Account ID | Region | Authorization status |
|--------------|----------------|----------------------|
| 042025557788 | ap-southeast-1 | Authorized |

External AWS Account

Trusted Advisor

Recommendations are always good

What is Trusted Advisor ?

AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five major categories:

Cost Optimization



6 ✓ 3 ▲ 0 !

\$10.63

Potential monthly savings

Performance



10 ✓ 0 ▲

0 !

Security



11 ✓ 1 ▲

5 !

Fault Tolerance



13 ✓ 2 ▲

2 !

Service Limits



48 ✓ 0 ▲

0 !

Trusted Advisor Check Categories

| Categories | Description |
|-------------------|--|
| Cost optimization | Recommendations that can potentially save you money. |
| Performance | Recommendations that can improve the speed and responsiveness of your applications. |
| Security | Recommendations for security settings that can make your AWS solution more secure. |
| Fault tolerance | Recommendations that help increase the resiliency of your AWS solution. |
| Service limits | Checks the usage for your account and whether your account approaches or exceeds the limit for AWS services and resources. |

CloudTrail

Let's Monitor Everything !

Importance of Recording Everything

Installing video surveillance systems allows us to monitor activities round the clock and provides lots of benefits, some of these include:

1. Deterring Criminals
2. Helps in Investigation.
3. Regular monitoring of activities.
4. Insurance Benefits.



Recording at AWS Level

It is **VERY** important for organizations to record the activities that happen within the Infrastructure as well as the servers.

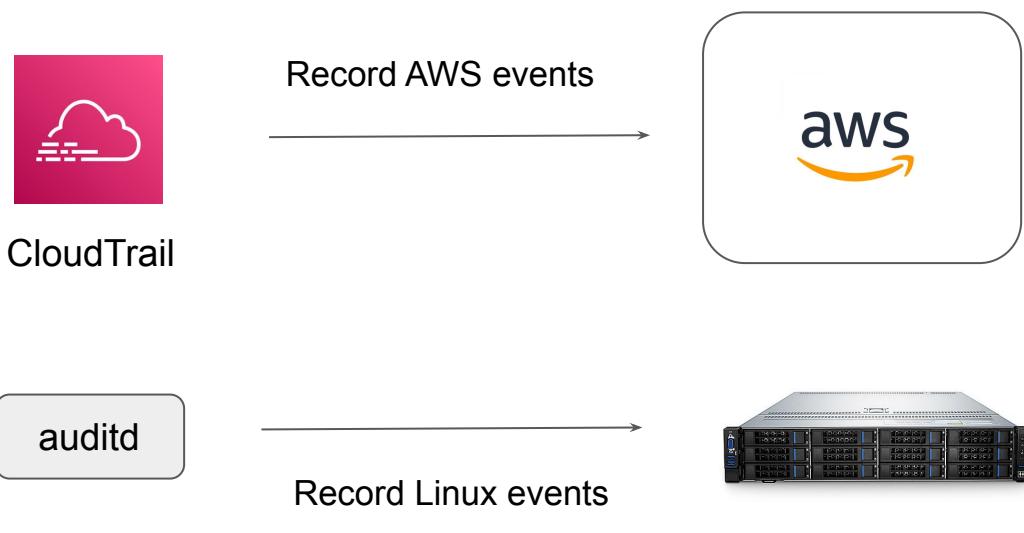
Example Auditor Question :-

Show me what did Anne did on 3rd of January 2017 between 10 AM to 2 PM.

| User | Action | Time |
|-------|-------------|----------|
| James | Logged In | 3:50 PM |
| Anne | Modified SG | 7:30 PM |
| Susan | New EC2 | 11:00 PM |

Tools for Recording

Depending on the type of resource you use, the tools for recording might also change.



CloudTrail Event Types

Monitor Everything

Type of Events

There are three types of events that can be logged in CloudTrail:

1. Management events
2. Data events
3. Insights events.

The screenshot shows the 'Events' configuration page. It includes a summary section for 'Events' with an 'Info' link and a note about additional charges. Below this, there's a 'Event type' section with a sub-instruction to choose the type of events to log. Three checkboxes are present: 'Management events' (checked), 'Data events' (unchecked), and 'Insights events' (unchecked). Each checkbox has a descriptive subtitle below it.

Events [Info](#)
Record API activity for individual resources, or for all current and future resources in AWS account. [Additional charges apply](#)

Event type
Choose the type of events that you want to log.

Management events
Capture management operations performed on your AWS resources.

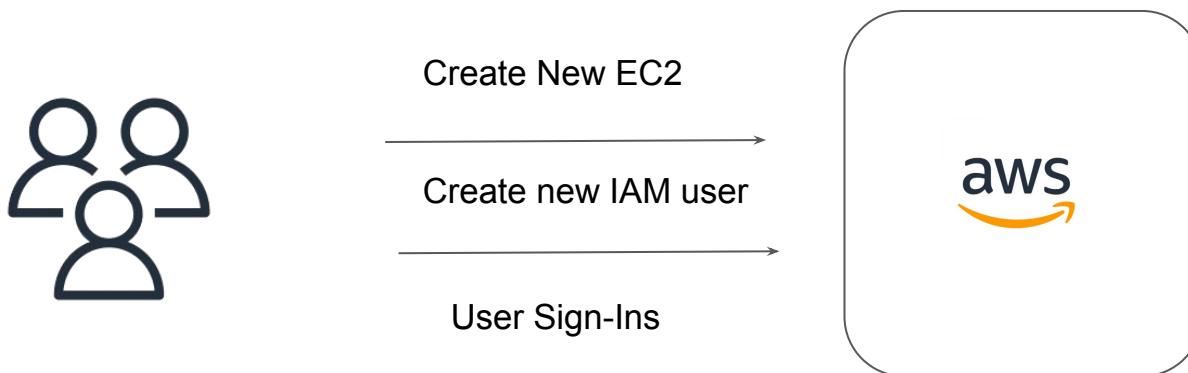
Data events
Log the resource operations performed on or within a resource.

Insights events
Identify unusual activity, errors, or user behavior in your account.

By default, trails log management events, but not data or Insights events.

1. Management Events

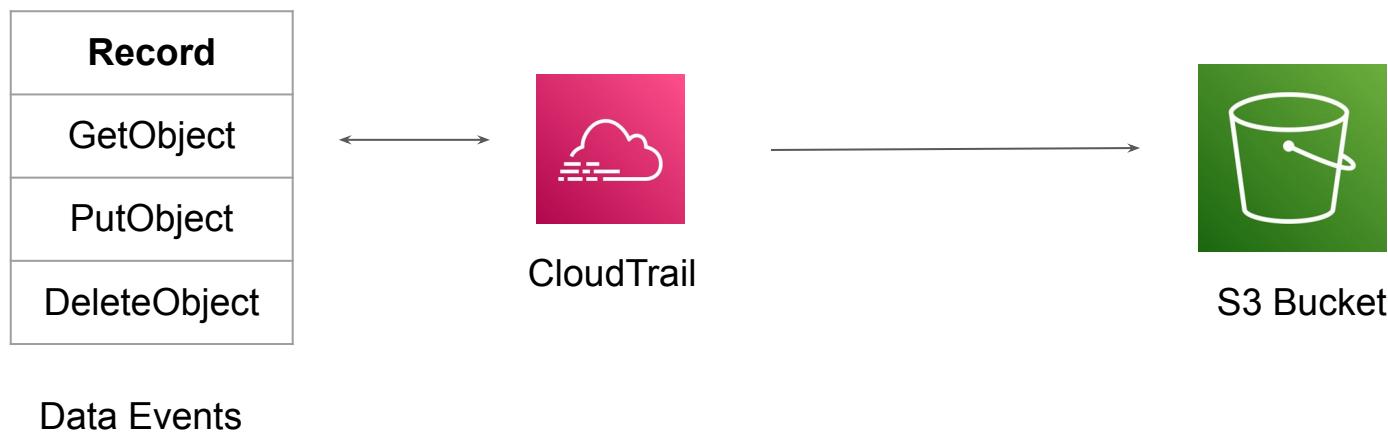
Management events provide information about management operations that are performed on resources in your AWS account.



2. Data Events

Data events provide information about the resource operations performed on or in a resource and are often high-volume activities.

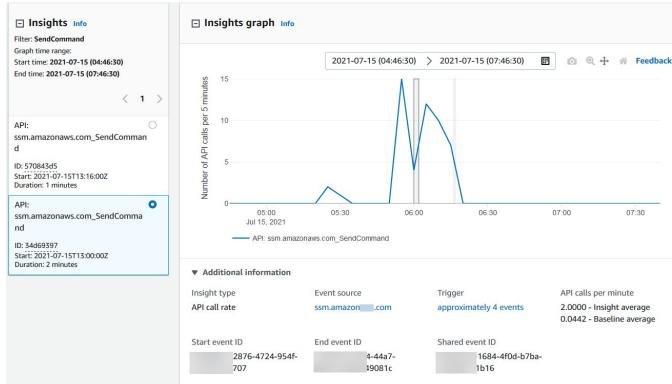
Following diagram shows type of events capture at S3 level when Data events is enabled.



3. Insights Events

Insight Events helps customers identify unusual operational activity in their AWS accounts such as spikes in resource provisioning, bursts of AWS Identity and Access Management (IAM) actions

Is designed to automatically analyze management events to establish a baseline for normal behavior, and then raise issues by generating Insights events when it detects unusual patterns.



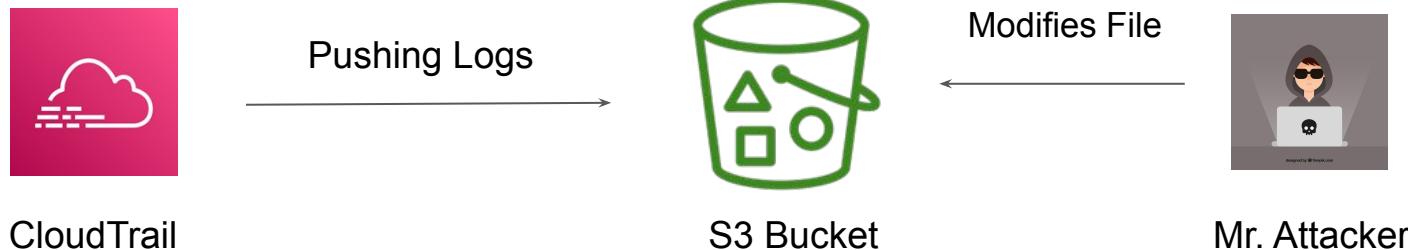
CloudTrail - Log File Integrity Validation

Back to Security!

Getting Started

CloudTrail log file integrity validation allows us to determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it.

This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing.



Basic Working

When you enable log file integrity validation, CloudTrail creates a hash for every log file that it delivers.

Every hour, CloudTrail also creates and delivers a file that references the log files for the last hour and contains a hash of each. This file is called a digest file.

Relax and Have a Meme Before Proceeding

Do you have a special talent?

Me:



Amazon Macie

Machine Learning based Security

Core Feature of Macie

S3 might contain sensitive information like PII data, database backups, SSL private keys and various others.

Amazon Macie **makes use of machine learning** to identify sensitive data stored in AWS.

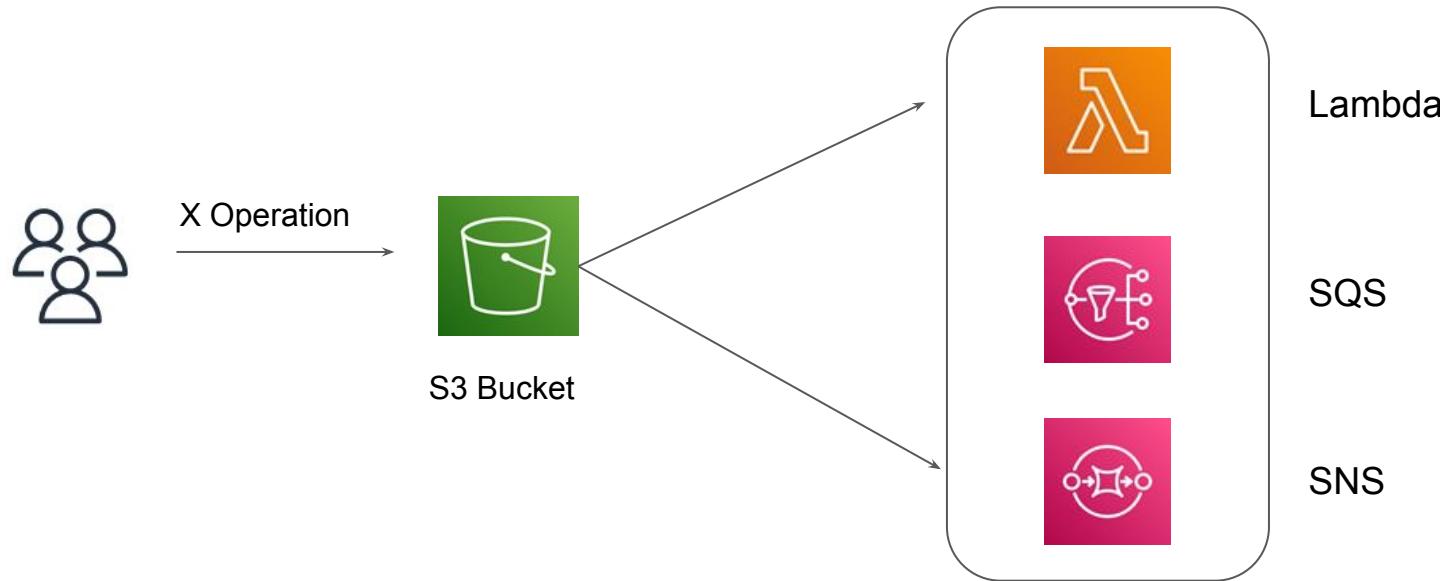
| Policy findings | | C |
|-----------------------------|---|--------------|
| Most recent policy findings | | |
| High | Policy:IAMUser/S3BucketReplicatedExternally | 1 minute ago |
| High | Policy:IAMUser/S3BlockPublicAccessDisabled | 1 minute ago |
| High | Policy:IAMUser/S3BucketSharedExternally | 1 minute ago |
| Medium | Policy:IAMUser/S3BucketEncryptionDisabled | 1 minute ago |
| High | Policy:IAMUser/S3BucketPublic | 1 minute ago |

S3 Event Notification

S3 is more than just storage

Overview of S3 Event Notification

The Amazon S3 notification feature enables you to receive notifications when certain events happen in your bucket.



VPC Flow Logs

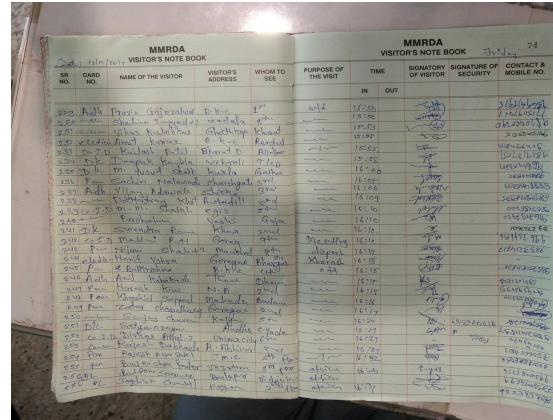
Logs are Awesome

Simple Analogy - Visitor Register

In many of the societies across India, whenever a visitor visits, they first have to fill in their information in the visitor register.

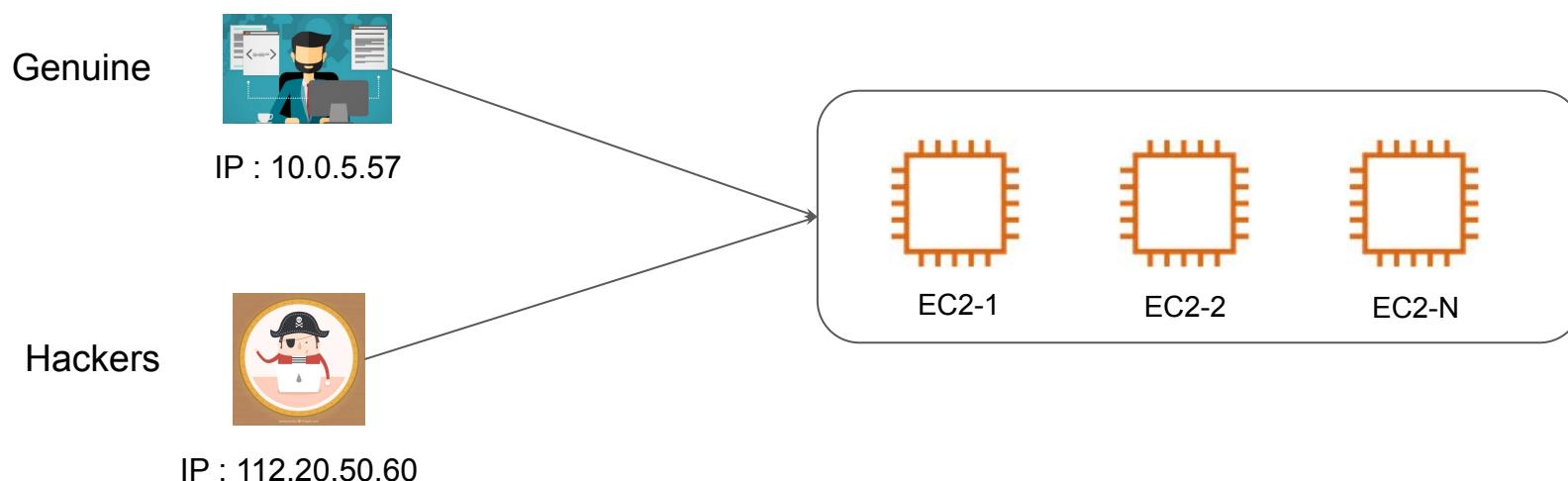
Some of the information includes:

- Name
- Source Place.
- Destination Place.
- Entry and Exit Date/Time
- Purpose of Work



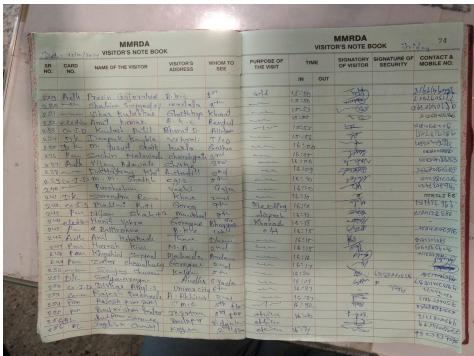
Comparing Analogy with AWS Environment

Even in AWS, there can be thousands of users across the world who might be visiting your environment.

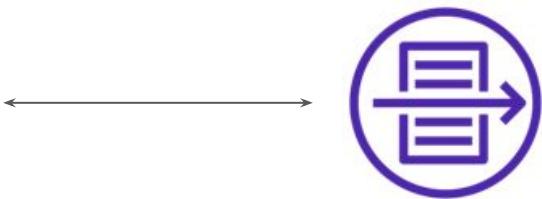


VPC Flow Logs

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC.



Visitor Register

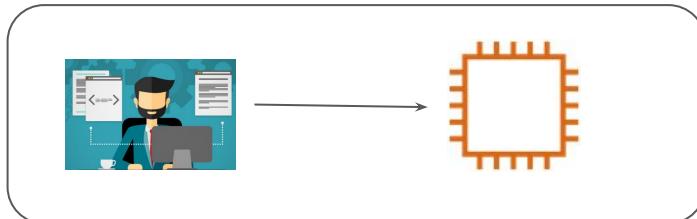


VPC Flow Log

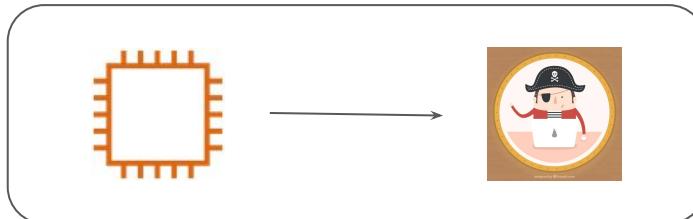
Capture Information Scope

The scope of the VPC Flow logs:

1. Record the traffic information that is visiting the resource (eg EC2)
2. Record data about resource connecting to which outbound endpoint.



10.77.2.50 → EC2 Instance



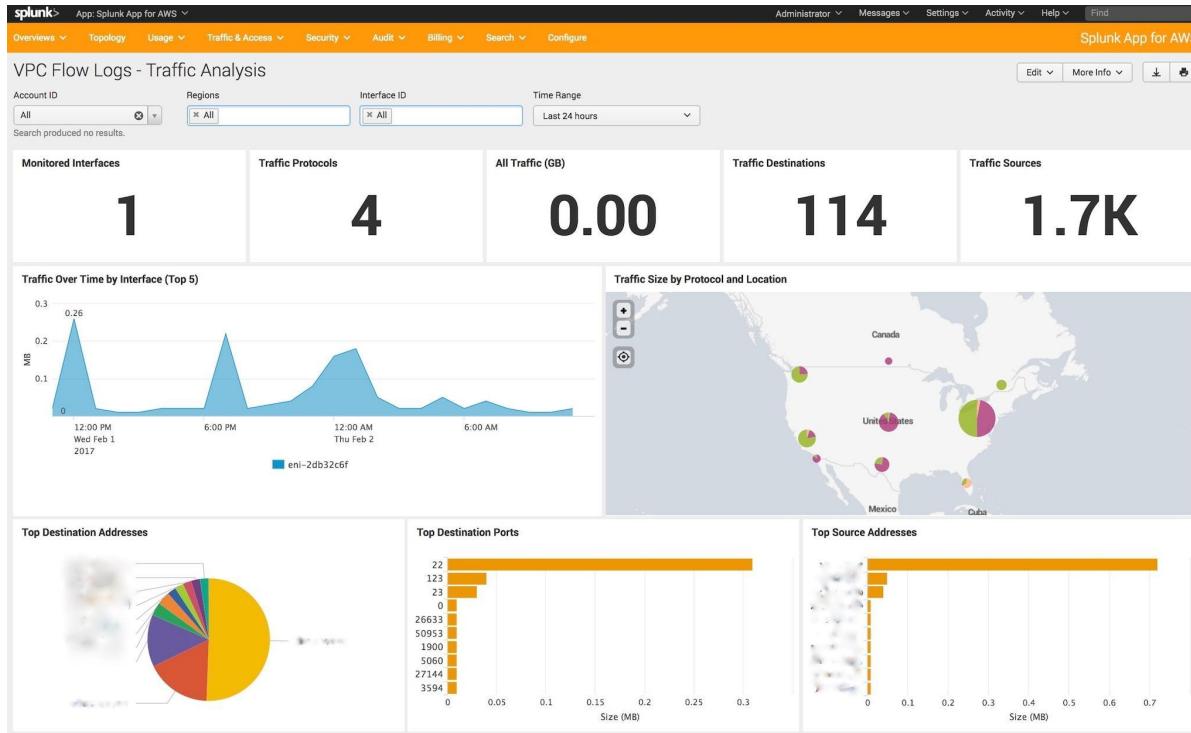
EC2 Instance → 192.168.0.5

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

| <input type="checkbox"/> View as text |  Actions ▾ | Create Metric Filter |
|---|---|--|
| Filter events | | Clear 1m 30m 1h 12h Custom  |
| ▶ | Timestamp | Message |
| No older events at this moment. Retry | | |
| ▶ | 2021-06-08T21:40:11.000+05:30 | 2 693331494763 eni-025ffffb751de82493 50.205.244.36 172.31.94.239 123 34874 17 1 76 1623168611 1623168640... |
| ▶ | 2021-06-08T21:40:11.000+05:30 | 2 693331494763 eni-025ffffb751de82493 172.31.94.239 1.116.229.53 80 59807 6 1 40 1623168611 1623168640 AC... |
| ▶ | 2021-06-08T21:40:11.000+05:30 | 2 693331494763 eni-025ffffb751de82493 8.129.43.176 172.31.94.239 48507 2376 6 1 40 1623168611 1623168640 ... |
| ▶ | 2021-06-08T21:40:11.000+05:30 | 2 693331494763 eni-025ffffb751de82493 172.31.94.239 204.11.201.12 39609 123 17 1 76 1623168611 1623168640... |
| ▶ | 2021-06-08T21:40:11.000+05:30 | 2 693331494763 eni-025ffffb751de82493 172.31.94.239 138.68.201.49 55618 123 17 1 76 1623168611 1623168640... |
| ▶ | 2021-06-08T21:40:11.000+05:30 | 2 693331494763 eni-025ffffb751de82493 204.11.201.12 172.31.94.239 123 39609 17 1 76 1623168611 1623168640... |
| ▶ | 2021-06-08T21:40:11.000+05:30 | 2 693331494763 eni-025ffffb751de82493 138.68.201.49 172.31.94.239 123 55618 17 1 76 1623168611 1623168640... |
| ▶ | 2021-06-08T21:40:11.000+05:30 | 2 693331494763 eni-025ffffb751de82493 172.31.94.239 69.89.207.199 53680 123 17 1 76 1623168611 1623168640... |
| ▶ | 2021-06-08T21:40:11.000+05:30 | 2 693331494763 eni-025ffffb751de82493 1.116.229.53 172.31.94.239 59807 80 6 1 40 1623168611 1623168640 AC... |
| ▶ | 2021-06-08T21:40:11.000+05:30 | 2 693331494763 eni-025ffffb751de82493 69.89.207.199 172.31.94.239 123 53680 17 1 76 1623168611 1623168640... |
| ▶ | 2021-06-08T21:40:11.000+05:30 | 2 693331494763 eni-025ffffb751de82493 162.142.125.150 172.31.94.239 62446 9143 6 1 44 1623168611 16231686... |
| ▶ | 2021-06-08T21:40:11.000+05:30 | 2 693331494763 eni-025ffffb751de82493 172.31.94.239 50.205.244.36 34874 123 17 1 76 1623168611 1623168640... |
| ▶ | 2021-06-08T21:40:46.000+05:30 | 2 693331494763 eni-025ffffb751de82493 107.173.140.175 172.31.94.239 49640 8088 6 1 44 1623168646 16231687... |
| ▶ | 2021-06-08T21:40:46.000+05:30 | 2 693331494763 eni-025ffffb751de82493 50.205.244.36 172.31.94.239 123 35182 17 1 76 1623168646 1623168700... |
| ▶ | 2021-06-08T21:40:46.000+05:30 | 2 693331494763 eni-025ffffb751de82493 172.31.94.239 50.205.244.36 35182 123 17 1 76 1623168646 1623168700... |

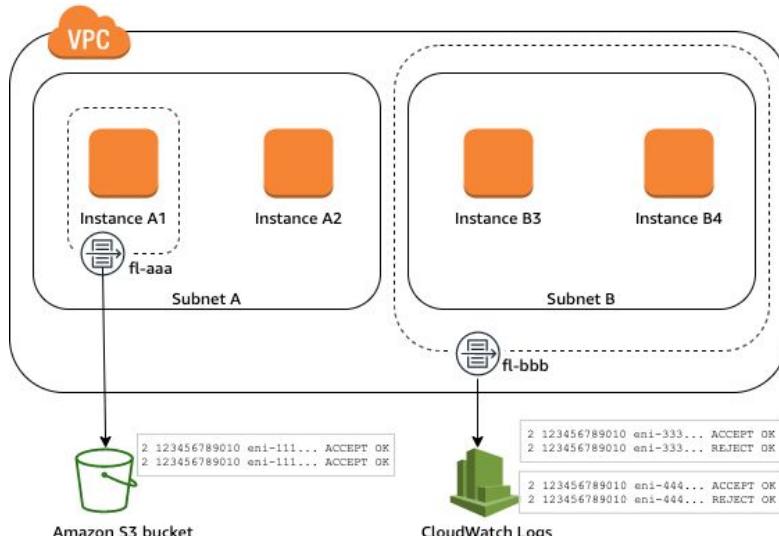
Dashboards Built using VPC Flow Logs Data



Interface Level Flow Logs

VPC Flow Logs captures traffic at an interface level.

Flow logs do not capture real-time log streams for your network interfaces.



High-Level Flow Logs Format

| | |
|--------------|---------------------------------|
| version | - The VPC Flow Logs Version |
| account-id | - AWS Account ID |
| interface-id | - The network interface id |
| srcaddr | - The source address |
| destaddr | - Destination Address |
| src port | - Source Port |
| dest port | - Destination Port |
| protocol | - The protocol number |
| packets | - Number of packets transferred |
| bytes | - Number of bytes transferred |
| start | - Start time in unix seconds |
| end | - End time in unix seconds |
| action | - ACCEPT or REJECT |
| log status | - Logging status of flow log |

2 7742829482 eni-4d788e3d 115.73.149.218 10.0.5.157 12053 23 6 2 88 1485439809 1485440090 REJECT OK

Type of Traffic Not Logged

Flow logs do not capture all IP traffic. Some of these include:

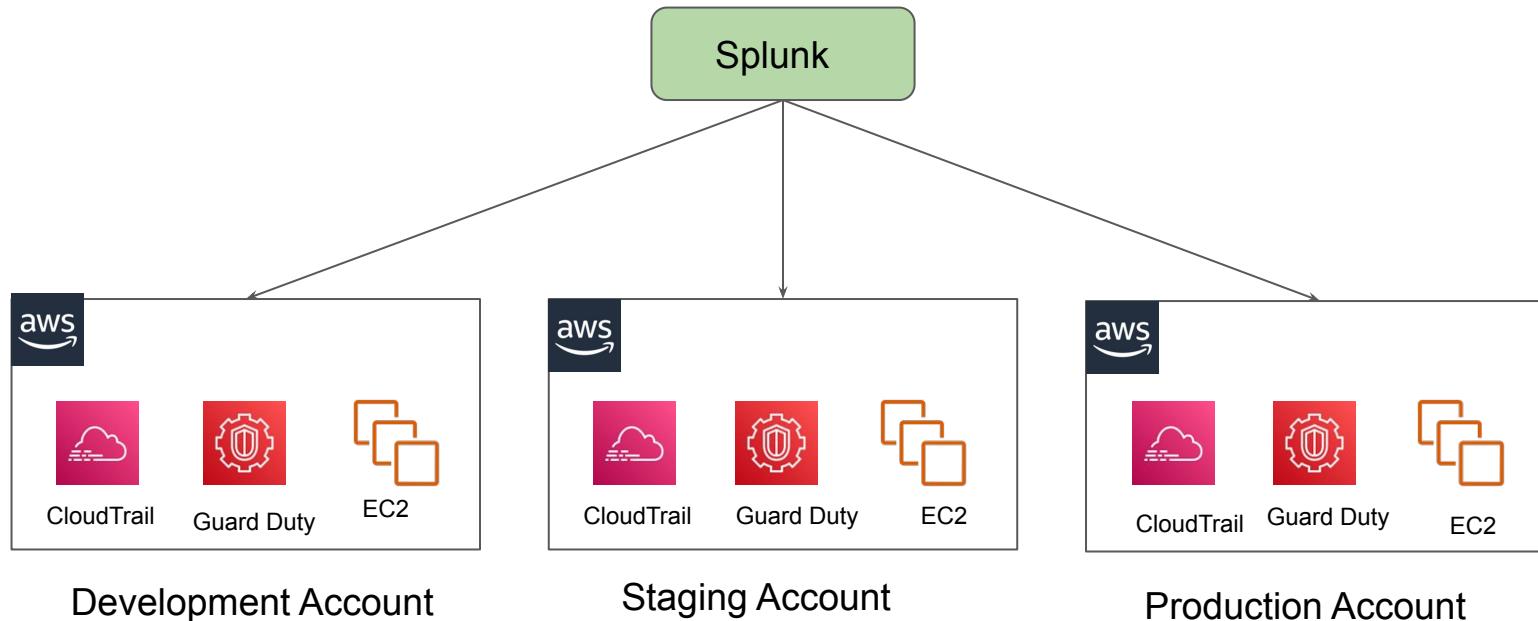
- Traffic generated by instances when they contact the Amazon DNS server. If you use your own DNS server, then all traffic to that DNS server is logged.
- Traffic generated by a Windows instance for Amazon Windows license activation.
- Traffic to and from 169.254.169.254 for instance metadata.
- DHCP traffic.

Centralized Logging

Architectural Perspective

Challenges with Logging

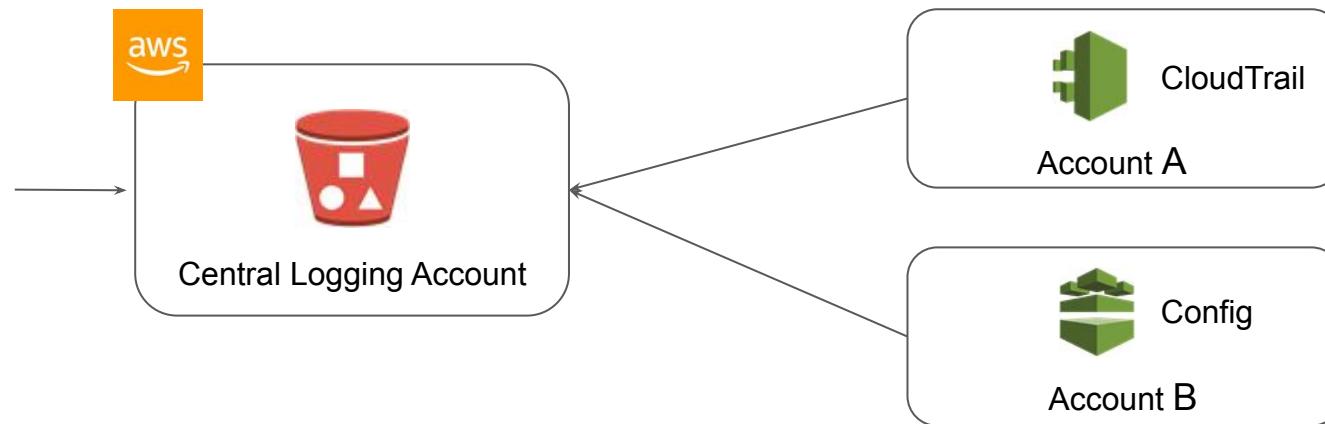
In a Multi-Account based architecture, log monitoring at an individual account level is not the best of the approaches.



Recommended Architecture for Logging

A comprehensive log management and analysis strategy is mission critical in an organization.

One of the recommended approaches is to use a Centralized Logging Account.



Considerations while implementing Logging

Define log retention requirements and lifecycle policies early on.

Incorporate tools and features to automate the lifecycle policies.

Automate the installation and configuration of log shipping agent.

Make sure the solution supports hybrid environment to support the needs.

AWS Services to Help!

We can make use of AWS Managed service to build centralized logging solutions.

Services which can help here:

- AWS ElasticSearch Service
- AWS CloudWatch Logs
- Kinesis Firehose
- AWS S3

Ways to configure centralized logging for each AWS service (CloudTrail, VPCFlow) differs.

Considerations - S3 Bucket Policy for Cross-Account

Architectural Perspective

Challenges with S3 Bucket Policy

A wildcard based S3 bucket policy allowing CloudTrail service would mean that any AWS account's CloudTrail can put its data to your S3 bucket.

```
{  
    "Sid": "AWSCloudTrailWrite20131101",  
    "Effect": "Allow",  
    "Principal": {  
        "Service": "cloudtrail.amazonaws.com"  
    },  
    "Action": "s3:PutObject",  
    "Resource": "arn:aws:s3:::kplabs-central-log-cloudtrail/*",  
    "Condition": {  
        "StringEquals": {  
            "s3:x-amz-acl": "bucket-owner-full-control"  
        }  
    }  
}
```

Bucket Policy with Conditional Statement

As a security best practice, add an `aws:SourceArn` condition key to the Amazon S3 bucket policy. This helps prevent unauthorized access to your S3 bucket.

```
{  
  "Sid": "AWSCloudTrailWrite20131101",  
  "Effect": "Allow",  
  "Principal": {  
    "Service": "cloudtrail.amazonaws.com"  
  },  
  "Action": "s3:PutObject",  
  "Resource": "arn:aws:s3:::kplabs-central-log-cloudtrail/*",  
  "Condition": {  
    "StringEquals": {  
      "aws:SourceArn": "arn:aws:cloudtrail:ap-southeast-1:693331494763:trail/demo-trail",  
      "s3:x-amz-acl": "bucket-owner-full-control"  
    }  
  }  
}
```

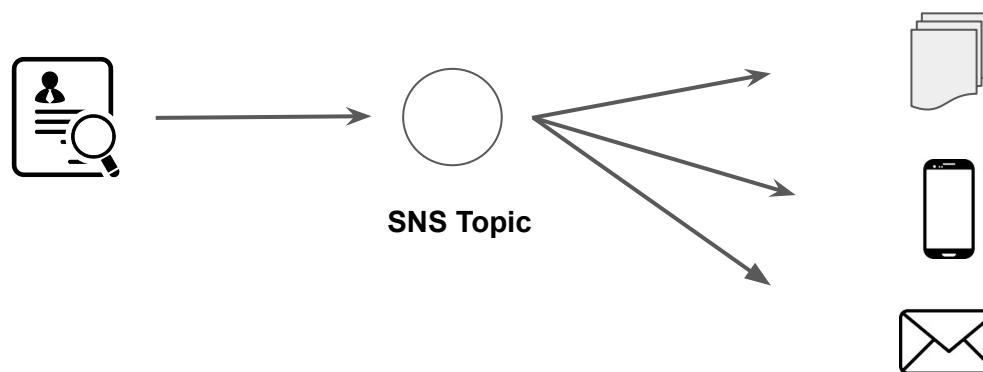
Simple Notification Service

Notification Service

Let's Message

SNS stands for simple notification service.

SNS is a fully managed messaging and mobile notification service for delivering messages to the subscribed endpoints.



Use-Cases for SNS

AWS CloudWatch integrates well with SNS.

Whenever a disk usage of a server exceeds 95%, send an EMAIL and SMS notification to the NOC team.

Whenever a server load in production is more than 90%, send and email and SMS notification.

Amazon Kinesis Services

Capabilities of Kinesis Set of Services

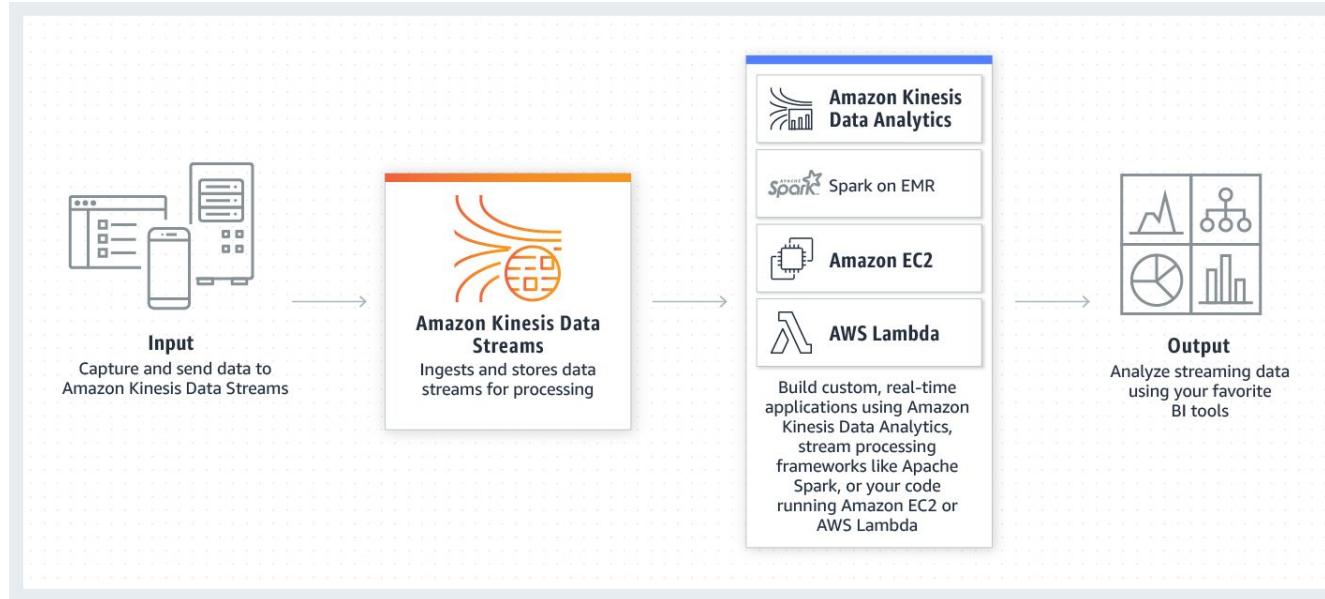
Kinesis Offerings

Amazon Kinesis is a set of services which makes it easy to work with set of streaming data on AWS.

| Sr No | Kinesis Services | Description |
|-------|------------------------|---|
| 1 | Kinesis Data Stream | Captures, processes and stores data streams in real-time |
| 2 | Kinesis Data Firehose | Primary to move data from point A to point B. |
| 3 | Kinesis Data Analytics | Analyze streaming data in real-time with SQL / Java code. |
| 4 | Kinesis Video Stream | Capture, processes and stores video streams. |

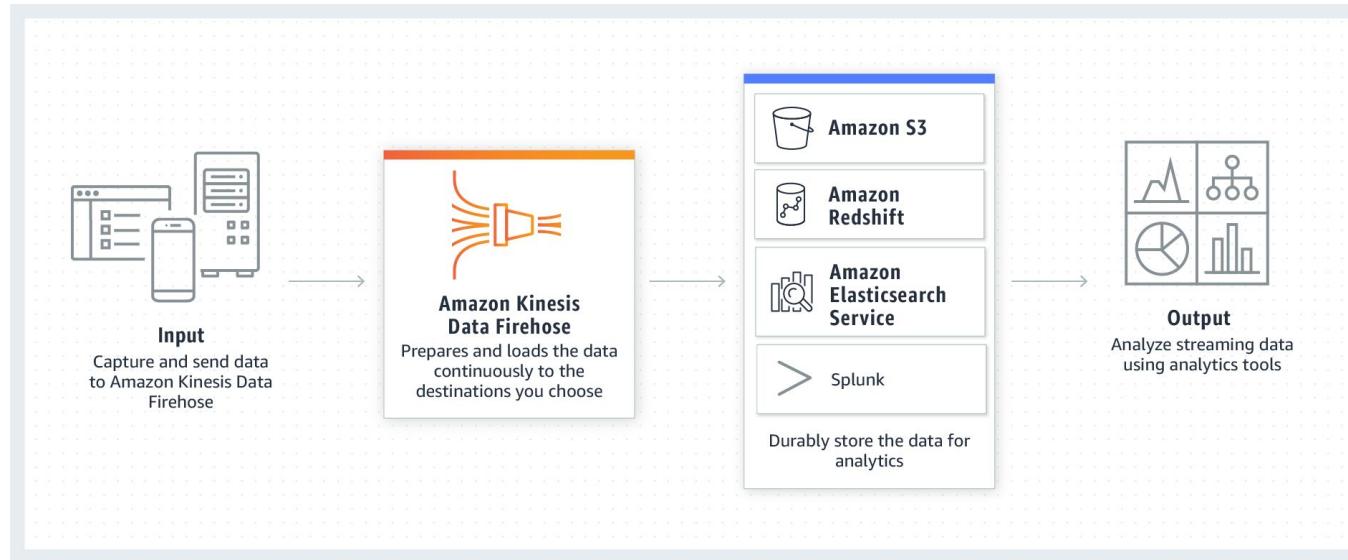
Kinesis Data Stream

It allows us to capture, process and store data streams.



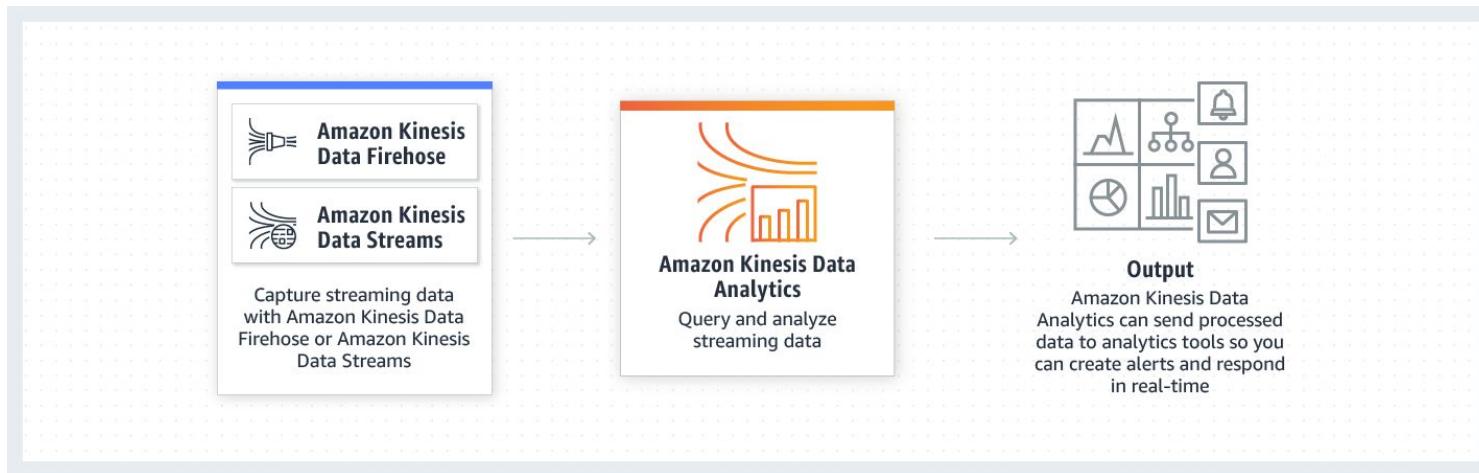
Kinesis Firehose

Kinesis firehose delivers data from point A to point B.



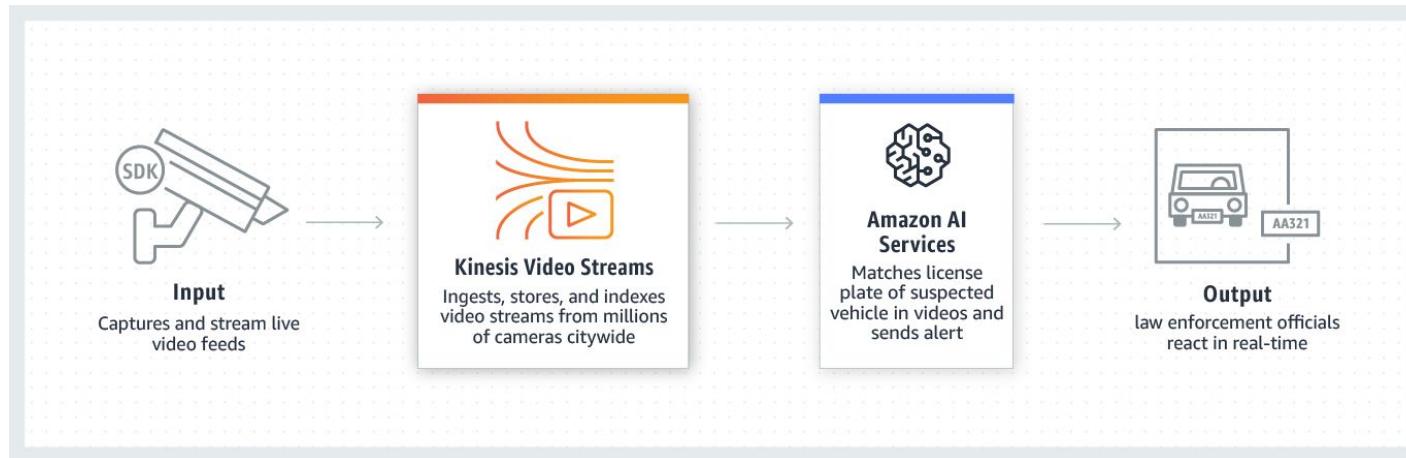
Kinesis Data Analytics

Kinesis Data Analytics has ability to analyze data streams in real time.



Kinesis Video Stream

Amazon Kinesis Video Streams makes it easy to securely stream video from connected devices to AWS

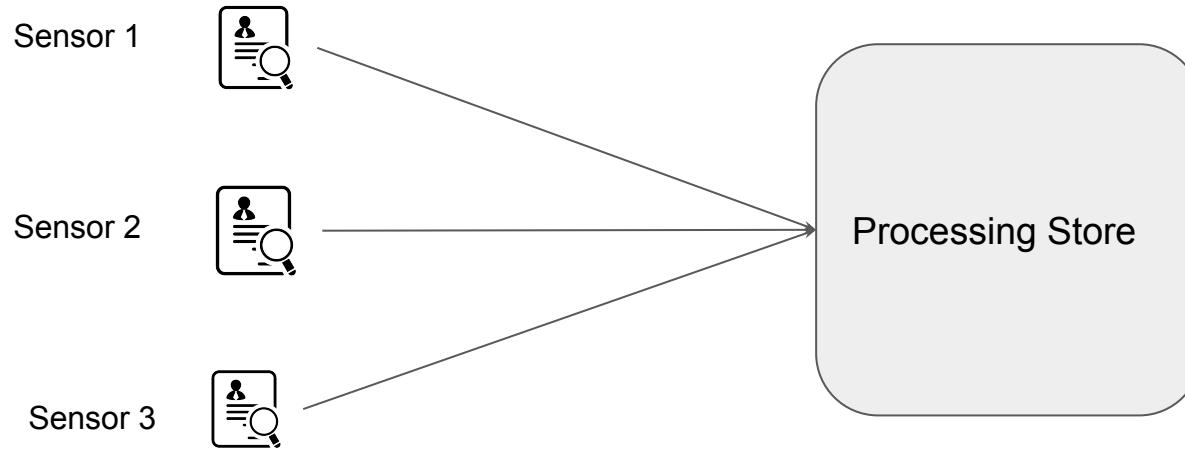


Amazon Kinesis

Streaming Data

Basics of Streaming Data.

Streaming data is the continuous flow of data generated by various sources



Examples of Streaming Data

A financial institution tracks changes in the stock market in real time and adjust it's portfolio accordingly.

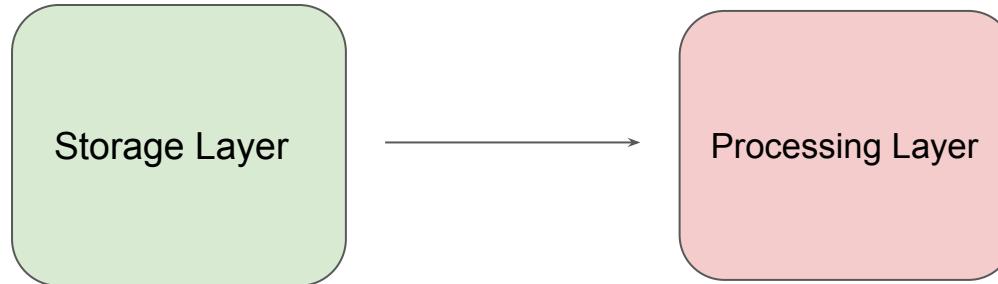
A media publisher streams billions of clickstream records from its online properties



Challenges with Working of Streaming Data

Streaming data processing requires two layers: a storage layer and a processing layer.

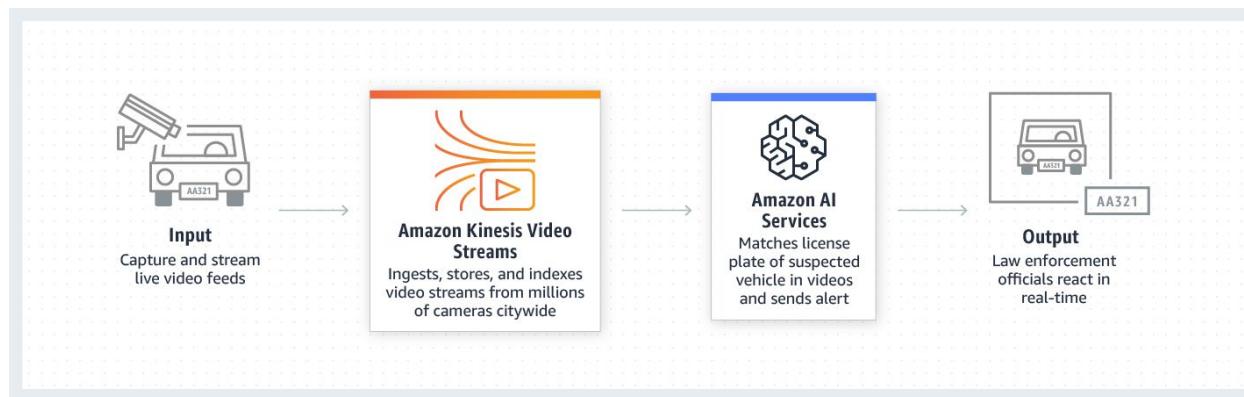
The storage layer needs to support record ordering and strong consistency, replayable reads and the processing layer is responsible for consuming data from the storage layer, running computation on that data and many other tasks.



Basics of Amazon Kinesis

Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information.

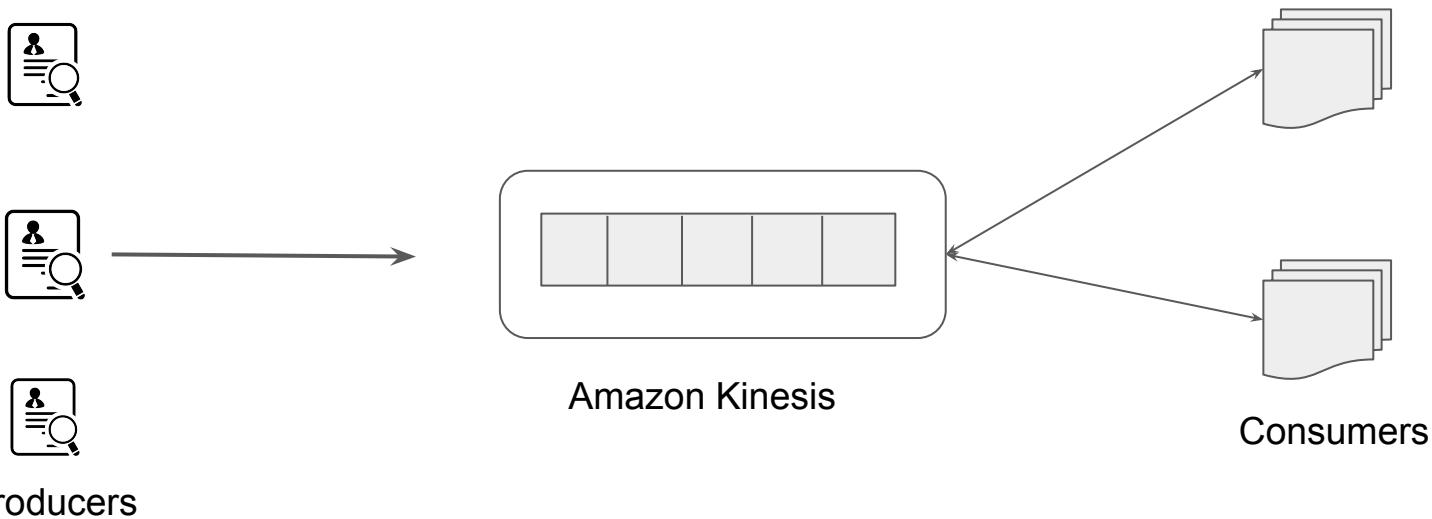
Amazon Kinesis offers key capabilities to cost-effectively process streaming data at any scale



3 entities

There are 3 entities in this kind of use case:

Producer, Stream Store, Consumer

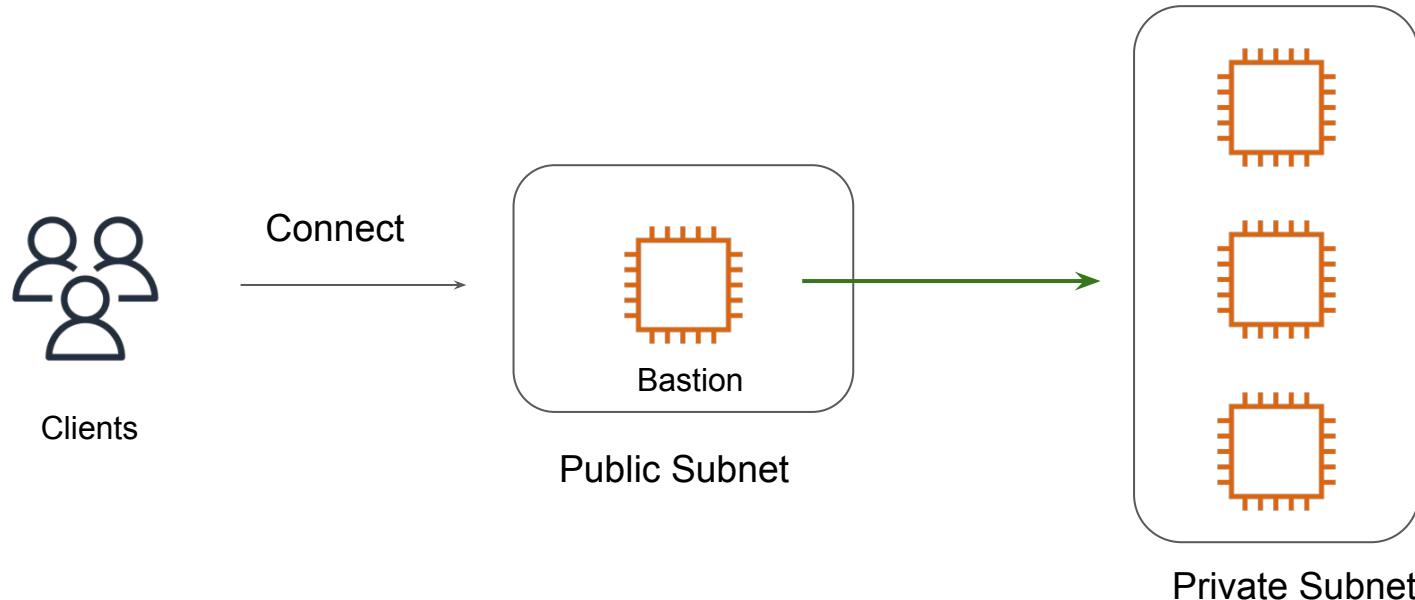


Bastion Host

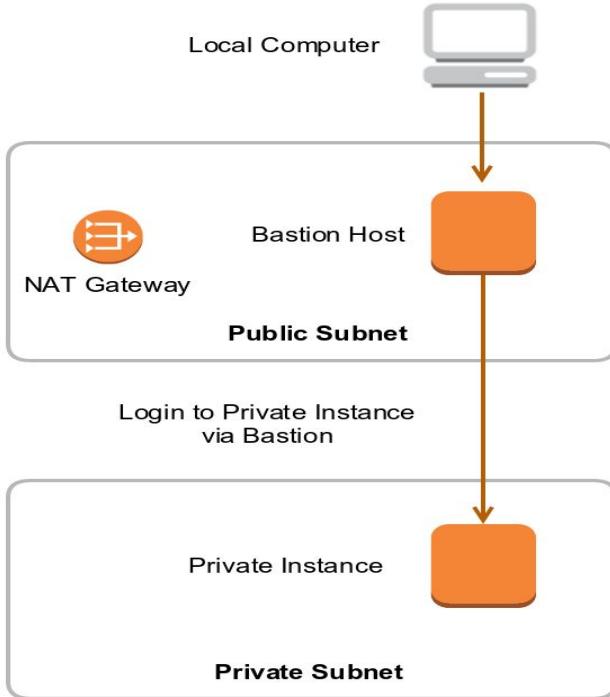
Time to Defend

Basics of Bastion Hosts

Bastion hosts also referred as jump box acts like a proxy server and allows the client machines to connect to the remote server in the private subnets.



The Bastion Host



- Bastion Host → “Jump Box” from public to private subnet.
- User needs to have access for jump box and the private instance.

The Security of Jump Box

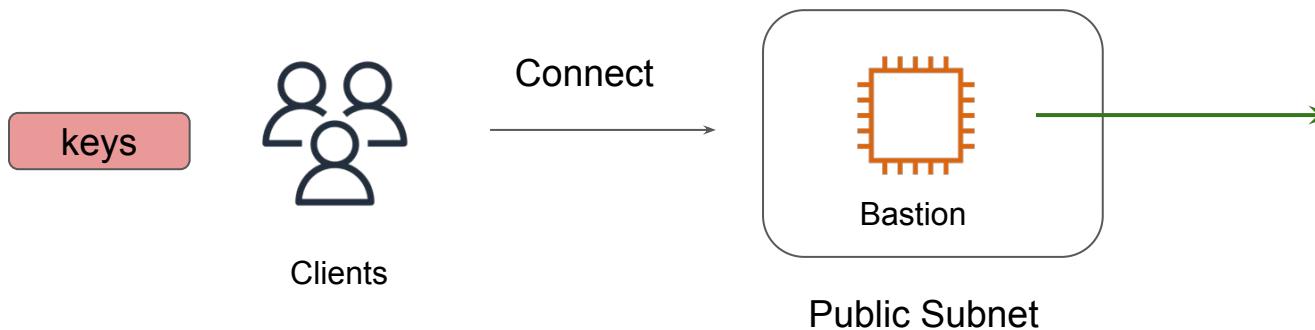
- All the unnecessary packages should be removed in the Bastion machine to minimize the attack surface area.
- Proper Server Hardening should be applied to the Bastion Host.
- Private Keys should never be stored on the bastion. We should use “Agent Forwarding” for Linux instances.

Challenge with this Setup

Every user have private keys stored securely on their laptop.

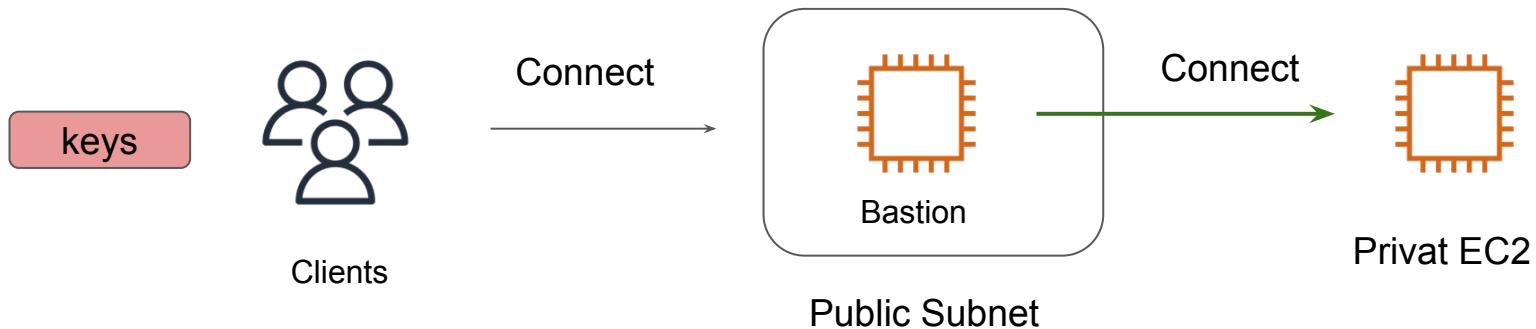
This private key can be used to connect to Bastion Host.

Once logged into Bastion, how will he login to private EC2 instance?



SSH Agent Forwarding

SSH Agent forwarding allows users to use their local SSH keys to perform some operation on remote servers without keys being left from your workstation.

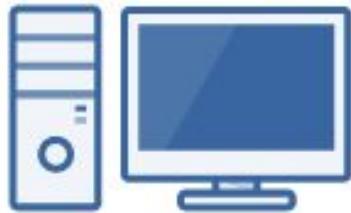


Virtual Private Network

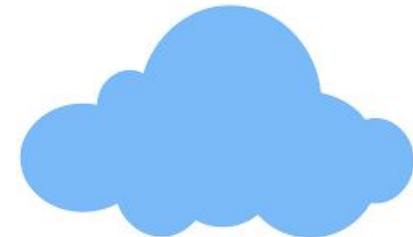
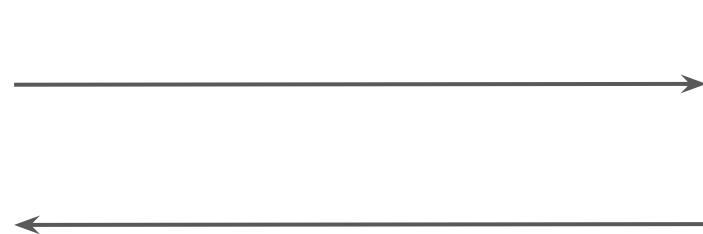
Let's Route

VPN

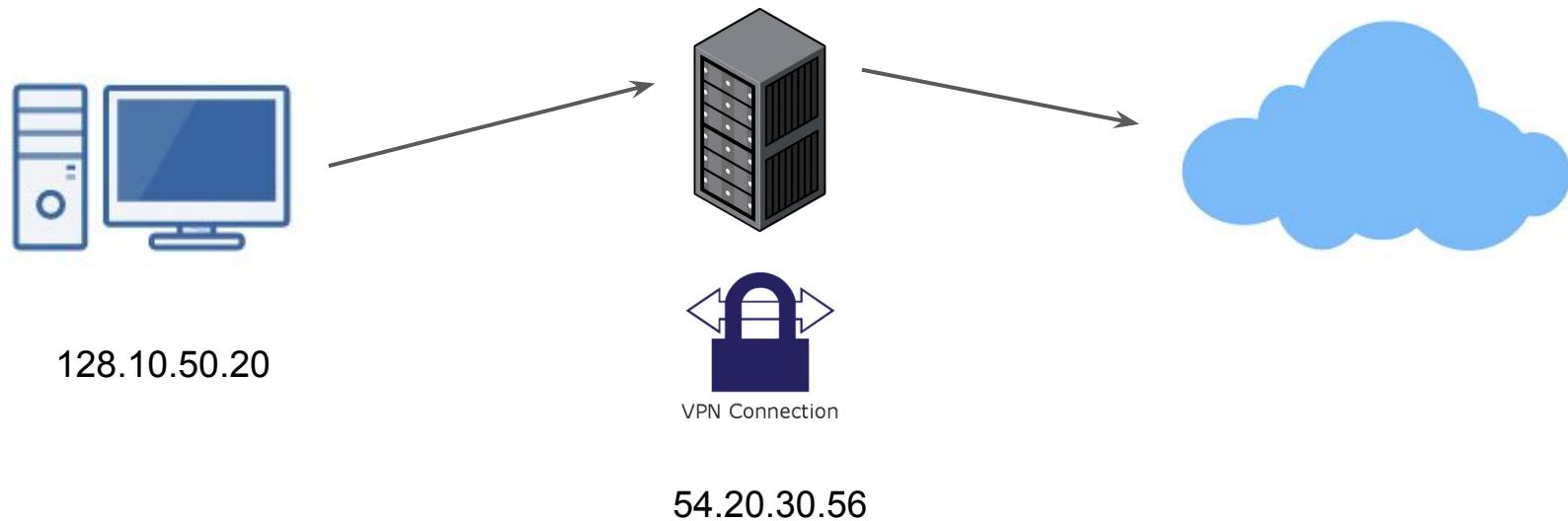
- VPN enables you to route traffic from yourself towards destination through itself.
- Something similar to Proxy.



128.10.50.20

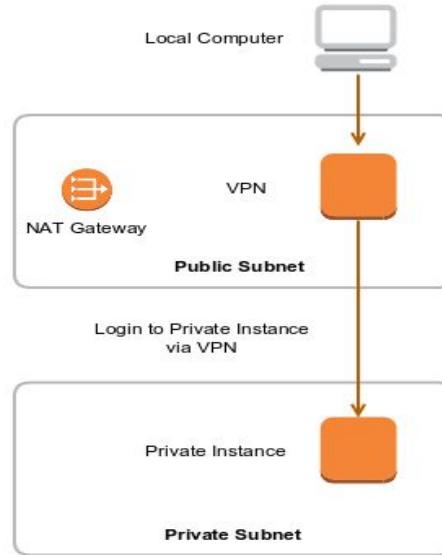


Routing via VPN Server



VPN use in Corporate Network

- In Corporate environments, VPN is used to connect to instances in Private Subnet.
- VPN Server resides in the Public Subnet and you route your traffic via VPN server to instances in Public Subnet.

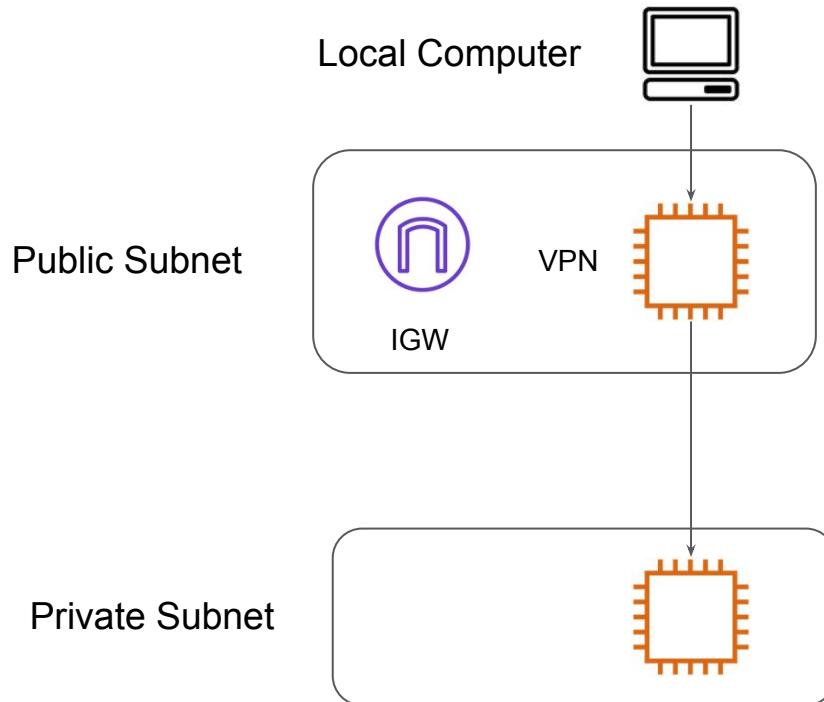


AWS Client VPN

Creating our First VPN in AWS

EC2 Based VPN Architecture

In this approach, you install VPN softwares like OpenVPN in the EC2 instance and use it to route traffic to private subnets.

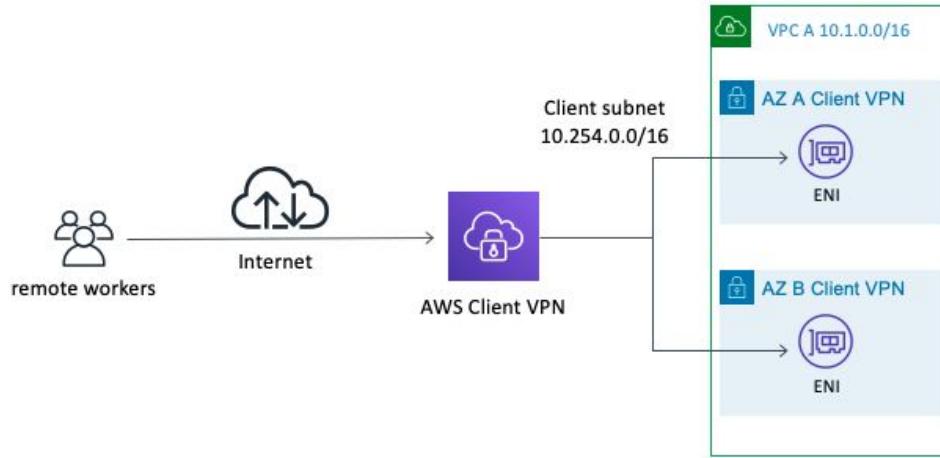


Challenges with EC2 VPN Based Architectures

1. High-Availability (What if VPN EC2 goes down)
2. Patch Management.
3. Upgrade of VPN Software
4. Performance Optimization
5. VPN Server Configuration

AWS Client VPN

AWS Client VPN is a managed client-based VPN service that enables you to securely access your AWS resources and resources in your on-premises network.



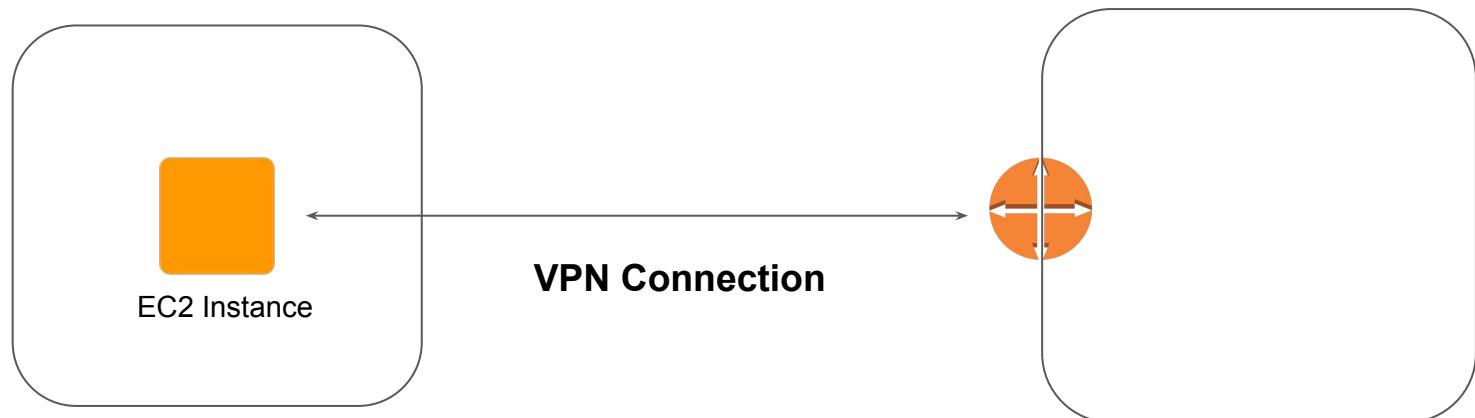
Site to Site Tunnel

Let's Route

Site to Site VPN

A Site to Site (S2S) VPN allows two networking domains to communicate securely between each other over an untrusted network like Internet.

The two sites can be AWS and on-premise data-center or even two different VPC's.

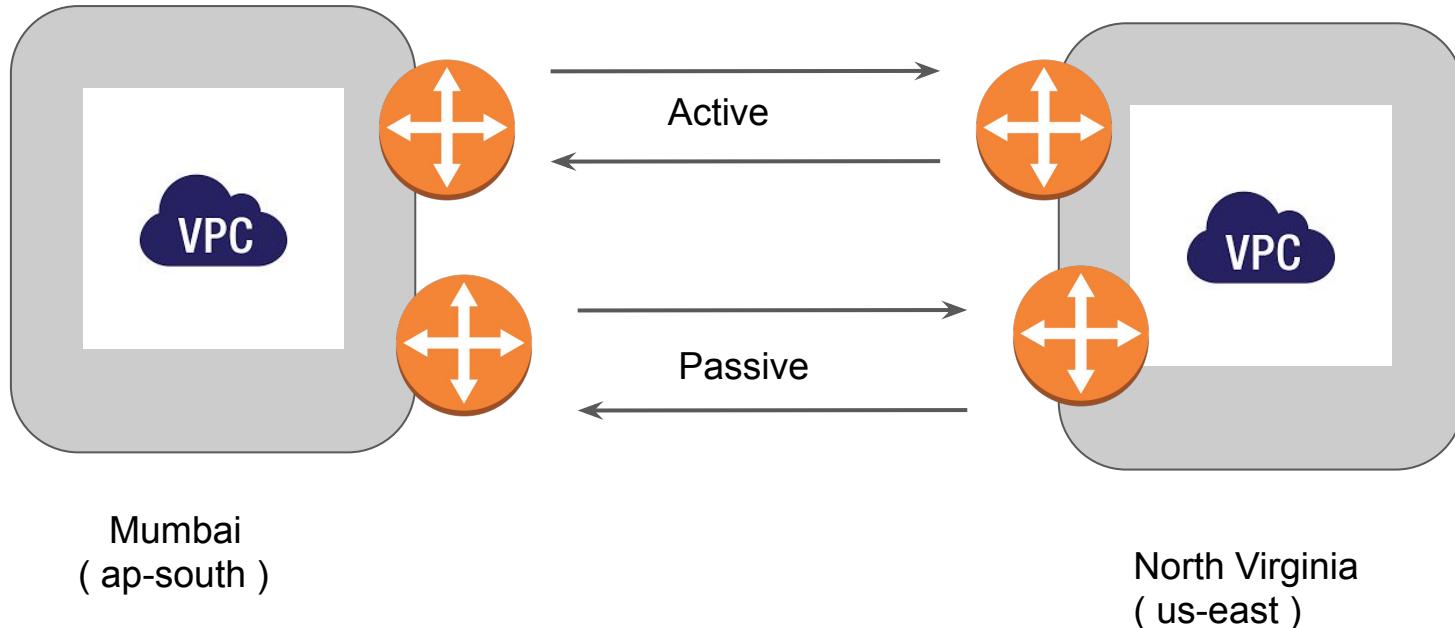


Availability Challenges in S2S VPN

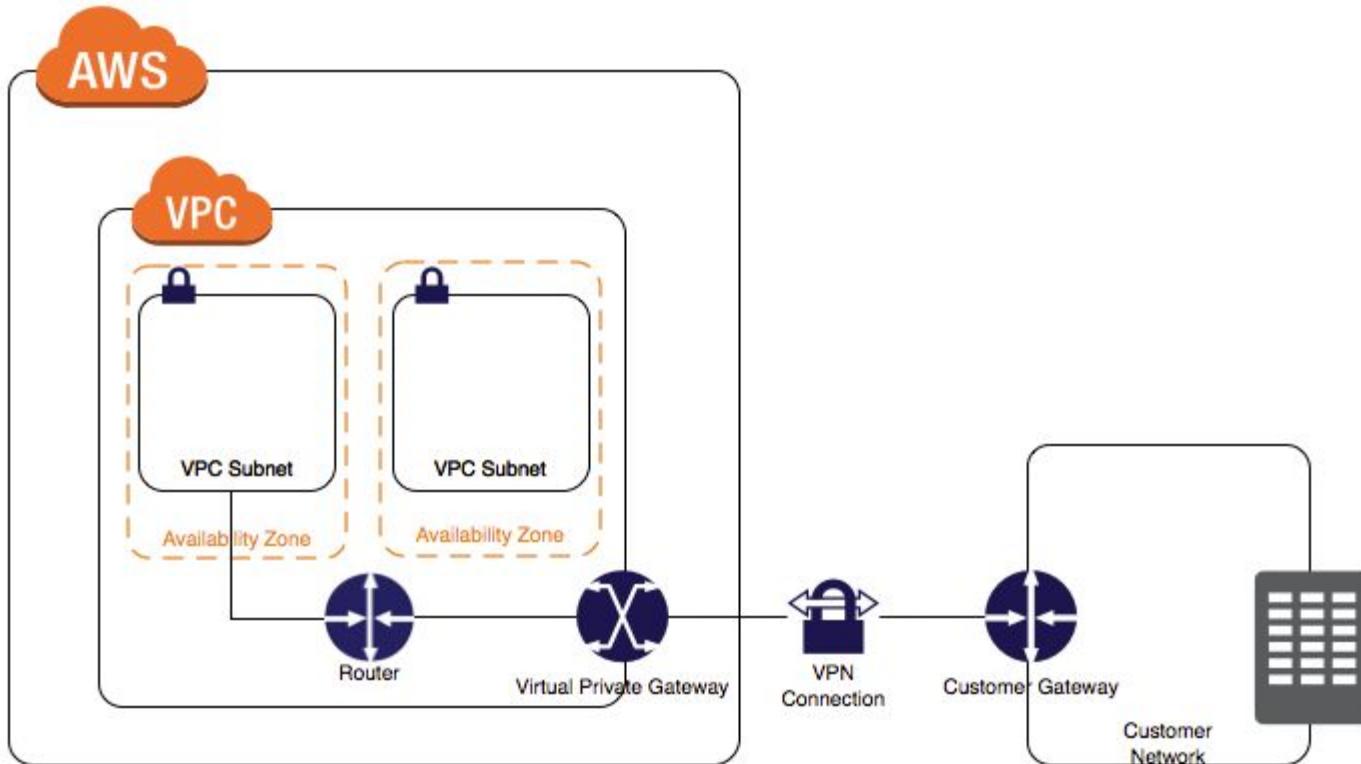
If you have a single tunnel endpoint and if one of the side goes down, then the entire tunnel breaks.



High Availability in S2S VPN

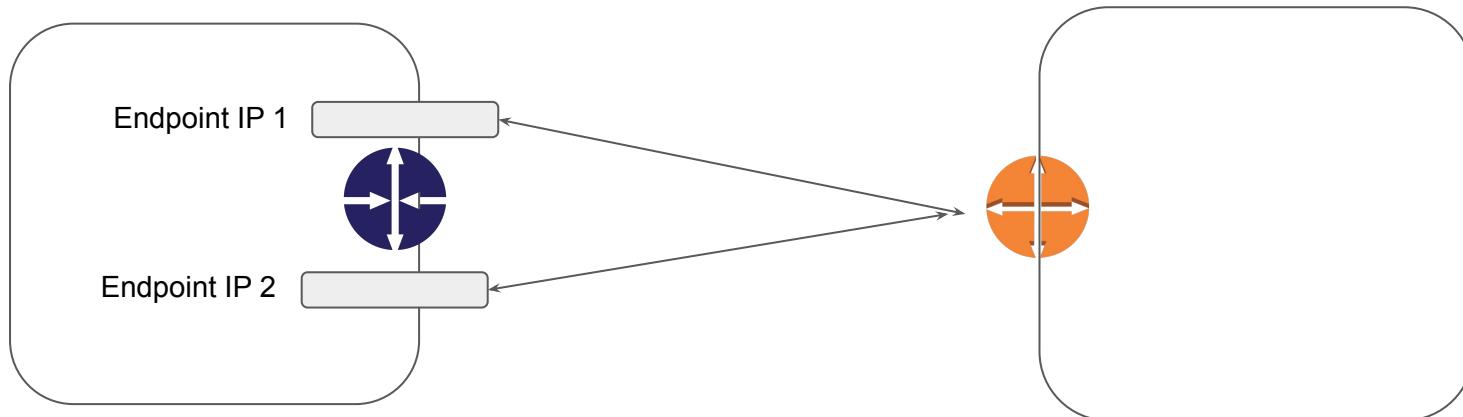


Site to Site VPN



Importance of VGW

- A Virtual Private Gateway (VGW) has built-in high-availability for VPN connection.
- AWS automatically creates 2 HA endpoints, each in a different AZ.



Importance of VGW

The screenshot shows a CloudWatch interface with a table of VPN connections and a detailed view of one connection.

Table Headers:

- Name
- VPN ID
- State
- Virtual Private Gateway
- Customer Gateway

Table Data:

| Name | VPN ID | State | Virtual Private Gateway | Customer Gateway |
|-------------|--------------|-----------|----------------------------|----------------------------|
| ohio-mumbai | vpn-5cdf0a6b | available | vgw-7072fd40 ohio-mumbai | cgw-27058b17 ohio-mumbai |

VPN Connection Details:

VPN Connection: vpn-5cdf0a6b

Tunnel Details:

| Outside IP Address | Inside IP CIDR | Status | Status Last Changed | Details |
|--------------------|-------------------|--------|--------------------------------------|---------|
| 18.216.150.193 | 169.254.59.32/30 | UP | December 24, 2017 at 7:42:19 PM U... | - |
| 18.220.211.76 | 169.254.57.128/30 | DOWN | December 24, 2017 at 7:36:56 PM U... | - |

Relax and Have a Meme Before Proceeding

That stupid walk you do when
someone's mopping a floor and you
know you're gonna walk over it but you
want them to see how sorry you are to
be walking over it so you make
yourself look like you're walking over
hot lava.



It ain't much, but it's honest work

VPC Peering

Let's Route

VPC Peering

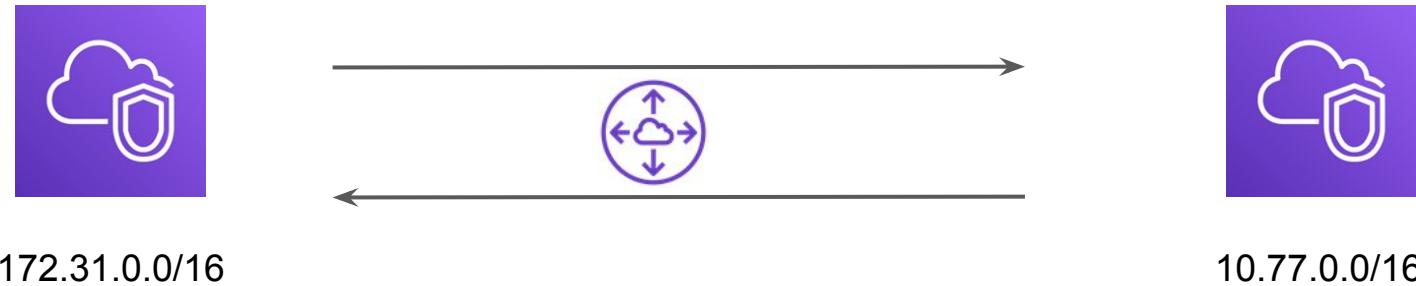
VPC peering is a network connection between two VPC that enables the communication between instances of both the VPC.



Today's Architecture - 1

First VPC - 172.31.0.0/16

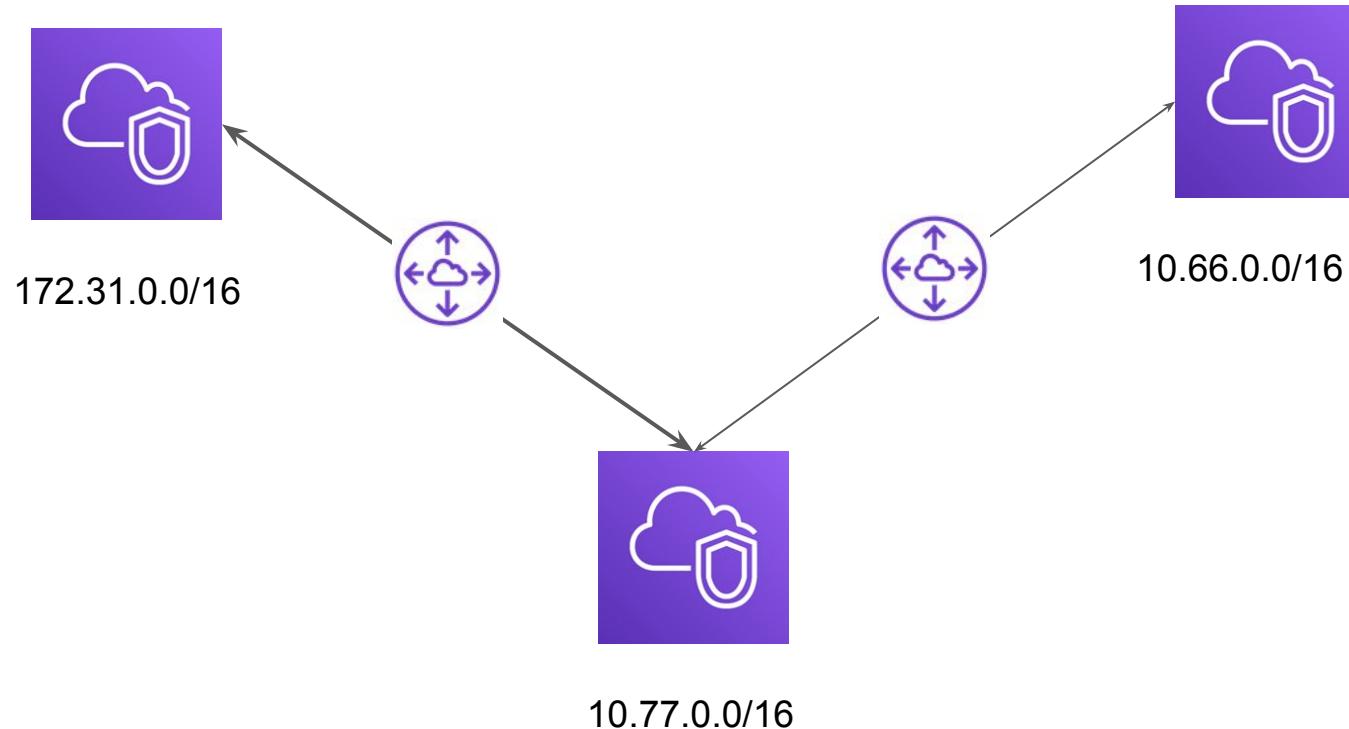
Secondary VPC - 10.77.0.0/16



172.31.0.0/16

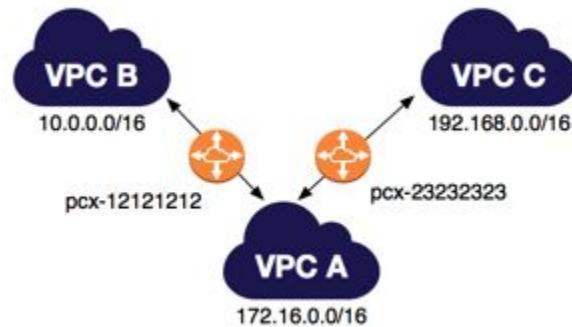
10.77.0.0/16

Today's Architecture - 2



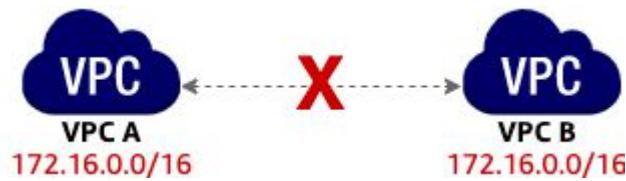
Things to Remember

- VPC Peering is now possible between regions.
- VPC Peering does not act like a Transit VPC



Unsupported VPC Peering Configurations - 1

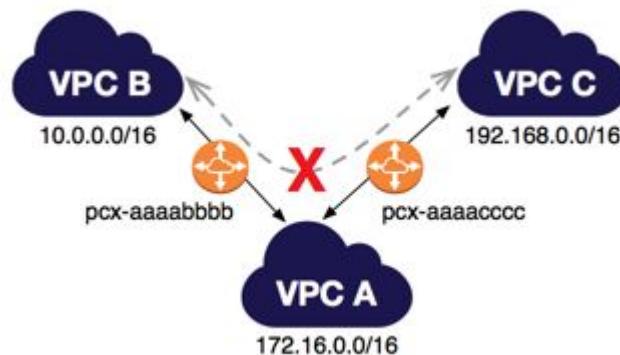
You cannot create a VPC peering connection between VPCs with matching or overlapping IPv4 CIDR blocks.



Unsupported VPC Peering Configurations - 2

You have a VPC peering connection between VPC A and VPC B (pcx-aaaabbbb), and between VPC A and VPC C (pcx-aaaacccc).

There is no VPC peering connection between VPC B and VPC C. You cannot route packets directly from VPC B to VPC C through VPC A.

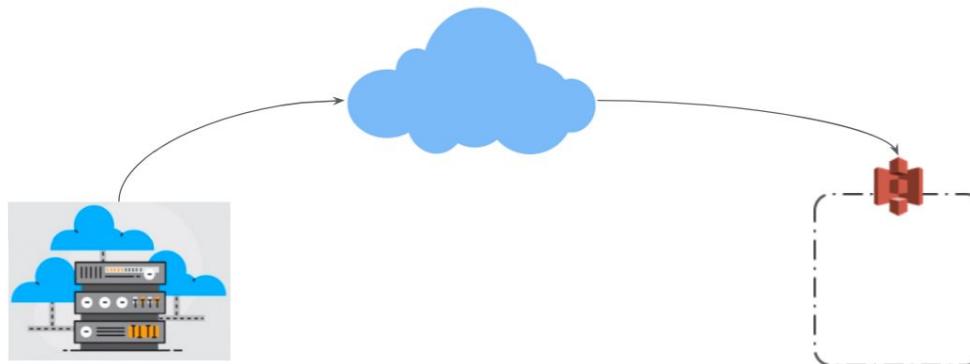


VPC Endpoints

Private Communication is Better

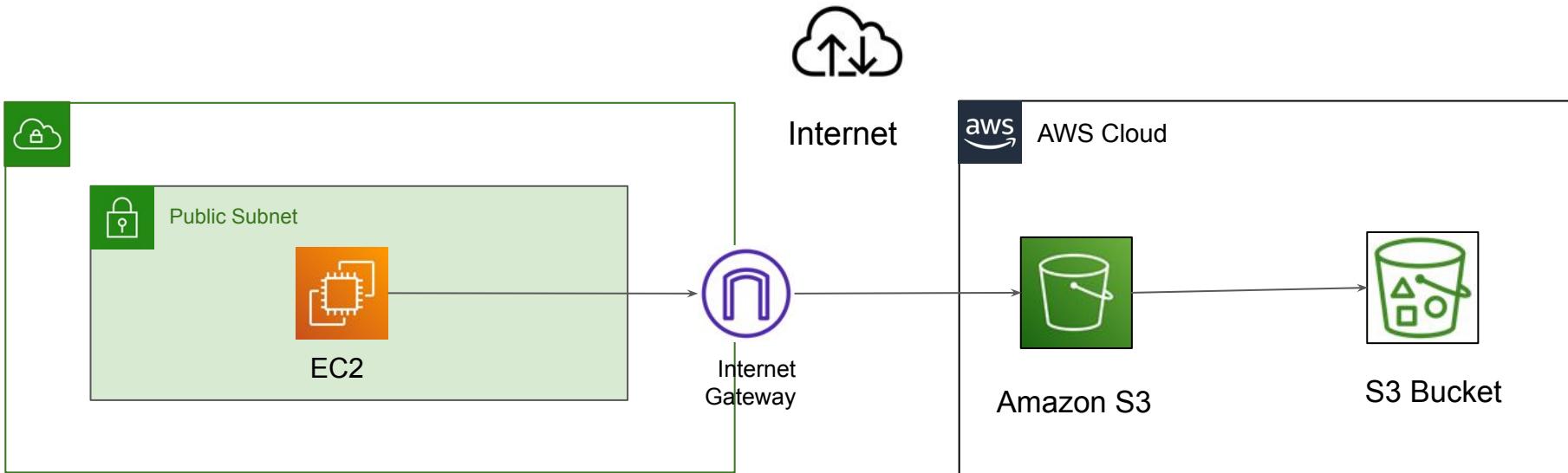
Use-Case: EC2 and S3 Communication

For EC2 instances to be able to access public resources like S3, DynamoDB and others, the traffic needed to be passed via Internet Gateway.

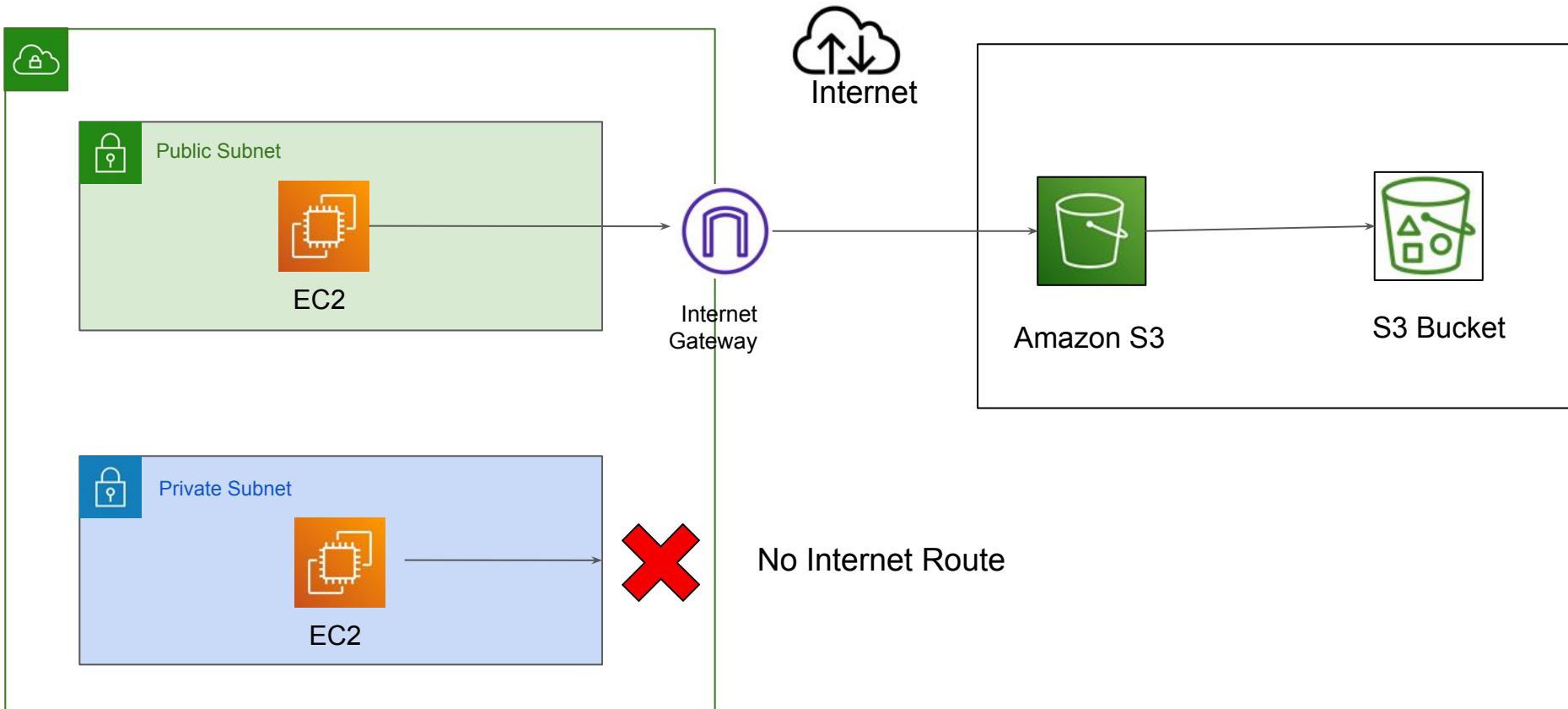


Architectural Perspective

EC2 traffic towards S3 is routed to Internet Gateway



Challenge with Private Workloads

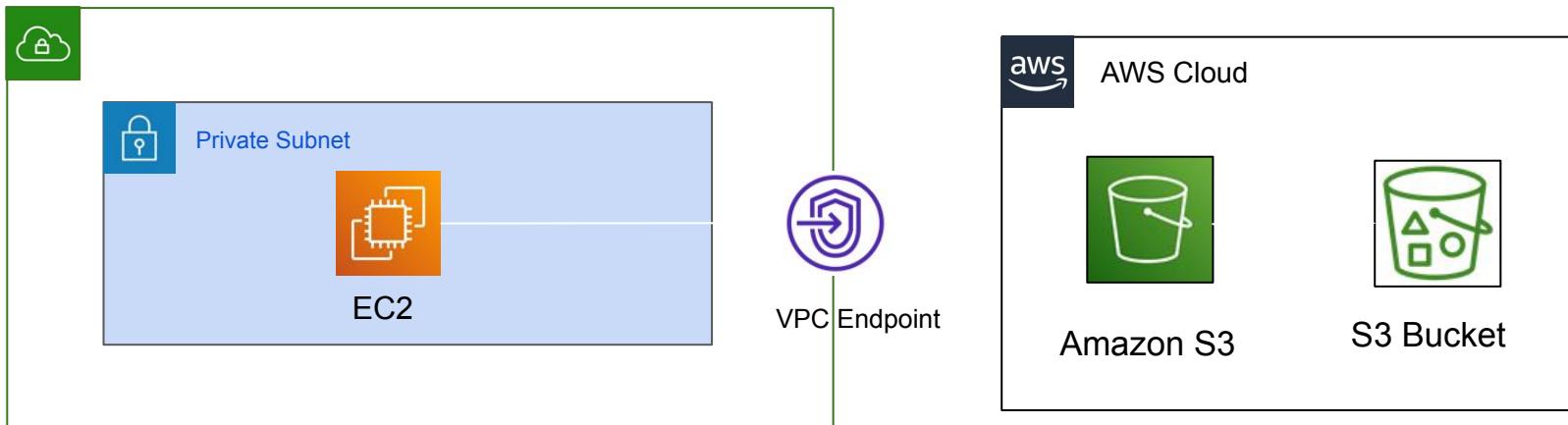


Downsides of Using Public Internet

1. Data transfer cost of AWS
2. Higher Latency
3. Can bottleneck your internet gateway.
4. Security

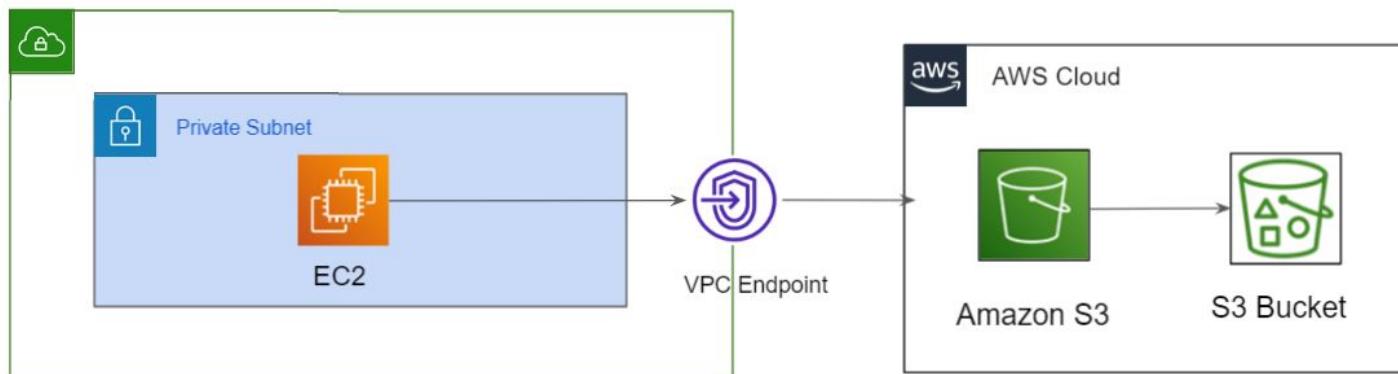
Overview of VPC Endpoints

VPC Endpoints allows us to connect VPC to another AWS services OR other supported services over AWS private network.



Overview of VPC Endpoints

VPC Endpoints allows us to connect VPC to another AWS services OR other supported services over AWS network.



Revising Important Pointers

AWS PrivateLink is a technology that enables you to privately access services by using private IP addresses.

To use AWS PrivateLink, you can create a VPC endpoint for a service in your VPC.

VPC Endpoint allows us to connect VPC to another AWS services over AWS network.

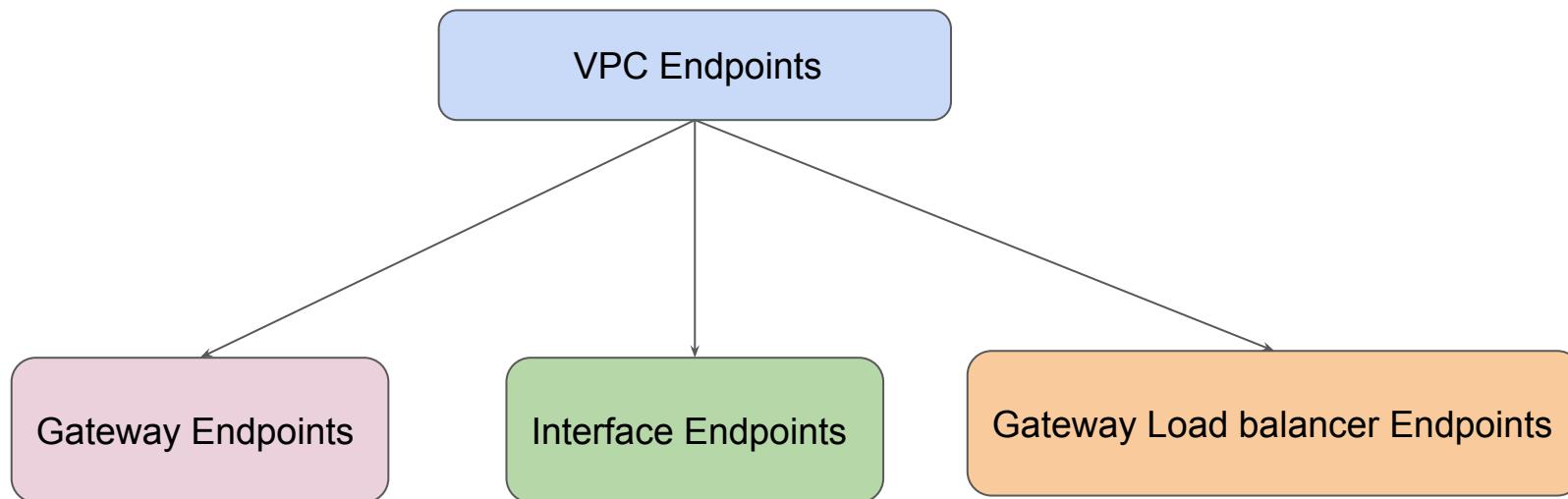
Traffic between your VPC and the other service does not leave the Amazon network.

Gateway VPC Endpoints

Understanding Types

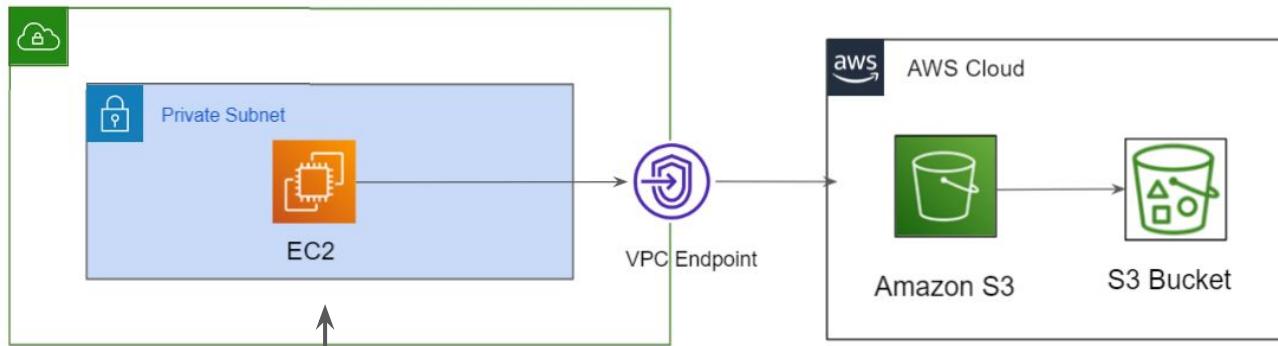
VPC Endpoints Type

There are three primary types of VPC Endpoints available.



Gateway VPC Endpoints

We specify the Gateway Endpoint as a route table target that is destined for supported AWS services.



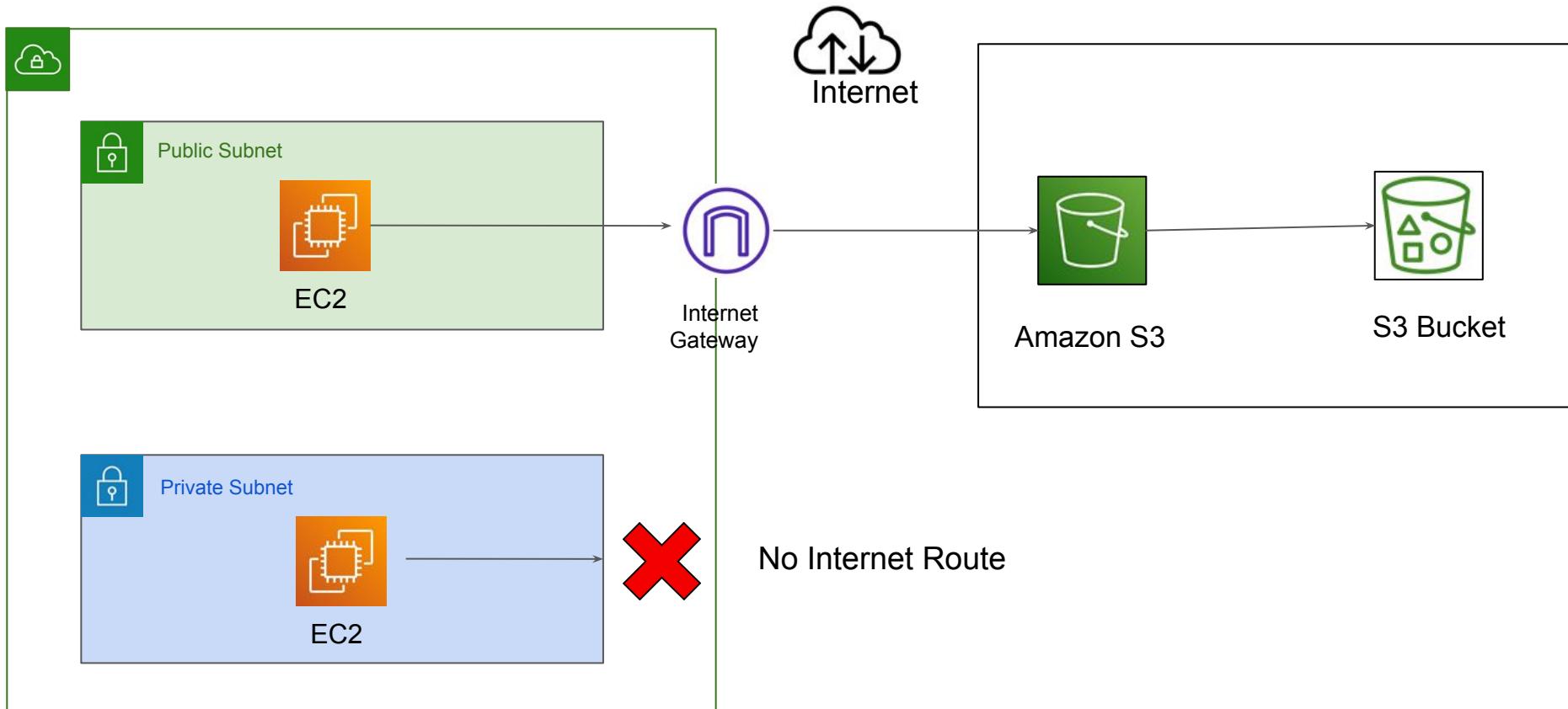
| Destination | Target |
|---------------|---------------|
| 172.31.0.0/16 | local |
| 54.231.0.0/17 | vpce-11bb22cc |

Supported Services

A gateway endpoint is for the following supported AWS services:

1. Amazon S3
2. DynamoDB

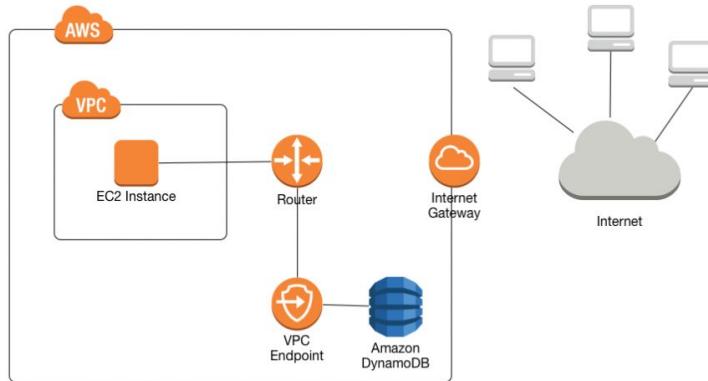
Today's Architecture



Downsides of Gateway Endpoints - 1

In Gateway endpoints approach, the VPC endpoint was created outside your VPC and traffic was routed via route table.

Thus, it is not possible to use it directly from VPN's or Direct connects and various others.



Downsides of Gateway Endpoints - 2

Endpoints are supported within the same Region only. You cannot create an endpoint between a VPC and a service in a different Region.

Endpoints support IPv4 traffic only.

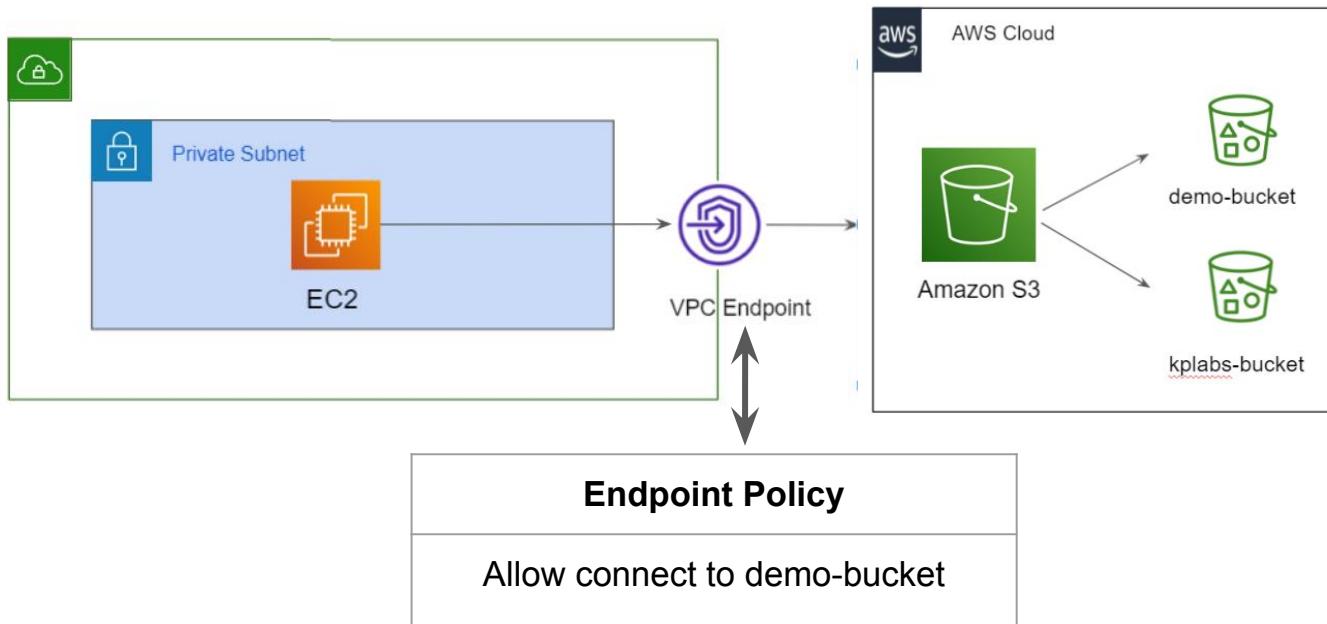
You must turn on DNS resolution in your VPC, or if you're using your own DNS server, ensure that DNS requests to the required service (such as Amazon S3) are resolved correctly to the IP addresses maintained by AWS.

VPC Endpoint Policies

Endpoint Based Access Control

Overview of VPC Endpoint Policies

When you create a gateway endpoint, you can attach an endpoint policy to it that controls access to the service to which you are connecting.



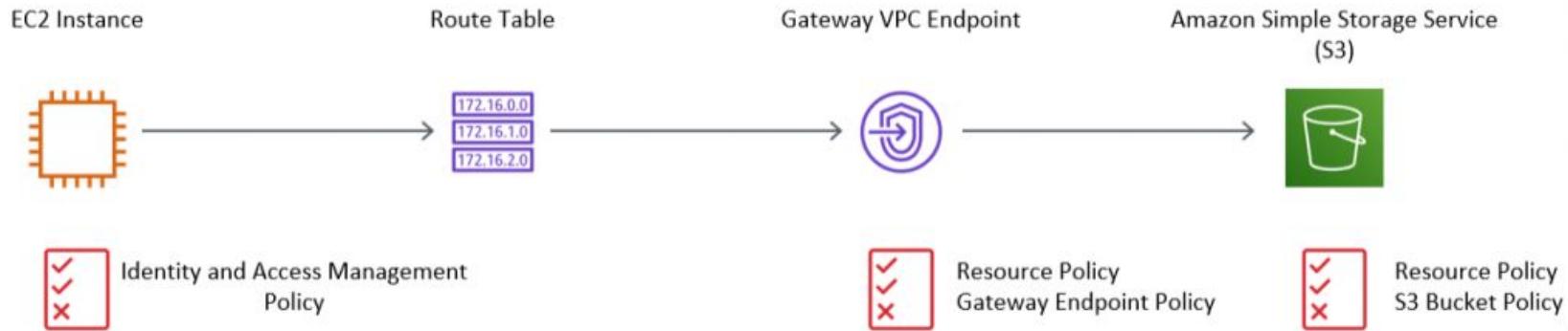
Default Policy

The default VPC Endpoint policy allows all the operations

The screenshot shows the AWS VPC Endpoint console. At the top, there is a table listing endpoints. One endpoint is selected, showing its details below the table. The selected endpoint is named 'vpce-09172dfaef7ae4a2ff'. Below the table, there are tabs for 'Details', 'Route Tables', 'Policy' (which is highlighted in yellow), and 'Tags'. A button labeled 'Edit Policy' is visible. A large text area displays the JSON policy document:

```
{  
  "Statement": [  
    {  
      "Action": "*",  
      "Effect": "Allow",  
      "Resource": "*",  
      "Principal": "*"  
    }  
  ]  
}
```

Policy Decision



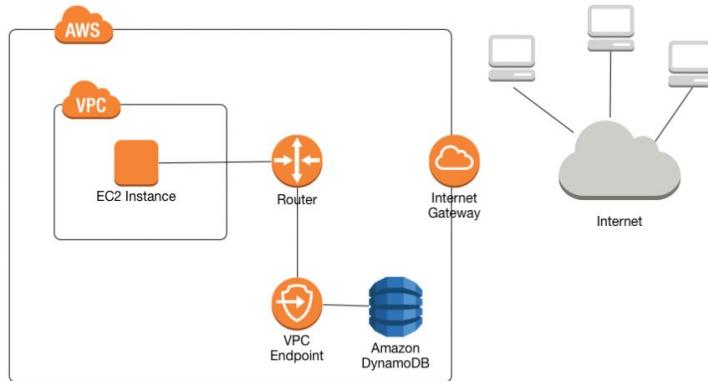
Interface Endpoints

New Generation Endpoint

Downsides of Gateway Endpoints - 1

In Gateway endpoints approach, the VPC endpoint was created outside your VPC and traffic was routed via route table.

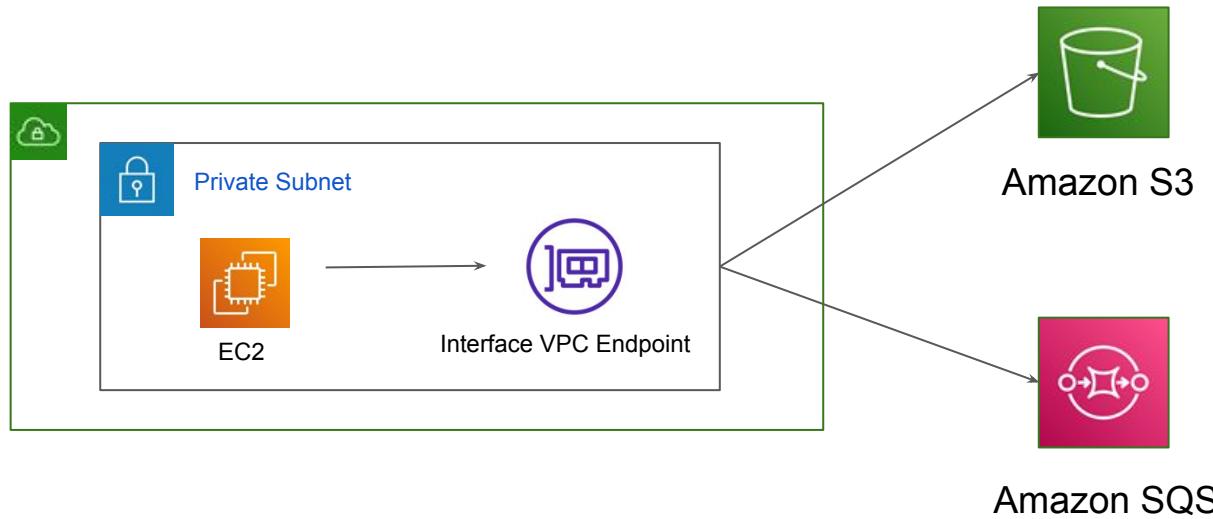
Thus, it is not possible to use it directly from VPN's or Direct connects and various others.



Interface Endpoints

An interface endpoint is an elastic network interface with a private IP address from the IP address range of your subnet.

It serves as an entry point for traffic destined to a supported AWS service or a VPC endpoint service.



Benefits of Interface Endpoint

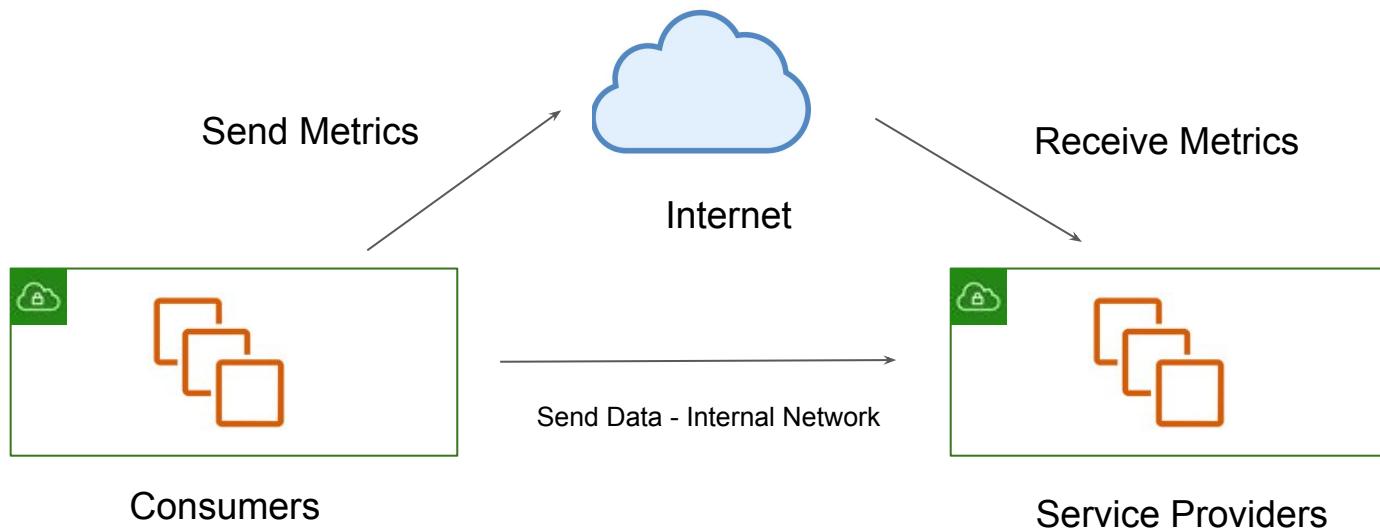
1. Interface endpoints enable the use of security groups to restrict access to the endpoint.
2. VPN's and Direct Connect based connections are supported.
3. Interface endpoints supports lot of services unlike Gateway endpoints.

VPC Endpoint Services

More Use-Cases Supported

Sample Use-Case

There are many service providers like DataDog, New Relic for which we need to upload our server/application metrics through Internet.



Dashboards using Metrics Collected

New Relic University > **SELECT** | Run New Relic University

Calagator Demo App Created by evose@newrelic.com Last edited 4/3/18

Search 2 attributes Add Dashboard Note Edit

Default 30m 60m 6h 1d 7d Custom

Calagator Demo App
AN OPEN SOURCE CALENDAR AGGREGATOR

This demo app is built using the open source calagator project.

[Calagator on Github](#)

Transaction Duration & Queing Since 60 minutes ago

| NAME | TRANS... | Avg D... | Avg Q... |
|---|----------|----------|----------|
| Controller/Middleware/Rack/ActionDispatch::Static/call | 971 | 0.01 | 0.07 |
| Controller/calagator/site/index | 319 | 0.56 | 0.1 |
| Controller/calagator/events/search | 313 | 5.78 | 0.1 |
| Controller/Middleware/Rack/ActionDispatch::Routing::RouteSet/call | 187 | 0.21 | 0.12 |
| Controller/calagator/sources/new | 20 | 0.17 | 0.04 |

Frequent Transactions in the past 4 weeks Since 4 weeks ago

Transactions

| |
|--------------------------------------|
| 631 K Controller/Middleware/Rack/ |
| 210 K Controller/calagator/site/inde |
| 197 K Controller/calagator/events/s |
| 120 K Controller/Middleware/Rack/ |
| 29.4 K Controller/Middleware/Rack/ |
| 13 K Controller/calagator/sources/ |
| 10.3 K Controller/calagator/sources/ |

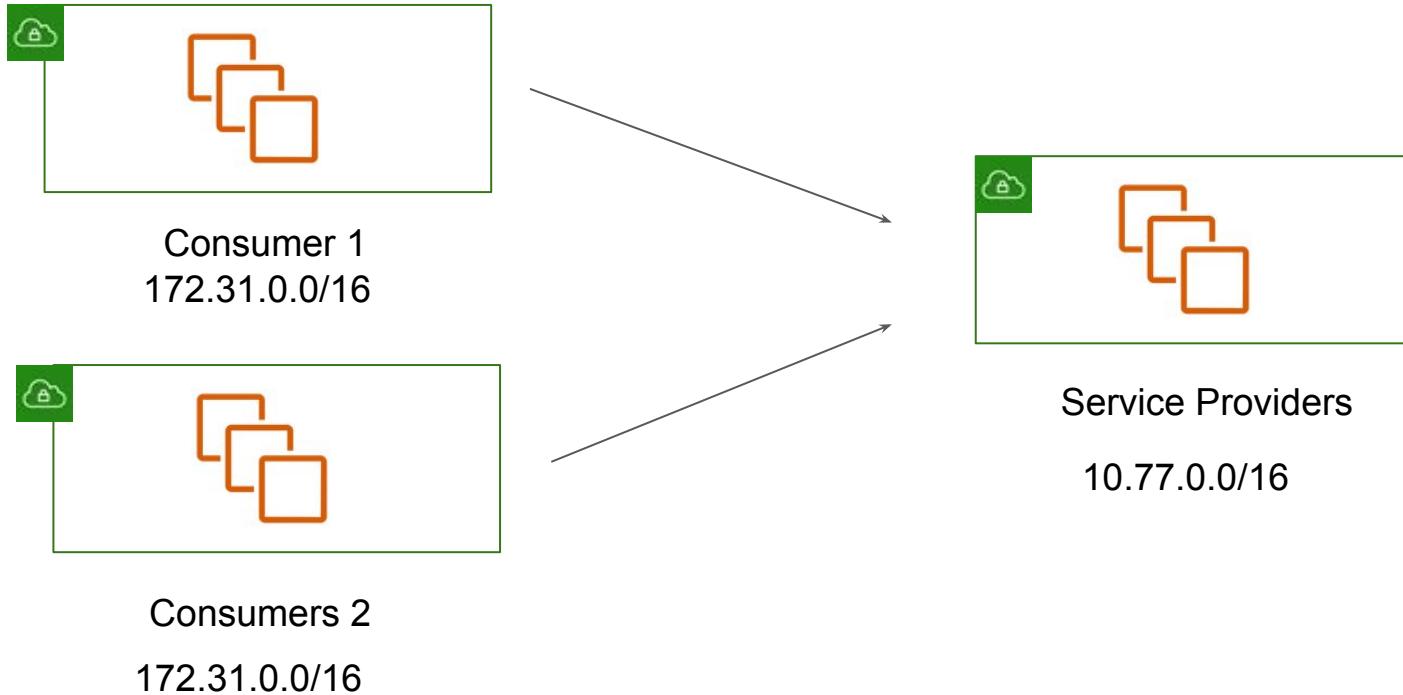
NRU Calagator Demo - Apdex Since 12 hours ago

Apdex Since 60 minutes ago

Transaction Duration Since 1 month ago

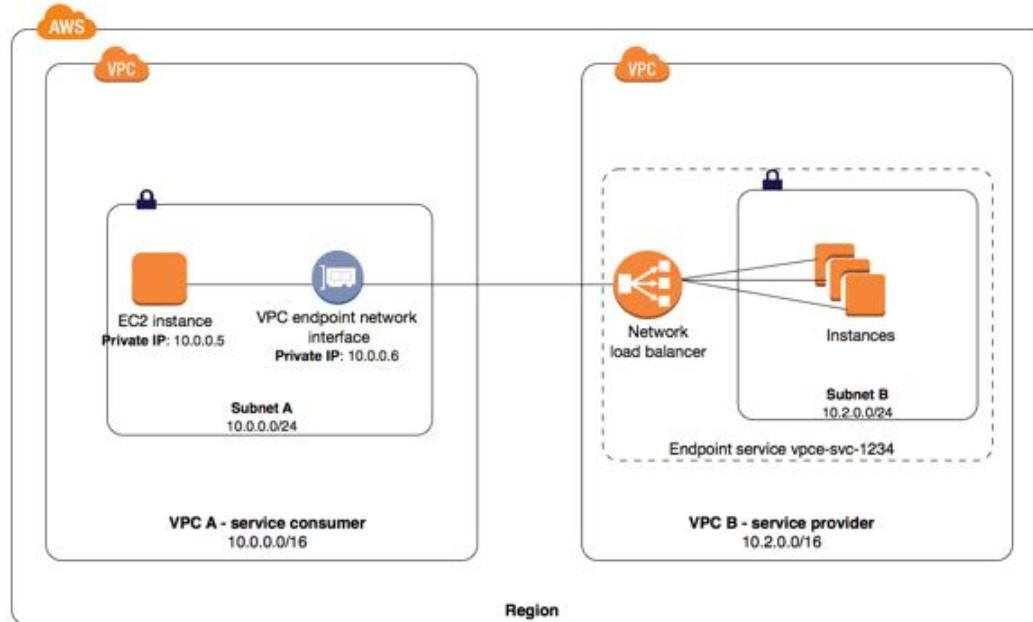
Possible Approach - VPC Peering

VPC Peering Approach will have multiple challenges related to CIDR overlap between clients.



Service VPC Endpoints

You can create your own application in your VPC and configure it as an AWS PrivateLink-powered service (referred to as an endpoint service)



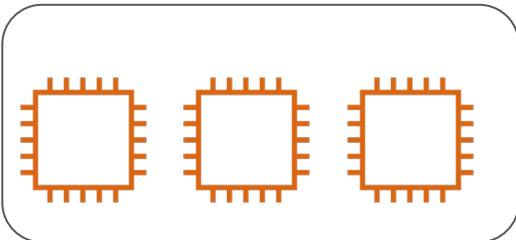
Network ACL

Multiple Layers for Defense

Understanding the Basics

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.

- Security Group works at an EC2 instance level.
- Network ACL works at a Subnet Level.



Security Group

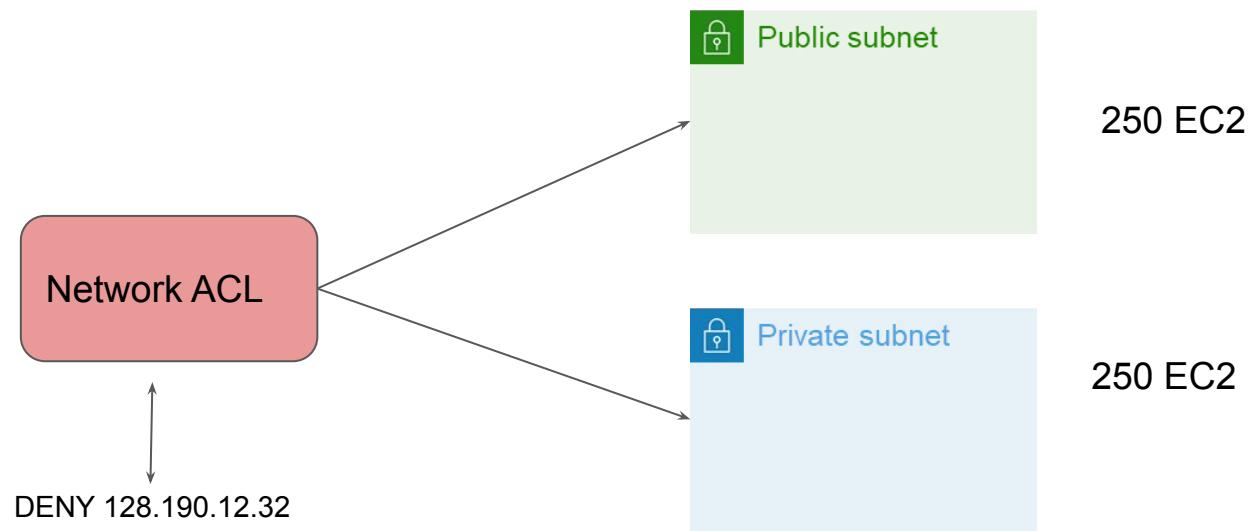


Network ACL

Understanding with Use-Case

Company XYZ is getting **lot of attacks** from a random IP **128.190.12.32**. The company has more than 500 servers and Security team decided to block that IP in firewall for all the servers.

How to go ahead and achieve that goal ?



Important Pointers

Each subnet in your VPC must be associated with a network ACL. If you don't explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL.

Default NACL allows all inbound and outbound IPv4 traffic and, if applicable, IPv6 traffic.

You can associate a network ACL with multiple subnets. However, a subnet can be associated with only one network ACL at a time.

Network ACL - Rule Ordering

Setting Right Set of NACL Rules

Basics of Rules

You can add or remove rules from the default network ACL

When you add or remove rules from a network ACL, the changes are automatically applied to the subnets that it's associated with.

The screenshot shows the AWS Network ACL management interface. The top navigation bar includes tabs for 'Details', 'Inbound rules' (which is selected and highlighted in orange), 'Outbound rules', 'Subnet associations', and 'Tags'. Below the tabs, the title 'acl-1888e173' is displayed. The main content area is titled 'Inbound rules (2)' and contains a table with two rows of rules. A 'Filter inbound rules' search bar is located at the top left of the table. At the top right, there is a 'Edit inbound rules' button and a navigation bar with icons for back, forward, and refresh. The table has columns for Rule number, Type, Protocol, Port range, Source, and Allow/Deny. The first rule (Rule number 100) is an 'Allow' rule for all traffic (Type: All traffic, Protocol: All, Port range: All, Source: 0.0.0.0/0) with a green checkmark icon next to 'Allow'. The second rule (Rule number *) is a 'Deny' rule for all traffic (Type: All traffic, Protocol: All, Port range: All, Source: 0.0.0.0/0) with a red crossed-out circle icon next to 'Deny'.

| Rule number | Type | Protocol | Port range | Source | Allow/Deny |
|-------------|-------------|----------|------------|-----------|---|
| 100 | All traffic | All | All | 0.0.0.0/0 | <input checked="" type="checkbox"/> Allow |
| * | All traffic | All | All | 0.0.0.0/0 | <input type="checkbox"/> Deny |

Rule Ordering

Rules are evaluated starting with the lowest numbered rule.

As soon as a rule matches traffic, it's applied regardless of any higher-numbered rule that might contradict it.

| Rule Number | Rule Contents |
|-------------|----------------------|
| 99 | ALLOW from 10.77.0.5 |
| 100 | DENY from ALL |

Important Pointers - Deciding Ports

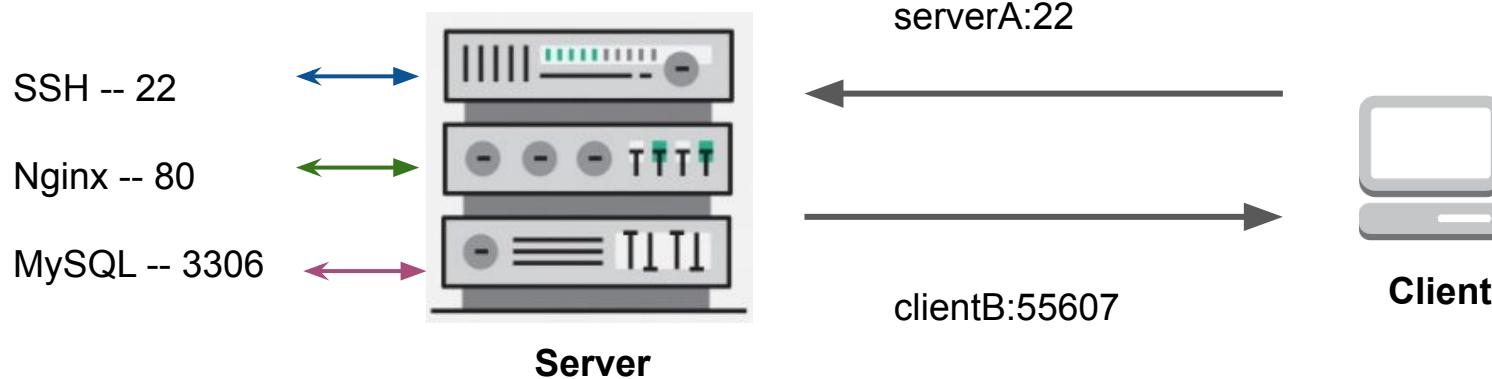
- Clients that initiates the request chooses ephemeral port range.
- Port 0 to 1023 are well known or reserved ports.
- This range varies depending on the Operating System.

Example :-

Many Linux kernels uses ports 32768-61000.

Request originating from the ELB uses 1024-65535

Windows XP uses 1025-5000 port range.



- Clients opens an **port 55607** from which it sends data to serverA port 22
- serverA has to respond back to the same IP (clientB) & port (55607).

TCP/IP Communication

```
fczv329@fcblr-l003:~/Documents$ cat handshake
19:46:27.378297 3c:a9:f4:a0:fa:e0 > 08:5b:0e:47:be:1e, ethertype IPv4 (0x0800), length 74: 172.20.1.55.55427 > 128.199.106.4.80: Flags [S], seq 3002048179, win 29200, options [mss 1460,sackOK,TS val 202385607 ecr 0,nop,wscale 7], length 0

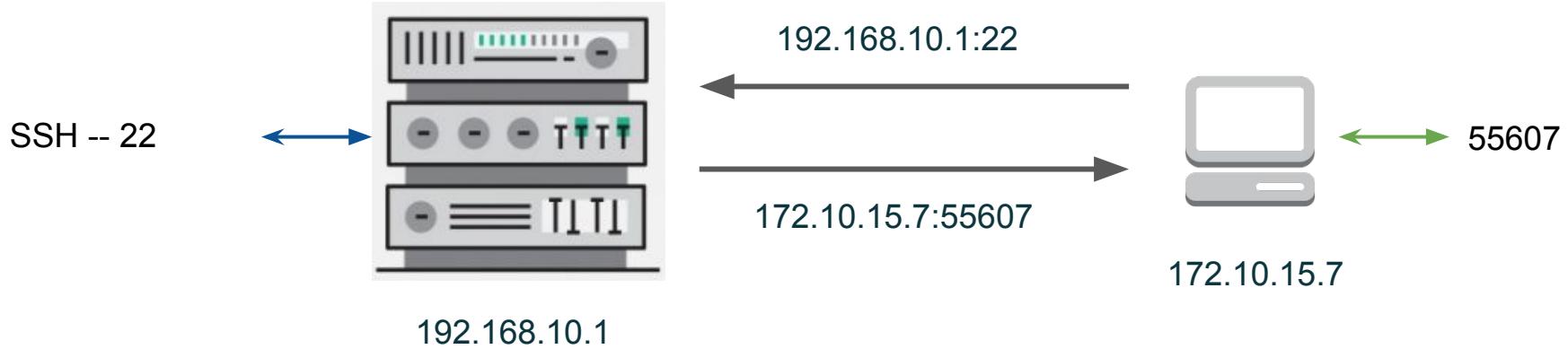
19:46:27.798037 08:5b:0e:47:be:1e > 3c:a9:f4:a0:fa:e0, ethertype IPv4 (0x0800), length 74: 128.199.106.4.80 > 172.20.1.55.55427: Flags [S.], se
q 2402250441, ack 3002048180, win 14480, options [mss 1460,sackOK,TS val 2028995051 ecr 202385607,nop,wscale 8], length 0

19:46:27.798119 3c:a9:f4:a0:fa:e0 > 08:5b:0e:47:be:1e, ethertype IPv4 (0x0800), length 66: 172.20.1.55.55427 > 128.199.106.4.80: Flags [.], ack
1, win 229, options [nop,nop,TS val 202385712 ecr 2028995051], length 0
```

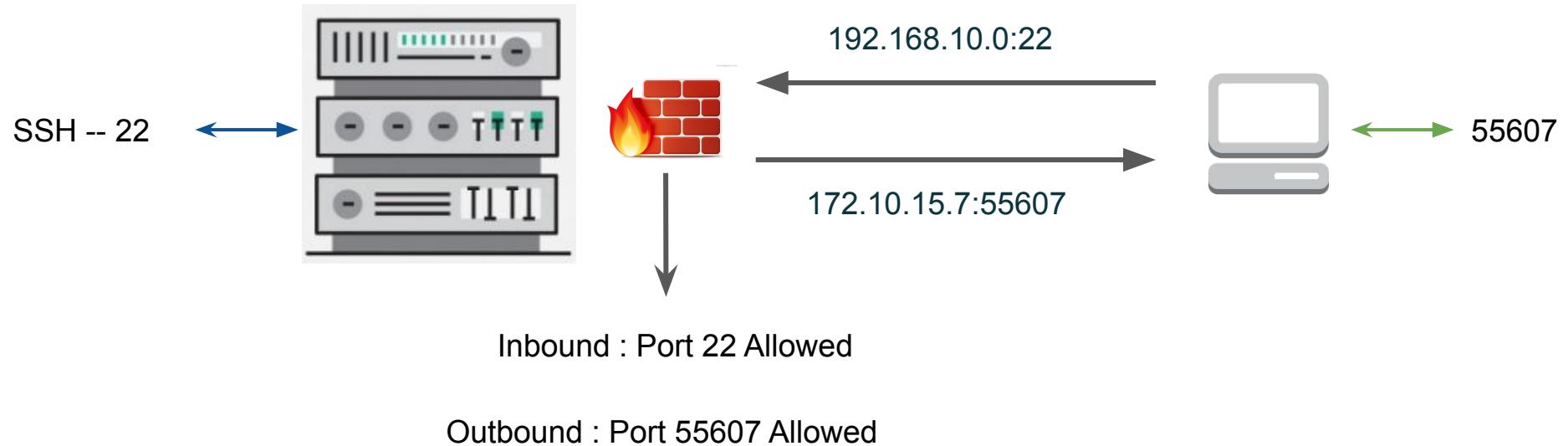
Stateful vs Stateless Firewalls

2 types of Firewall

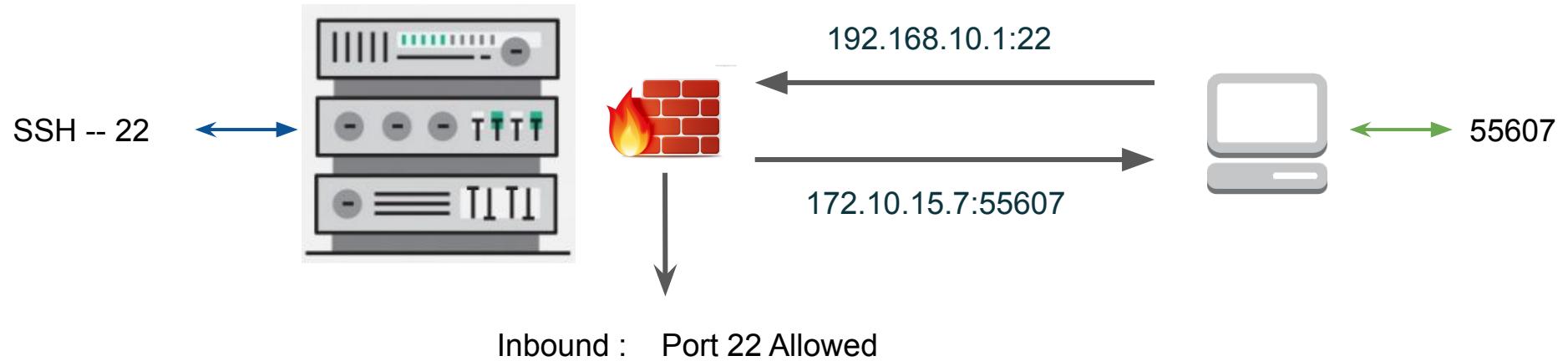
Basic TCP/IP Communication



When Stateless Firewall is Involved



Stateful Firewall



The Finale

There are 2 main types of Firewall :-

- Stateful Firewall
- Stateless Firewall

Stateful firewall maintains the connection state and knows which packets to allow Outbound even when outbound is restricted.

Stateless firewall does not maintain the connection state and for them each packet traversing inbound or outbound is a new separate packet.

IDS / IPS

TCP/IP - Back to the Origin

Simple Analogy

Firewall :-

- It keeps everyone out who tries to sneak in via basement windows, back side doors etc BUT if someone enters through official door, the entry is given.



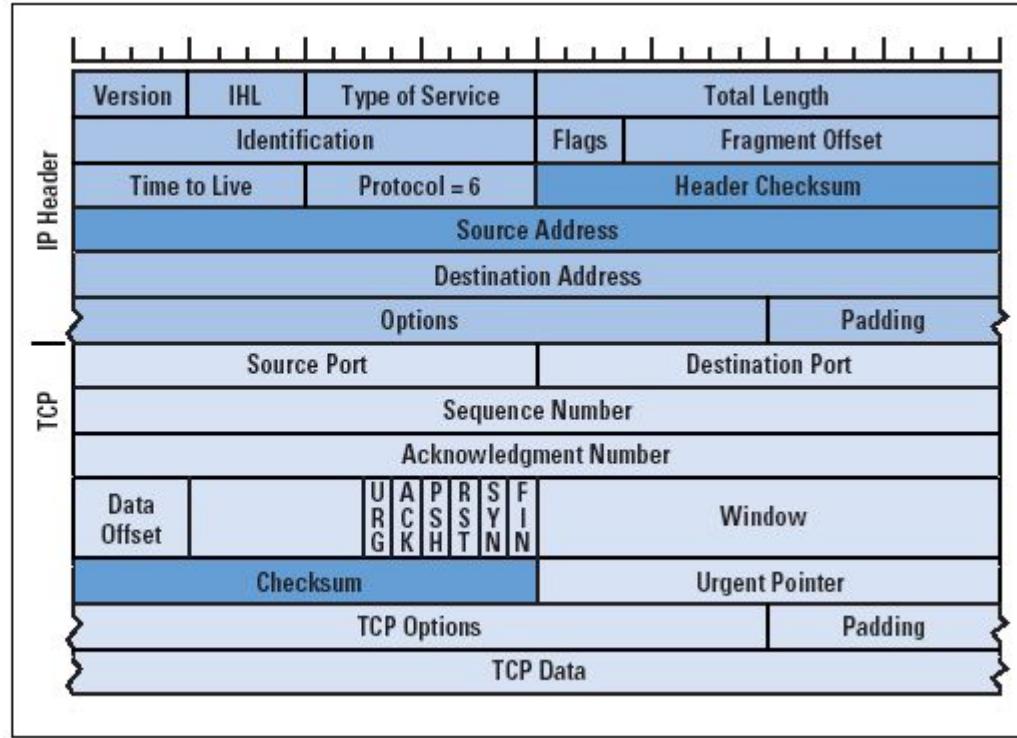
IDS / IPS :-

It can search the people to check if they are carrying weapons with them.

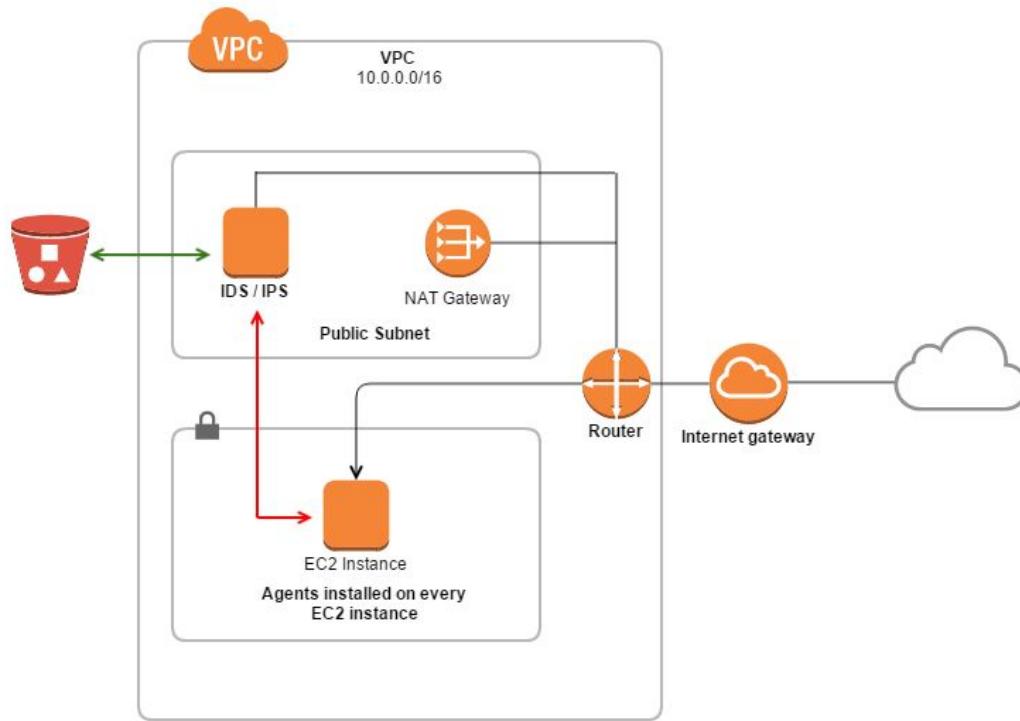


TCP/IP Header

Figure 1: TCP/IP Header
Fields Altered by NATs
(Outgoing Packet)



IDS / IPS Architecture



Things to Remember

- IDS - Intrusion Detection System
- IPS - Intrusion Prevention System
- You have a IDS / IPS agents installed in the EC2 instance which will communicate to the central IDS / IPS appliance.

Content Delivery Network

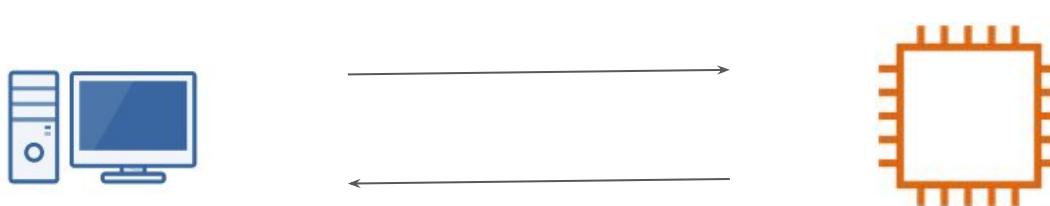
CDN is Awesome

Generic Scenario

Let's consider a typical scenario where everything is hosted in a single server.

On a smaller scale this seems to be an ideal approach.

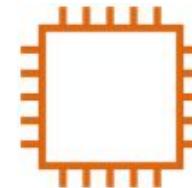
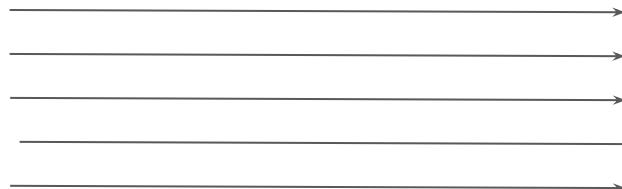
But when the traffic and popularity grows, there are a lot of challenges.



Challenge 1 - Performance

With an increase in number of visitors, the performance can go down.

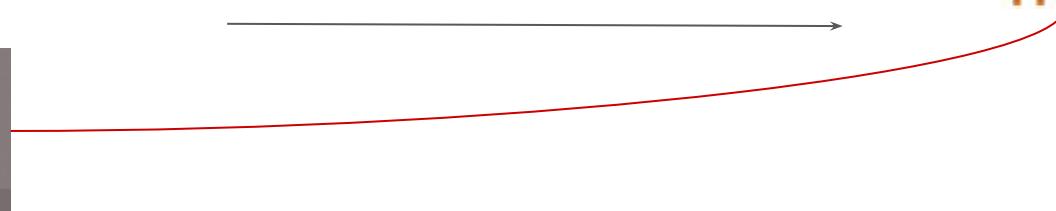
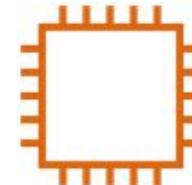
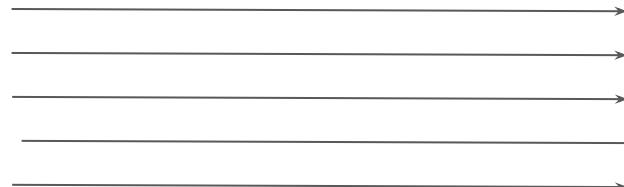
If website has 1 image and 1000 users are visiting it, then the same single image will need to be sent to 1000 users.



Challenge 2 - Security

Attackers love the Internet.

A typical website and web-application face various type of attacks ranging from DOS, Web-Application attacks and so on.



Typical Solution

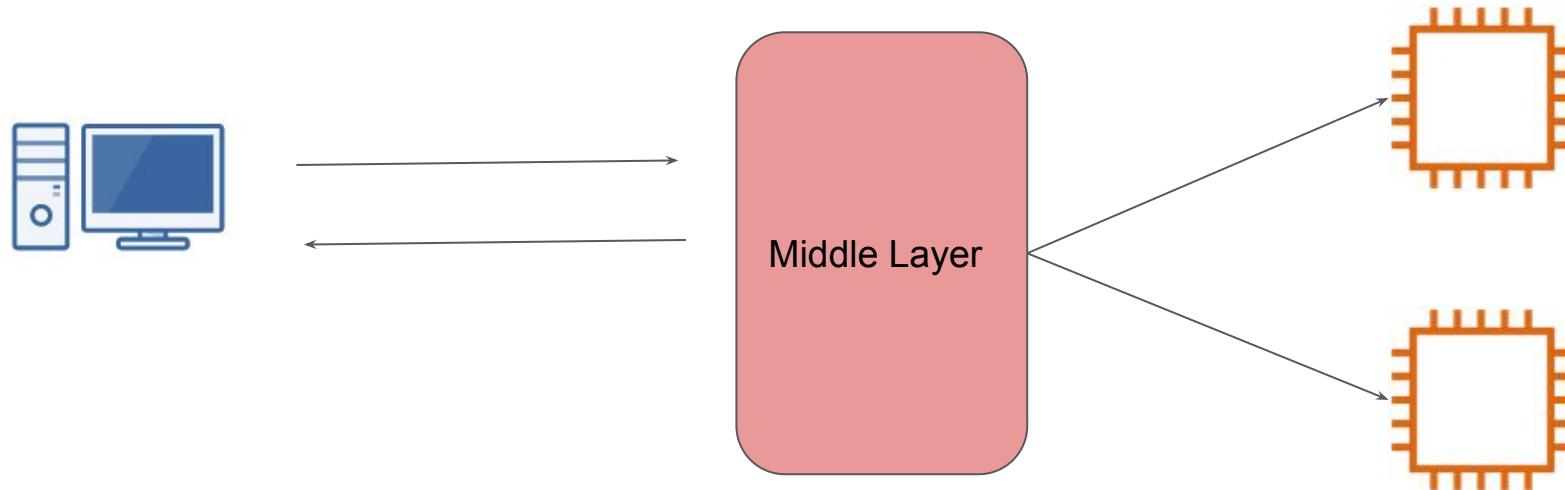
Some of the approaches to the challenges that we discussed:

1. Increase the size of server / increase number of servers for better performance.
2. Configure DDoS protection, Web-Application Firewall etc at the server level.

Doing these things on each server is a tedious task and it cannot scale very well.

Better Architecture

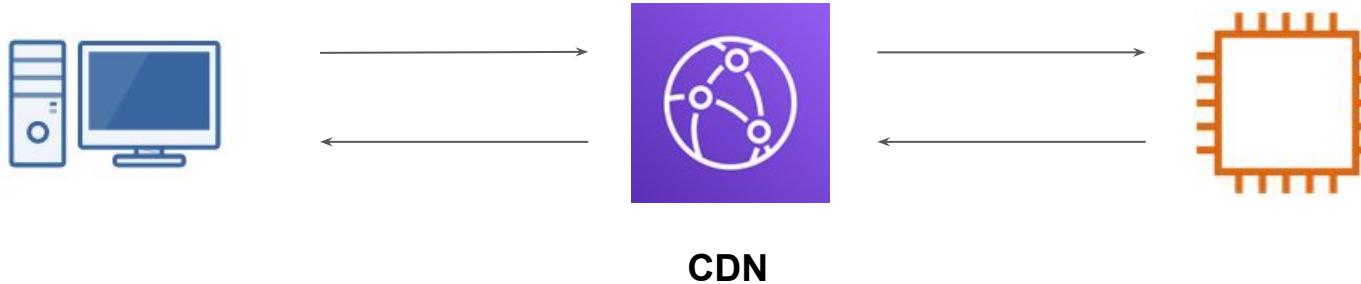
Better architecture would be to introduce a middle layer that has all functionalities related to protecting against attacks, caching of commonly requested objects for better performance.



Content Delivery Network

A CDN acts as a proxy that receives the request and then forwards it to the backend systems.

Various CDN's also comes with features like DDoS Protection, WAF, Cachig and others.



Edge Locations

CDN is Awesome

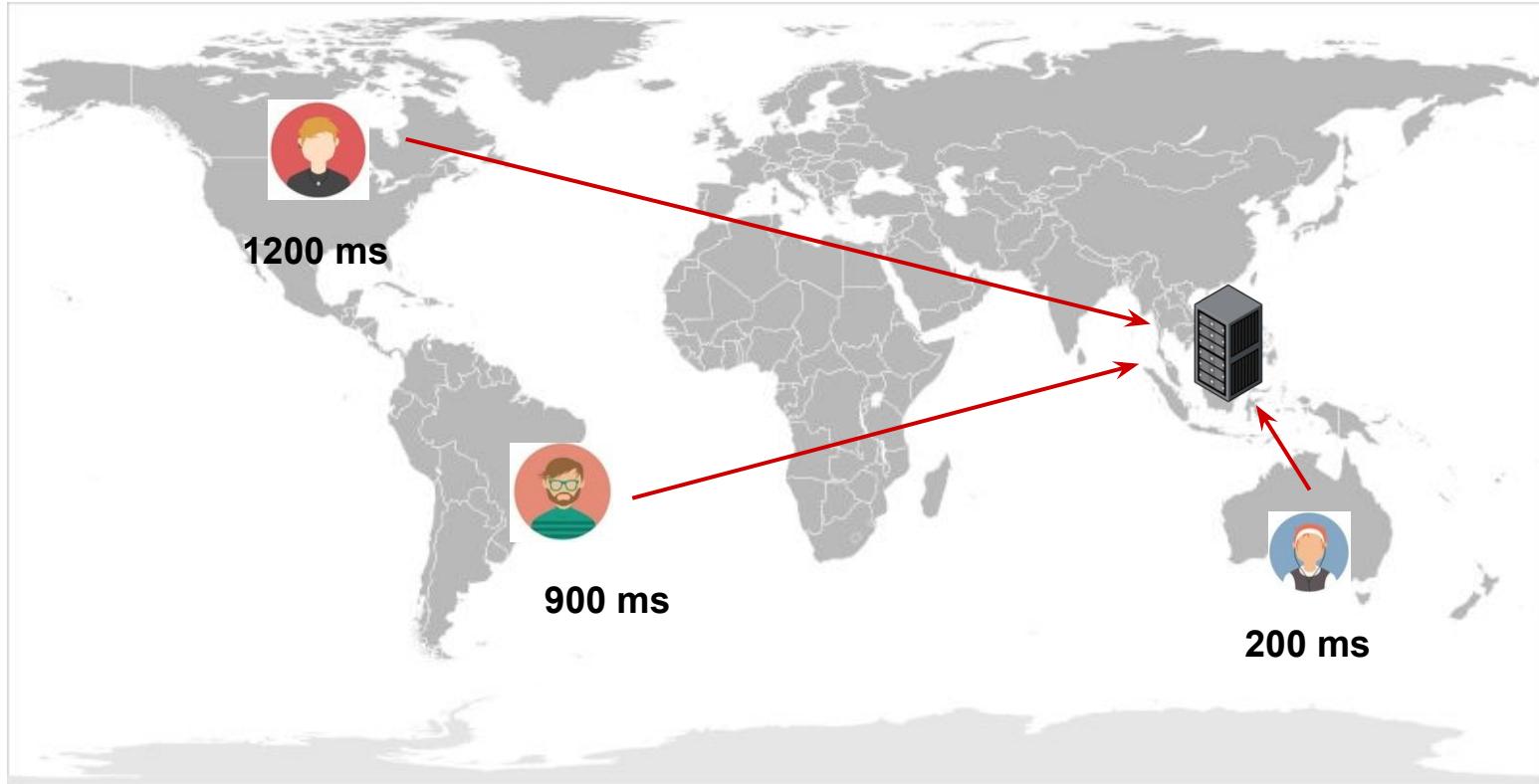
Reverse Proxy Caching Scenario

Many organization uses CDN for various reasons :-

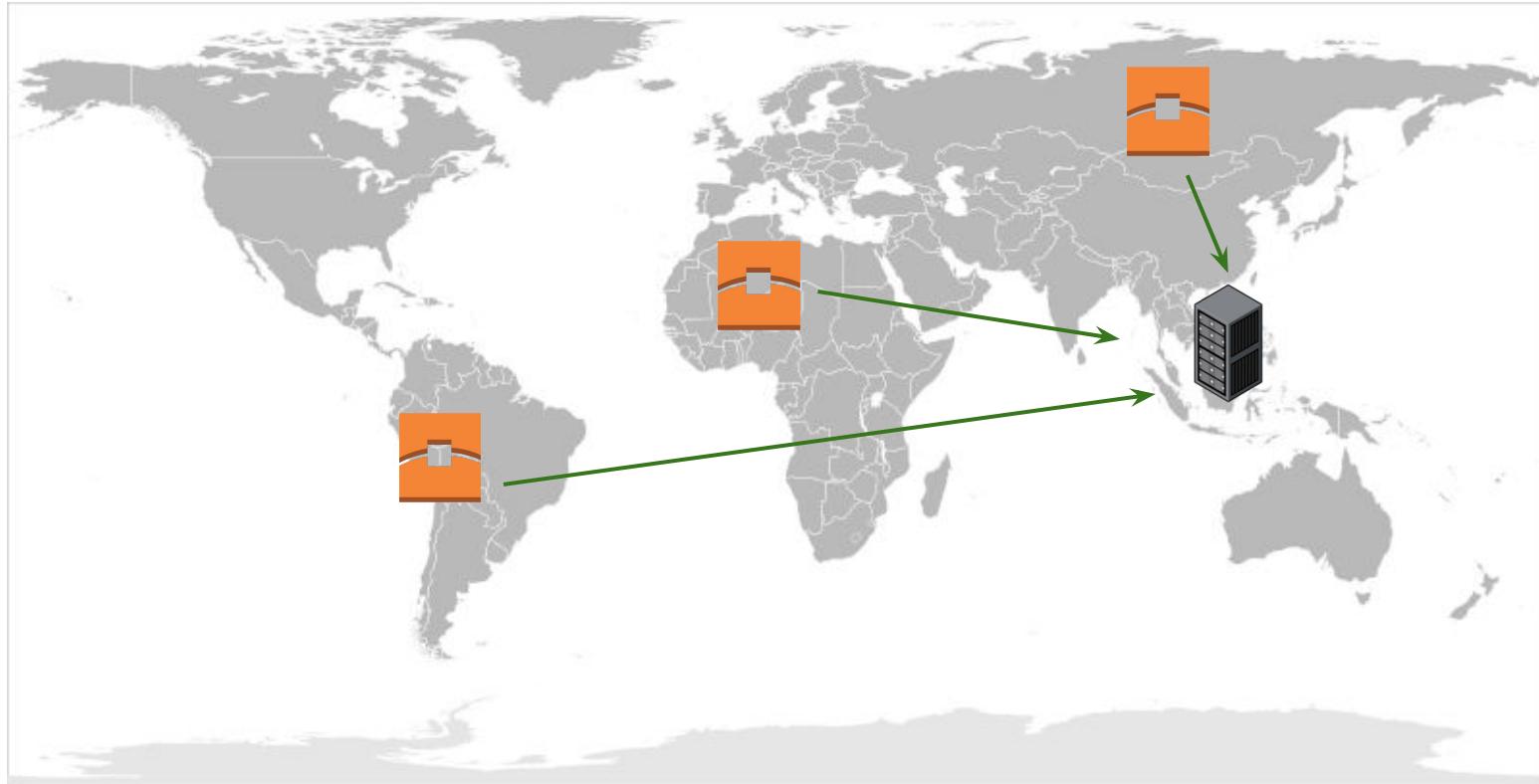
- Content Caching
- Web Application Firewall
- DDOS Attacks
- For ALL of Above



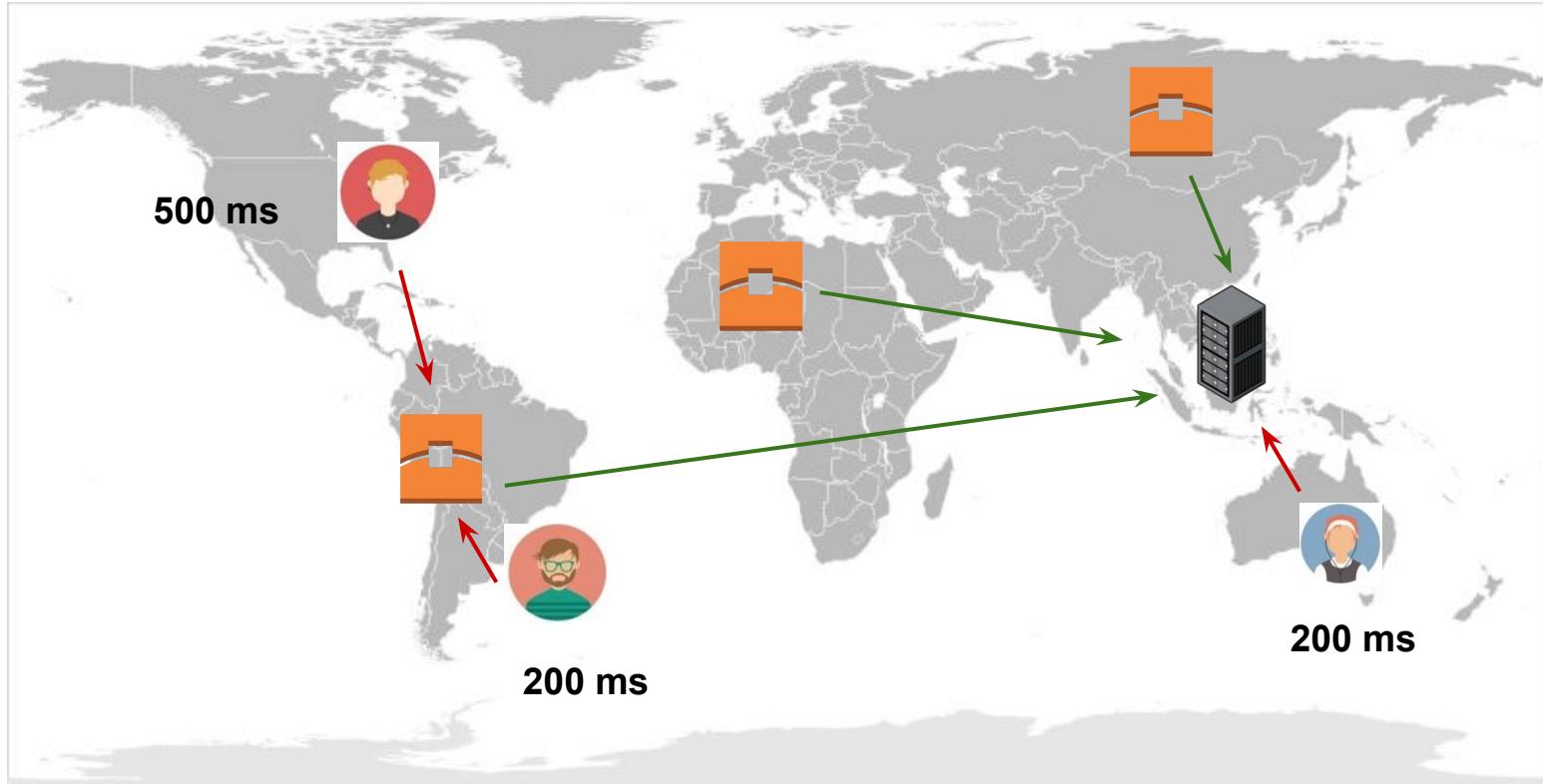
Understanding CDN



Edge Locations



Edge Locations



CloudFront Edge Locations

| North America | Europe | Asia | South America |
|---|---|--|---|
| United States | Edge Locations | Edge Locations | Edge Locations |
| Edge Locations | | | |
| <ul style="list-style-type: none">Ashburn, VA (3)Atlanta, GA (2)Chicago, ILDallas/Fort Worth, TX (2)Hayward, CAJacksonville, FLLos Angeles, CA (2)Miami, FLMinneapolis, MNNew York, NY (3)Newark, NJPalo Alto, CAPhiladelphia, PASan Jose, CASeattle, WASouth Bend, INSt. Louis, MO | <ul style="list-style-type: none">Amsterdam, The Netherlands (2)Berlin, GermanyDublin, IrelandFrankfurt, Germany (5)London, England (4)Madrid, SpainMarseille, FranceMilan, ItalyMunich, GermanyParis, France (2)Stockholm, SwedenVienna, AustriaWarsaw, Poland | <ul style="list-style-type: none">Chennai, IndiaHong Kong, China (3)Mumbai, India (2)Manila, the PhilippinesNew Delhi, IndiaOsaka, JapanSeoul, Korea (3)Singapore (2)Taipei, TaiwanTokyo, Japan (3) | <ul style="list-style-type: none">São Paulo, Brazil (2)Rio de Janeiro, Brazil |
| | Regional Edge Caches | | Regional Edge Caches |
| | | | <ul style="list-style-type: none">Mumbai, IndiaSingaporeSydney, AustraliaSeoul, South KoreaTokyo, Japan |
| | | Australia | |
| | | Edge Locations | |

Deploying CloudFront Distribution

CDN is Awesome

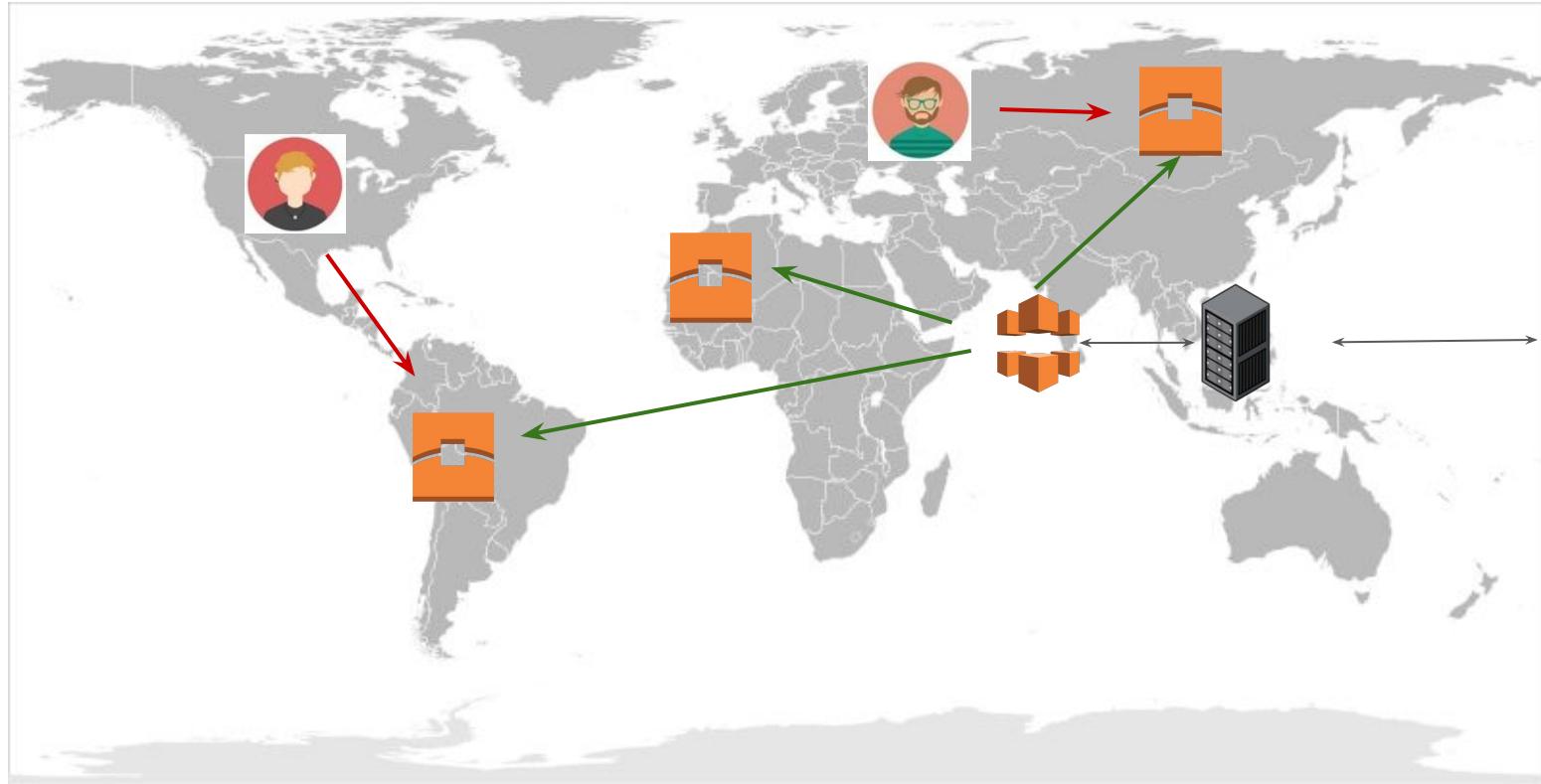
Deploying CloudFront

Steps Involved :-

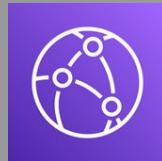
1. Create a sample HTML Website
2. Create CloudFront Distribution
3. Connect CloudFront with Website Endpoint.



Understanding CDN

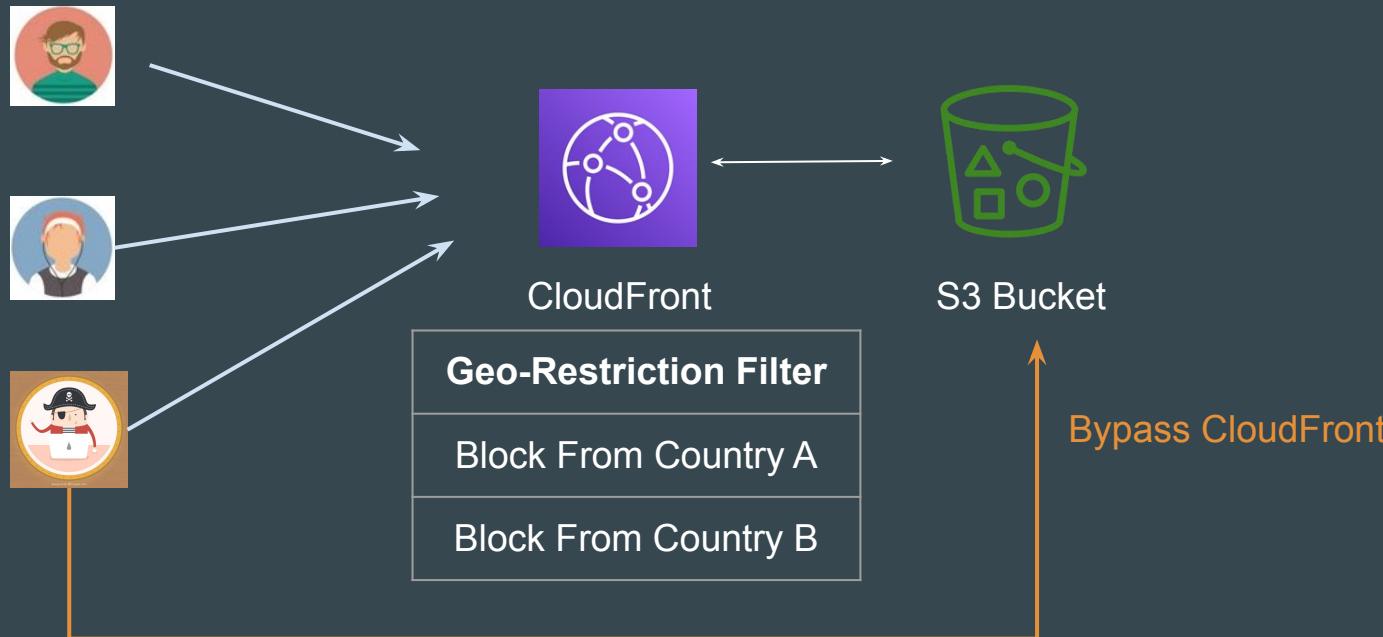


Origin Access Identity



Understanding the Challenge

Security measures applied at Cloudfront can easily be bypassed if attacker sends queries directly to the origin.



CloudFront Origin Access Identity

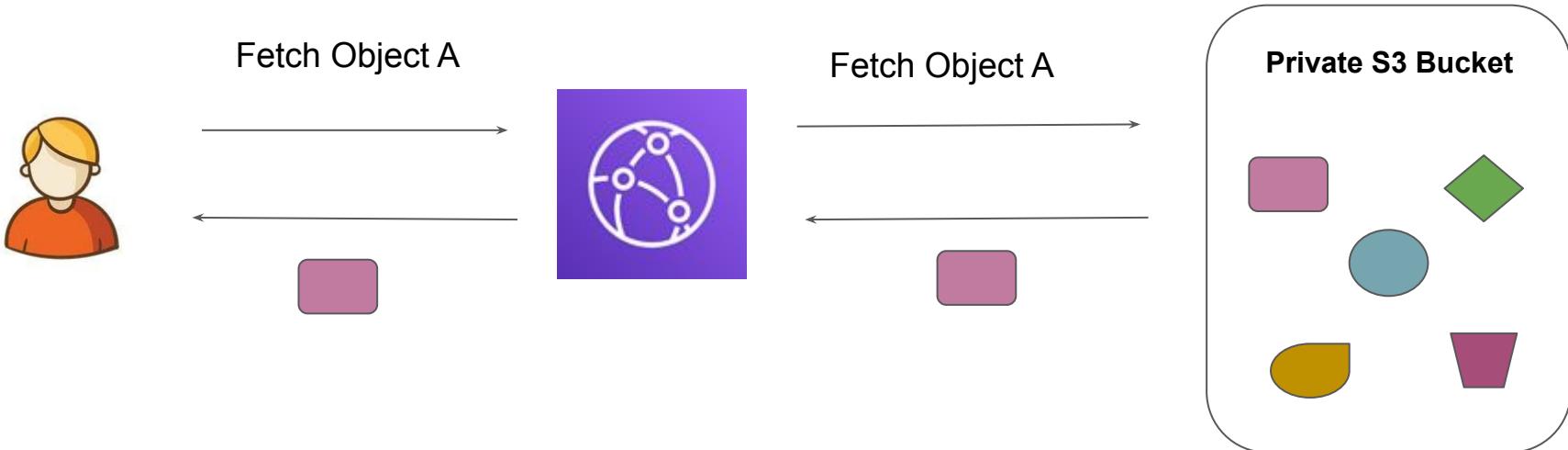
CloudFront Origin Access Identity **ensures** that only users coming through CloudFront distribution are able to access the contents of your S3 Buckets.



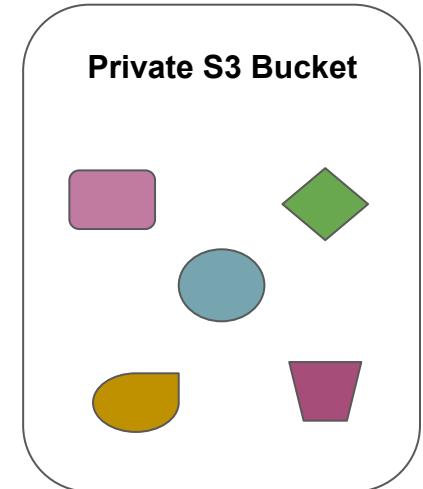
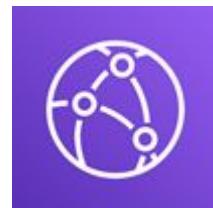
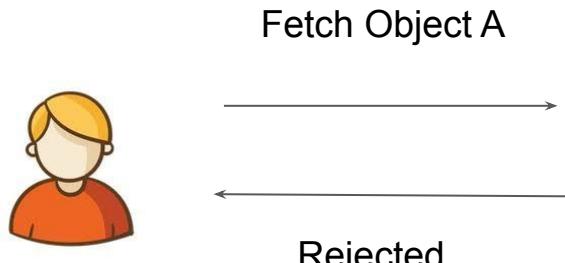
CloudFront Signed URLs

CDN is Awesome

Generic Approach

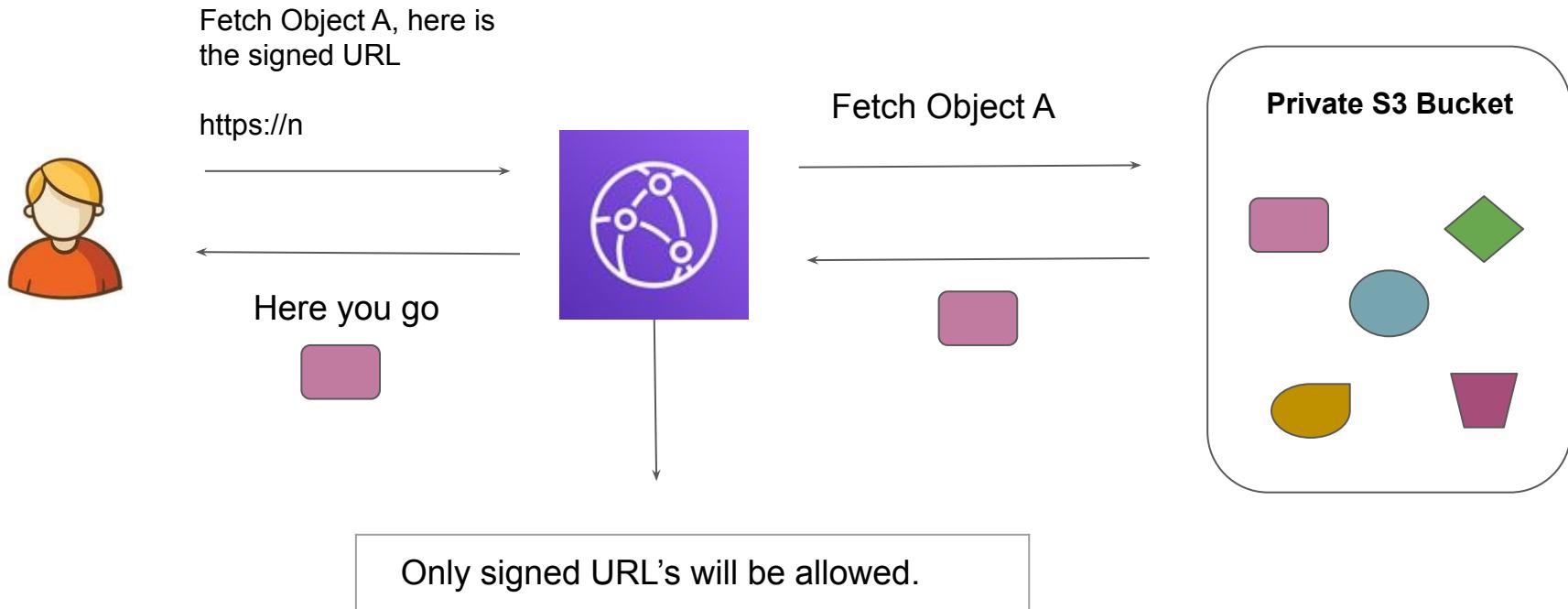


Allow only special URLs



Only special URL's will be allowed.

Architecture Overview of Signed URLs



CloudFront Signed URLs

CloudFront Signed URLs mandates users to provide signed URLs or signed cookies to access the private content.

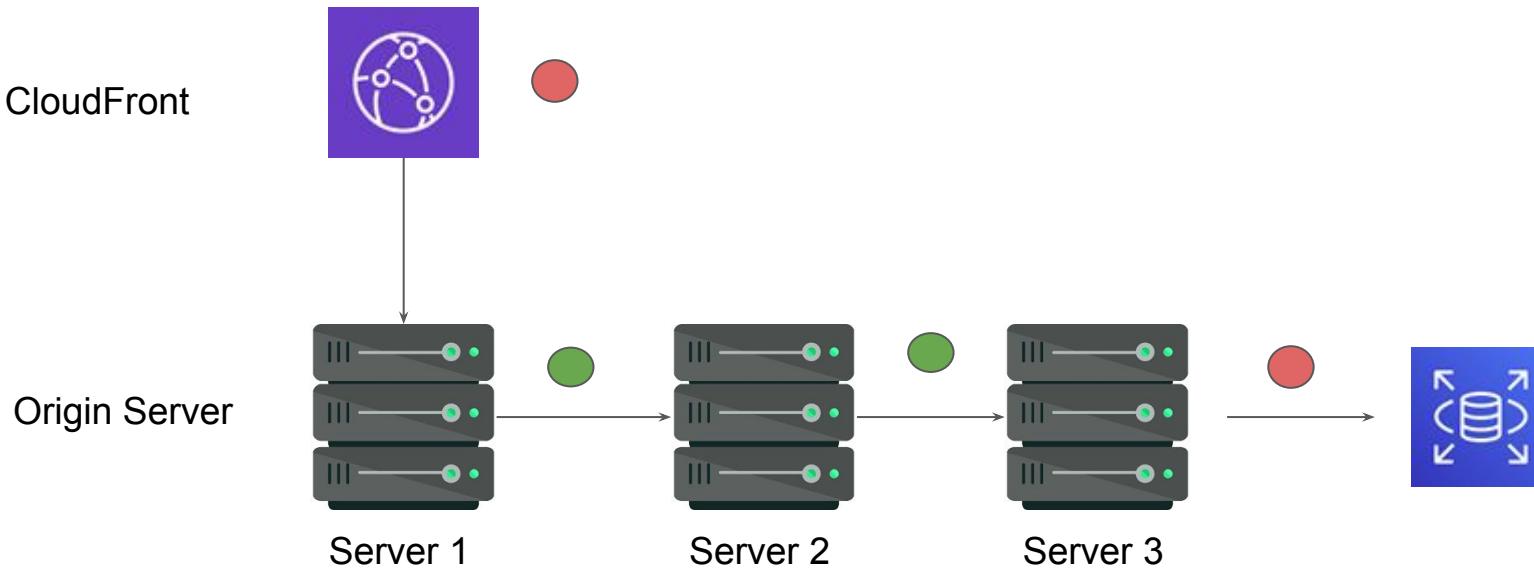
CloudFront signed URLs can be generated by the trusted signers assigned in your AWS account.

Field Level Encryption - CloudFront

Cryptography Yet Again!

Understanding The Challenge

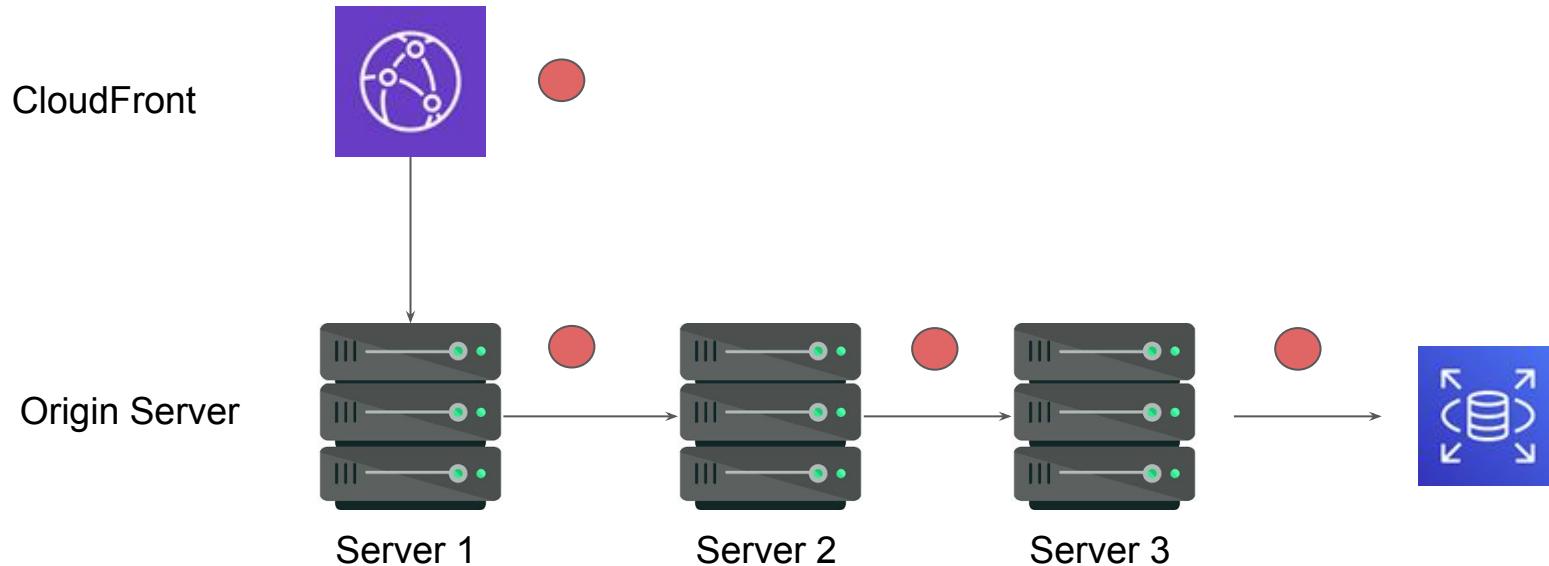
Sensitive Data when travelling via multi-tier architectures leads to security challenges.



Possible Solution

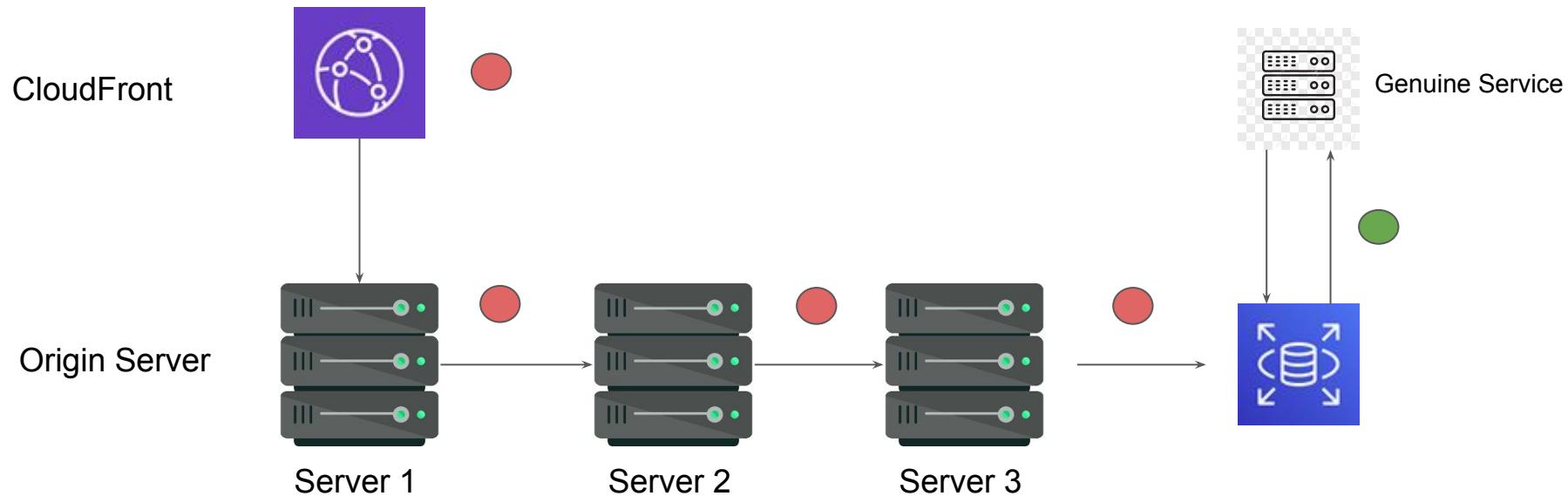
Encrypting Data end-to-end so that no intermediary service have access to it.

Only specific service which has genuine business need should be able to fetch and decrypt data.



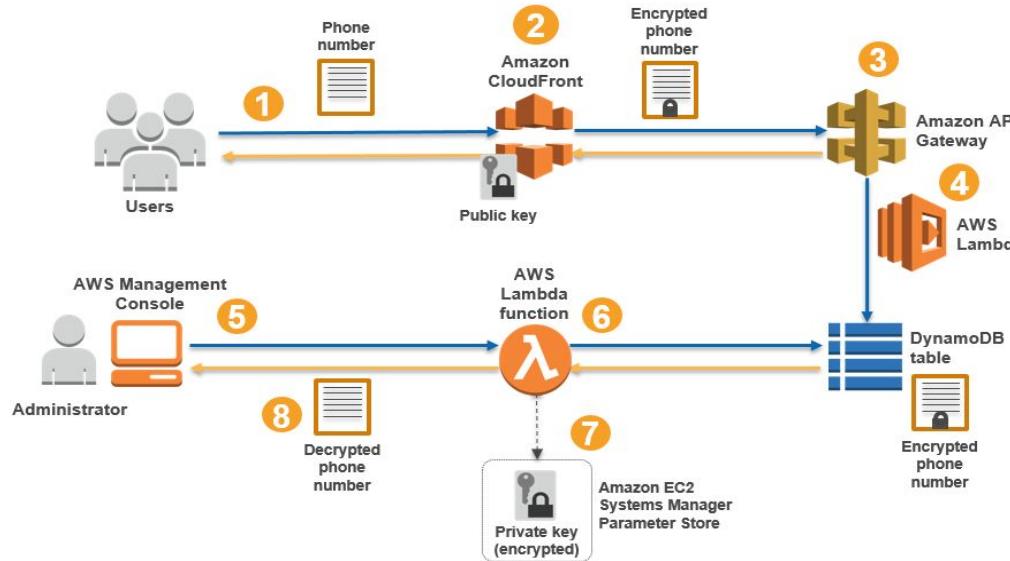
Plain Text Data to Only Genuine Service

Only specific service which has genuine business need should be able to fetch and decrypt data.



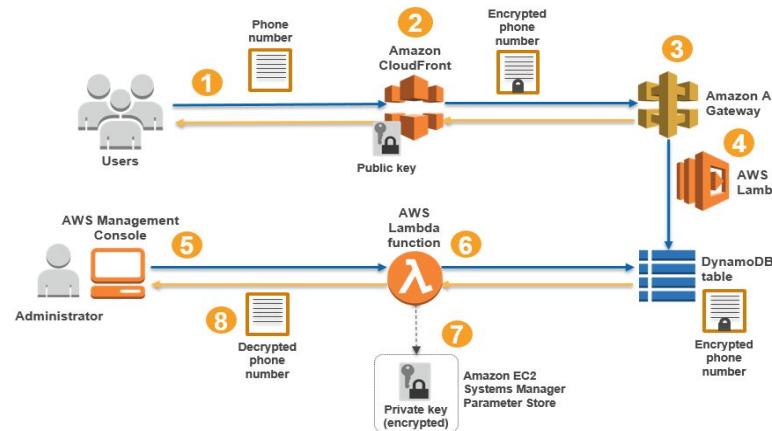
Field Level Encryption

CloudFront field-level encryption encrypts the sensitive PII data before the request is forwarded to the origin.



High Level Steps

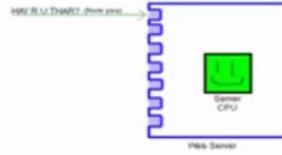
1. Application sends POST request with PII data.
2. FLE intercepts POST request, encrypts the data with public key and forwards to origin.
3. Origin takes the data and processes it normally and stores to DynamoDB table.
4. Lambda Function stores the data in DynamoDB.
5. Admin uses Lambda function to retrieve encrypted data from DynamoDB.
6. Admin uses key-material stored in parameter store to decrypt sensitive data.
7. Decrypted Data is returned to the Administrator.



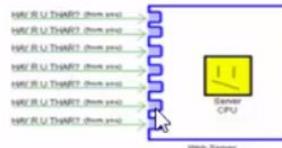
Denial of Service

Attack difficult to mitigate

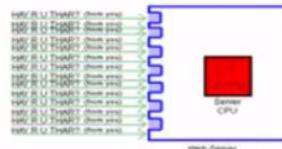
normal service →



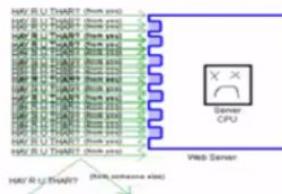
high traffic →



single DOS →



LOL DDOS'D →



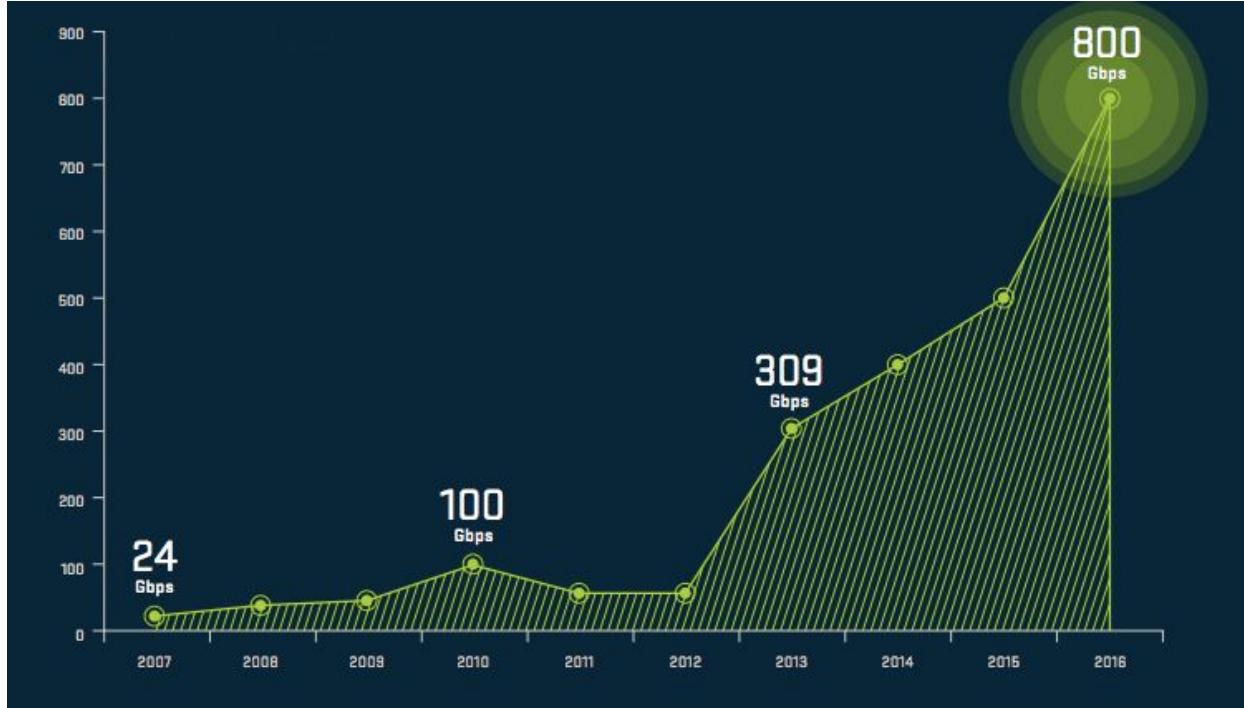
DOS and DDoS are part and parcel of servers life

DOS and DDoS attacks are very common attack vectors used nowadays to bring down the servers or flood the network.

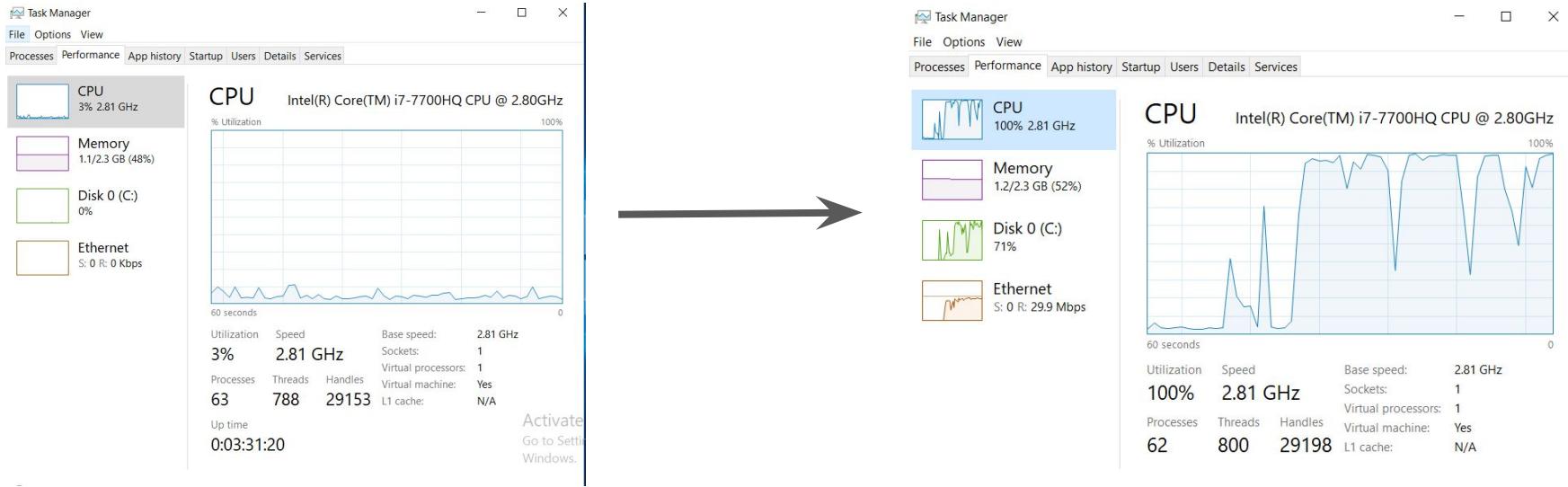
The reason why they are so successful is because of ease of ability to launch the attack and most of the protection mechanisms are based on expensive hardware.



DDOS attacks are going really big!



Before vs After (DOS Attack)



DDOS Attacks Crush Twitter, Hobble Facebook

Posted Aug 6, 2009 by Michael Arrington (@arrington)



The image shows the Twitter homepage. At the top, there's a navigation bar with links for Home, Profile, Find People, Settings, Help, and Sign out. Below the navigation, a large message box contains the text: "We had network issues today related to a denial-of-service attack. Service now is restored for most people and we're investigating further." This message was posted 8 minutes ago from the web. At the bottom of the page, there's a Facebook logo and a link to their site. The footer contains links for About Us, Contact, Blog, Status, Goodies, API, Business, Help, Jobs, Terms, and Privacy.

Crunchbase

| Facebook | |
|------------|---|
| FOUNDED | 2004 |
| OVERVIEW | |
| LOCATION | Menlo Park, California |
| CATEGORIES | |
| WEBSITE | http://www.facebook.com |

AWS Shield

DDoS Protection

Understanding AWS Shield

AWS Shield is a managed Distributed Denial of Service (DDoS) service that safeguards the workloads running on AWS against DDoS attacks.

There are two tiers of AWS Shield:

- Shield Standard
- Shield Advanced

Understanding AWS Shield

AWS Shield standard provides basic level protection against most common network and transport layer DDoS attacks.

For a higher level of protection, we can subscribe to the Shield Advanced. Shield Advanced protects against large and sophisticated DDoS attacks with near-real-time visibility into the attacks that might be occurring.

AWS Shield Advanced also gives customers 24x7 access to the AWS DDoS Response Team (DRT) during ongoing attacks.

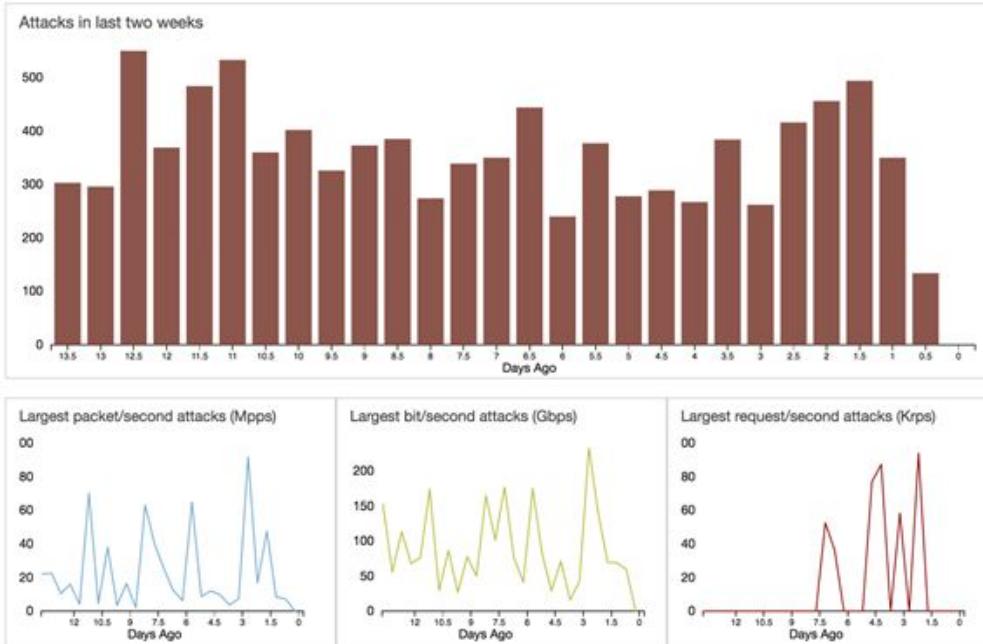
AWS Shield Costs and Credits

AWS Shield Advanced costs 3000\$ per organization and requires Business or Enterprise Support.

One interesting part about AWS Shield Advanced is that during the attack, if your infrastructure has scaled, AWS will return you the amount occurred during scaling in the form of credits. This is also referred to as Cost protection.



AWS Shield Dashboard



Mitigating DDOS

The stronghold for Fort

Mitigating DDOS

- Be ready to scale as traffic surges.
- Minimize the attack surface area.
- Know what is normal and abnormal.
- Create a Plan for Attacks.



Be Ready to Scale

1. Be Ready to Scale

- Your infrastructure should be designed to scale when the traffic increases.
- It not only helps in Business but also during DDOS Attacks.

Example :

Whenever CPU load is more than 70% in Application servers, automatically add one more Application server to meet the needs.

AWS Services : ELB, Auto Scaling

Let's Minimizing is the Key

2. Minimize the attack surface area.

Decouple your infrastructure.

Example :

Application and Database should not be on the same server.

AWS Services : SQS, Elastic BeanStalk

Normal and Abnormal

3. Know what is normal and abnormal

- Key metrics need to be defined to understand the behavior.

Example :

Website getting a huge surge in traffic in the middle of the night at 3 AM

AWS Services :- CloudWatch, SNS.

Create a Plan

4. Create a Plan for Attacks.

For example :

- Check whether the Source IP Address is the same.
- Check from which country the increased traffic is coming from.
- Nature of the attack (SYN Flood, Application Level)
- Can it be blocked with NACL or Security Group level.



It is recommended to have AWS Support. At-least Business Support.

AWS Services for DDoS Attack Mitigation

Following are some of the key AWS services involved in DDoS attack mitigation

- **AWS Shield**
- **Amazon CloudFront**
- **Amazon Route53**
- AWS WAF
- Elastic Load Balancing
- VPC & Security Groups

Basics of API



Understanding the Challenge

Book Distributor maintains the list of available books in it's backend systems.

Operator has access to Backend system to check the availability.

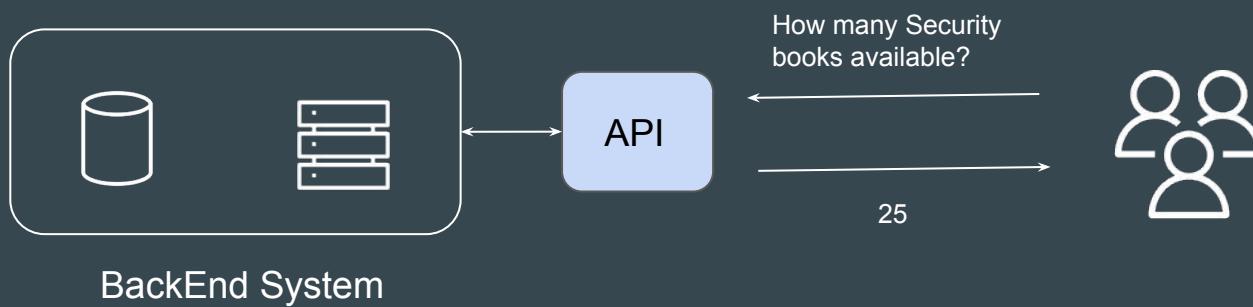
Clients they connect to Operator via Phone call / Chat option



API Based Approach

The book distributor could provide an API to check stock availability.

APIs let you open up access to your resources while maintaining security and control.



Simple Use-Case

James wants to build a weather report application.

OpenWeatherMap is an online service that provides global weather data via API.

He decided to connect his application to OpenWeatherMap API to fetch the latest reports and populate it in application.



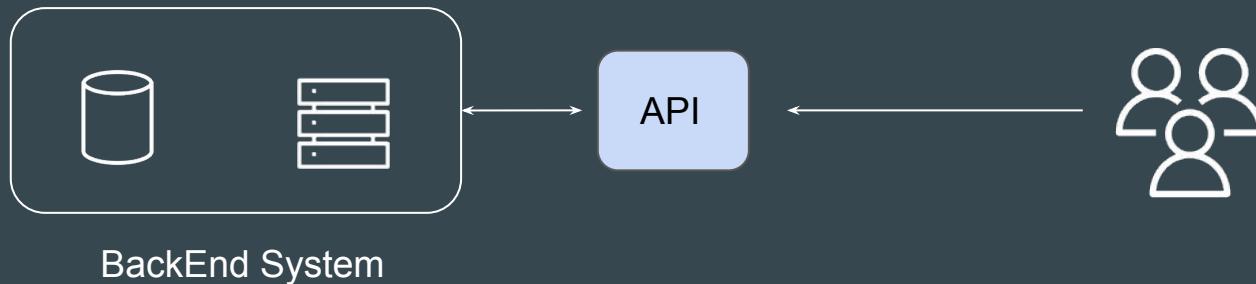
API Gateway



Introduction to Topic

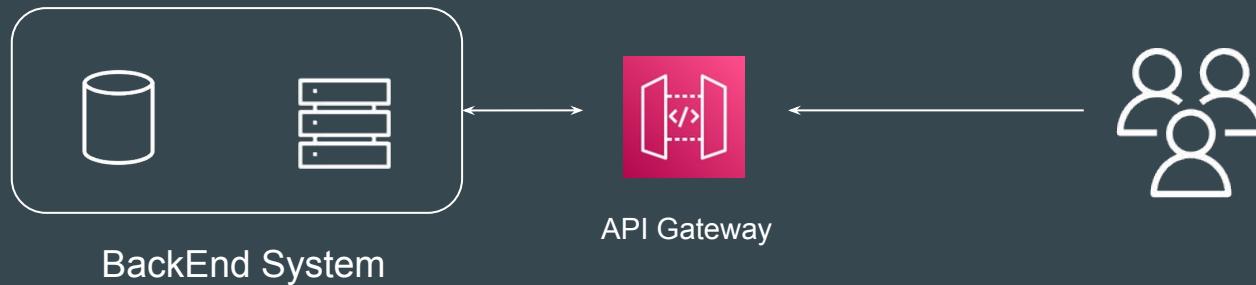
APIs act as the "**front door**" for applications to access data, business logic, or functionality from your backend services.

Hence API should be able to be highly available and handle thousands of requests.



Understanding the Basics

Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale.



REST APIs vs HTTP APIs



Understanding the Basics

REST APIs and HTTP APIs are both RESTful API products.

REST APIs support more features than HTTP APIs, while HTTP APIs are designed with minimal features so that they can be offered at a lower price.

Which to Choose?

Choose REST APIs if you need features such as API keys, per-client throttling, request validation, AWS WAF integration, or private API endpoints.

Choose HTTP APIs if you don't need the features included with REST APIs.

Core Differences - Security

API Gateway provides a number of ways to protect your API from certain threats, like malicious actors or spikes in traffic.

| Security features | REST API | HTTP API |
|---|----------|----------|
| Mutual TLS authentication | ✓ | ✓ |
| Certificates for backend authentication | ✓ | |
| AWS WAF | ✓ | |

Core Differences - API Management

Choose REST APIs if you need API management capabilities such as API keys and per-client rate limiting

| Features | REST API | HTTP API |
|-----------------------------|----------|----------|
| Custom domains | ✓ | ✓ |
| API keys | ✓ | |
| Per-client rate limiting | ✓ | |
| Per-client usage throttling | ✓ | |

Core Differences - Monitoring

API Gateway supports several options to log API requests and monitor your APIs

| Feature | REST API | HTTP API |
|---|----------|----------|
| Amazon CloudWatch metrics | ✓ | ✓ |
| Access logs to CloudWatch Logs | ✓ | ✓ |
| Access logs to Amazon Kinesis Data Firehose | ✓ | |
| Execution logs | ✓ | |
| AWS X-Ray tracing | ✓ | |

Core Differences - Endpoint Type

The endpoint type refers to the endpoint that API Gateway creates for your API

| Endpoint types | REST API | HTTP API |
|----------------|----------|----------|
| Edge-optimized | ✓ | |
| Regional | ✓ | ✓ |
| Private | ✓ | |

Core Differences - Development

As you're developing your API Gateway API, you decide on a number of characteristics of your API.

These characteristics depend on the use case of your API.

| Features | REST API | HTTP API |
|----------------------------------|----------|----------|
| CORS configuration | ✓ | ✓ |
| Test invocations | ✓ | |
| Caching | ✓ | |
| User-controlled deployments | ✓ | ✓ |
| Automatic deployments | | ✓ |
| Custom gateway responses | ✓ | |
| Canary release deployments | ✓ | |
| Request validation | ✓ | |
| Request parameter transformation | ✓ | ✓ |
| Request body transformation | ✓ | |

**When someone deployed HTTP
API for prod environment**

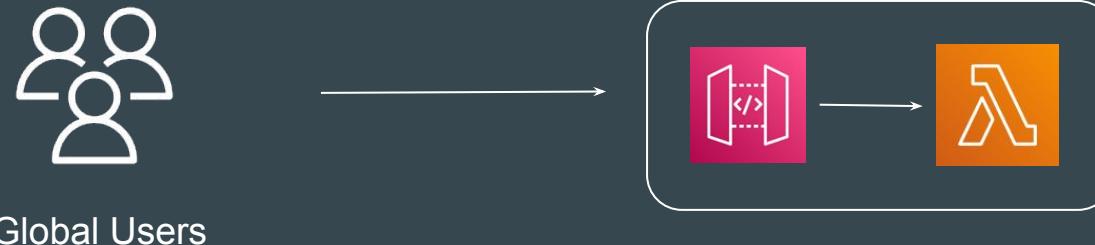


API Gateway Practical



Overall Implementation Architecture

1. Create HTTP API
2. API will invoke a backend Lambda function.

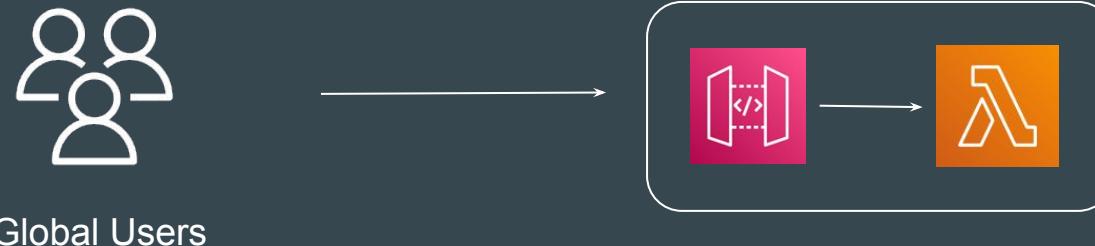


Creating REST API



Overall Implementation Architecture

1. Create REST API
2. API will invoke a backend Lambda function.

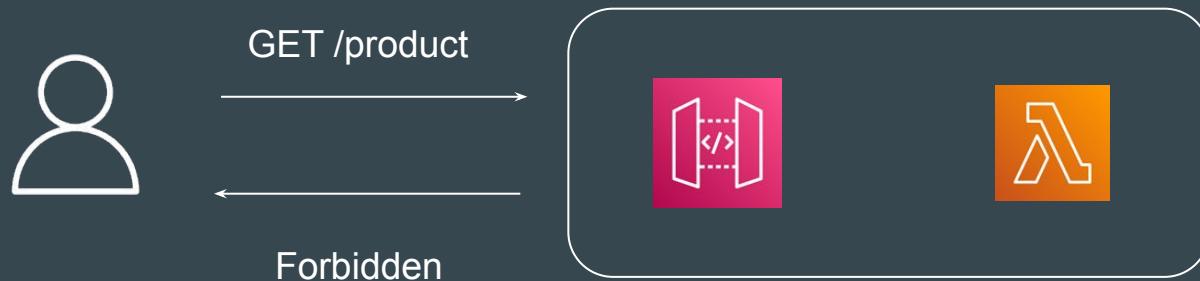


API Keys and Usage Plans



Basics of API Keys

API keys are alphanumeric string values that you distribute to application developer customers to grant access to your API.



Connecting Through API Key

You can use the **X-API-KEY** header while connecting to the API Endpoint.

```
C:\Users\zealv>curl --header "x-api-key: bDa2v0891F9TBgusPLptR253M4QzpVlrlTzKPPg3" https://9jxbr4wdac.execute-api.us-east-1.amazonaws.com/dev
{"statusCode":200,"body":"\"Hello from Lambda!\""}
```

Usage Plan

A **usage plan** specifies who can access one or more deployed API stages and methods—and optionally sets the target request rate to start throttling requests.

The plan uses API keys to identify API clients and who can access the associated API stages for each key.

The screenshot shows the 'demo-usage-plan' configuration page. The top navigation bar has tabs for 'Details', 'API Keys', and 'Marketplace'. The 'API Keys' tab is selected. Below the tabs, the usage plan details are listed:

- ID:** 8ad74n
- Name:** demo-usage-plan
- Description:** No description.
- Rate:** 10 requests per second
- Burst:** 20 requests
- Quota:** 1,000 requests per month starting on the 1st day

Below these details is a section titled 'Associated API Stages' with a 'Add API Stage' button. A table lists the associated API stage:

| API | Stage | Method Throttling | Configure Method Throttling |
|----------|-------|-----------------------|-----------------------------|
| demo-api | dev | No Methods Configured | Configure Method Throttling |

Points to Note

After you create, test, and deploy your APIs, you can use API Gateway usage plans to make them available as product offerings for your customers.

You can configure usage plans and API keys to allow customers to access selected APIs, and **begin throttling requests** to those APIs based on defined limits and quotas.

These can be set at the API, or API method level.

Points to Note

API Gateway throttles requests to your API using the token bucket algorithm, where a token counts for a request

When request submissions exceed the steady-state request rate and burst limits, API Gateway begins to throttle requests. Clients may receive **429 Too Many Requests**

There is a default quota of 10,000 requests per second (RPS) applicable at per account per region.

Lambda and S3

Going Serverless

Getting the basics right

AWS S3 provides a feature to publish events (for example, when an object is uploaded in the bucket) to AWS Lambda function.

Example Use-Case:

User would upload various files to S3 bucket which are suspicious.

Your Lambda function will analyze those files and return result on whether it's clean or infected.

Getting the basics right

Example Use-Case:

User would upload various files to S3 bucket which are suspicious.

Your Lambda function will analyze those files and return result on whether it's clean or infected.

Solution:

Lambda function should know when the object is getting uploaded.

Lambda function should have permission to get the object file.

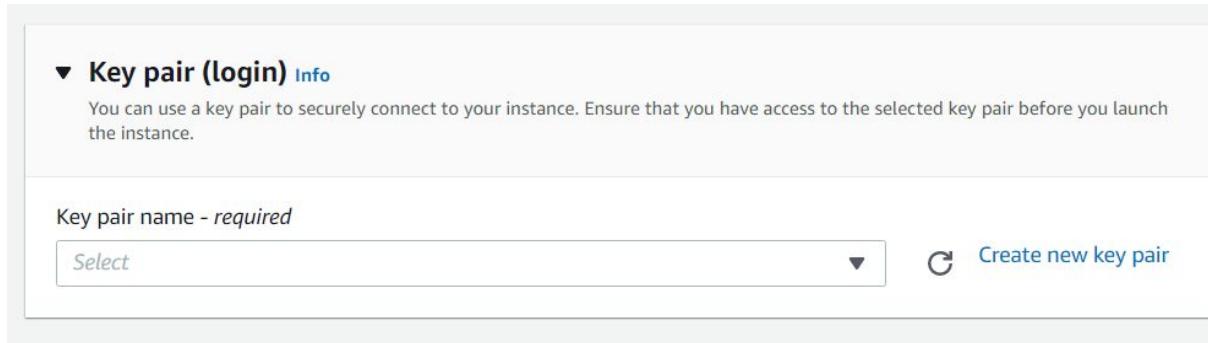
EC2 Key-Pair Troubleshooting

Public Private Keys

Understanding the Basics

Whenever we create an EC2 instance, we generally specify the associated key-pair

Once selected, the public key associated with key-pair gets added as part of the `~/.ssh/authorized_keys` file.



Troubleshooting - Point 1

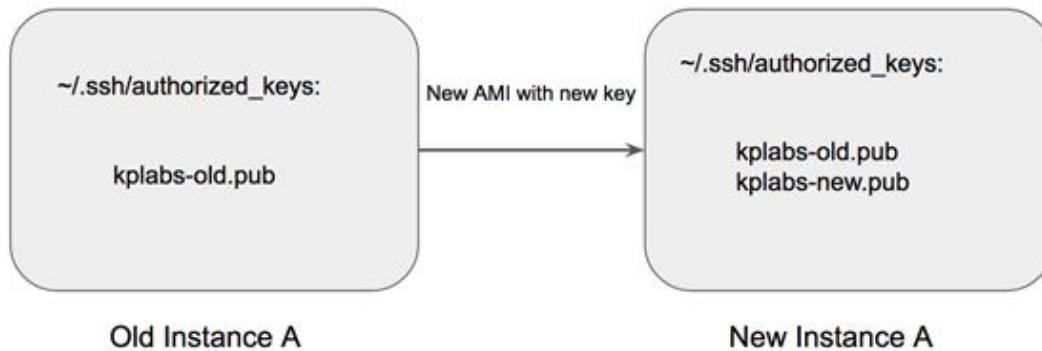
There are two specific troubleshooting scenario that we should be aware of:

- i) Deleting the key-pair from the console will not delete the associated key from the EC2 instance.



Troubleshooting - Point 2

- i) If we create a new instance from AMI of older instance, the public key specified while AMI creation will be appended to the authorized_keys.



EC2 Tenancy

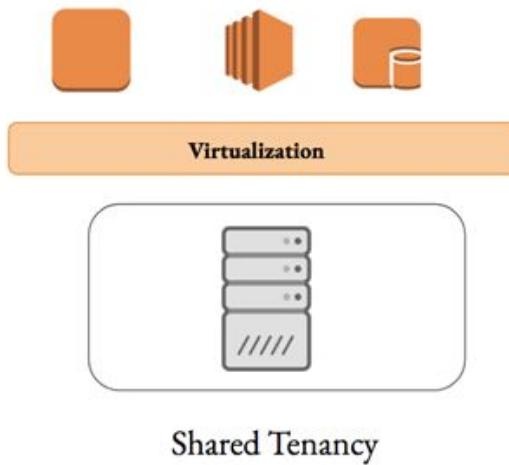
Understanding the EC2 Tenancy

Every EC2 instance that we launch in the VPC has a specific tenancy attribute associated with it. There are three tenancy attributes which are available:

| Tenancy Attribute | Description |
|-------------------|---|
| Shared | The EC2 instance runs on shared hardware. |
| Dedicated | EC2 instance runs on hardware which will only be shared between same account AWS instances. |
| Hosts | Instance runs on dedicated hosts with very granular level of hardware access. |

Shared Tenancy

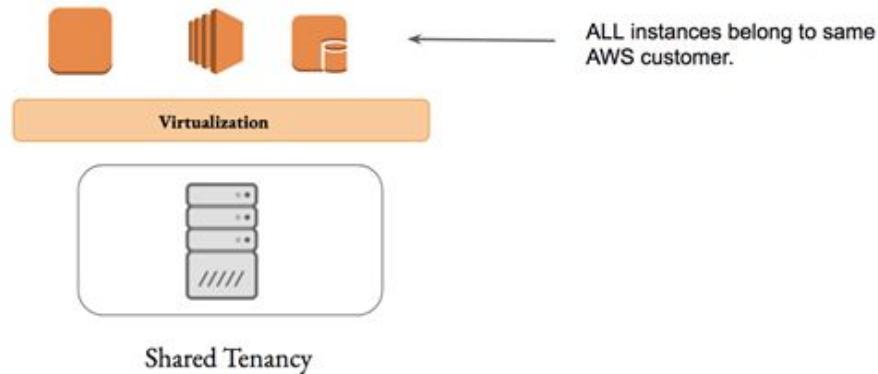
In this approach, your EC2 instance is launched on the shared hardware where EC2 instances of other customers also run.



Dedicated Instance

Dedicated Instances are EC2 instances that run on the hardware which is dedicated to a single customer.

Dedicated instances may share the hardware with other EC2 instances that belongs to the same AWS accounts.



Dedicated Hosts

Dedicated Host is a physical server that allows us to use our existing per-socket, per-core or even per-VM based software licenses which includes Windows Server, SUSE, and various others.

With dedicated hosts, we can use the same physical server over the time, even if the instance is stopped and started.

AWS Artifact

Compliance Time

Understanding AWS Artifacts

The AWS Artifact portal provides on-demand access to AWS' security and compliance documents, also known as audit artifacts.

Lots of AWS services are compliant against various compliance like PCI DSS, HIPAA and others.

If the organization is using certain AWS services, then auditor will ask the organization to show certificate that the service is compliant.

Lambda@Edge

Running Serverless at the Edge

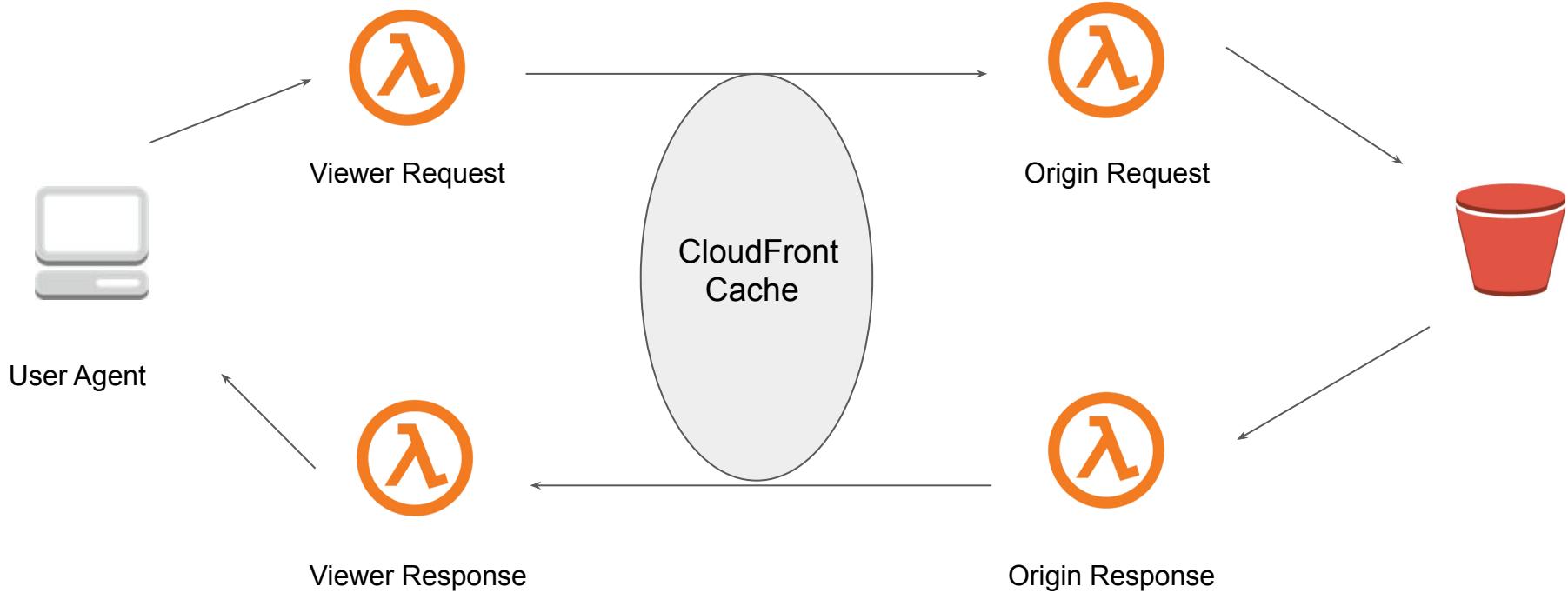
Getting started

Lambda@Edge lets you run Lambda functions to customize content that CloudFront delivers.

You can use Lambda functions to change CloudFront requests and responses at the following points:

1. After CloudFront receives a request from a viewer ([viewer request](#))
2. Before CloudFront forwards the request to the origin ([origin request](#))
3. After CloudFront receives the response from the origin ([origin response](#))
4. Before CloudFront forwards the response to the viewer ([viewer response](#))

Diagrammatic Representation



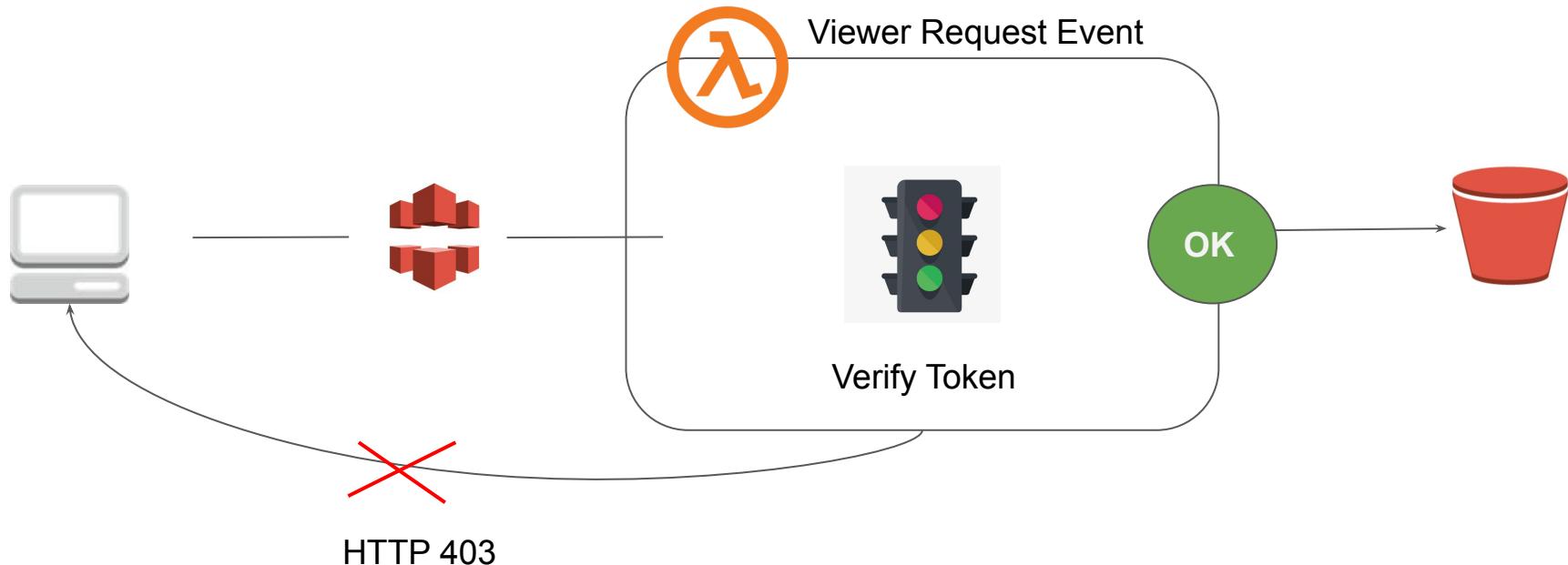
Viewer Request

Viewer Request is executed on every request before CloudFront cache is checked.

There are various things that we can do at this stage, like:

- Modify URLs, cookies query strings etc.
- Perform Authentication and Authorization Checks.

Viewer Request



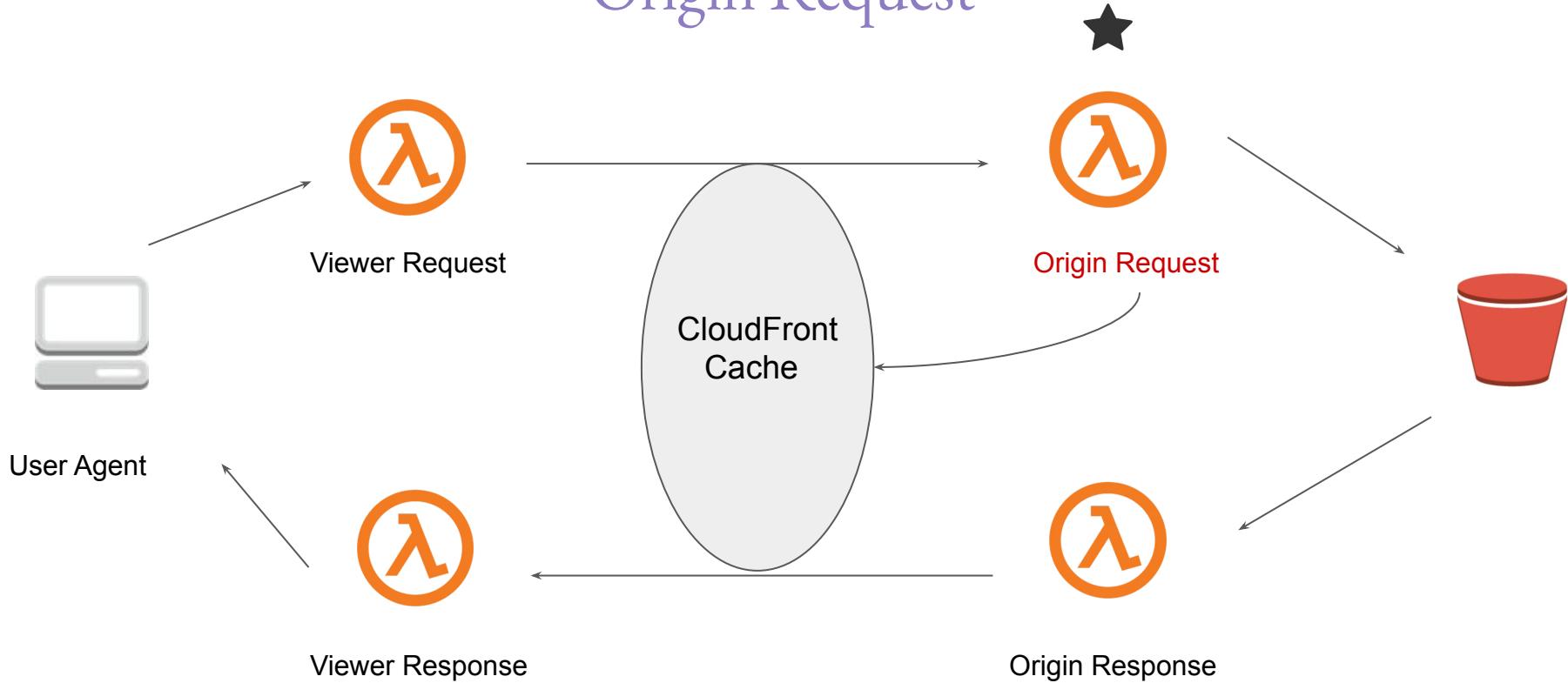
Origin Request

Executed on cache miss, before a request is forwarded to the origin.

There are various things that we can do at this stage, like:

- Dynamically select origin based on the request headers

Origin Request



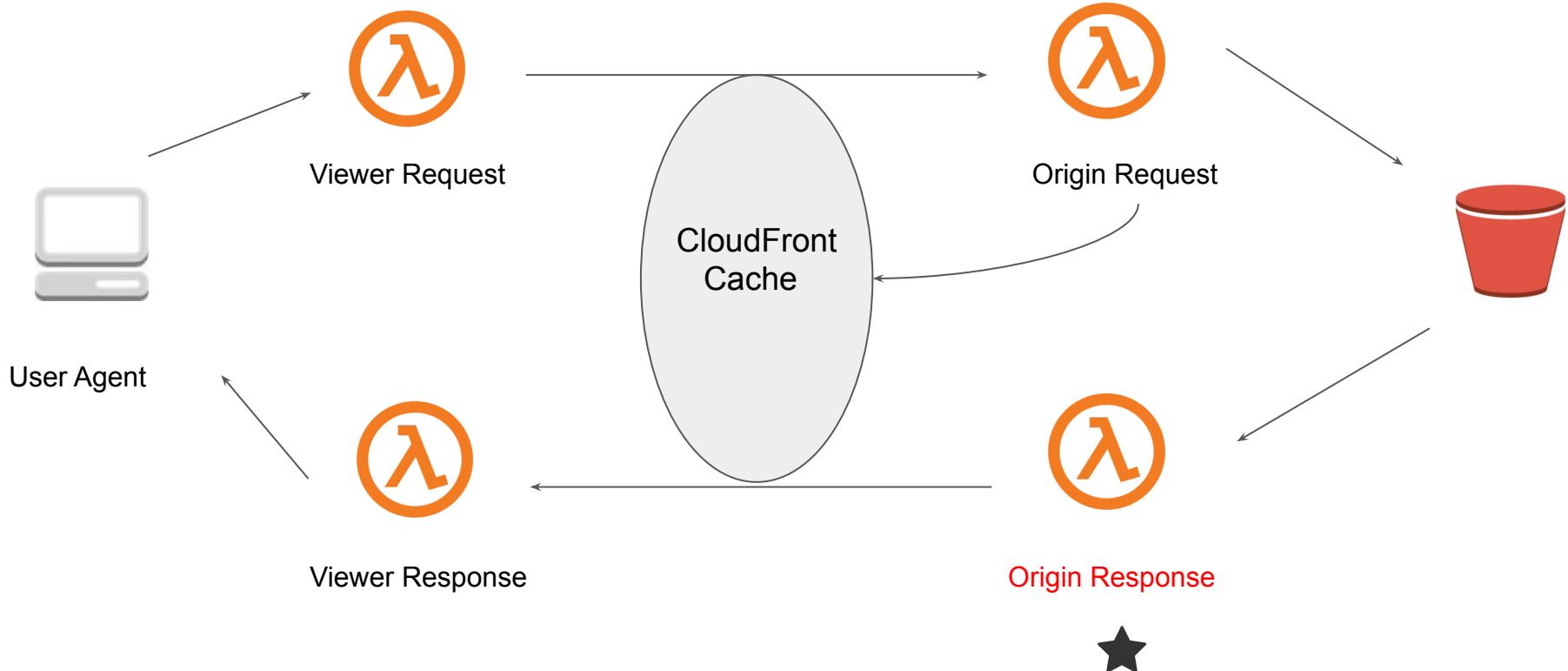
Origin Response

Executed on a cache miss, after a response is received from the origin.

There are various things that we can do at this stage, like:

- Modify the response headers.
- Intercept and replace various 4XX and 5XX errors from the origin.

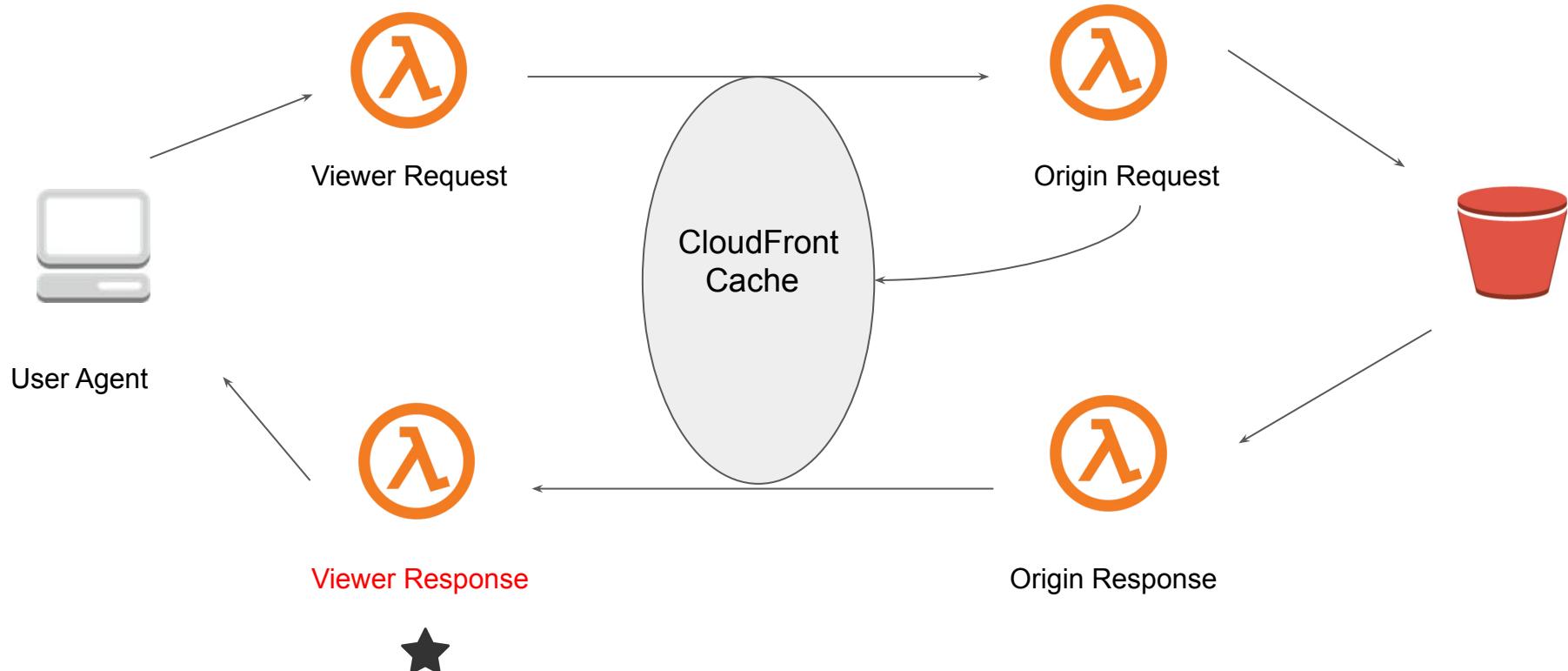
Origin Response



Viewer Response

Executed on all the responses received either from the origin or the cache.

Modifies the response headers before caching the response.



Relax and Have a Meme Before Proceeding

That stupid walk you do when
someone's mopping a floor and you
know you're gonna walk over it but you
want them to see how sorry you are to
be walking over it so you make
yourself look like you're walking over
hot lava.



It ain't much, but it's honest work

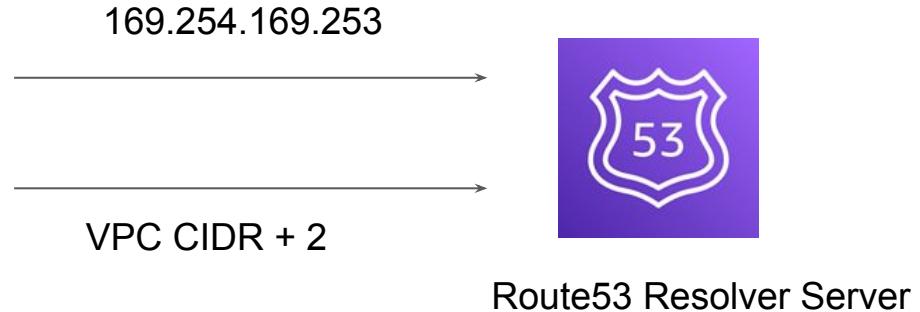
DNS Support in VPC

DNS Yet Again!

Amazon DNS Server

The Amazon DNS server enables DNS for instances that need to communicate over the VPC's internet gateway.

The Amazon DNS server does not reside within a specific subnet or Availability Zone in a VPC. It's located at the address 169.254.169.253 (and the reserved IP address at the base of the VPC IPv4 network range, plus two). For 10.0.0.0/16, the IP is 10.0.0.2



DNS attributes in your VPC

There are two primary attributes that determine the DNS Support provided for your VPC.

| Attribute | Description |
|--------------------|--|
| enableDnsHostnames | <p>Indicates whether instances with public IP addresses get corresponding public DNS hostnames.</p> <p>If this attribute is true, instances in the VPC get public DNS hostnames, but only if the enableDnsSupport attribute is also set to true.</p> |
| enableDnsSupport | <p>Indicates whether the DNS resolution is supported through Amazon Provided DNS server.</p> <p>If this attribute is false, the Amazon-provided DNS server that resolves public DNS hostnames to IP addresses is not enabled.</p> |

Case 1 - Both Attributes Are True

If both attributes are set to true, the following occurs:

- Instances with a public IP address receive corresponding public DNS hostnames.
- The Amazon-provided DNS server can resolve Amazon-provided private DNS hostnames.

Case 2 - Both Attributes Are False

If both attributes are set to false, the following occurs:

- Instances with a public IP address do not receive corresponding public DNS hostnames.
- The Amazon-provided DNS server cannot resolve Amazon-provided private DNS hostnames.

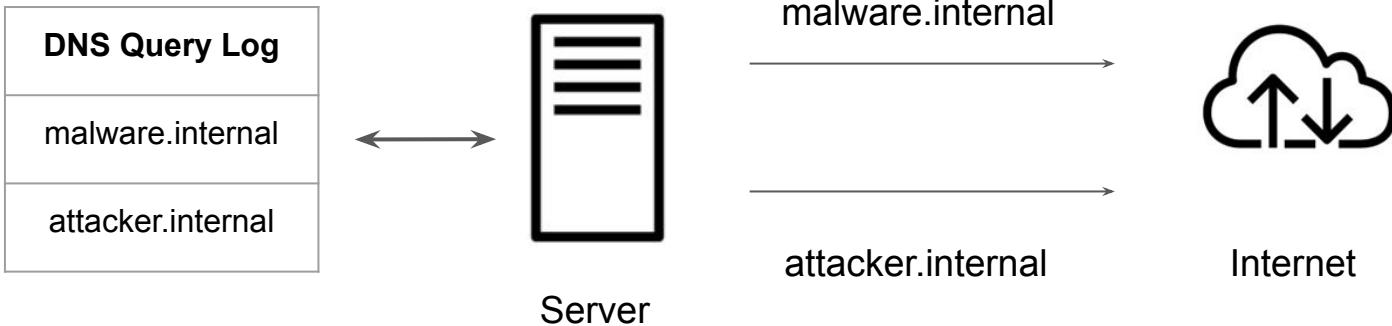
DNS Query Logging

DNS Logs are Important

DNS Logs Are Important

Each connection made to a domain by the client devices is recorded in the DNS logs.

Inspecting DNS traffic between client devices and your local recursive resolver could reveal a wealth of information for security and forensic analysis



Route53 Query Logging

Query logs contain only the queries that DNS resolvers forward to Route 53.

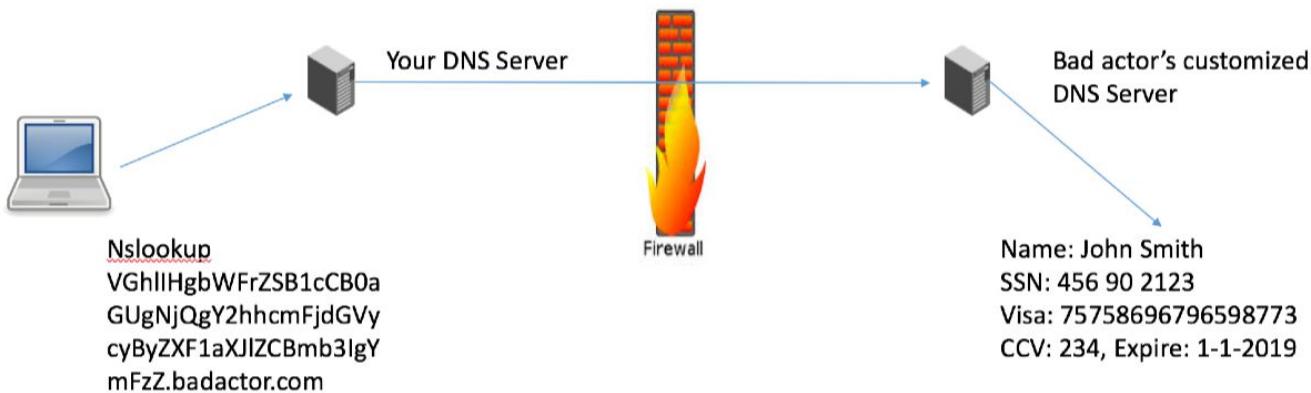
These log contain various information including:

Domain Requested, Timestamp of Request, DNS Record Type, and others.

```
2022-12-13T08:16:02.130Z Z123412341234 example.com A NOERROR UDP FRA6 192.168.1.1 -
2022-12-13T08:15:50.235Z Z123412341234 example.com AAAA NOERROR TCP IAD12 192.168.3.1 192.168.222.0/24
2022-12-13T08:15:50.342Z Z123412341234 bad.example.com A NXDOMAIN UDP IAD12 192.168.3.1 192.168.111.0/24
2022-12-13T08:16:05.744Z Z123412341234 txt.example.com TXT NOERROR UDP JFK5 192.168.1.2 -
```

Security Attack via DNS

DNS Exfiltration is an unauthorized transfer of data via DNS queries routes to the attacker's server, providing them with a covert command and control channel, and data exfiltration path.

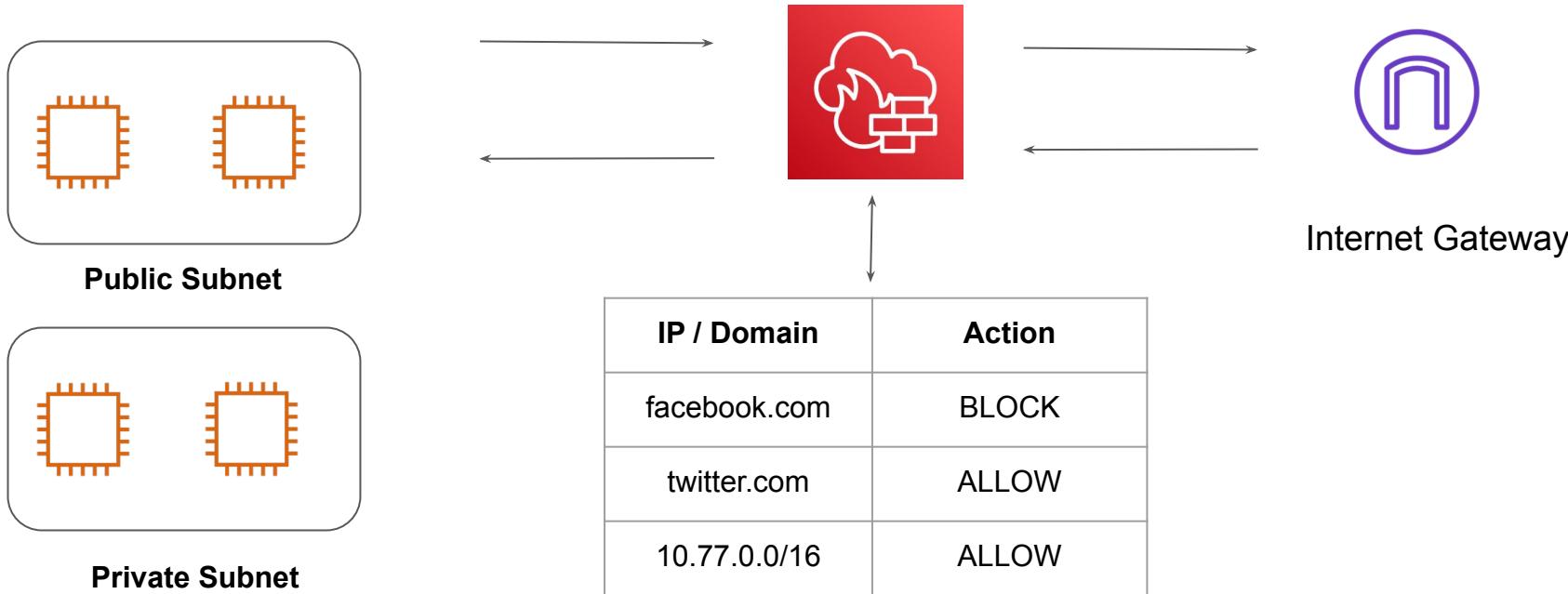


AWS Network Firewall

Yet Another Firewall

Basics of Network Firewall

AWS Network Firewall is a stateful, managed, network firewall and intrusion detection and prevention service for your virtual private cloud (VPC)



Benefits of Network Firewall

You can use Network Firewall to monitor and protect your Amazon VPC traffic in a number of ways, including the following:

1. Pass traffic through only from known AWS service domains or IP address endpoints, such as Amazon S3.
2. Use custom lists of known bad domains to limit the types of domain names that your applications can access
3. Perform deep packet inspection on traffic entering or leaving your VPC

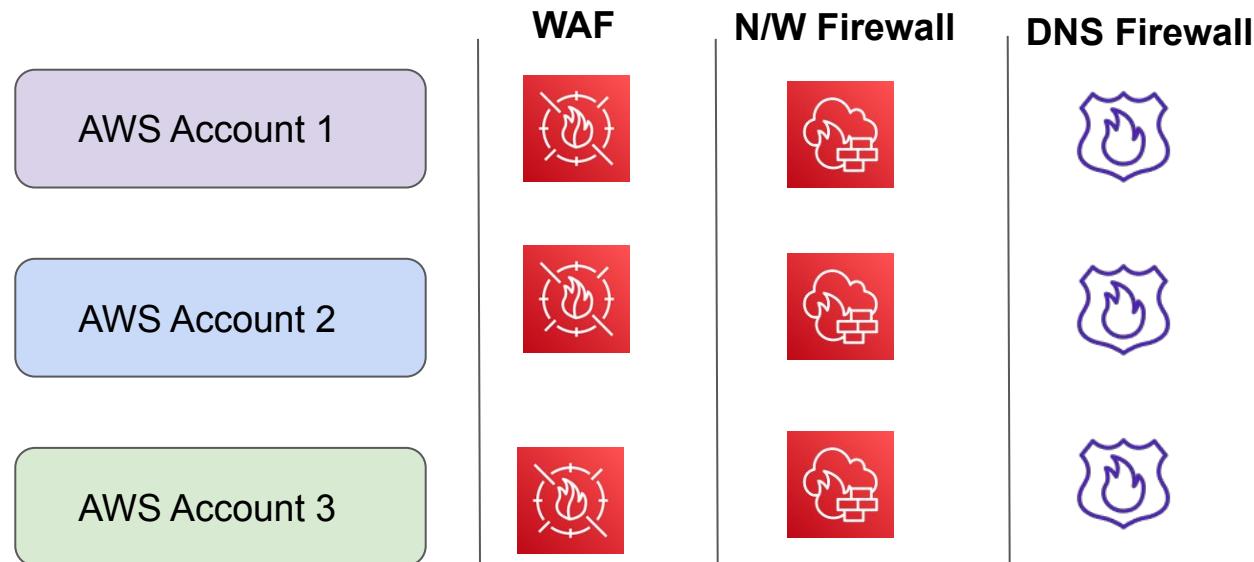
Firewall Manager

Centrally Manage Rules

Understanding the Challenge

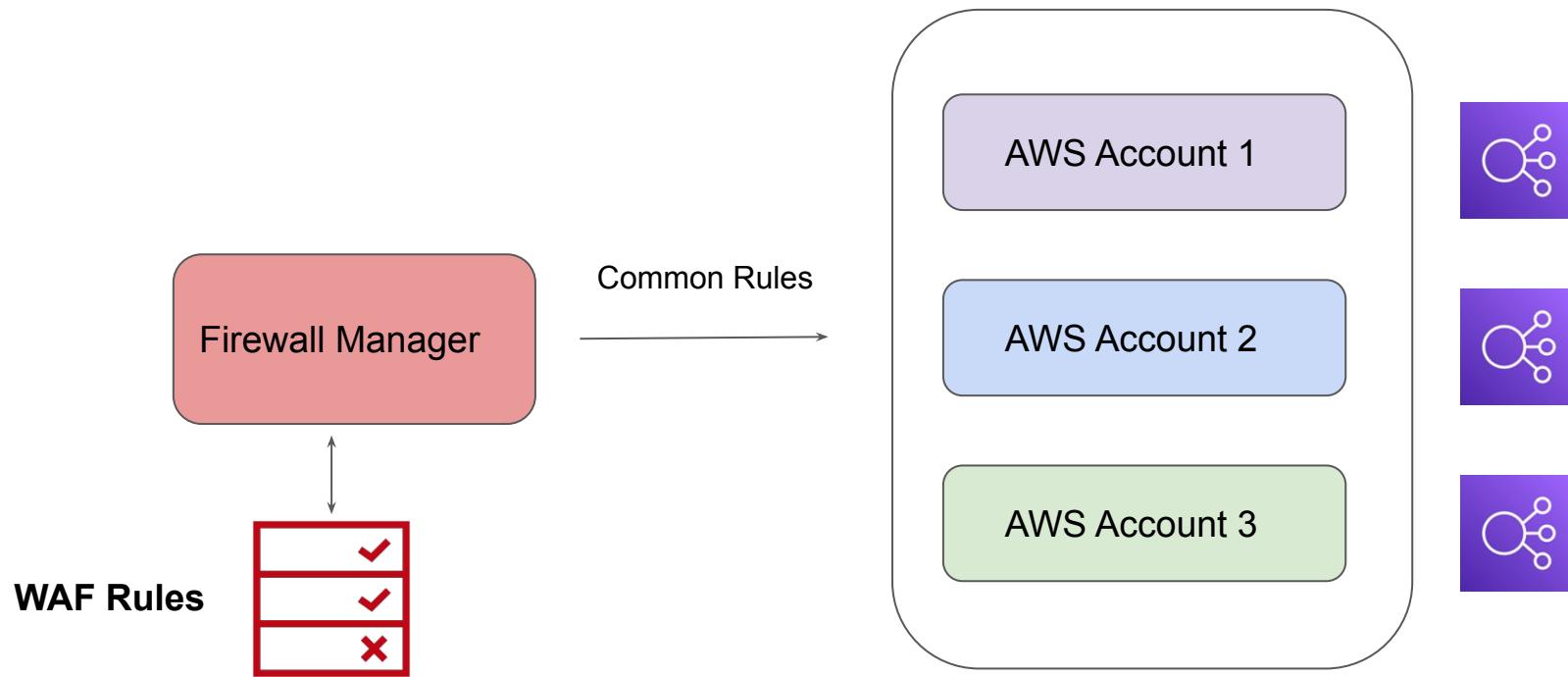
Most of the organizations are opting for Multi-Account based strategy for separation of environments (dev, stage, prod)

Security Team needs to create, maintain and update security services across all of the accounts.



Understanding the Basics

AWS Firewall Manager is a security management service which allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organizations



Supported Service

Firewall Manager supports wide variety of services, including:

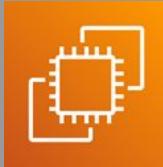
- AWS WAF
- VPC Security Groups
- AWS Network Firewall
- Route53 DNS Firewall
- AWS Shield Advanced
- Palo Alto Cloud Next-generation firewalls

Important Prerequisite: AWS Organizations + AWS Config.

Benefits of Firewall Manager

1. Simplify management of firewall rules across your accounts
2. Ensure compliance of existing and new applications
3. Easily deploy managed rules across accounts
4. Centrally deploy protections for your VPCs

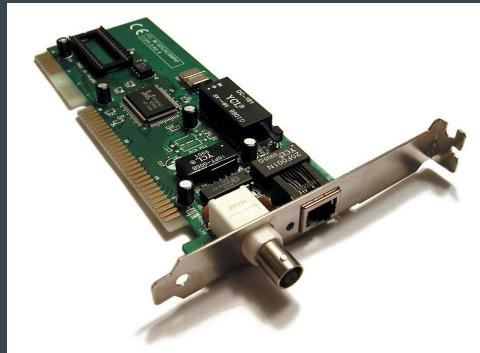
Elastic Network Interface (ENI)



Revising Basics of Network Interface

Network interface is a hardware component that connects a computer to a computer network

A virtual network interface (VIF) is an abstract virtualized representation of a computer network interface.



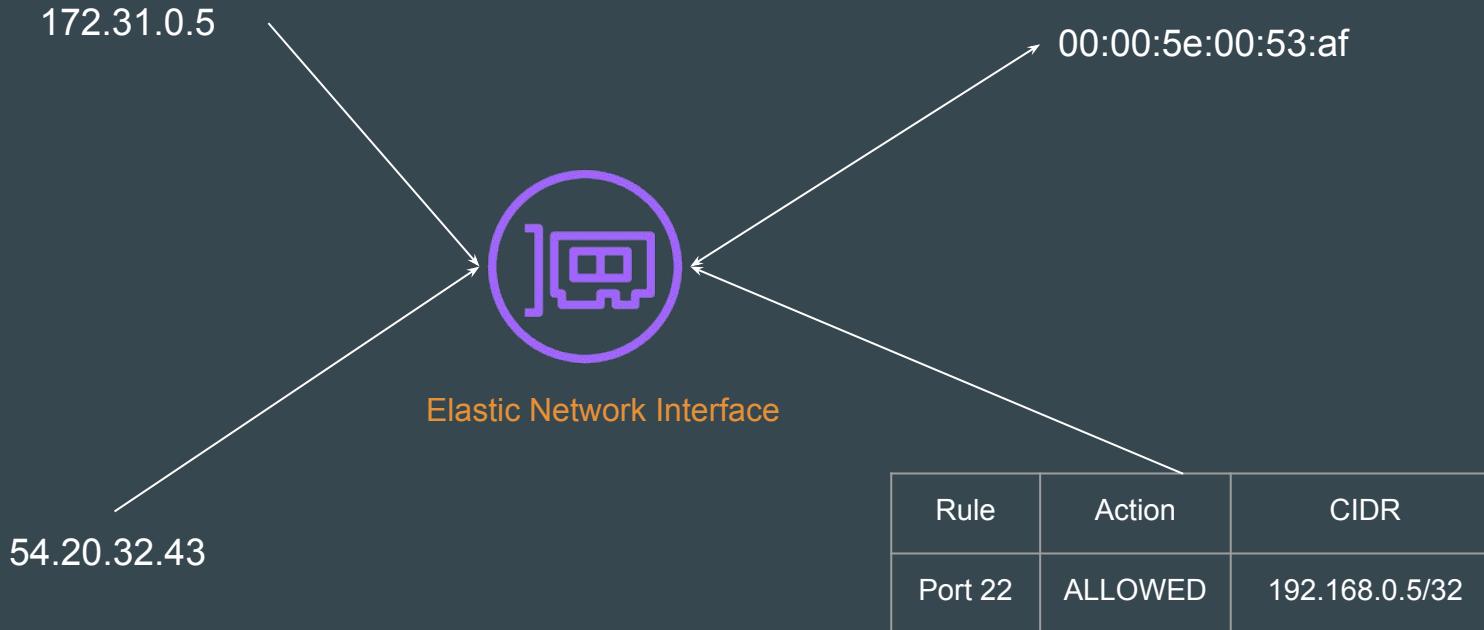
Elastic network interfaces

An **elastic network interface** is a logical networking component in a VPC that represents a virtual network card.

Some of the following attributes include:

- A primary private IPv4 address
- One or more secondary private IPv4 addresses
- One Elastic IP address (IPv4) per private IPv4 address
- One or more security groups
- A MAC address
- A source/destination check flag

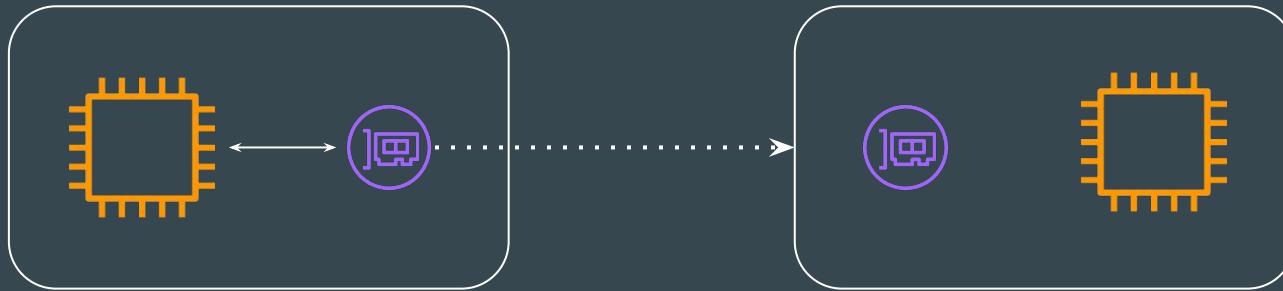
Sample Attributes of ENI



Portable NICs

You can create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance.

The **attributes of a network interface follow it as it's attached or detached from an instance and reattached to another instance.**



172.31.0.5

172.31.0.5

Importance of Default NICs

Each instance has a **default network interface**, called the primary network interface. You cannot detach a primary network interface from an instance.

You can create and attach additional network interfaces.

The maximum number of network interfaces that you can use varies by instance type.

NICs are availability zone specific.

Bring your own IP addresses



Basics of IP Reputation

IP reputation is a measure that helps evaluate the quality of an IP address and determine how legitimate its requests are

Bad IP Reputation generally corresponds to activities like sending spam emails, viruses etc that originate from the IP.

| LOCATION DATA | | REPUTATION DETAILS | |
|-----------------------------|----------------|---|------------|
| North Bergen, United States | | SENDER IP REPUTATION | Poor |
| | | Submit Sender IP Reputation Ticket | |
| OWNER DETAILS | | EMAIL VOLUME DATA | |
| IP ADDRESS | 161.35.125.167 | LAST DAY | LAST MONTH |
| FWD/REV DNS MATCH | Yes | EMAIL VOLUME | 3.4 |
| HOSTNAME | fe.sati.com.py | VOLUME CHANGE | -17.07% |
| DOMAIN | sati.com.py | SPAM LEVEL | Critical |
| NETWORK OWNER | digital ocean | | |
| CONTENT DETAILS | | | |

Use-Case: Organization Migrating to Cloud

Organization's infrastructure is hosted in the on-premise datacenter.

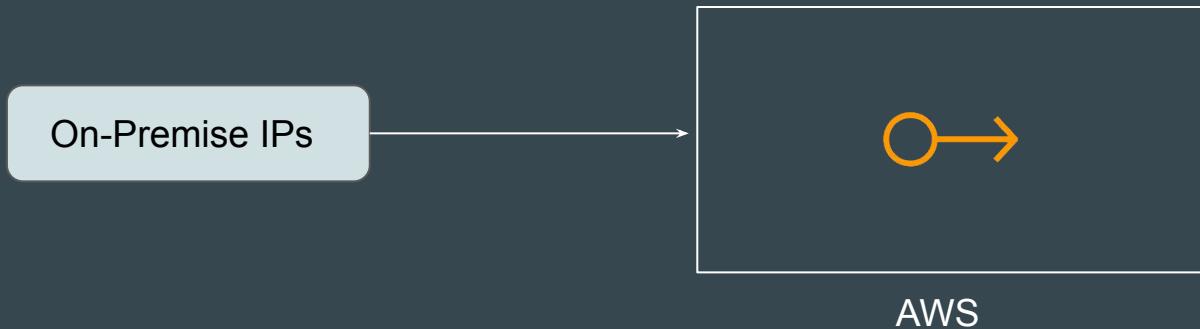
They have certain Public IPs from years with very good reputation.

They decide to migrate to Cloud and server receive IP with NOT as good reputation as their previous IPs.



Introducing Bring Your Own IP

You can bring part or all of your publicly routable IPv4 or IPv6 address range from your on-premises network to your AWS account.



Benefits of Bring Your Own IP

| Benefits | Description |
|---------------------------|--|
| IP Reputation | Many customers consider the reputation of their IP addresses to be a strategic asset and want to use those IPs on AWS with their resources. |
| Customer whitelisting | BYOIP also enables customers to move workloads that rely on IP address whitelisting to AWS without the need to re-establish the whitelists with new IP addresses |
| Regulation and compliance | Many customers are required to use certain IPs because of regulation and compliance reasons. They too are unlocked by BYOIP. |

Important Requirements - Part 1

The address range must be registered with your regional internet registry (RIR) such as ARIN, RIPE, APNIC.

It must be registered to a business or institutional entity and cannot be registered to an individual person.

The most specific IPv4 address range that you can bring is /24.

The most specific IPv6 address range that you can bring is /48 for CIDRs that are publicly advertised, and /56 for CIDRs that are not publicly advertised.

Important Requirements - Part 2

The addresses in the IP address range **must have a clean history**. AWS might investigate the reputation of the IP address and reserve the right to reject an IP address range if an IP has a poor reputation or is associated with malicious behavior.

Points to Note

Customers can create Elastic IPs from the IPv4 space they bring to AWS and use them with EC2 instances, NAT Gateways, and Network Load Balancers.

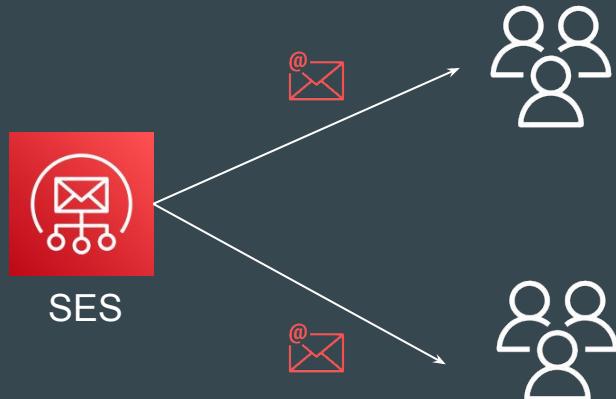
Simple Email Service (SES)



Understanding the Basics

Amazon SES is an **email platform** that provides an easy, cost-effective way for you to send and receive email using your own email addresses and domains.

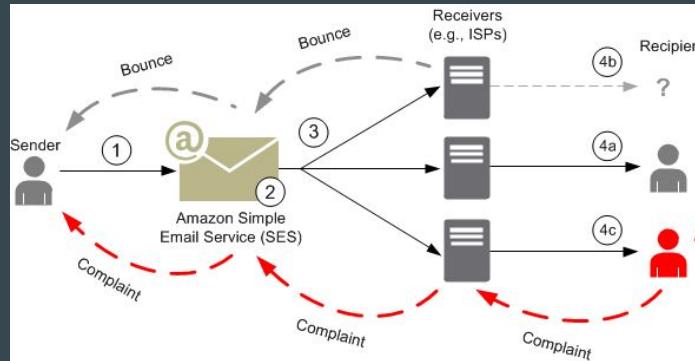
Many organization has generic emails like `noreply@example.com` which is used to send emails to users upon registration or other use-cases.



How email sending works in Amazon SES

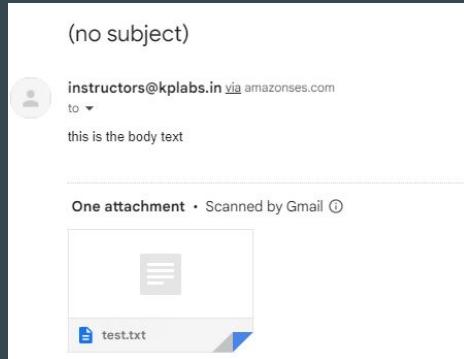
- Email sender makes a request to SES to send email to recipients.
- If the request is valid, SES accepts the email.
- SES sends the message over the Internet to the recipient's receiver.

Bounce Notifications (email not exist) & Complaints (feedback) are sent back to SES which then forwards it to the sender.



Email format in Amazon SES

| Email Format | Description |
|--------------|--|
| Formatted | Construct simple test message using the form provided. |
| Raw | For more complex use-cases like using HTML or attachments. |



Raw Mail Example

Types of Amazon SES credentials



Understanding the Basics

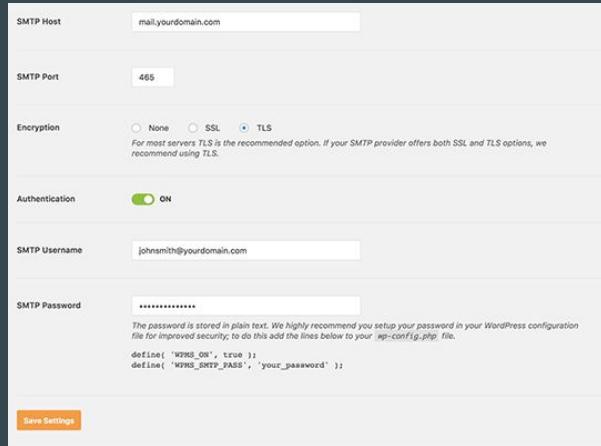
To interact with Amazon SES you use security credentials to verify who you are and whether you have permission to interact with Amazon SES

| Access Type | Credentials to Use |
|--------------------|---------------------------|
| Amazon SES API | AWS Access Keys |
| SES SMTP Interface | Username and Password |
| SES Console | IAM User and Password |

Use-Case: SMTP Interface

There are a number of commercial and open source software packages that support sending email through SMTP

You can configure any such SMTP-enabled software to send email through the Amazon SES SMTP interface.



SMTP Endpoint

| Region Name | Region | Endpoint | Protocol |
|-------------------------|----------------|---|----------|
| US East (Ohio) | us-east-2 | email-smtp.us-east-2.amazonaws.com | SMTP |
| US East (N. Virginia) | us-east-1 | email-smtp.us-east-1.amazonaws.com | SMTP |
| | | email-smtp-fips.us-east-1.amazonaws.com | |
| US West (N. California) | us-west-1 | email-smtp.us-west-1.amazonaws.com | SMTP |
| US West (Oregon) | us-west-2 | email-smtp.us-west-2.amazonaws.com | SMTP |
| | | email-smtp-fips.us-west-2.amazonaws.com | |
| Asia Pacific (Mumbai) | ap-south-1 | email-smtp.ap-south-1.amazonaws.com | SMTP |
| Asia Pacific (Osaka) | ap-northeast-3 | email-smtp.ap-northeast-3.amazonaws.com | SMTP |

Connecting to an Amazon SES SMTP endpoint



Understanding the Basics

To send email using the Amazon SES SMTP interface, you connect to an SMTP endpoint.

The Amazon SES SMTP endpoint requires that all connections be encrypted using Transport Layer Security (TLS).



Mechanism for TLS

Amazon SES supports two mechanisms for establishing a TLS-encrypted connection

1. STARTTLS
2. TLS Wrapper

Approach 1 - STARTTLS

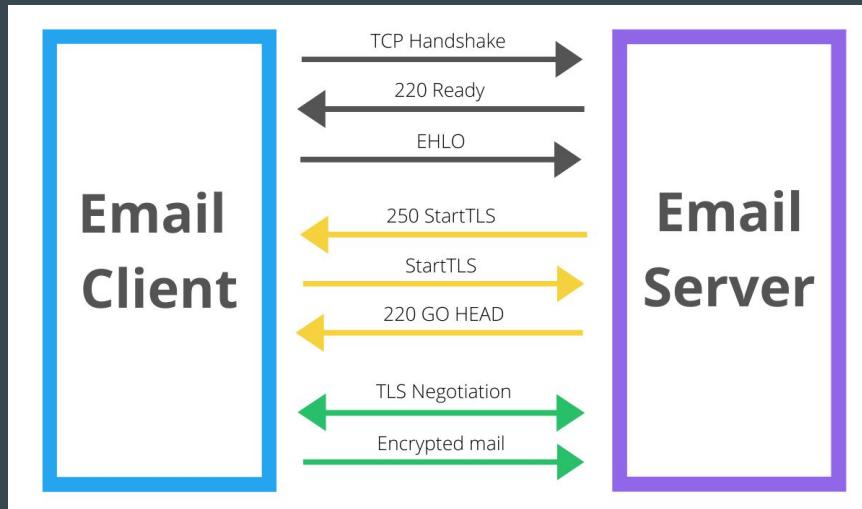
STARTTLS is a means of upgrading an unencrypted connection to an encrypted connection

To set up a STARTTLS connection, the SMTP client connects to the SES SMTP endpoint on port 25, 587, or 2587, issues an EHLO command, and waits for the server to announce that it supports the STARTTLS SMTP extension.

The client then issues the STARTTLS command, initiating TLS negotiation.

When negotiation is complete, the client issues an EHLO command over the new encrypted connection, and the SMTP session proceeds normally.

Overall Flow



Approach 2 - TLS Wrapper

TLS Wrapper is a means of initiating an encrypted connection without first establishing an unencrypted connection.

With TLS Wrapper, the Amazon SES SMTP endpoint doesn't perform TLS negotiation: it's the client's responsibility to connect to the endpoint using TLS, and to continue using TLS for the entire conversation.

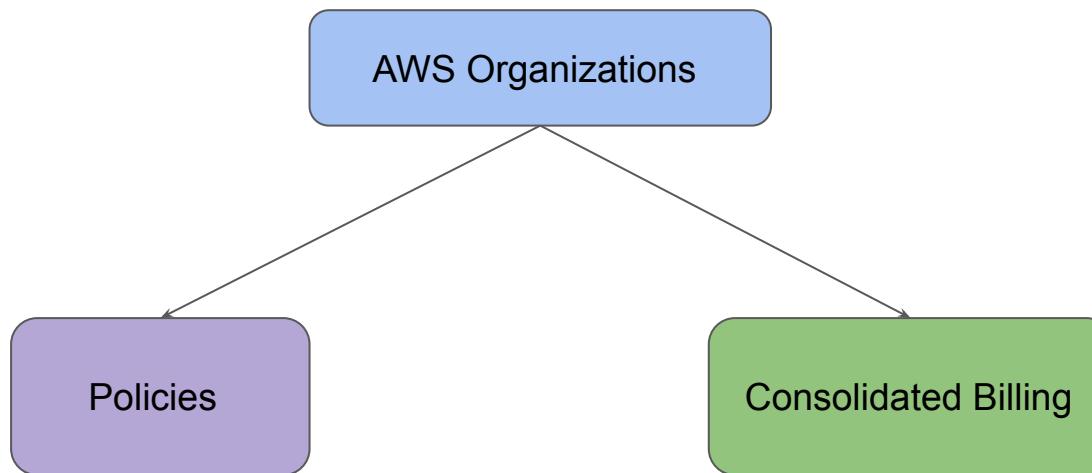
To set up a TLS Wrapper connection, the SMTP client connects to the Amazon SES SMTP endpoint on port 465 or 2465.

AWS Organizations

Centralized Control

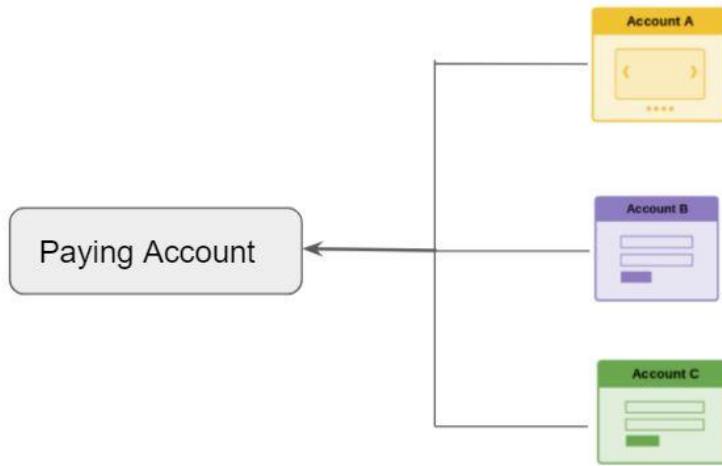
Getting the basics right

AWS offers centralized policy-based management as well as the feature of consolidated billing for multiple AWS accounts through the feature of AWS Organizations.



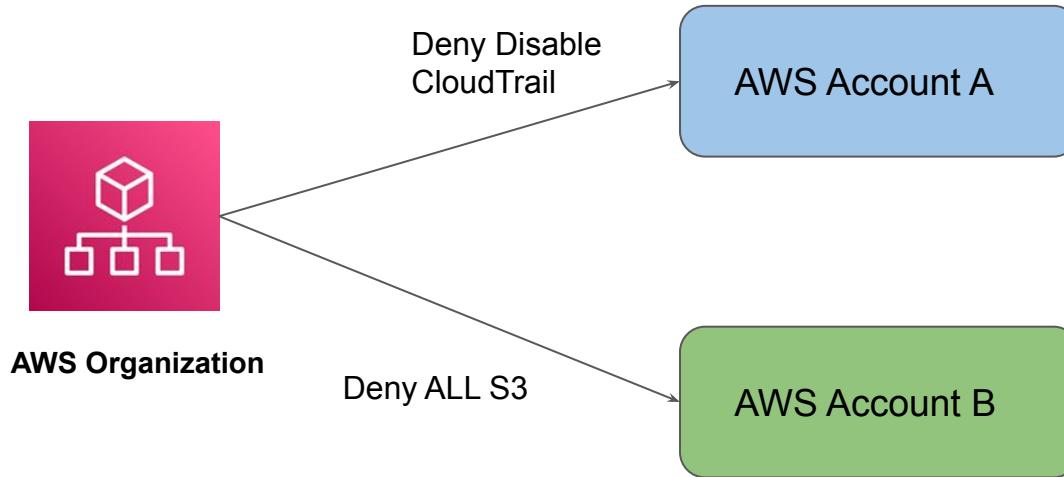
Part 1 - Consolidated Billing

In consolidated billing, management account to access the billing information and pay for all member accounts.



Part 2 - Policies

Policies in AWS Organizations enable you to apply additional types of management to the AWS accounts in your organizations.



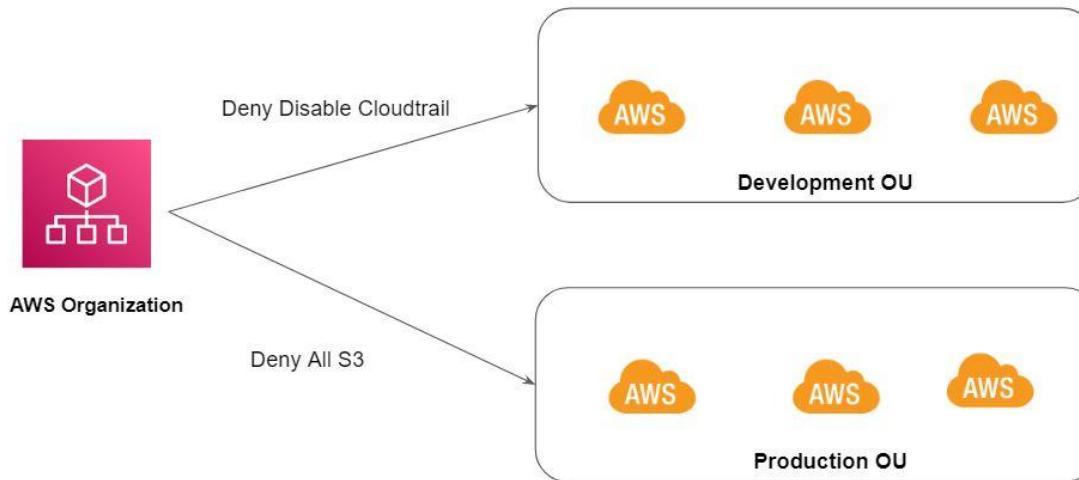
OU in AWS Organization

Were Complex becomes Easy

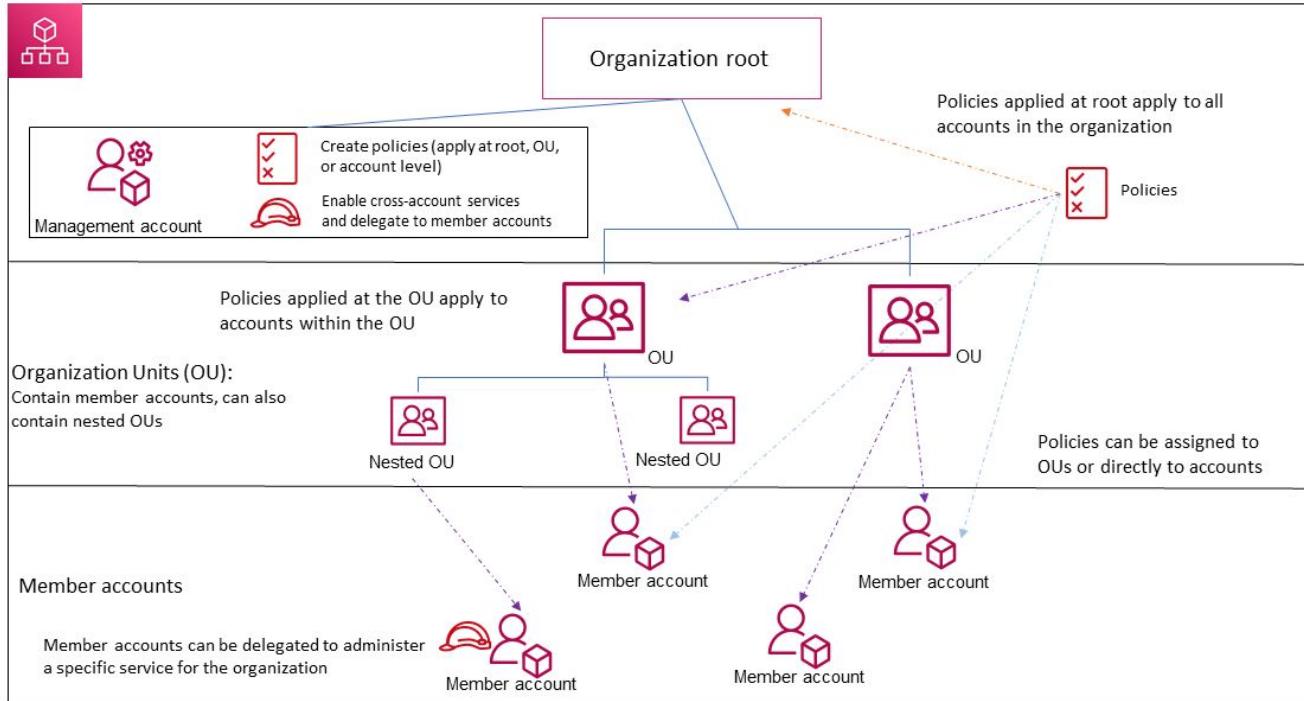
Getting the basics right

Organizational units (OUs) to group accounts together to administer as a single unit

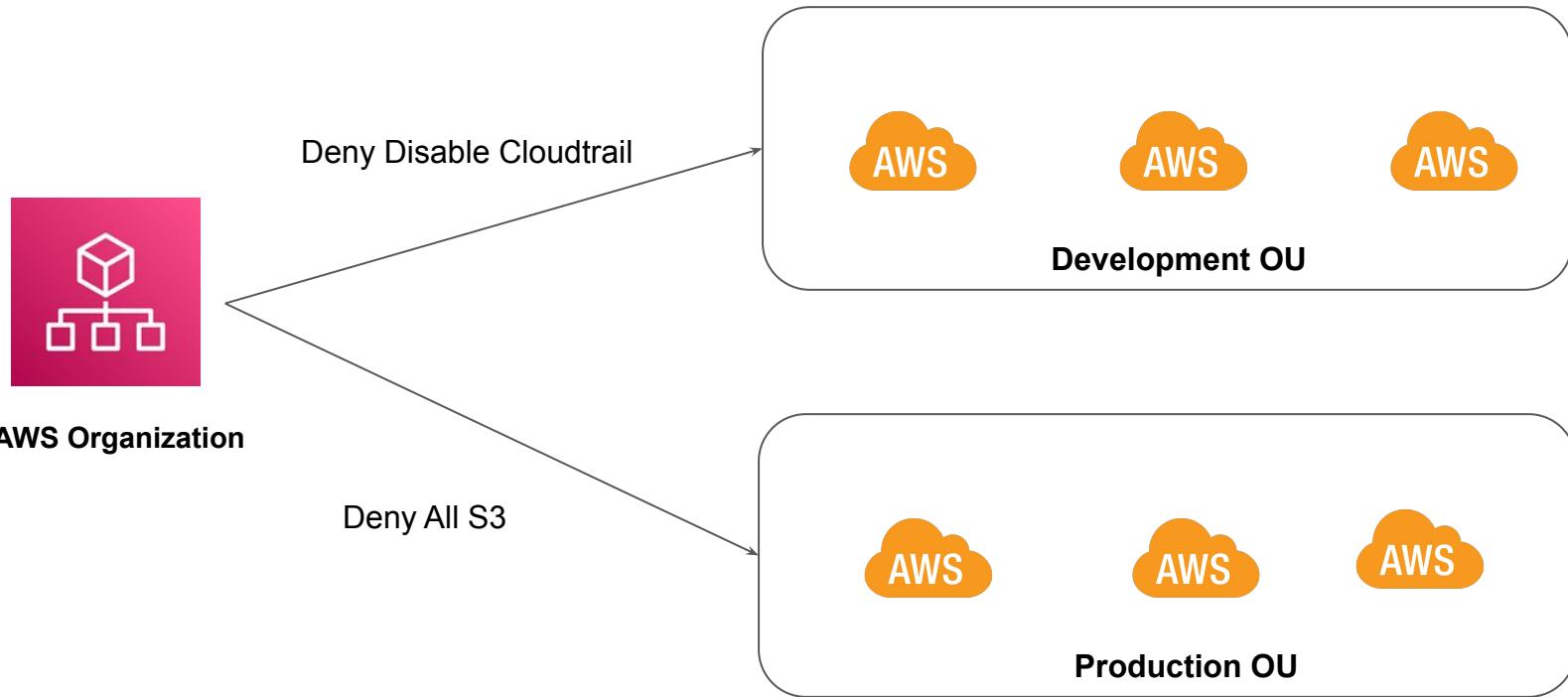
This greatly simplifies the management of your accounts. For example, you can attach a policy-based control to an OU, and all accounts within the OU automatically inherit the policy.



Important Concepts



Grouping AWS Accounts



Important Pointers

SCPs don't affect users or roles in the management account. They affect only the member accounts in your organization.

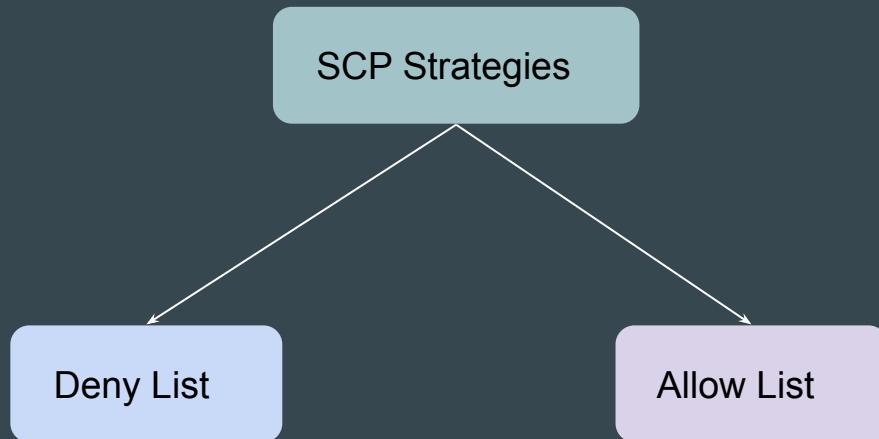
By default, AWS Organizations attaches an AWS managed policy called FullAWSAccess to all roots, OUs, and accounts. This helps ensure that, as you build your organization, nothing is blocked until you want it to be.

Strategies for using SCPs



Understanding the Basics

There are two strategies that you can use to configure SCPs in your account.



Strategy 1 - Deny List

In **deny list**, actions are allowed by default, and you specify what services and actions are prohibited

To support this, AWS Organizations attaches an AWS managed SCP named **FullAWSAccess** to every root and OU when it's created.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

Benefits of Deny List Strategy

Using a deny list strategy, account administrators can delegate all services and actions until you create and attach an SCP that denies a specific service or set of actions.

Deny statements require less maintenance, because you don't need to update them when AWS adds new services.

Deny statements usually use less space, thus making it easier to stay within the maximum size for SCPs

Sample Deny List Based Policy

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowsAllActions",  
            "Effect": "Allow",  
            "Action": "*",  
            "Resource": "*"  
        },  
        {  
            "Sid": "DenyDynamoDB",  
            "Effect": "Deny",  
            "Action": "dynamodb:*",  
            "Resource": "*"  
        }  
    ]  
}
```

Strategy 2 - Allow List

To use SCPs as an allow list, you must replace the AWS managed FullAWSAccess SCP with an SCP that explicitly permits only those services and actions that you want to allow.

By removing the default FullAWSAccess SCP, all actions for all services are now implicitly denied.

Your custom SCP then overrides the implicit Deny with an explicit Allow for only those actions that you want to permit

Sample Allow List Based Policy

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:*",  
                "cloudwatch:*"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

Points to Note

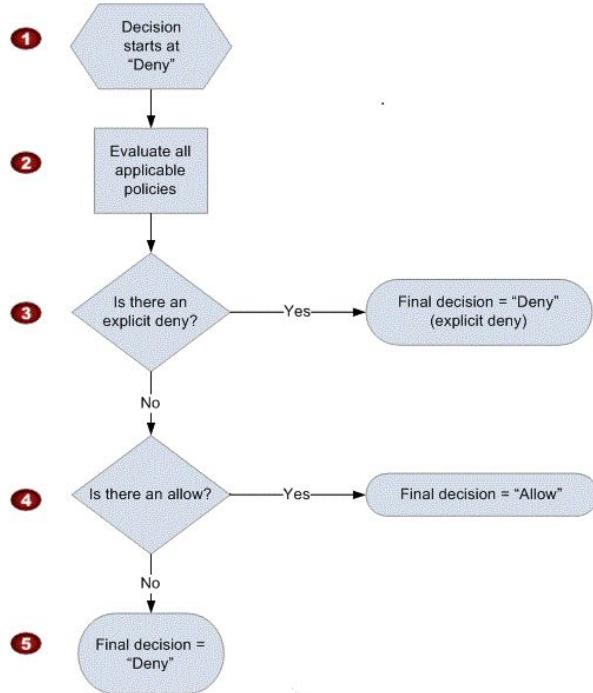
Every root, OU, and account must have at least one SCP attached.

If you want to replace the default FullAWSAccess policy with an SCP that limits the permissions that can be delegated, you must attach the replacement SCP before you can remove the default SCP.

IAM Policy Evaluation Logic

Access Management

Decision Making Process



- 1) Decision starts with assumption that the request will be denied.
- 2) Then, all the attached policies are evaluated.
- 3) Code will look if there is any explicit deny in the policy.
- 4) If explicit deny is not found, code will look for allowed instruction and if yes then decision is allowed.
- 5) If no allow is found, decision is deny.

Example Scenario

- Four AWS S3 buckets are available
- We want to give access to all the buckets in our S3, except 1



Step 1 :

Allow access to all
the buckets in S3.

Step 2:

Deny access to
bucket 05

Explicit Deny vs Deny by Default

- A request will be denied by default if there is no allow policy present for the resource.

Example:

If user has EC2 ReadOnlyAccess and tries to open S3 console, it will be denied.

- A request will be denied irrespective of full access if it is explicitly denied in the policy

Example:

Deny user from accessing bucket 05.

Identity and Resource [Based Policies]

Were Complex becomes Easy

Overview of Identity Based Policy

Identity-based policies are attached to an IAM user, group, or role.

These policies define what an Identity can do.

Example:

We attach IAM policy to a user name John and define that John can start and stop EC2 instances which belongs to development environment.

Overview of Resource Based Policy

Resource-based policies are attached to a resource.

We attach these policies directly to a resource like S3 bucket, SQS Queue, KMS keys.

With resource-based policies, you can specify who has access to the resource and what actions they can perform on it.

Identity and Resource Based Policy

Identity-based policies

Alice

Can read and write on S3 bucket A

Bob

Can read and write on S3 bucket A

John

No policy.

Resource-based policies

S3 Bucket A

Alice: Can list, read, write.

Bob : Can read.

John: Full Access.

Identity-based policies

Alice

Can read and write on S3 bucket A

Bob

Can read and write on S3 bucket A

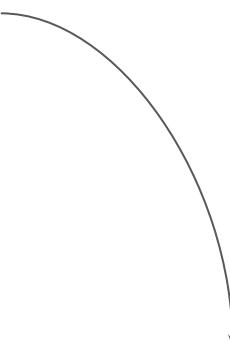
John

No policy.

Resource-based policies

S3 Bucket A

Alice: Can list, read, write.
Bob : Can read.
John: Full Access.



| IAM User | Operations | Resource |
|----------|-------------------|-------------|
| Alice | List, Read, Write | S3 Bucket A |
| Bob | Read, Write | S3 Bucket A |
| John | Full Access | S3 Bucket A |

IAM Policies

Access Management

Identity Access Management

- IAM Policies allows us to define at granular level access on what permissions needs to be given to access a particular AWS resource.
- There are 4 important elements of IAM Policy :

Statement
Effect
Action
Resource



```
{  
  "Statement": {  
    "Effect": "Allow",  
    "Action": "ec2:Describe*",  
    "Resource": "*"  
  }  
}
```

Component 0

- Statement element is the main element for the IAM policy.
- This element is a must.
- The statement element can contain multiple individual statements in order of [{ .. } { ... }] . Each of the individual statement is enclosed in blocks of { }

```
{  
  "Statement": {  
    "Effect": "Allow",  
    "Action": "ec2:Describe*",  
    "Resource": "*"  
  }  
}
```

Example policy with multiple statements

```
{  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:Describe*",  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "elasticloadbalancing:Describe*",  
            "Resource": "*"  
        }  
    ]  
}
```

Component 1

- Effect basically specified whether the statement is allowed or explicitly denied.
- There are two possible values : Allow or Deny

```
{  
  "Statement": {  
    "Effect": "Allow",  
    "Action": "ec2:Describe*",  
    "Resource": "*"  
  }  
}
```

Component 2

- Action element defines list of actions that will be allowed or denied.
- Each AWS service has it's own set of actions.

Example :

- ec2:CreateKeyPair
- ec2:CreateVpc
- sqs>ListQueues
- sqs:SendMessage
- s3:CreteBucket
- s3:DeleteBucket



Component 3

- Resource element defines the object that the statement covers.
- Amazon Resource Name (ARN) uniquely identified the AWS resources.

Example :

arn:aws:ec2:us-west-2:836802967410:instance/i-0067dce1525f98ab2



arn:aws:ec2:region:account-id:instance/instance-id

IAM Policies 02

Access Management

Identity and Access Management (IAM) is a critical component of modern cloud computing architectures. It provides a central mechanism for managing user identities, access rights, and audit logs across multiple applications and services.

The core principles of IAM include:

- Identity Management:** Managing user identities, including creation, authentication, and single sign-on.
- Access Control:** Granting or revoking access to specific resources based on user roles and permissions.
- Audit and Logging:** Monitoring and logging access activities to detect and prevent unauthorized access.

Use Case

Alice has been given one EC2 instance for testing. As part of the access, she must be allowed to start and stop her EC2 instance. The instance ID is i-0508b5c481e123fd9 in the Oregon region.



Component 3

- Resource element defines the object that the statement covers.
- Amazon Resource Name (ARN) uniquely identified the AWS resources.

Example :

arn:aws:ec2:us-west-2:836802967410:instance/i-0067dce1525f98ab2



arn:aws:ec2:region:account-id:instance/instance-id

Relax and Have a Meme Before Proceeding

Me : Sit !

Dog : You SIT !

Me : ok



Identity Account Architecture

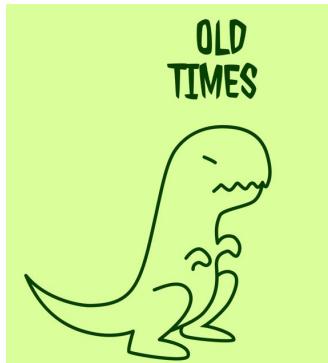
Multiple Accounts are Good

The Initial Start

During the earlier days of AWS, most of the organizations had a single AWS account.

Management was simple.

User would have had a single set of username/password AND access/secret keys.

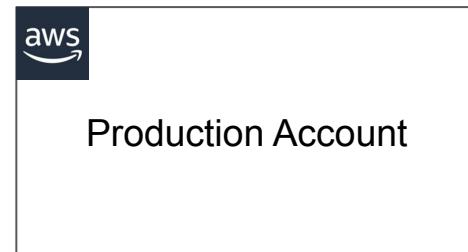
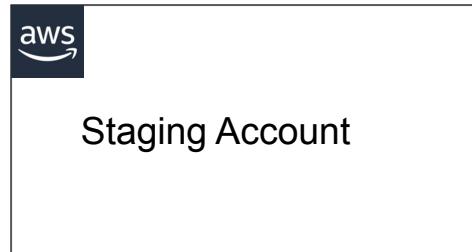
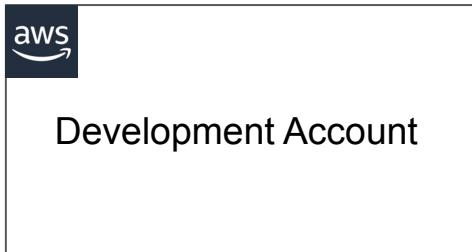


Organizations Became Big

A better architecture with multiple AWS account per function was adopted.

Each user had different username/password AND access/secret keys for each account.

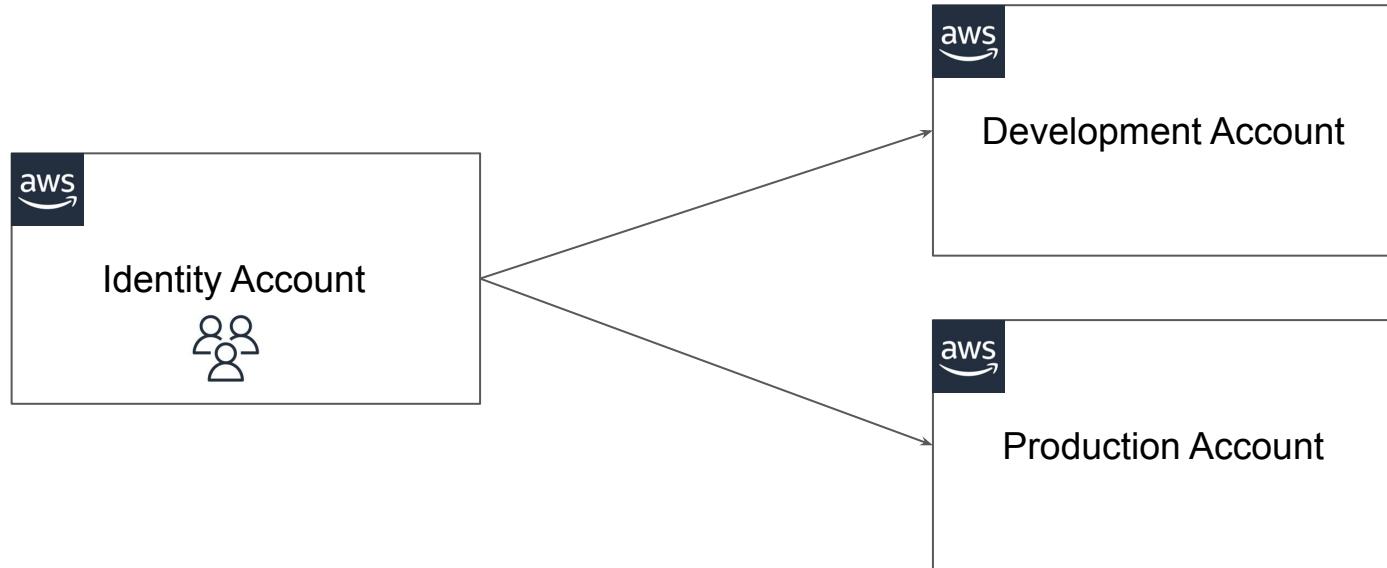
Difficult to Work with. Required a lot of Bookmarks



Rise of Identity Account

In Identity Account architecture, all the IAM Users are stored in central AWS Account.

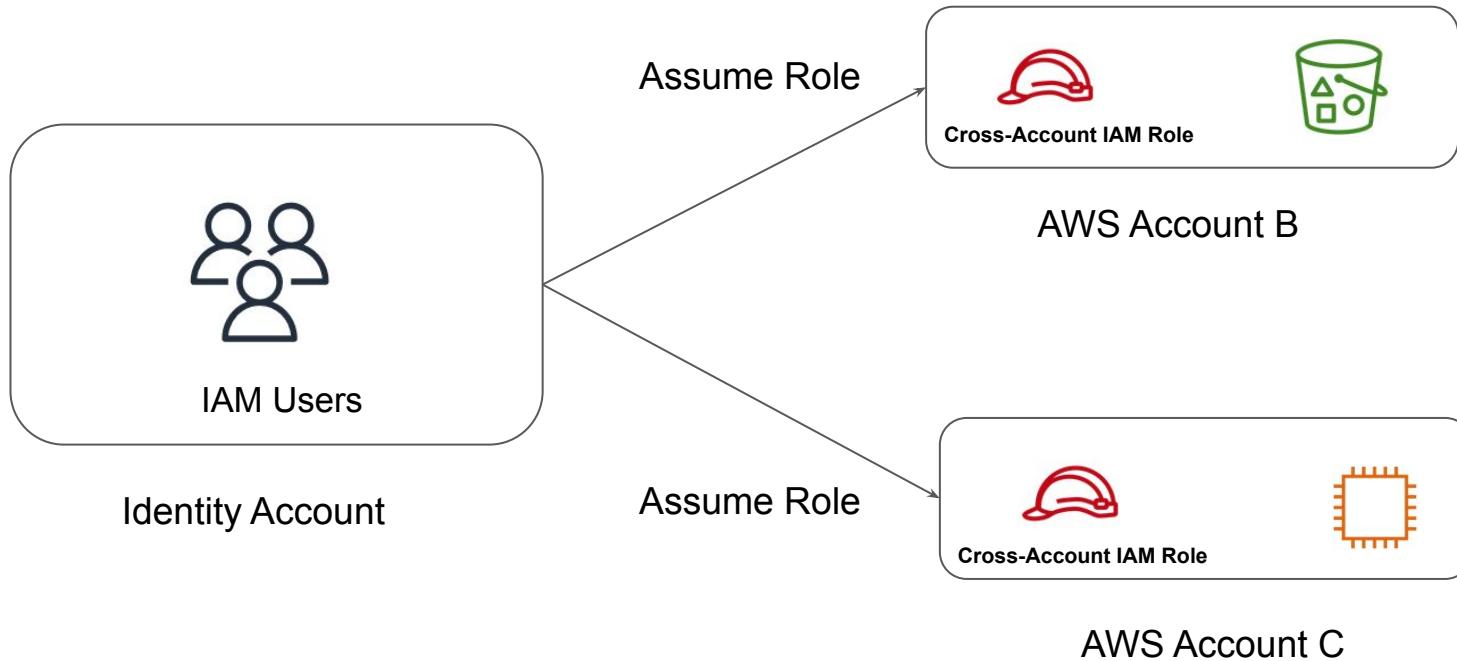
They could easily connect to Dev/Prod accounts without separate credentials.



The Architecture

- i) Create a user in Account A.
- ii) Create a Cross-Account role in Account B.
- iii) Allow User to switch to Account-B Role.

The Practical Architecture

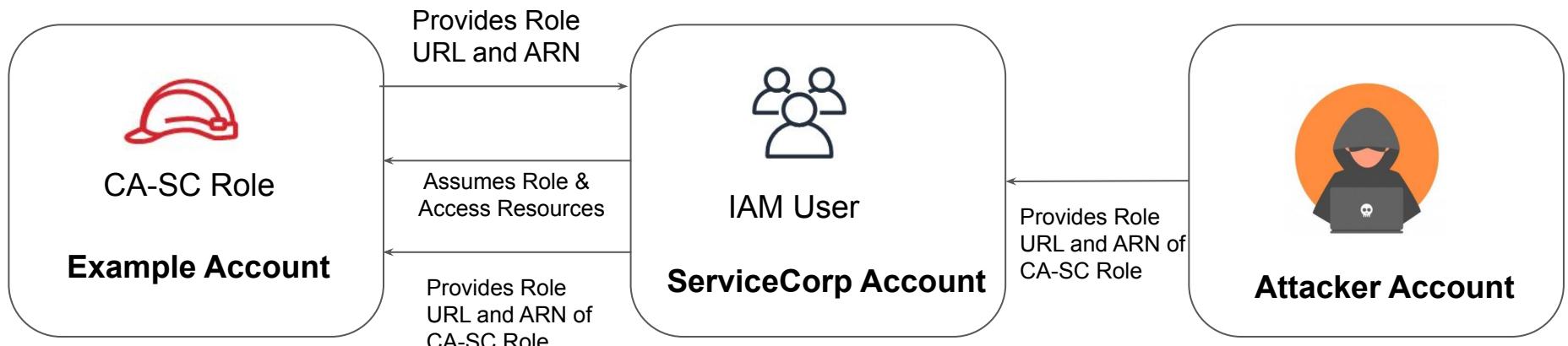


External ID

Secure Delegation

Understanding the Challenge

External ID is a piece of data that can be passed to the AssumeRole API of the Security Token Service (STS).



Important Points to Remember

Once the External ID is set, when someone uses the AWS CLI or AWS API to assume that role, they must provide the external ID.

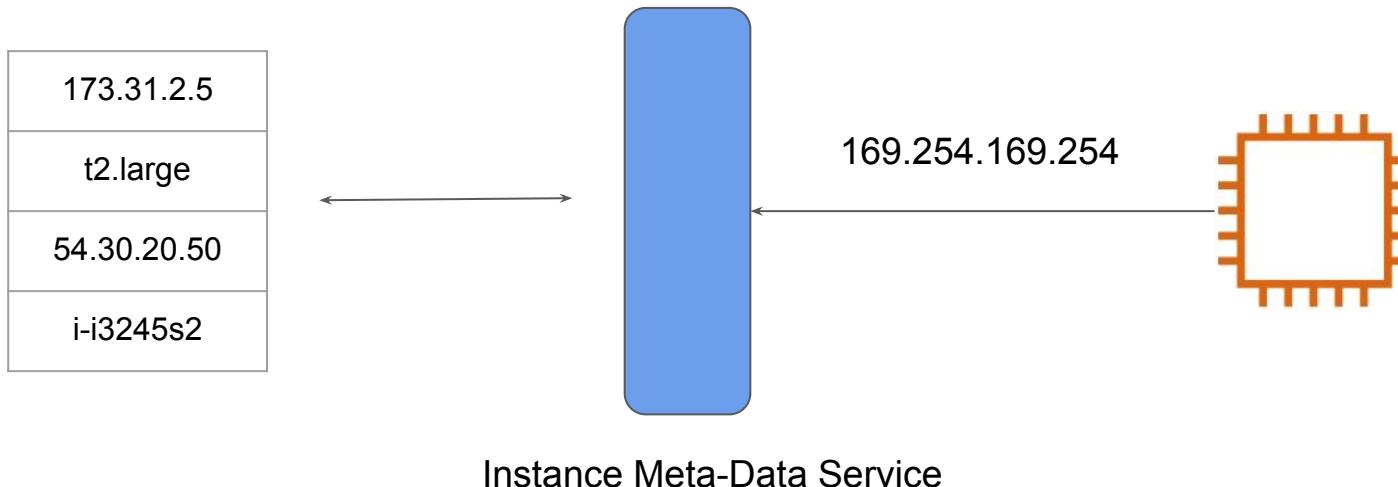
You cannot switch roles at the AWS console to a role that has an external ID condition in its trust policy.

EC2 Instance Metadata

Getting to know thy self

Overview of Metadata Service

- Instance Metadata is basically data about your instance.
- This data can be accessed within the instance itself.



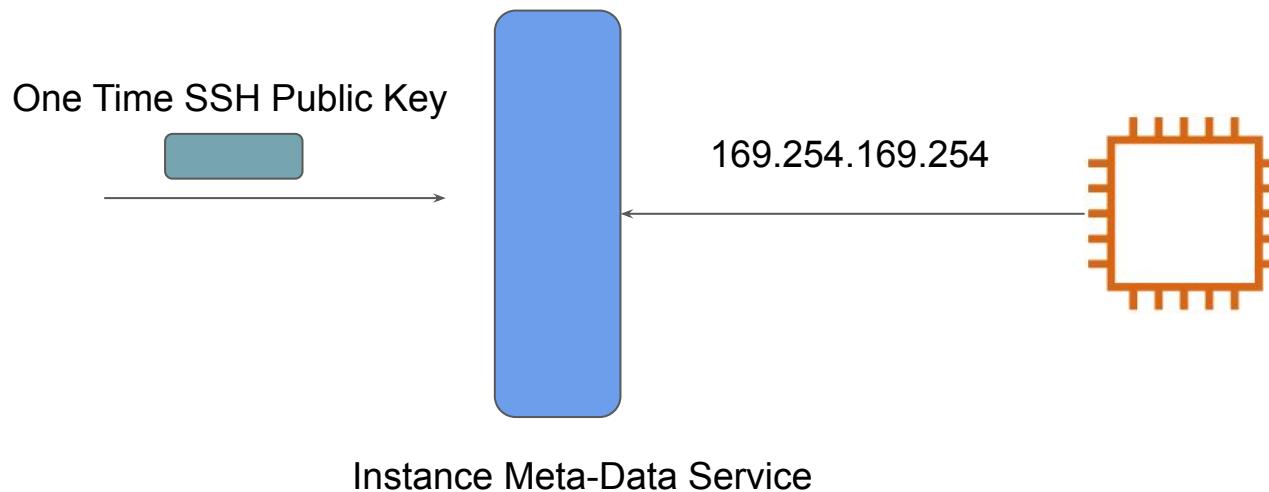
Categories of Information

Information is divided into top level metadata items. Some of these include:

- ami-id
- hostname
- iam
- instance-type
- mac
- profile
- public-keys
- security-groups

Data Pushed to Instance Meta-Data

AWS can push multiple things to the Instance Meta-Data that can subsequently be used by the EC2 instance.

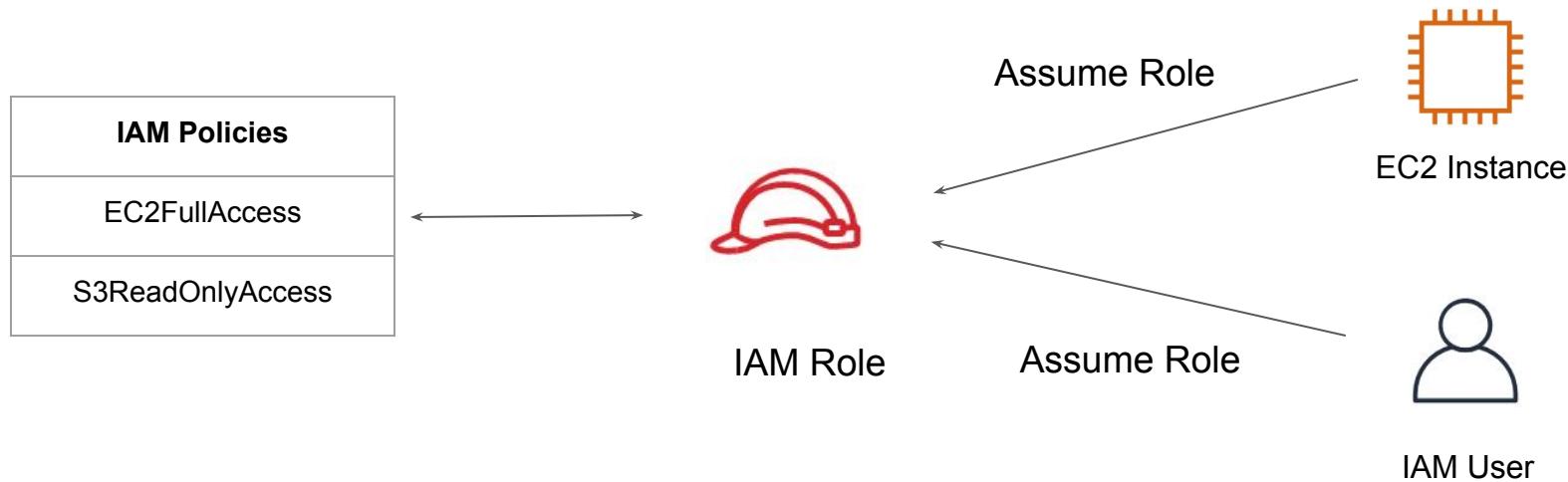


IAM Roles

Access Management

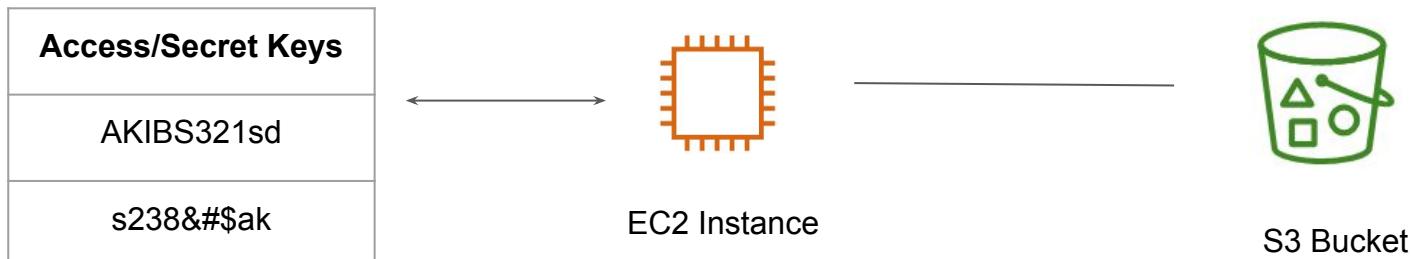
Overview of IAM Role

IAM Role is an entity that contains set of policies and any resource assuming that role will be able to have permissions mentioned in the role.



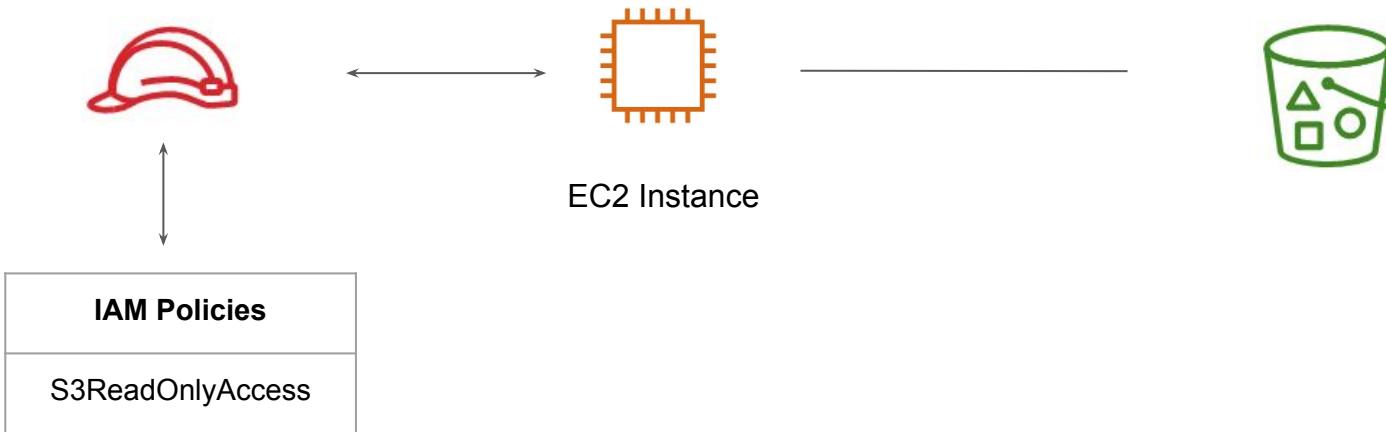
Sample Use-Case- No No Scenario

EC2 Instance wants to get data from an S3 bucket.



Example - Best Practice

It is recommended to always make use of IAM Role instead of hard coding the AWS Access Keys within EC2 instance / software code.



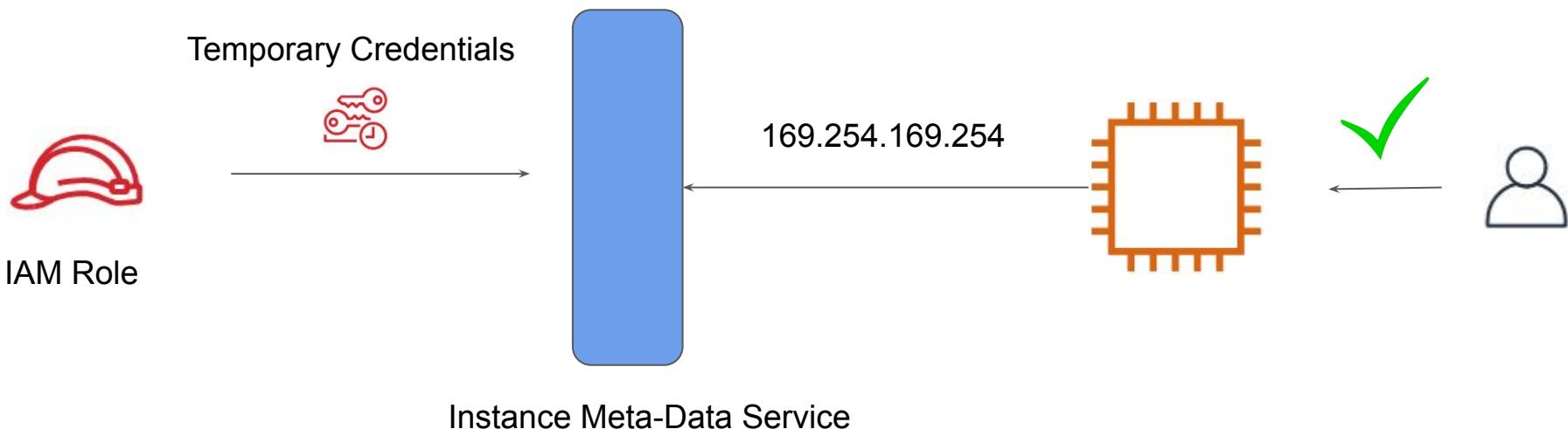
IPTABLES & Instance Meta-Data

Security of Temporary Credentials

Pushing of Temporary Credentials

AWS Pushes set of temporary credentials to the EC2 Instance Meta-Data Service.

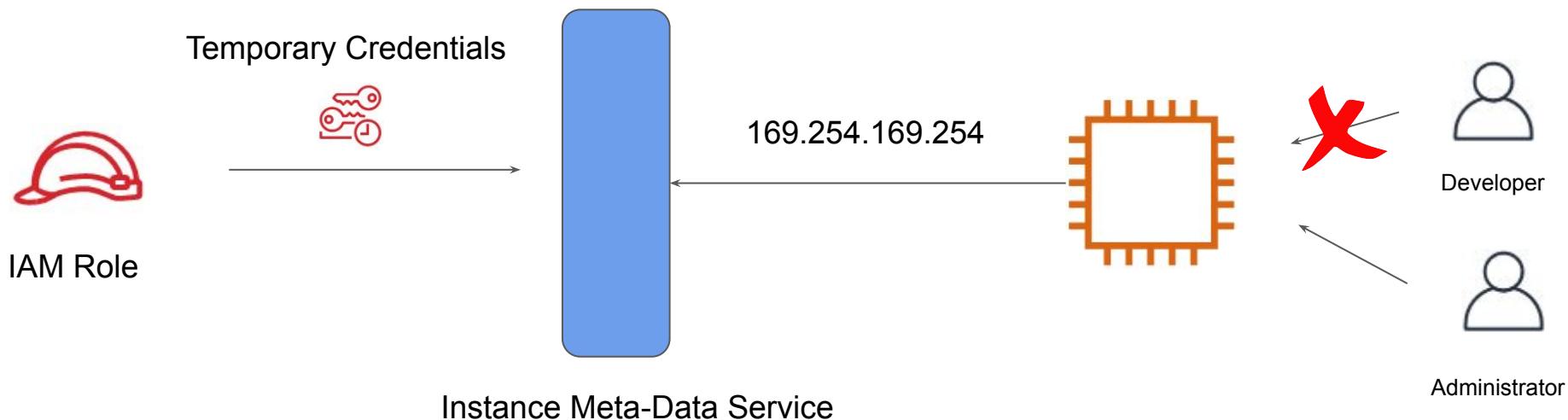
You can retrieve these temporary credentials from Instance Metadata to authenticate.



```
{  
    "Code" : "Success",  
    "LastUpdated" : "2020-07-09T12:51:06Z",  
    "Type" : "AWS-HMAC",  
    "AccessKeyId" : "ASIAQIW66DN24BDYFPVU",  
    "SecretAccessKey" : "cAeG+gnCriAkOX6xuRx1L67CdMANhVucINVMIzS7",  
    "Token" : "IQojb3JpZ2luX2VjEG0aCXVzLwVhc3QtMSJHMEUCIQCTFnaRSEyf9aAT3UzWcaC66eq1vFpSs5zF3Z0hg7yRKgIgZqTLZedEc6T/XM  
nFfOSySayWKWYrE6oPMZ1B8WFNmIqtAMIFhABGgwMTg3MjExNTE4NjEiDIw4Jd1UWuxQUDTq0CqRA5rKdZnVfb6ZCgxN91v/X8dPR91CfwX3L9cpm5s  
/8wn4TApK+62eiThgRAba0FiupqJn6YSw2hL0NxPhWT2GuNPQblyL49yT2GIBkMwRLq8jTRBzeZp6RCzLrdVsWMDUIwJ23sMm0anacSYVGU6J+1hPMoY  
T91/loQNb8HrYesOt1lG8PThFODwTj0nvM0ni1m1i7qlwZ1/9nB9a/V6Djsek6upVAepZdRIG2D7KcFEUq/+dEj4zqARnLG0bdu/f3V+WX1j1fZELAo1  
PSSPH2lKTLnE3qyQpG/8oMyaUeNE0n2dUtmGdiw1CTBgHBXgOM3Nts05kRCX2Io8tfmgjfQpYQ7UYqcxCK5FxLv658vrw7MMDOPxgFxuzSVbqBEtSGL  
pP8SuIOYk7rxsCukrFzNHiwFdRwu0EYg8DgD6ZYFivlaAepuQGTwMG3Ct/C2zu4IoAusqm1j2EK5wqfvGkLref0jmr1VDveEDs6KgBUe6GZ42ceftDa  
aSr8w30TVbDFQtliqhKcN/92seulr/JGIMNylnPgFOusB6vEgubgaBtwWftIf3bdpF1P+mEupA0IBh4JIUNm04lh1fyTotqmiNbqibZC7gmTyElxQfrQ  
cvIdInajPNhmGAE7kdkXH/Dv5t84DXBP1fpaQ1vf8+otaNCdgyr93OV09j2ud8HhwCVcc1m9tHFFIb06k0i2wczt/RPNR47QB1jxLDDxPcceoJ9a1NUK  
c4ajpT6dT5/ugU9ZHLLSDK7puFm3DIPGVFeEkAbQUHJDqdE7/0LcfMt0jiueNm2qcDaSo8ma8quSenk6eb9PNrsrZzOAF1mHjb8qSsiGxyP250qCfpz  
vsCA5r5KPPw==",  
    "Expiration" : "2020-07-09T19:26:40Z"
```

Blocking Access At User Level

With the instance-level firewalls like iptables, you can easily block access to the instance metadata at the user level.



IAM Policy Element - Version

Security Angle

Overview of Version Element

A Version element defines the version of the policy language.

The overall syntax rules can differ based on the version of policy language being used.

Syntax:

```
"Version": "2012-10-17"
```

Available Versions

There are two supported Version Element Values:

| Version | Description |
|------------|---|
| 2012-10-17 | <ul style="list-style-type: none">• Current version of the policy element.• It is recommended to always define version element to 2012-10-17 |
| 2008-10-17 | <ul style="list-style-type: none">• Earlier version of the policy element.• Avoid defining this version in any new policies.• If you do not include “Version Element”, it defaults to this. |

Important Pointer

Version Element != Policy Versions.

Version Element specifies the language of policy.

Policy Version is created when we change the customer managed policy.

Policy Variables

Mastering IAM

Overview of Policy Variables

Policy Variables are used when you don't know the exact value of a resource or condition key when you write the policy.

Example:

```
"arn:aws:iam::888913816489:user/${aws:username}"
```

Principal and NotPrincipal

Security Angle

Overview of Principal Element

A Principal element is used to specify things like IAM user, federated user, IAM role, AWS account, AWS service, or other principal entity that is allowed or denied access to a resource.

You cannot use the Principal element in an IAM identity-based policy.

```
"Principal": { "AWS": "arn:aws:iam::123456789012:root" }
```

Identity-based policies

Alice

Can read and write on S3 bucket A

Bob

Can read and write on S3 bucket A

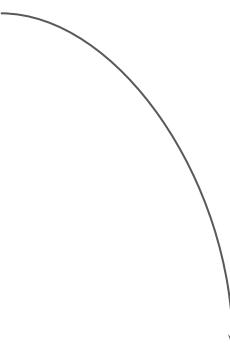
John

No policy.

Resource-based policies

S3 Bucket A

Alice: Can list, read, write.
Bob : Can read.
John: Full Access.



| IAM User | Operations | Resource |
|----------|-------------------|-------------|
| Alice | List, Read, Write | S3 Bucket A |
| Bob | Read, Write | S3 Bucket A |
| John | Full Access | S3 Bucket A |

Numerous Principal Options

Principal Field can include various aspects like:

- IAM User
- IAM Role
- IAM Service Name ("datipeline.amazonaws.com")
- Federated Users

NotPrincipal Element

When you use NotPrincipal in the same policy statement as "Effect": "Deny", the actions specified in the policy statement are explicitly denied to all principals except for the ones specified.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "NotPrincipal": {"AWS": [
                "arn:aws:iam::444455556666:user/Bob",
                "arn:aws:iam::444455556666:Alice"
            ]},
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3::::BUCKETNAME",
                "arn:aws:s3::::BUCKETNAME/*"
            ]
        }
    ]
}
```

Condition Element

Mastering IAM

Overview of Condition Element

The Condition element lets you specify conditions for when a policy is in effect.

We build it by making use of condition operators like (equal, less than, etc).

Sample policy:

Allow full access to User Alice on EC2 Resource {ONLY WHEN CONDITION IS MET}

```
"Condition": {  
    "DateGreaterThan" : {  
        "aws:CurrentTime" : "2013-12-15T12:00:00Z"  
    }  
}
```

Condition Operators

There are multiple condition operators available which you can make use of .

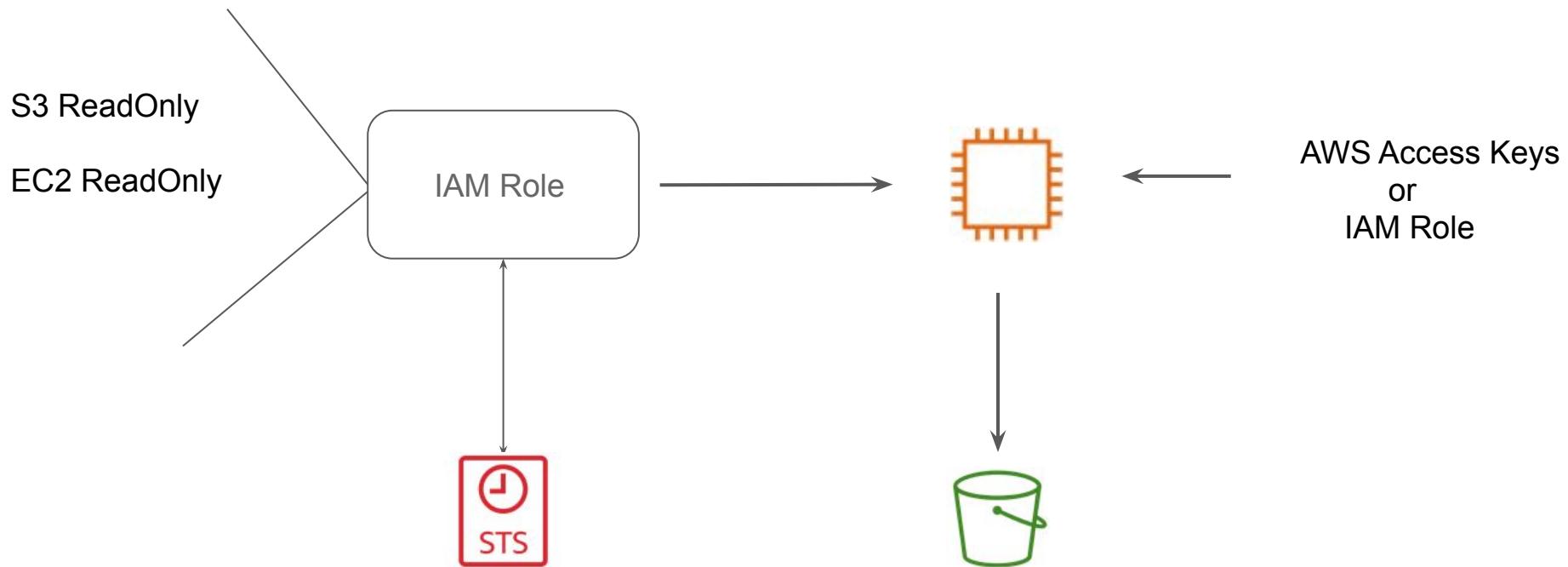
Some of these include:

- String Condition Operators
- Numeric Condition Operators
- Date Condition Operators
- Boolean Condition Operators
- Binary Condition Operators
- IP Address Condition Operators
- ARN Condition Operators

AWS Secure Token Service (STS)

Credentials Management

How IAM Role

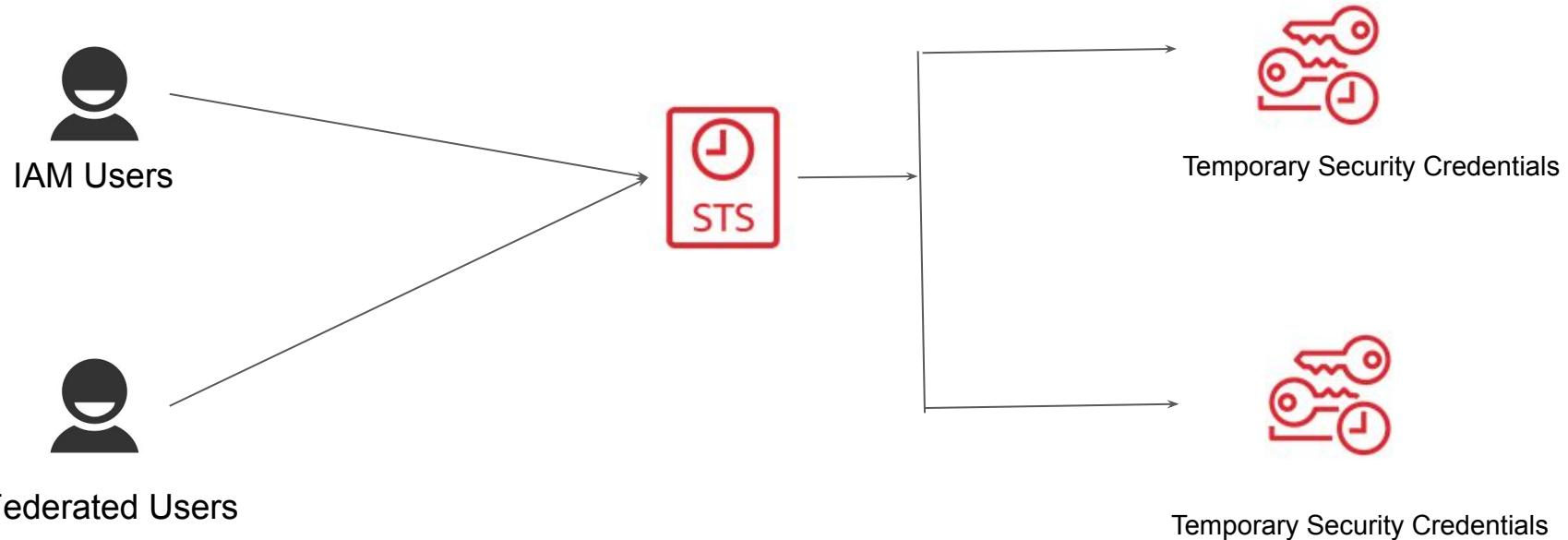


Overview of STS

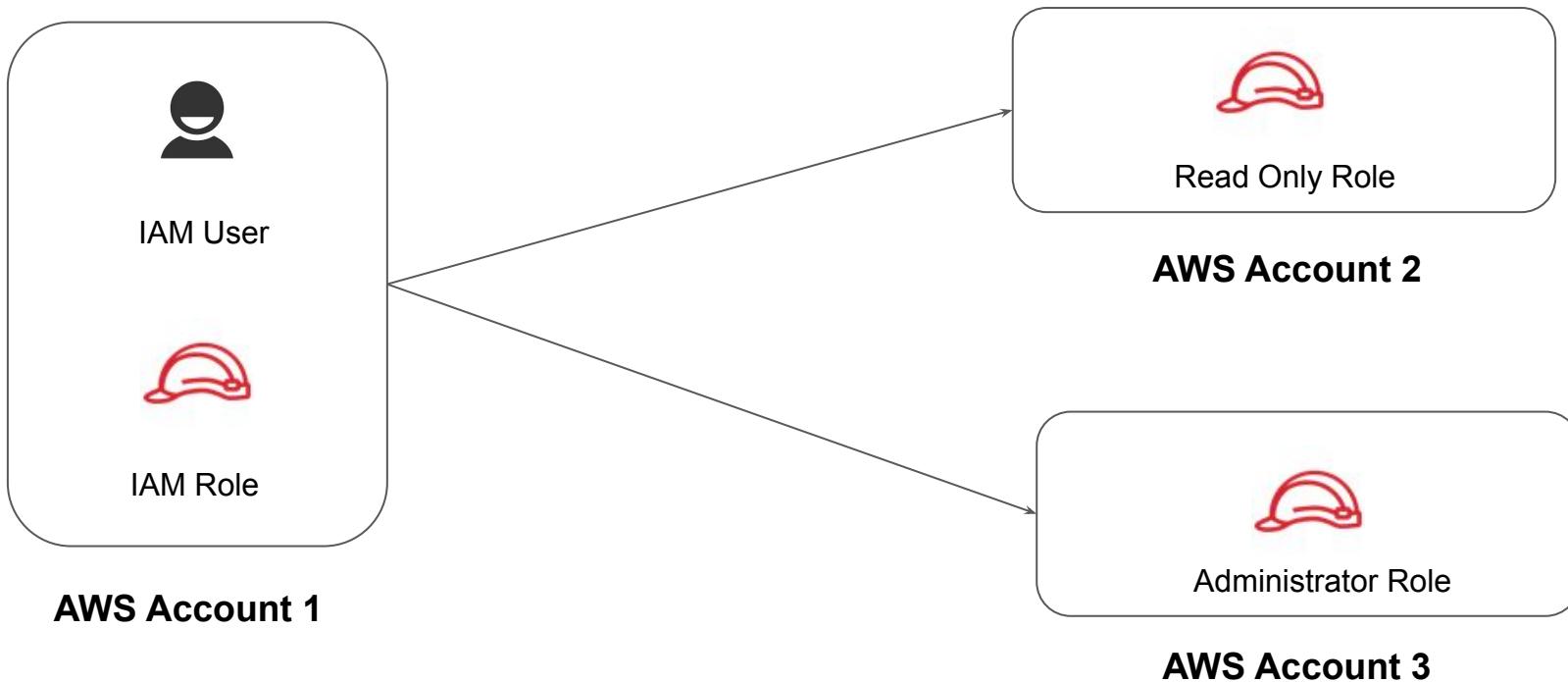
- The AWS STS is a web service that enables you to request temporary, limited-privilege credentials for AWS Identity and Access Management (IAM) users or for users that you authenticate (federated users).
- Temporary security credentials are short term and expire after a certain duration.
- Since they have a limited lifetime, the key rotation is no longer explicitly needed.

```
{  
    "AssumedRoleUser": {  
        "AssumedRoleId": "AROAJOTOADWSDZD53Z7VS:temp",  
        "Arn": "arn:aws:sts::836802967410:assumed-role/CA-EC2RO/temp"  
    },  
    "Credentials": {  
        "SecretAccessKey": "LKtyaWrhxGnBNP3tx7dMK2nv0H1VdwMP1RVP5Sob",  
        "SessionToken": "FQoDYXdzEMj//////////wEaDHwScBw1Hmr5eGqKXyLHAdeXEJZ0oSuJxFd/PGtU  
Z5F3XhjgIawg7ytJXXWRgpyvaq9eMKNfUqmiDca/NM+FLwqy5iek5VKPGkPut+/pAz0WH3ddVmcuhsJowHxaDGHa  
d6S21yhyMFAF9bk9FQjMFHNt1/oD174KvkAV6xAE4Q0cPZ4sDGes130Im4r5Tu1KT/I2qvg0w/LVRjraJ8UBnopMu  
gU=",  
        "Expiration": "2017-09-20T23:36:41Z",  
        "AccessKeyId": "ASIAJWPD367QI4GHCNAQ"  
    }  
}
```

Overview Architecture of STS



STS Architecture - Cross-AWS Account Access



Federation

Connecting Identities

Understanding the Challenge

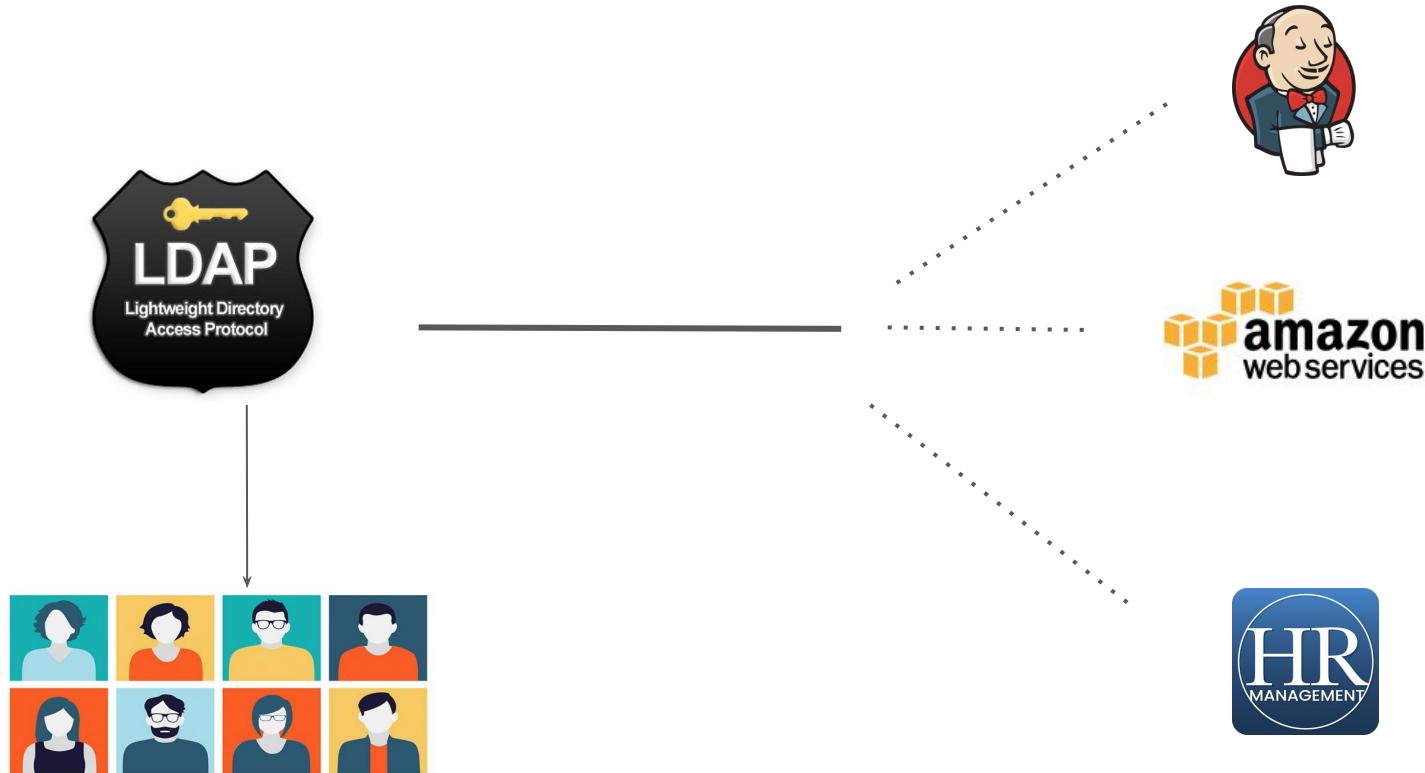
Let's assume there are 500 users within an organization. Your organization are using 3 services :-

- AWS (Infrastructure)
- Jenkins (CI / CD)
- HR Activator (Payroll)



You have been assigned role to give users access to all 3 services.

Storing Users Centrally



Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers [pdc.e]

Saved Queries

enterprise.com

- Builtin
- CEO
- Computers
- Contractors
- Disabled Computers
- Disabled Users
- Districts
- Domain Controllers
- ForeignSecurityPrincipals
- Groups
- Inactive Users
- LostAndFound
- Managed Service Accounts
- Managers
- Microsoft Exchange Security Groups
- Production
- Program Data
- System
- TestOU
- Users
- Microsoft Exchange System Objects
- NTDS Quotas
- TPM Devices

Name Type Description

| | | |
|-----------------|------|------------------------------------|
| Ian Scur | User | |
| Cain Decker | User | |
| Elena Anderson | User | |
| Bill Jackson | User | Moved from: CN=Bill Jackson,OU= |
| Phill Jefferson | User | Moved from: CN=Phill Jefferson,OU= |

Delegate Control...
Move...
Find...

New Computer
All Tasks Contact
Refresh Group
Export List... InetOrgPerson
View msExchDynamicDistributionList
Arrange Icons msImaging-PSPs
Line up Icons MSMQ Queue Alias
Properties Organizational Unit
Printer
Help User
Shared Folder

Create a new object...

The screenshot shows the Windows Active Directory Users and Computers (ADUC) management console. The left pane displays a tree view of the directory structure under 'enterprise.com'. The right pane lists several users with their details: Name, Type, and a note indicating they were moved from other locations. A context menu is open over the user list, with the 'New' option selected. A secondary dropdown menu shows various object types: Computer, Contact, Group, InetOrgPerson, msExchDynamicDistributionList, msImaging-PSPs, MSMQ Queue Alias, Organizational Unit, Printer, User, and Shared Folder. The 'User' option is also highlighted in this secondary menu. At the bottom of the main pane, there is a text input field for 'Create a new object...'.

Central Users

There are various solutions available which can store users centrally :-

- Microsoft Active Directory
- RedHat Identity Management / freeIPA



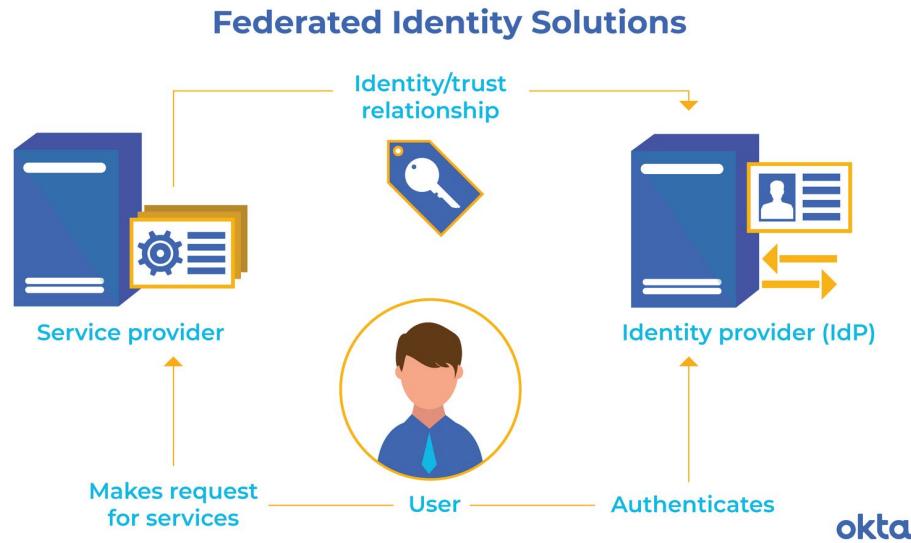
Basics of Federation - AWS Perspective

Federation allows external identities (Federated Users) to have secure access in your AWS account without having to create any IAM users.

These external identities can come from :-

- Corporate Identity Provider (AD, IPA)
- Web Identity Provider (Facebook, Google, Amazon, Cognito or OpenID)

Basic Workflow



Understanding Identity Broker

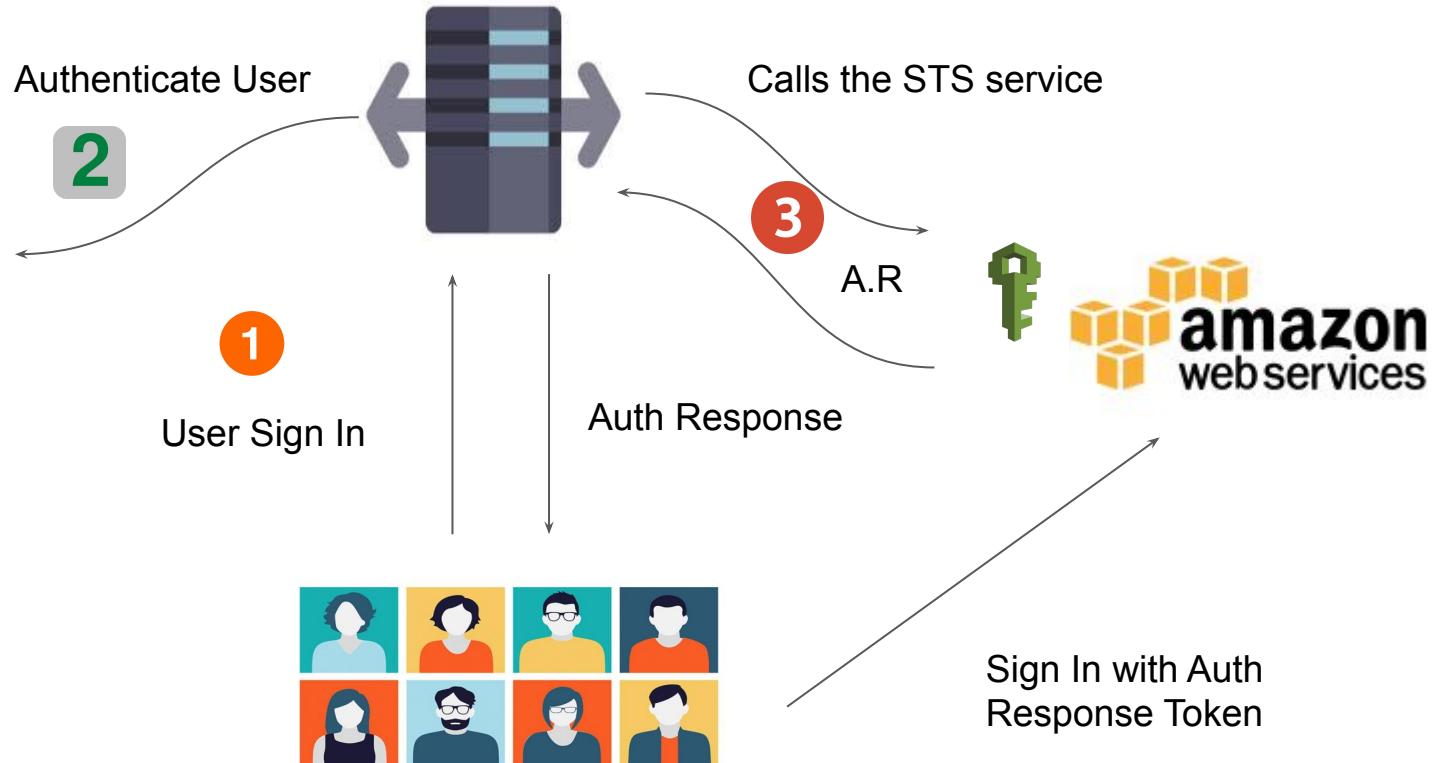
Identity Broker :-

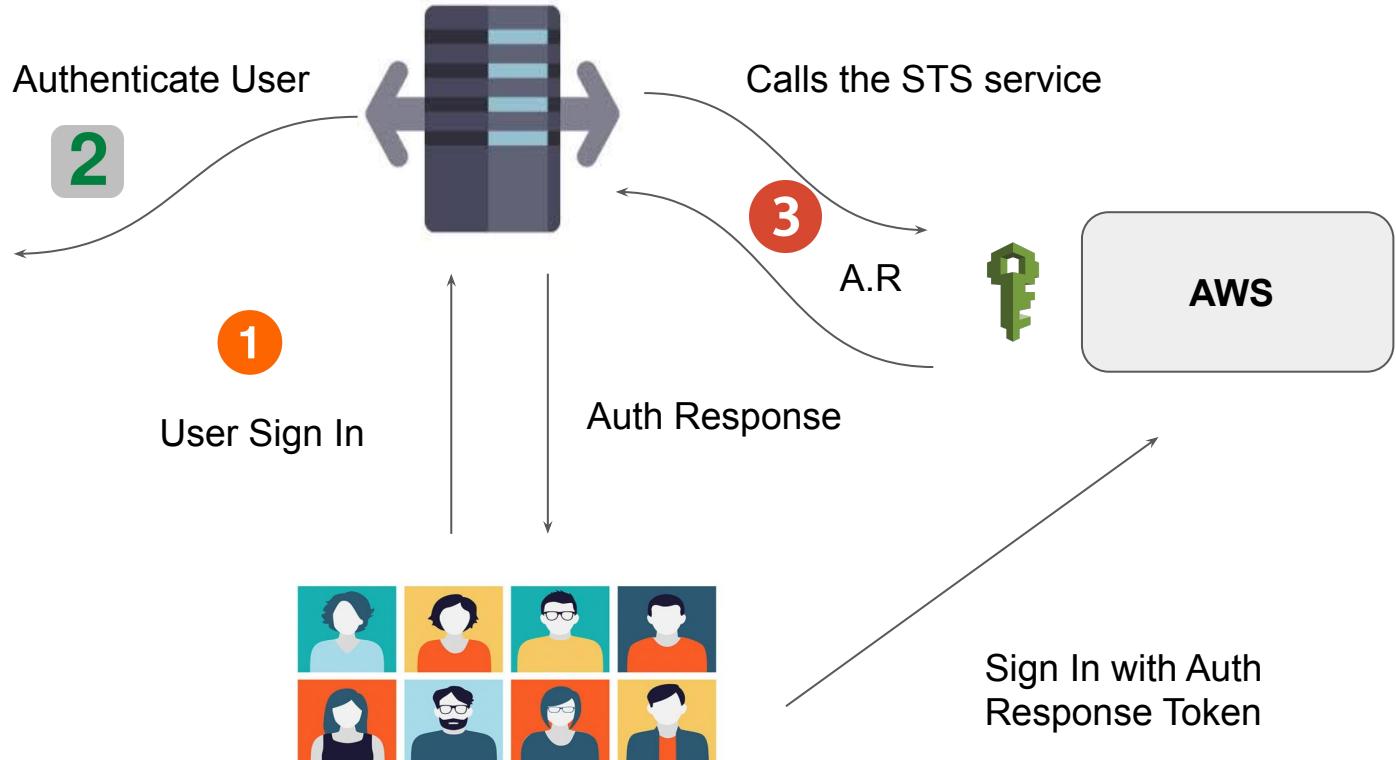
It is an intermediate service which connects multiple providers.

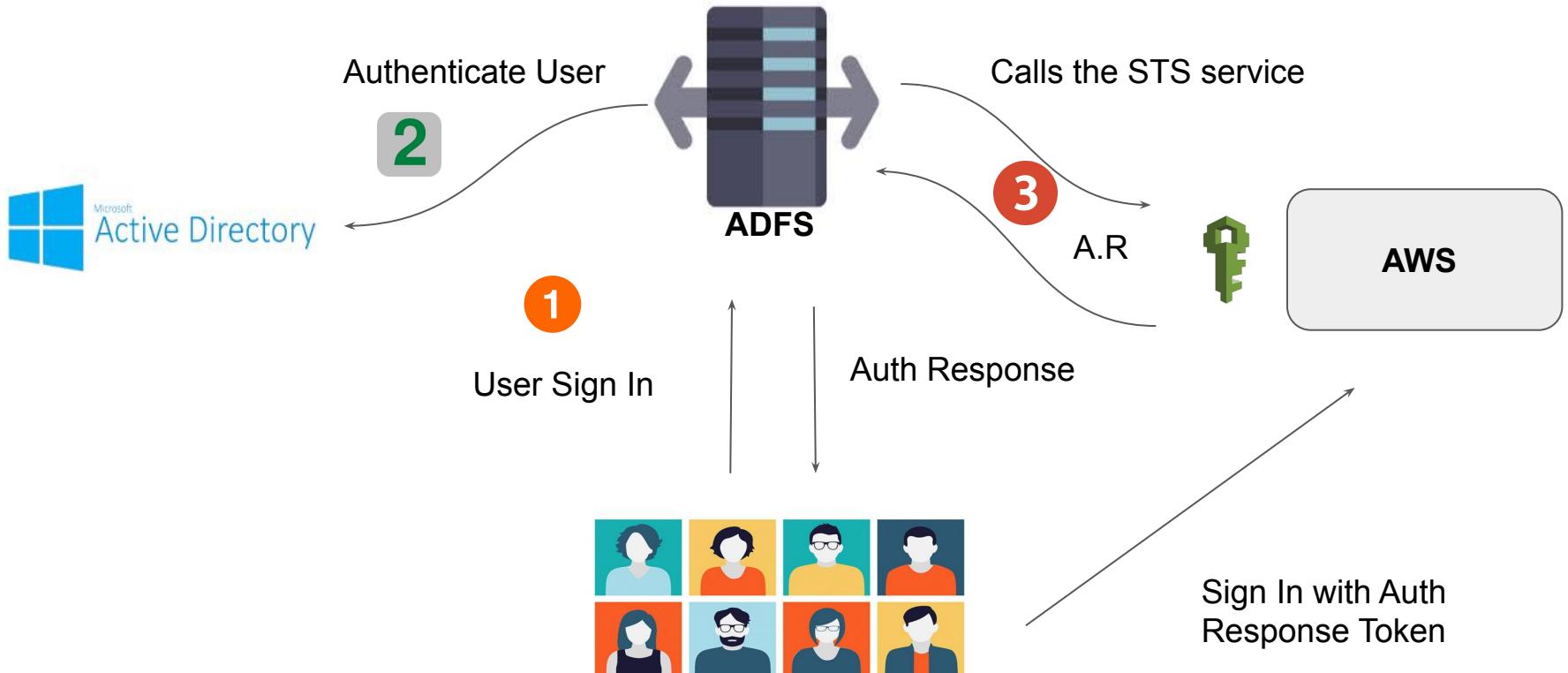




Microsoft
Active Directory







Steps to Remember

- User logs in with username & Password.
- This credentials are given to the Identity Broker.
- Identity Broker validates it against the AD.
- If credentials are valid, Broker will contact the STS token service.
- STS will share the following 4 things :-

Access Key + Secret Key + Token + Duration

- User can now use to login to AWS Console or CLI.

Notations to Remember

Identities : Users

Identity Broker :

- It is a middleware that takes the users from point A & help connect them to point B.

Identity Store :-

- Place where users are present. Eg : AD, IPA, Facebook etc.

Relax and Have a Meme Before Proceeding



Cole
@its_cmillz6

when you're sleeping and your alarm
didn't ring yet but the amount of
sleep you're getting is suspicious



SAML

Single Sign On

Introduction to SAML

- SAML stands for Security Assertion Markup Language.
- It is a secure XML based communication mechanism for communicating identities across organizations.
- SAML eliminates the need to maintain multiple authentication credentials, such as passwords in multiple locations.

Classic Way



Challenges with classic way

- The administrator does not have direct visibility with the underlying database of the SAAS provider.
- If there are multiple SAAS providers, it is difficult to keep track of which user has access to which SAAS application.
- When the user leaves the organization, he needs to be removed from all the entities (Jenkins, AWS, HR app)

Different Views

Administrator's View

Have to login to different providers to manage and control the permissions of an individual user across the organization.

User forgetting username and passwords, MFA :(

User's View

I have to remember passwords of all the applications in the organization.

It might be possible that even userID across apps is different, so have to remember that as well.

SAAS Provider's View

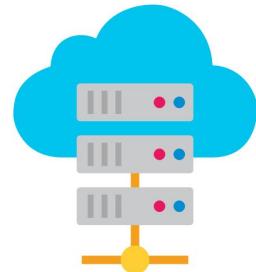
Have to maintain the user and password database of customers.

This is a big security liability.

SAML



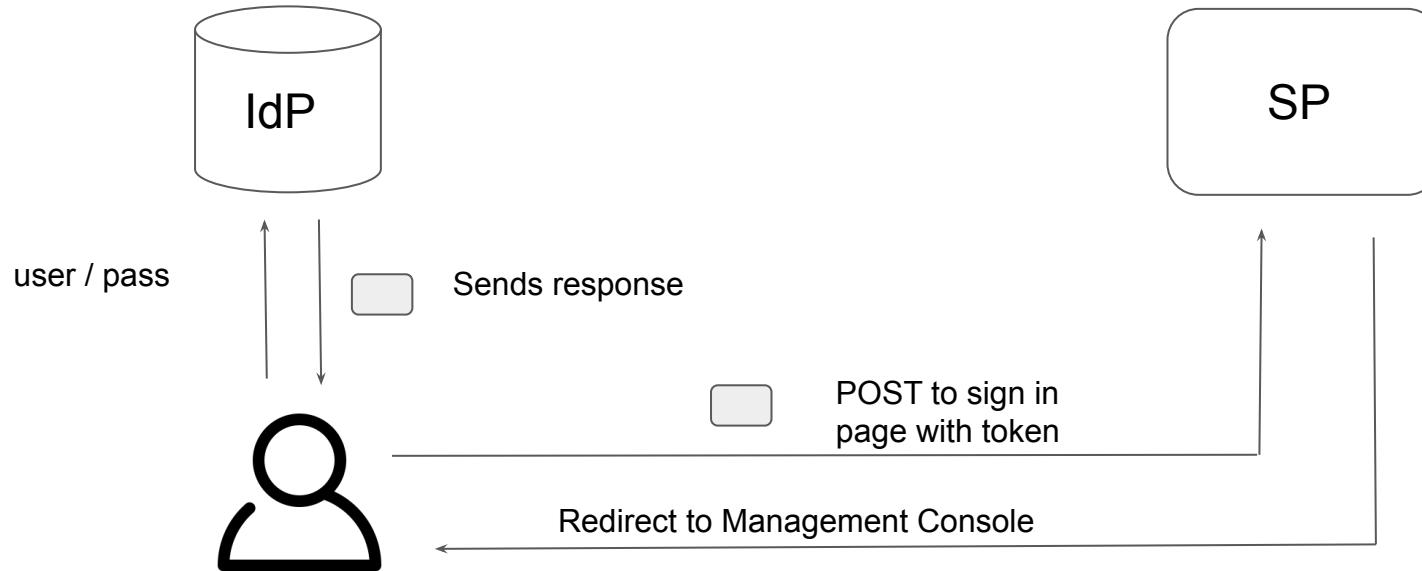
Identity Provider



Service Provider



The SAML Way



Introduction to SAML

- The flow gets initiated when user opens the IdP URL and enters the username and password and selects the appropriate application.
- IdP will validate the credentials and associated permissions and then user receives SAML assertion from the IdP as part of response.
- User does a POST of that SAML assertion to the SAAS sign in page and SP will validate those assertion.
- On validation, SP will construct relevant temporary credentials, and constructs sign in URL for the console and sends to the user.

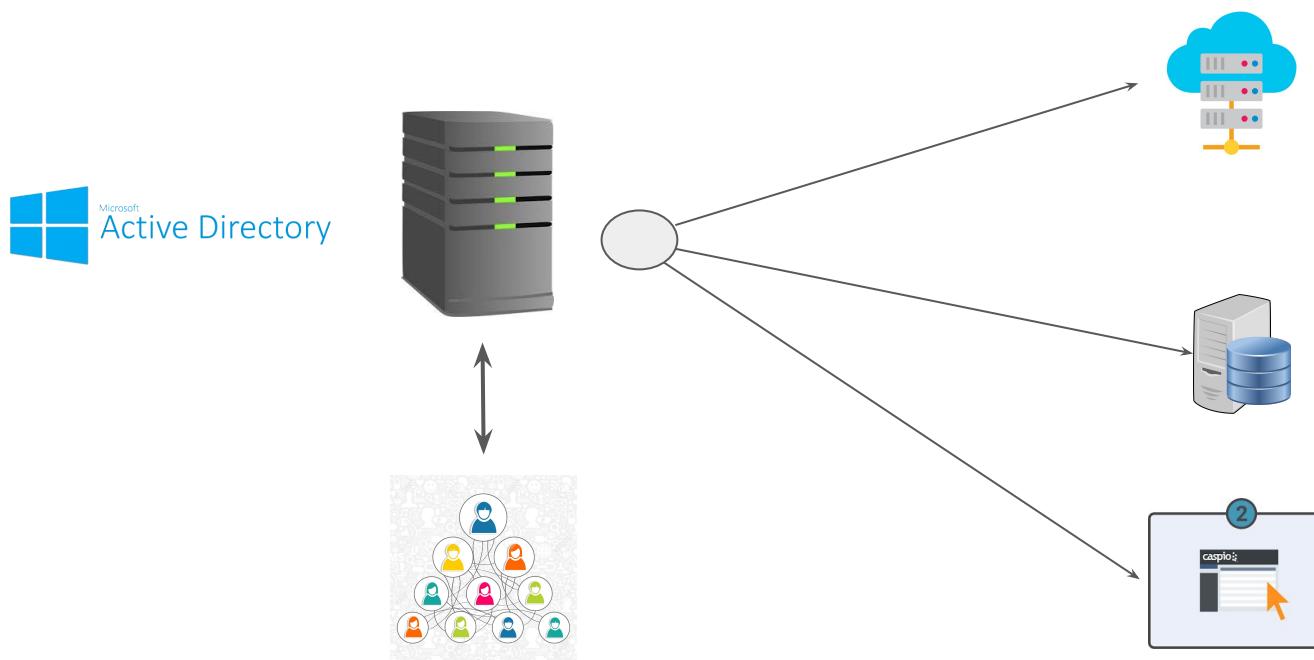
Active Directory

Directory Service

Traditional Way



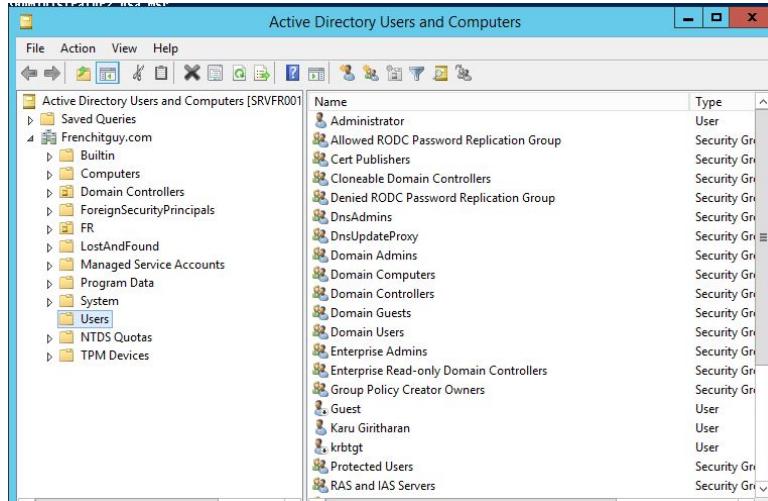
Better Way



Active Directory

Active Directory is one of the most popular directory service developed by Microsoft.

The server running the Active Directory service is called as the domain computer and it can authenticate and authorize the users and computers which are associated to it.



AWS Directory Service

Directory on the Cloud

Challenges with Active Directory

For those who have set up an AD knows, this can be a challenging and time-consuming process.

Some of the challenges involved can be:

- Provisioning the Infrastructure.
- Installing the directory software
- Getting replication setup between domain controllers for HA
- Monitoring / Patching and many more.



Directory Service in the Cloud

AWS Directory Service is a managed service based on the cloud that allows us to create directories and let AWS experts handle and manage the other parts like high availability, monitoring, backups, recovery, and others.

There are three important components :

- Active Directory Service with Microsoft Active Directory
- Simple AD
- AD Connector

Directory Service with Microsoft AD

AWS Directory Service for Microsoft Active Directory is powered by an actual Microsoft Windows Server Active Directory (AD) in the AWS Cloud.

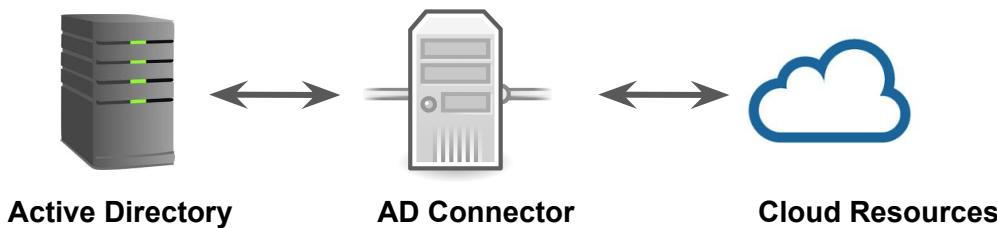
There are two types:

- Standard Edition -- For small and midsize (up to 5000 users)
- Enterprise Edition -- For larger deployments.



AD Connector

- It is a proxy service that provides easy way to connect applications in cloud to your existing on-premise Microsoft AD.
- When users log in to the applications, AD Connector forwards sign-in requests to your on-premises Active Directory domain controllers for authentication.



Simple AD

- Simple AD is a Microsoft Active Directory–compatible directory from AWS Directory Service that is powered by Samba 4.
- Simple AD supports basic Active Directory features such as user accounts, group memberships, joining a Linux domain or Windows based EC2 instances, Kerberos-based SSO, and group policies. AWS provides monitoring, daily snapshots, and recovery as part of the service.
- Simple AD does not support trust relationships, DNS dynamic update, schema extensions, multi-factor authentication, communication over LDAPS, PowerShell AD cmdlets, or FSMO role transfer.

Trusts in Active Directory

Security Angle

Overview of Trust Relationship

In AWS, we can create “Trust Relationships” for IAM Role so that we can have cross-account IAM Access.

Edit Trust Relationship

You can customize trust relationships by editing the following access control policy document.

Policy Document

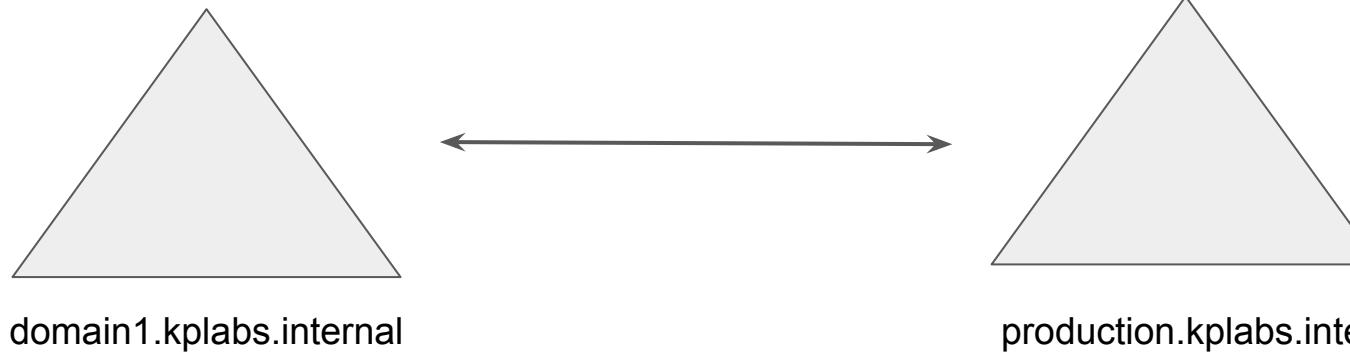
```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "AWS": "arn:aws:iam::888913816489:root"  
8       },  
9       "Action": "sts:AssumeRole",  
10      "Condition": {}  
11    }  
12  ]  
13 }
```

AD Trust

In AD, domain to domain communication can occur through Trusts.

An AD DS trust is a secured, authentication communication channel between entities, such as AD DS domains.

Trusts enable you to grant access to resources to users, groups and computers across entities

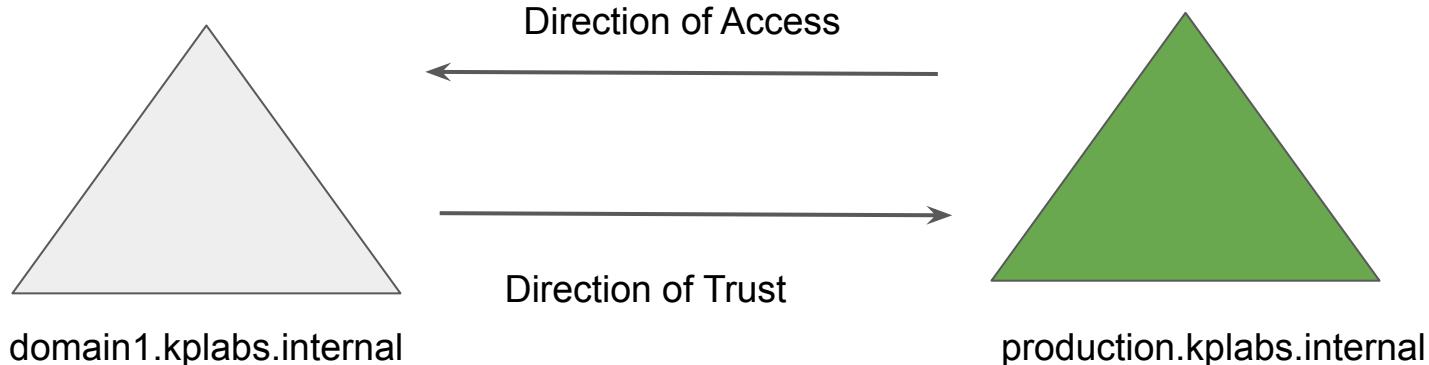


Direction of the Trust

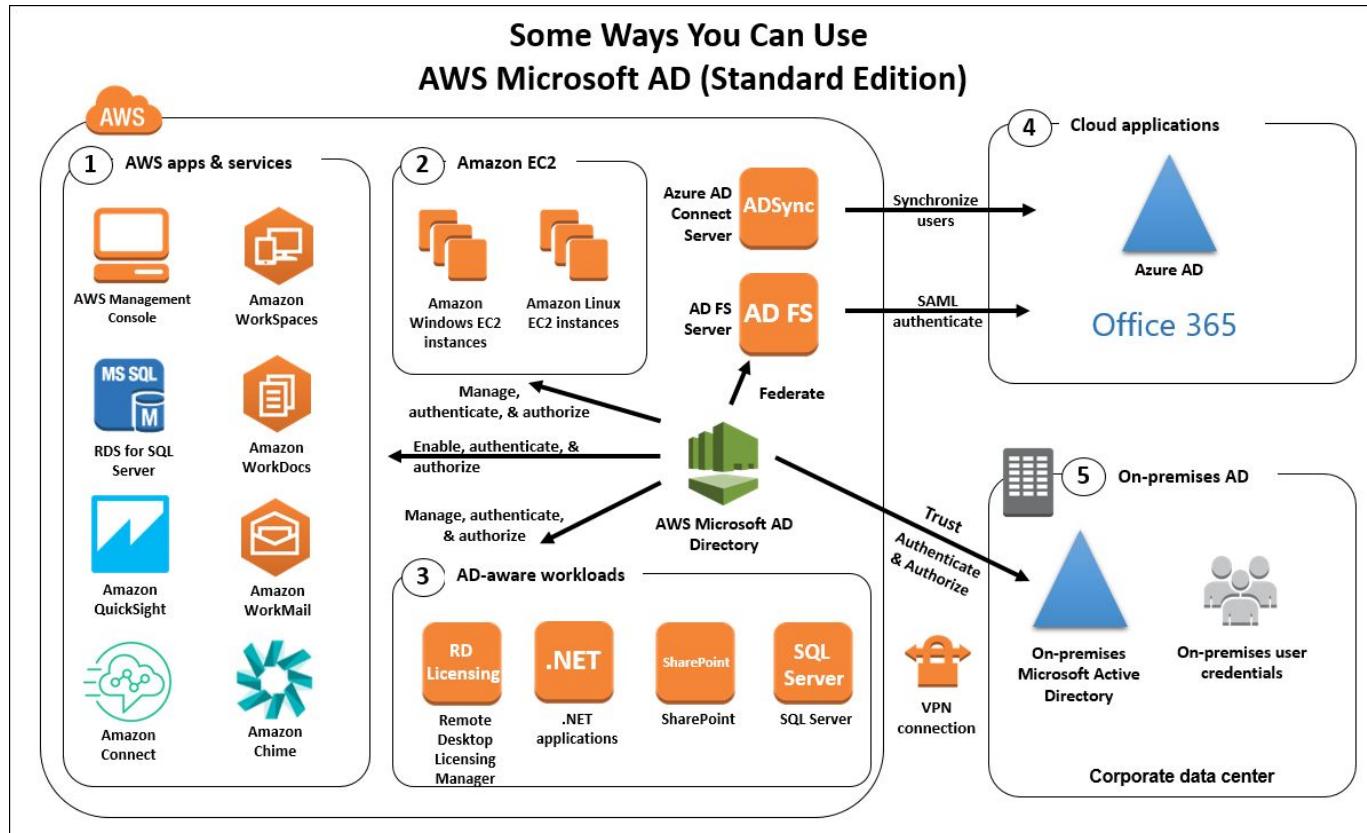
Trust can either be one-way or two-ways.

In a two-way trust, domain from either side can access the other side.

In the following diagram, we have one way trust.



AD Aware Workloads



Migrating AD Aware Workloads

If you already have an AD infrastructure and want to use it when migrating AD-aware workloads to the AWS Cloud, you can use AD trusts to connect AWS Microsoft AD (Standard Edition) to your existing AD.

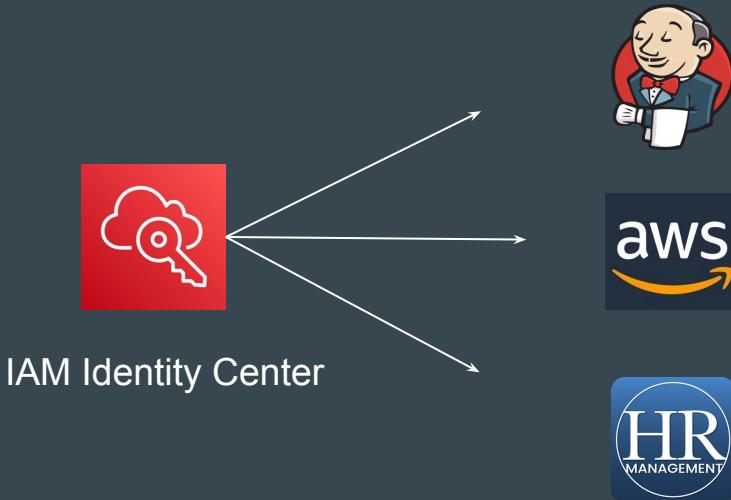
This means your users can access AD-aware and AWS applications with their on-premises AD credentials, without needing you to synchronize users, groups, or passwords.

IAM Identity Center



Understanding the Basics

IAM Identity Center (successor to AWS Single Sign-On) allows centralized access to multiple AWS accounts and applications and provide users with single sign-on access to all their assigned accounts and applications from one place.



Basic Steps

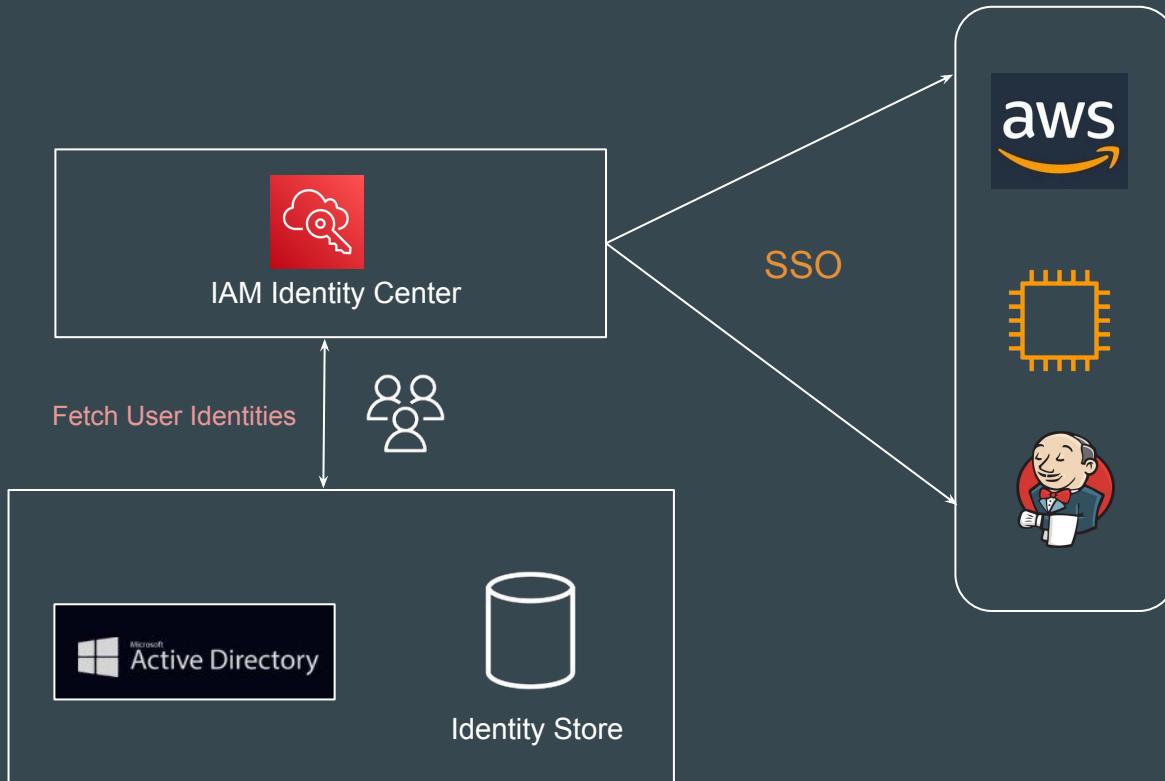


A screenshot of the AWS account selection screen. At the top right is a search bar with the placeholder 'Search'. Below it is a section titled 'AWS Account (2)'. It lists two accounts: 'Europa' (with ID #042025557788) and 'Sandbox Account' (with ID #004417287555). Each account entry has a small orange hexagonal icon and a dropdown arrow to its right.

Login to Access Portal

Connect with AWS Accounts / Apps available

Understanding the Workflow



SSO with AWS CLI

AWS CLI integrates with the SSO.

SSO users can authenticate via CLI, and they will be able to perform the CLI operations without having to add keys in their `~/.aws/credentials` file.

```
C:\Users\zealv>aws s3 ls --profile AdministratorAccess-004417287555
C:\Users\zealv>aws sso login --profile AdministratorAccess-004417287555
Attempting to automatically open the SSO authorization page in your default browser.
If the browser does not open or you wish to use a different device to authorize this request, open the following URL:
https://device.sso.us-east-1.amazonaws.com/
Then enter the code:
KQKZ-NRWR
Successfully logged into Start URL: https://d-9067a61937.awsapps.com/start
```

IAM Team After Implementing SSO



Benefits of IAM Identity Center

Your users can use their directory credentials for single sign-on access to multiple AWS accounts.

Enable single sign-on access to your AWS applications

Enable single sign-on access to Amazon EC2 Windows instances

Enable single sign-on access to cloud-based applications that support SAML

IAM Identity Center - Concepts & Considerations



Prerequisite for Identity Center

Your AWS account must be managed by AWS Organizations.

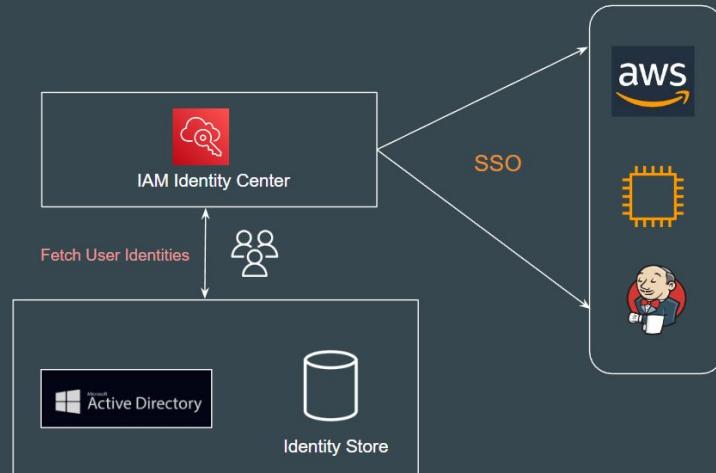
If you've already set up AWS Organizations, make sure that all features are enabled

When you enable IAM Identity Center, you will choose whether to have AWS create an organization for you.

Identity Source

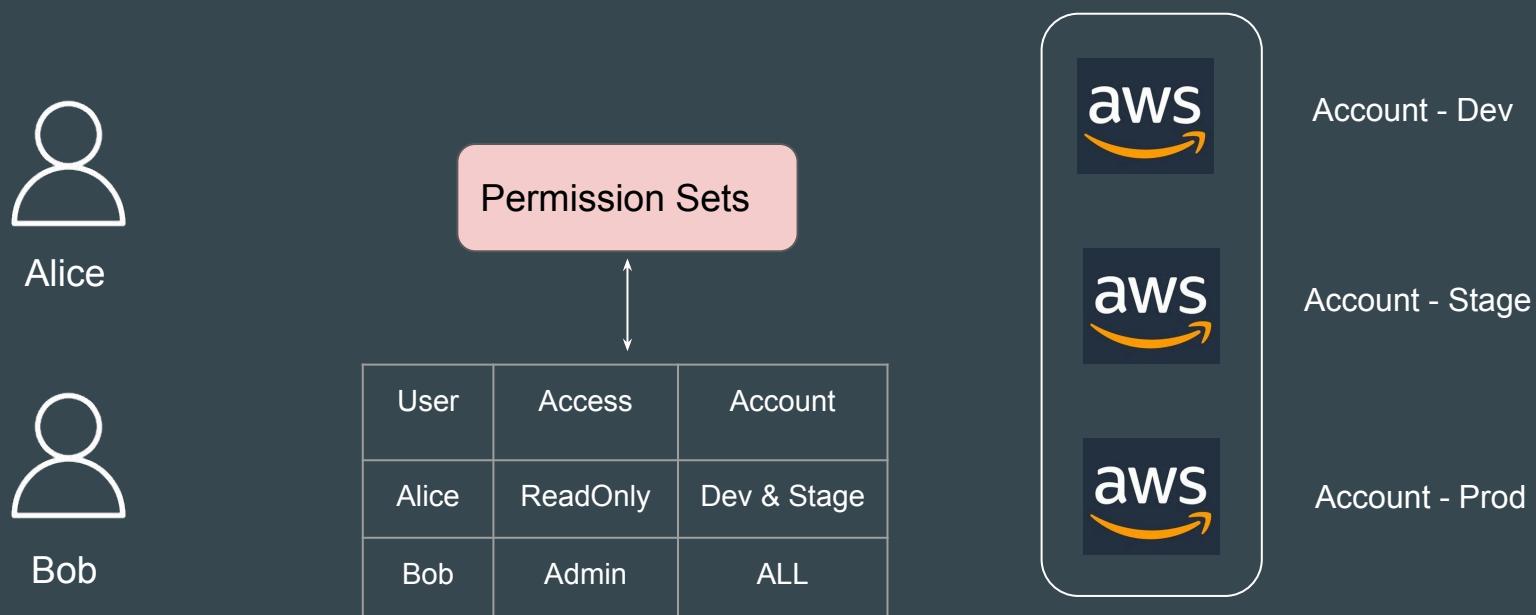
If you're already managing users and groups in Active Directory or an external IdP, it is recommended that you consider connecting this identity source when you enable IAM Identity Center and choose your identity source.

You can also create users and groups directly in IAM Identity Center.

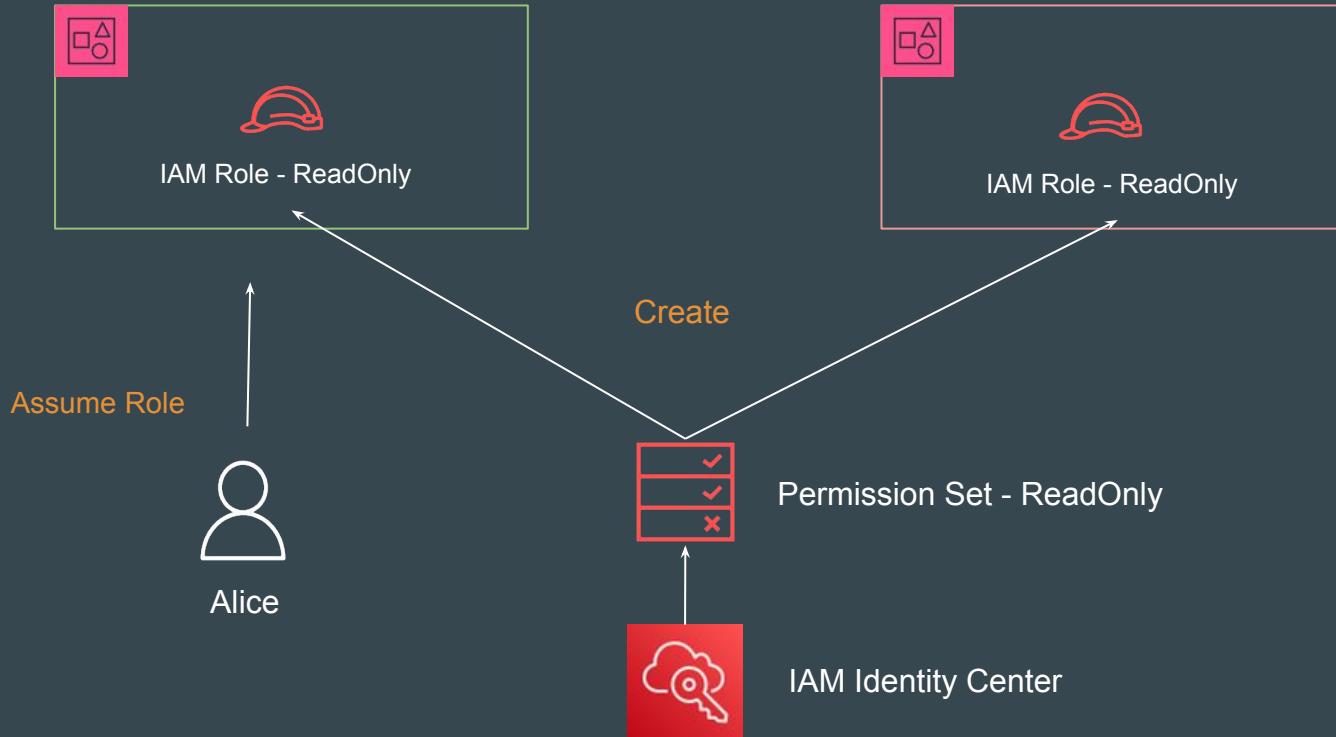


Permission Sets

Permission sets define the level of access that users in IAM Identity Center have to their assigned AWS accounts



How it Works

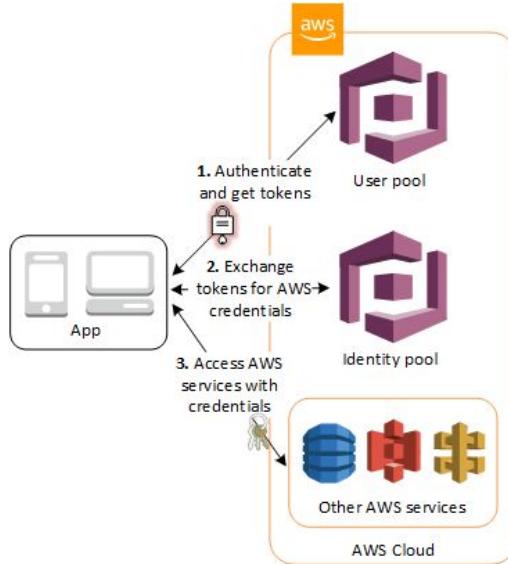


Amazon Cognito

Federation

Basics of Cognito

Amazon Cognito provides authentication, authorization, and user management service for your web and mobile apps.



Sample Use-Case

Alice is a mobile developer in a start-up organization. They have begun with mobile wallet system, and there are specific requirements as follows:

- Users should be able to sign-up with new credentials.
- User should be able to sign-in with social platforms like FB, Twitter, Google.
- There should be a post sign-up process (one-time password) for verification.
- Multi-Factor authentication should be present.
- Account recovery feature should be present.

In-Short: Build a Complete Authentication & Authorization System

Amazon Cognito

At a high level, there are two major features under Amazon Cognito

- i) User Pools
- ii) Identity Pools

Cognito user pool takes care of the entire authentication, authorization process .

Identity pool provides the functionality of federation for users in user pools.

Identity Pool

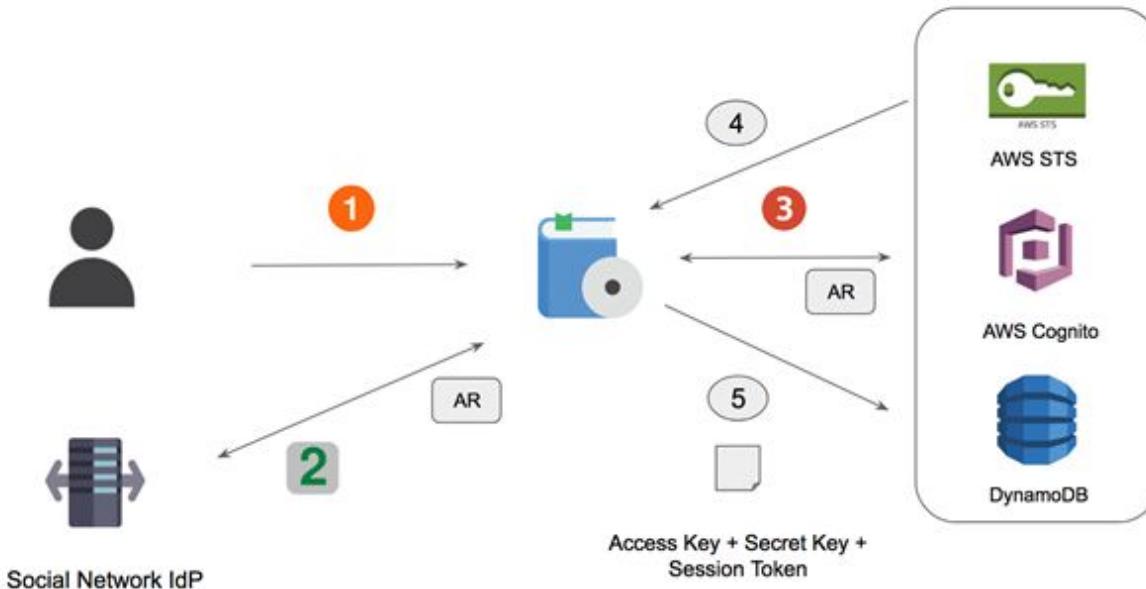
Cognito Identity pools also referred to as AWS Cognito Federated Identities allows developers to authorize the users of the application to use various AWS services.

Use-Case:

We have a quiz based mobile application. At the end of quiz, user's results should be stored in the DynamoDB table.

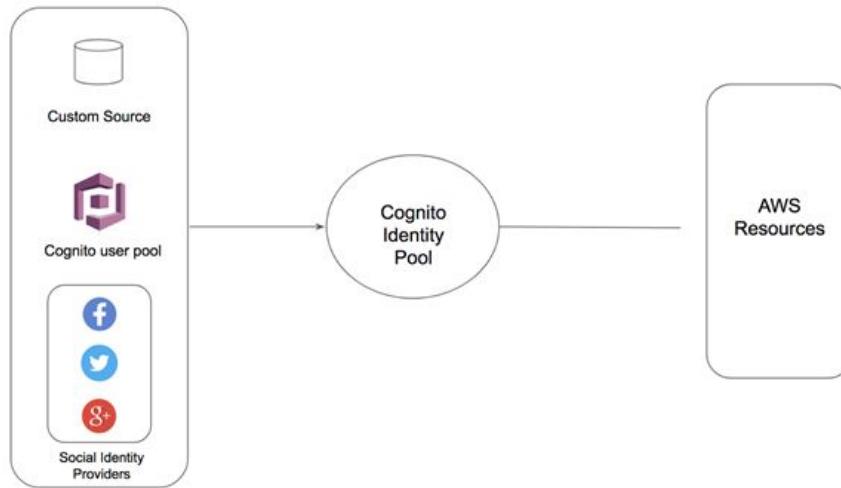
If we hard-code the access/secret keys, chances of reverse engineering are high.

Cognito Identity Pool Working - NO



User Pool vs Identity Pool - NO

The Cognito Identity pool then takes these identities and federates them and then can give secure access to the AWS services regardless of where the user comes from.



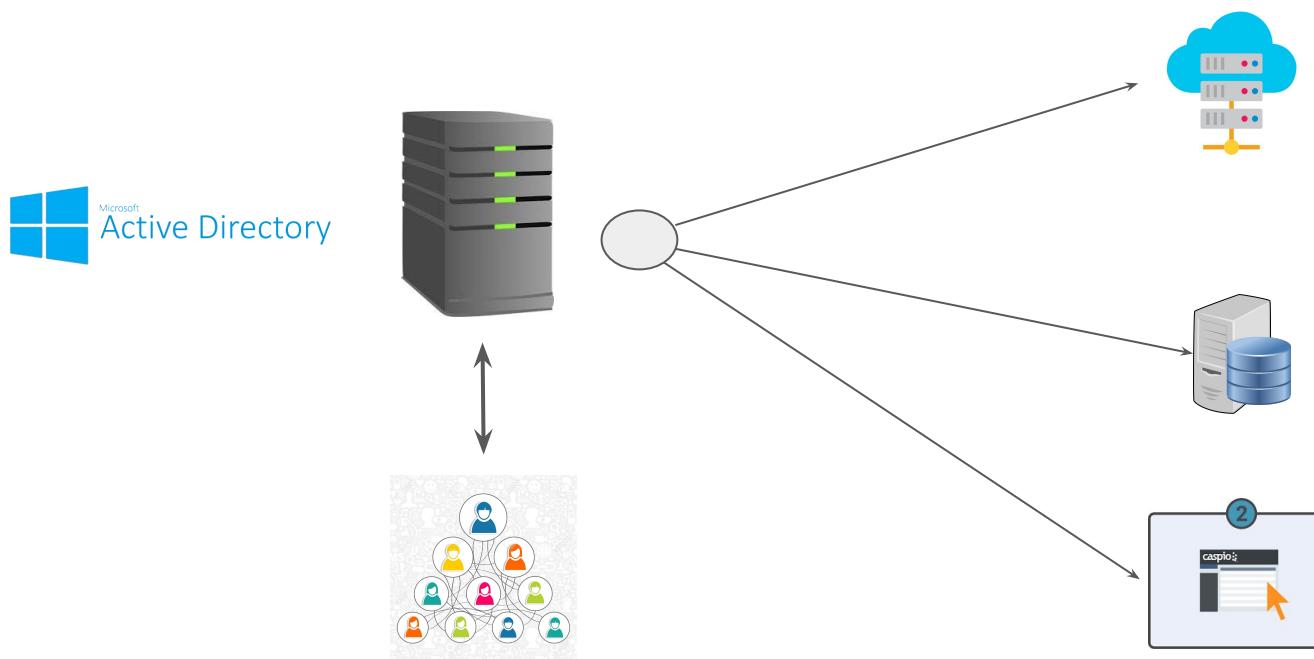
Active Directory

Directory Service

Traditional Way



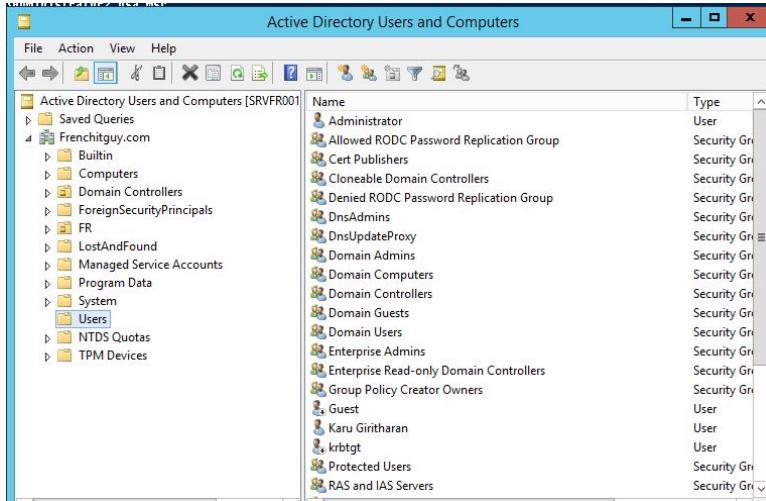
Better Way



Active Directory

Active Directory is one of the most popular directory service developed by Microsoft.

The server running the Active Directory service is called as the domain computer and it can authenticate and authorize the users and computers which are associated to it.

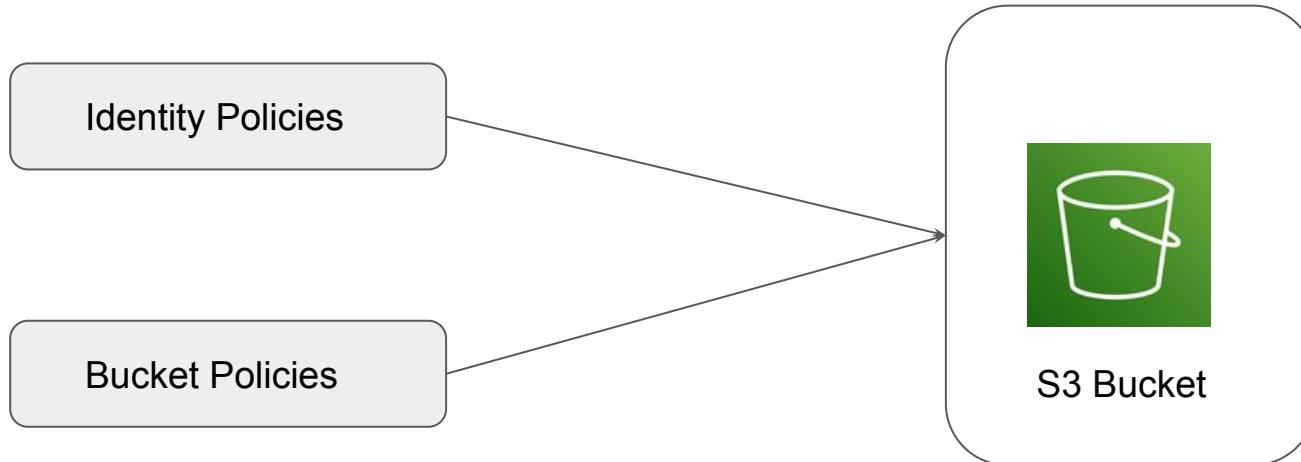


S3 Bucket Policy

Bucket Policies

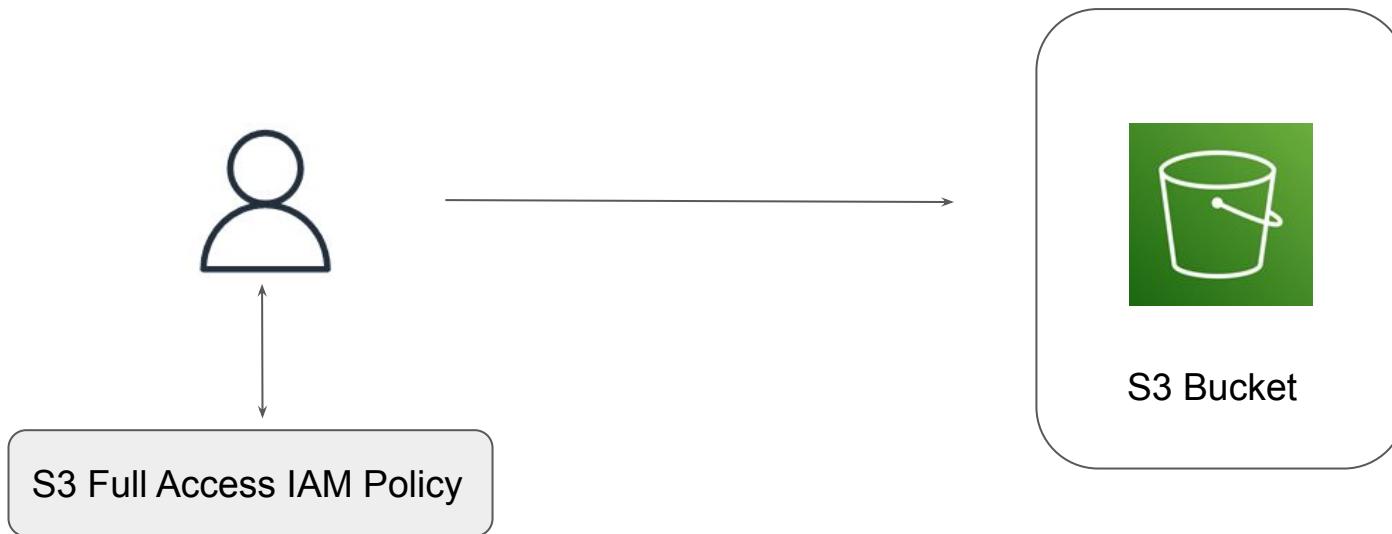
Granting Permission for S3 Resource

There are two primary ways in which a permission to a S3 resource is granted.



Use-Case 1: IAM User Needs Access to S3 Bucket

IAM User Named Bob needs Full Access to S3 Bucket.



Wider Scope of S3 Bucket

Files within the S3 bucket can have scope beyond the IAM entity.

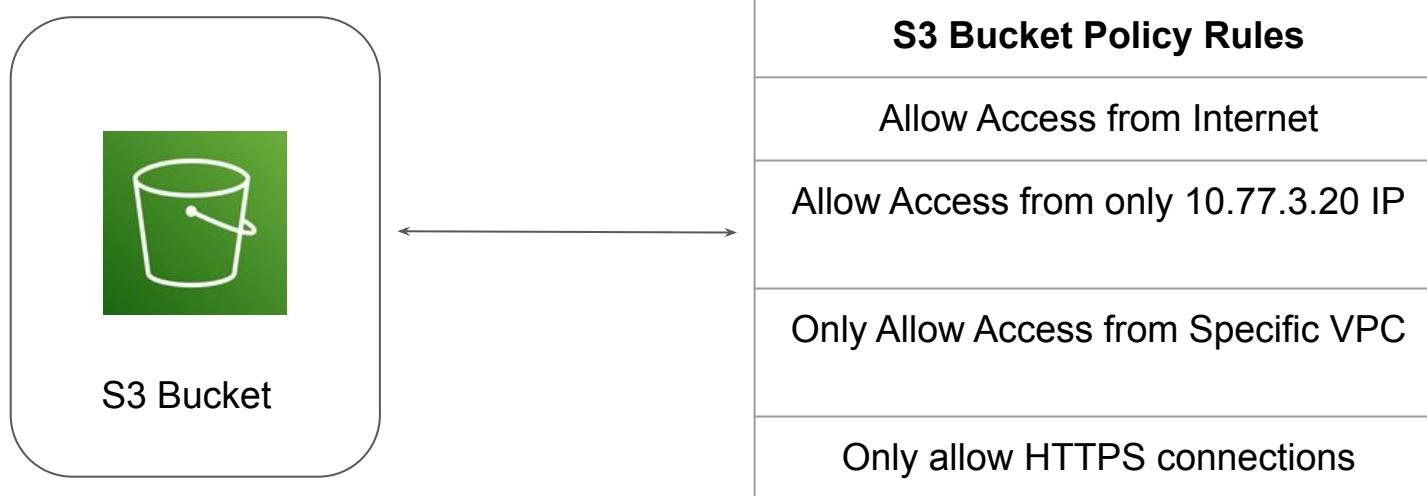
Organization can host entire websites in S3 Bucket.

S3 Buckets can even be used to host central files for download.



S3 Bucket Policy

A bucket policy is a resource-based AWS IAM policy associated with the S3 Bucket to control access permissions for the bucket and the objects in it .



Bucket Policy 1 - Public Access

The following example policy grants the s3:GetObject permission to any public anonymous users.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "PublicRead",  
            "Effect": "Allow",  
            "Principal": "*",  
            "Action": ["s3:GetObject"],  
            "Resource": ["arn:aws:s3:::demo-bucket/*"]  
        }  
    ]  
}
```

Bucket Policy 2 - Only HTTPS

Only the HTTPS requests should be allowed. All HTTP requests should be blocked.

```
{  
    "Id": "ExamplePolicy",  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowSSLRequests",  
            "Action": "s3:GetObject",  
            "Effect": "Allow",  
            "Resource": [  
                "arn:aws:s3:::demo-bucket/*"  
            ],  
            "Condition": {  
                "Bool": {  
                    "aws:SecureTransport": "true"  
                }  
            },  
            "Principal": "*"  
        }  
    ]  
}
```

Regaining Access to Locked S3 Bucket

Cloud Storage is Saviour

Lockout of S3 Bucket

With a S3 Bucket policy that is configured incorrectly, all the IAM users can be locked out.

The screenshot shows the AWS S3 console interface. The top navigation bar includes tabs for Objects, Properties, Permissions, Metrics, Management, and Access Points. The 'Objects' tab is selected. Below the tabs, there's a section titled 'Objects' with a sub-instruction: 'Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)'.

Below this are several action buttons: Copy S3 URI, Copy URL, Download, Open, Delete, Actions (with a dropdown arrow), Create folder, and Upload. There's also a search bar labeled 'Find objects by prefix' and a 'Show versions' toggle.

The main table header includes columns for Name, Type, Last modified, Size, and Storage class. A red-bordered callout box at the bottom left of the table area contains an error message: 'Insufficient permissions to list objects'. It includes a red circular icon with a white 'X' and the text 'After you or your AWS administrator have updated your permissions to allow the s3>ListBucket action, refresh the page. Learn more about [Identity and access management in Amazon S3](#)'.

Bucket Policy - Restriction by IP

Only allow request from a specific IP Address.

```
{  
    "Version": "2012-10-17",  
    "Id": "S3PolicyId1",  
    "Statement": [  
        {  
            "Sid": "IPAllow",  
            "Effect": "Deny",  
            "Principal": "*",  
            "Action": "s3:*",  
            "Resource": [  
                "arn:aws:s3:::demo-bucket",  
                "arn:aws:s3:::demo-bucket/*"  
            ],  
            "Condition": {"  
                "NotIpAddress": {"aws:SourceIp": "54.240.143.0/24"}  
            }  
        }  
    ]  
}
```

Important Note

Wrong set of S3 Bucket policy will lead to you being locked out of S3 bucket.

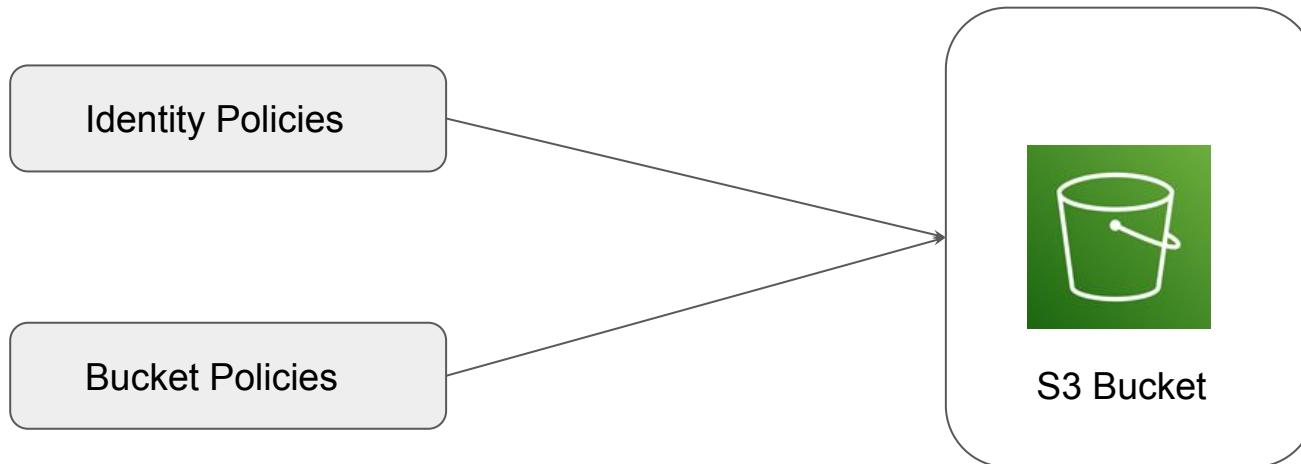
In order to regain the control of S3 bucket, login with ROOT user and delete the Bucket Policy.

S3 Bucket Policy

Bucket Policies

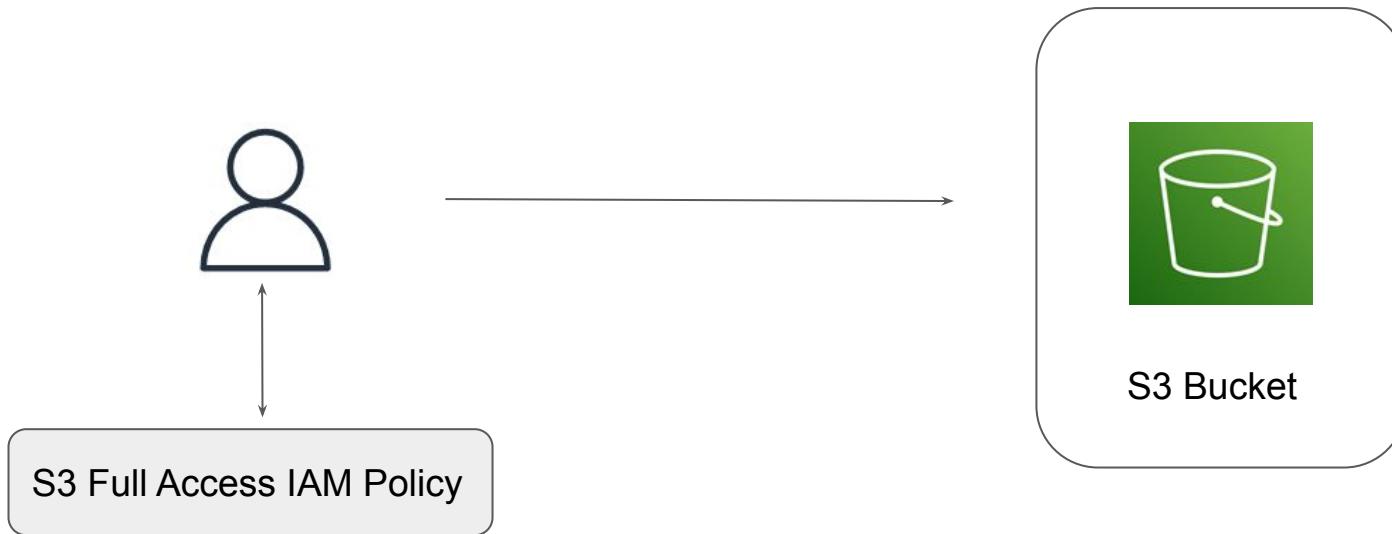
Granting Permission for S3 Resource

There are two primary ways in which a permission to a S3 resource is granted.



Use-Case 1: IAM User Needs Access to S3 Bucket

IAM User Named Bob needs Full Access to S3 Bucket.



Wider Scope of S3 Bucket

Files within the S3 bucket can have scope beyond the IAM entity.

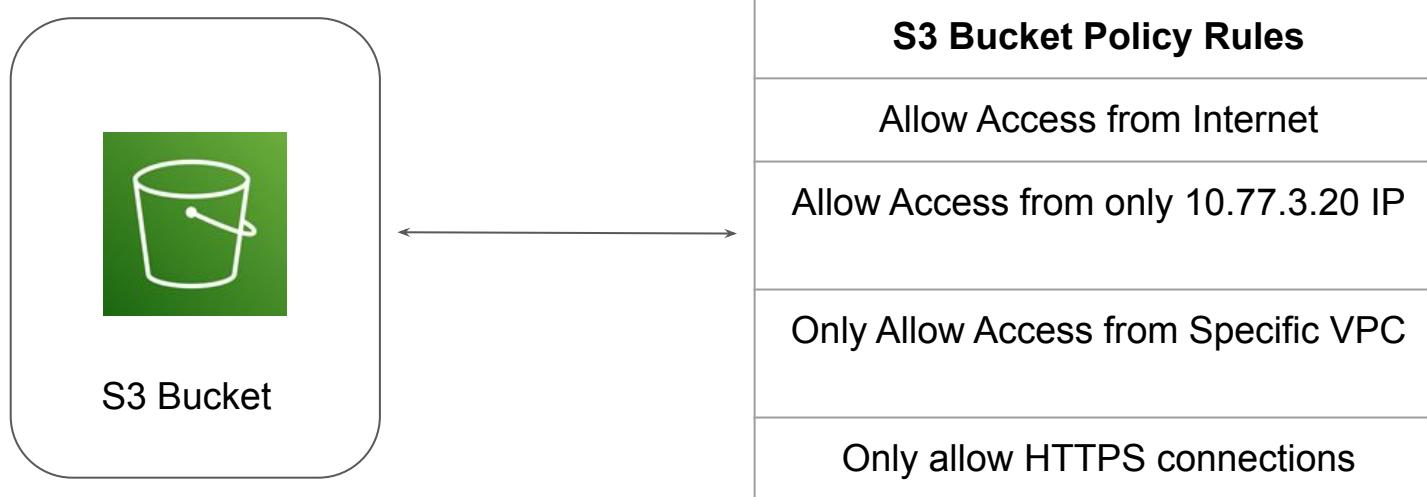
Organization can host entire websites in S3 Bucket.

S3 Buckets can even be used to host central files for download.



S3 Bucket Policy

A bucket policy is a resource-based AWS IAM policy associated with the S3 Bucket to control access permissions for the bucket and the objects in it .



Bucket Policy 1 - Public Access

The following example policy grants the s3:GetObject permission to any public anonymous users.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "PublicRead",  
            "Effect": "Allow",  
            "Principal": "*",  
            "Action": ["s3:GetObject"],  
            "Resource": ["arn:aws:s3:::demo-bucket/*"]  
        }  
    ]  
}
```

Bucket Policy 2 - Only HTTPS

Only the HTTPS requests should be allowed. All HTTP requests should be blocked.

```
{  
    "Id": "ExamplePolicy",  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowSSLRequests",  
            "Action": "s3:GetObject",  
            "Effect": "Allow",  
            "Resource": [  
                "arn:aws:s3:::demo-bucket/*"  
            ],  
            "Condition": {  
                "Bool": {  
                    "aws:SecureTransport": "true"  
                }  
            },  
            "Principal": "*"  
        }  
    ]  
}
```

Regaining Access to Locked S3 Bucket

Cloud Storage is Saviour

Lockout of S3 Bucket

With a S3 Bucket policy that is configured incorrectly, all the IAM users can be locked out.

The screenshot shows the AWS S3 console interface. The top navigation bar includes tabs for Objects, Properties, Permissions, Metrics, Management, and Access Points. The 'Objects' tab is selected. Below the tabs, there's a section titled 'Objects' with a sub-instruction: 'Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)'.

Below this are several action buttons: Copy S3 URI, Copy URL, Download, Open, Delete, Actions (with a dropdown arrow), Create folder, and Upload. There's also a search bar labeled 'Find objects by prefix' and a 'Show versions' toggle. At the bottom, there's a table header with columns: Name, Type, Last modified, Size, and Storage class.

A prominent error message box is displayed at the bottom left, containing a red circular icon with a white 'X', the text 'Insufficient permissions to list objects', and a explanatory note: 'After you or your AWS administrator have updated your permissions to allow the s3>ListBucket action, refresh the page. Learn more about [Identity and access management in Amazon S3](#)'.

Bucket Policy - Restriction by IP

Only allow request from a specific IP Address.

```
{  
    "Version": "2012-10-17",  
    "Id": "S3PolicyId1",  
    "Statement": [  
        {  
            "Sid": "IPAllow",  
            "Effect": "Deny",  
            "Principal": "*",  
            "Action": "s3:*",  
            "Resource": [  
                "arn:aws:s3:::demo-bucket",  
                "arn:aws:s3:::demo-bucket/*"  
            ],  
            "Condition": {"  
                "NotIpAddress": {"aws:SourceIp": "54.240.143.0/24"}  
            }  
        }  
    ]  
}
```

Important Note

Wrong set of S3 Bucket policy will lead to you being locked out of S3 bucket.

In order to regain the control of S3 bucket, login with ROOT user and delete the Bucket Policy.

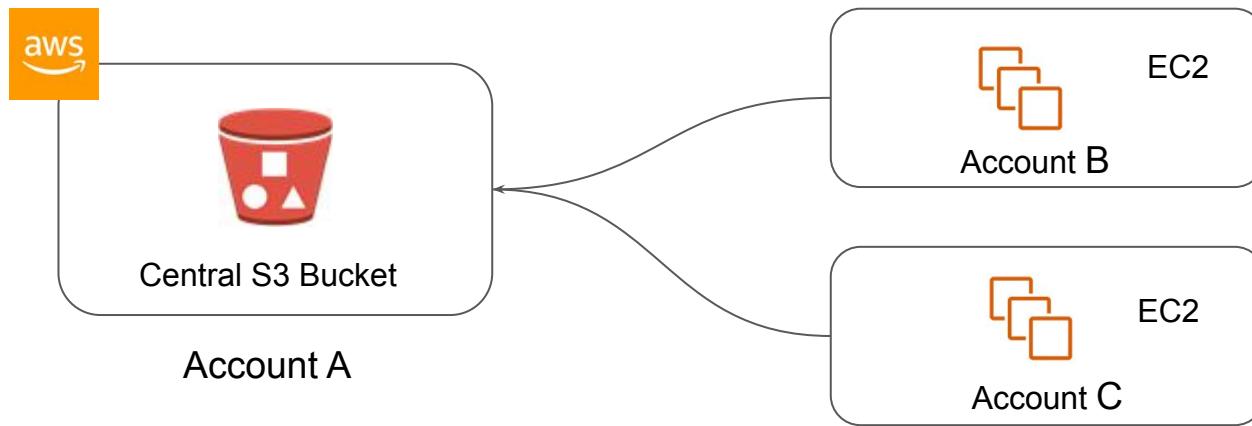
Cross Account S3 Access

Bucket Policies

Cross Account S3 Access

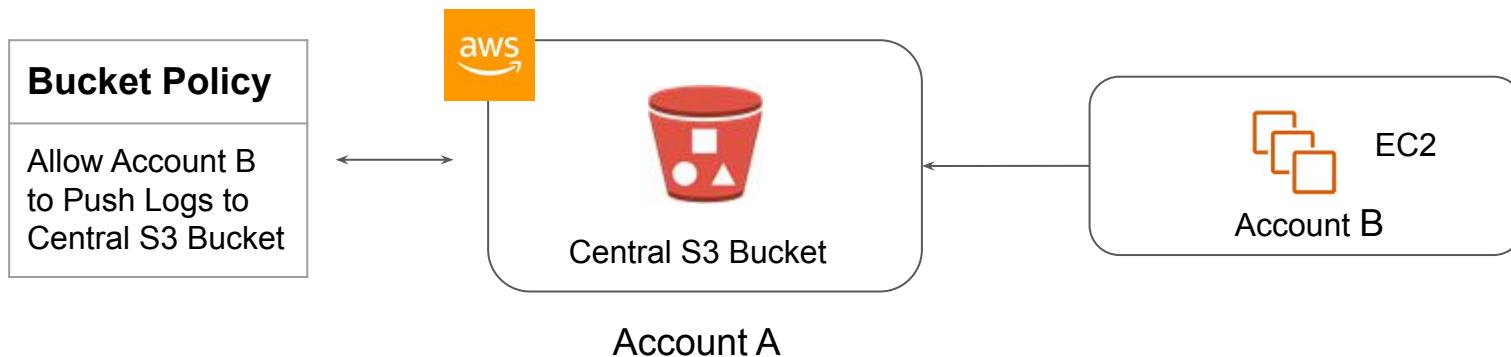
There are many requirements where logs across all AWS accounts need to be stored in a central account.

These logs can include, CloudTrail, CloudWatch, Application Logs, and others.



Creating Bucket Policy

The recommended approach is to add a Bucket Policy in the Central S3 bucket and allow the Account B to push the logs.



Bucket Policy Example - Central S3 Account

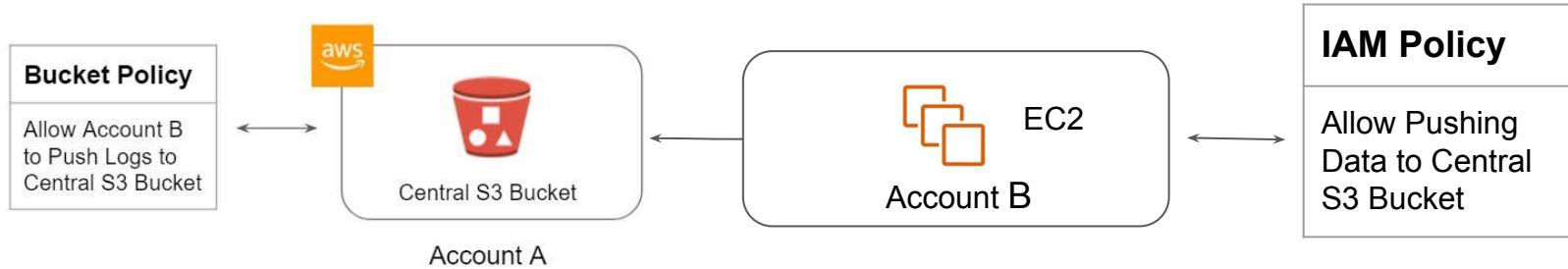
```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "AWS": "arn:aws:iam::453314488441:root"  
            },  
            "Action": [  
                "s3:GetObject",  
                "s3:PutObject",  
                "s3:PutObjectAcl"  
            ],  
            "Resource": [  
                "arn:aws:s3::::central-s3-bucket/*"  
            ]  
        }  
    ]  
}
```

← Account B ARN

← Central S3 Bucket

Part 2- Permission on Account B Side

The resource in the Account B also needs to have permission to push the logs to Central Account S3 Bucket.



IAM Policy - Account B

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "s3:GetObject",  
                "s3:PutObject",  
                "s3:PutObjectAcl"  
            ],  
            "Resource": "arn:aws:s3:::central-s3-bucket/*"  
        }  
    ]  
}
```



Central S3 Bucket

Relax and Have a Meme Before Proceeding

"Excuse me, sir, could yo-"

"NO! I CAN NOT TEACH YOU THIS
KAMEHAMEHA-THING! Why do you
kids keep asking me this?



Canned ACL

Setting Right Bucket Permissions

Understanding S3 Access ACL

Every bucket and it's objects have an ACL associated with them.

When a request is received, AWS S3 will check against the attached ACL to either allow or block access to that specific object.



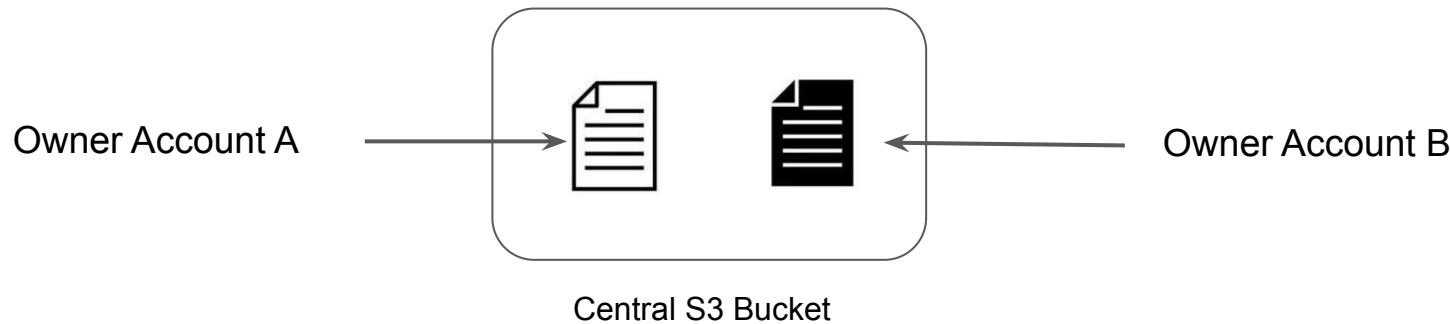
account-a.txt



account-b.txt

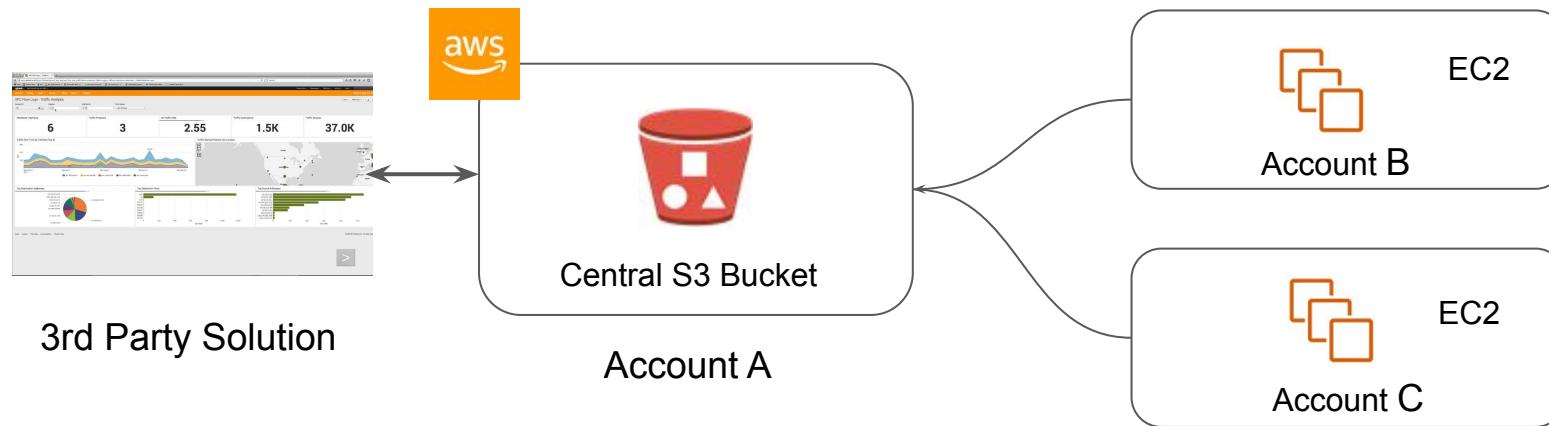
The Tricky Part

When we create a bucket or an object, AWS S3 by default will grant the resource owner full control over the resource.



Ideal Architecture

In most of the architectures, 3rd Party Log Monitoring / SIEM solutions connect to the Central S3 bucket to fetch all of the data.



Canned ACL

AWS S3 supports set of pre-defined grants, known as Canned ACL's.

Each canned ACL has predefined set of permission associated with them.

These canned ACL can be specified in the request using **x-amz-acl** header.

| ACL Name | Description |
|---------------------------|---|
| Private | Owner gets FULL_CONTROL. No one else will have access rights (default) |
| Public-read | Owner has FULL_CONTROL. All others will have public read permission. |
| Bucket-owner-read | Owner of the object has FULL_CONTROL. Bucket owner will get read permissions. |
| Bucket-owner-full-control | Both the object owner and the bucket owner get FULL_CONTROL over the object. |

Presigned URLs

S3 is Awesome

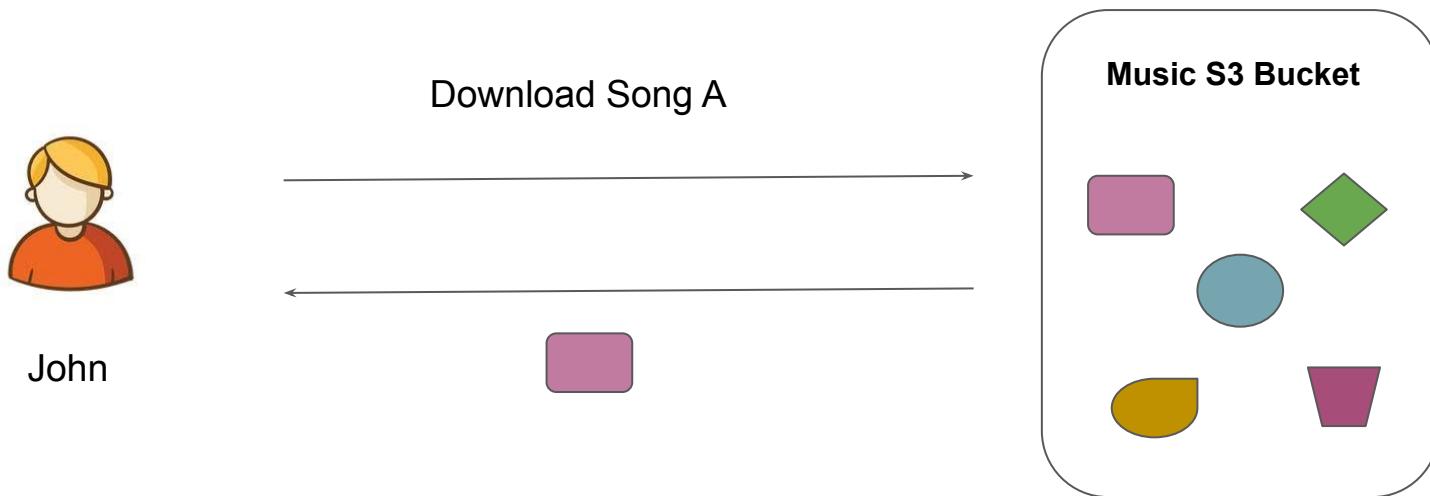
Use Case of Music Company

Company ABC is an online Music selling company. Once the user purchases a song, he should be able to download the song. Your company has decided to store all of its song data in S3 due to its highly durable option.

How will you go ahead with this scenario?



Understand in Graphical Way



Understanding Presigned URL

- All objects in S3 are ‘Private’ by default.
- However Object owner can optionally share objects with others by creating a pre-signed URL to grant time-limited permission to download the object.

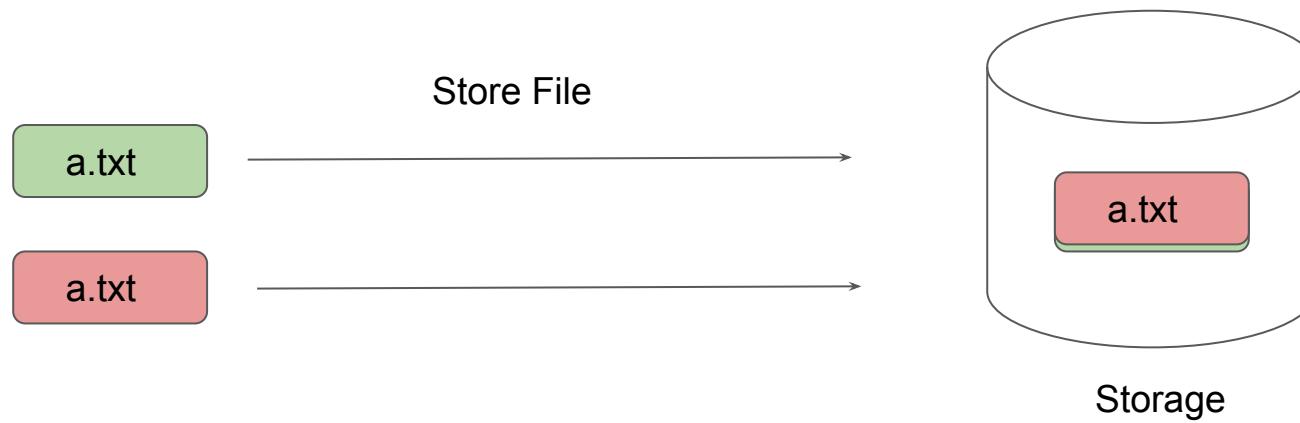
Achieving the Use Case :-

After a user purchases a song and requests to Download, the application should generate a pre-signed URL that will allow the ‘MP3’ file stored in S3 to be downloaded by the user.

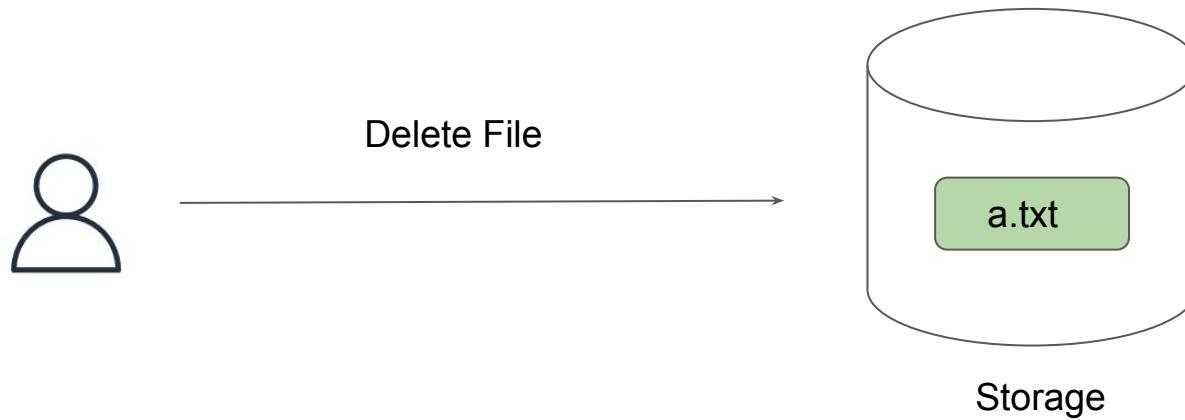
S3 Versioning

Versioning in Object Storage

Challenge 1 - Multiple Object with Same Key



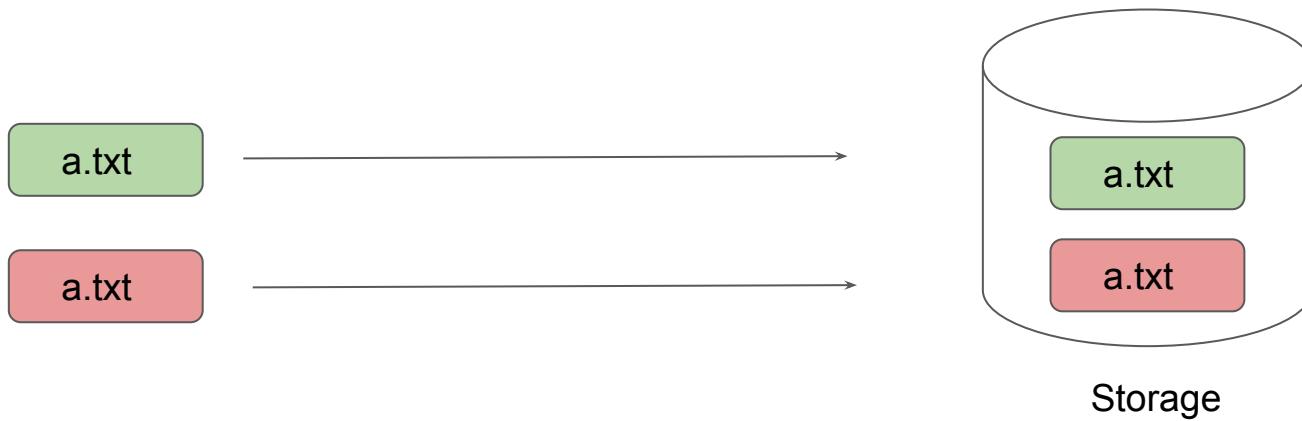
Challenge 2 - Accidental Deletion of Objects



Versioning in Object Storage

Versioning allows users to keep multiple variants of an object in the same S3 bucket.

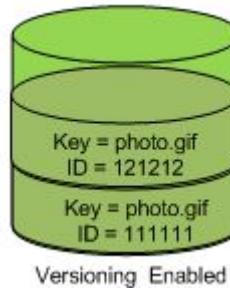
You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket.



Important Pointers for Versioning

Once you version enable a bucket, it can never return to an unversioned state. You can, however, suspend versioning on that bucket.

The versioning state applies to all (never some) of the objects in that bucket.



S3 Batch Operations



Understanding the Basics

S3 Batch Operations lets you **manage billions of objects at scale** with just a few clicks.



Points to Note

To create a job, you give S3 Batch Operations a list of objects and specify the action to perform on those objects.

A batch job performs a specified operation on every object that is included in its manifest.

You can use a comma-separated values (CSV)-formatted [Amazon S3 Inventory](#) report as a manifest, which makes it easy to create large lists of objects located in a bucket

Supported Operations

Some of the supported Batch operations, include:

- Copy objects
- Invoke AWS Lambda function
- Replace all object tags
- Delete all object tags
- Replace access control list
- Restore objects
- S3 Object Lock retention
- S3 Object Lock legal hold
- Replicating existing objects with S3 Batch Replication

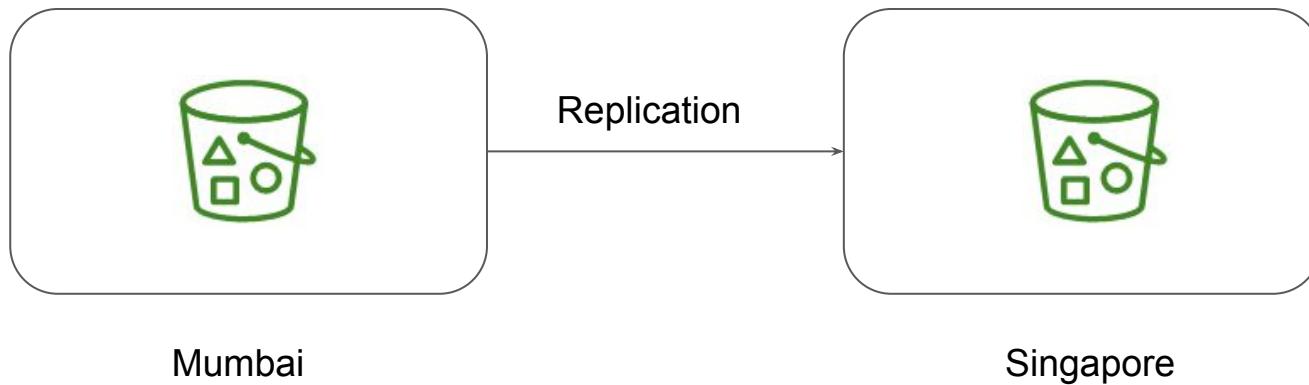
S3 - Cross Region Replication

Storage Service

Understanding the Use-Case

Many compliance has a requirement that the data must be replicated across greater distances.

Cross-Region Replication allows data from S3 buckets to be replicated across regions.



Important Pointers

Both source and destination buckets must have versioning enabled.

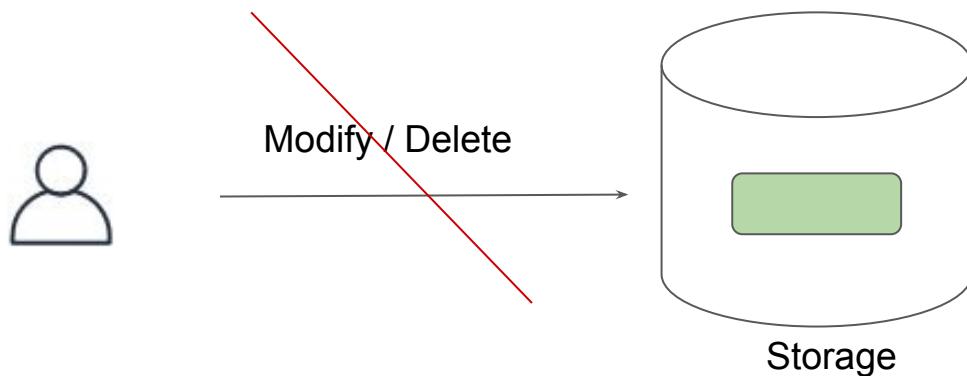
S3 Object Lock

Mastering S3

Overview of WORM

Write once read many (WORM) describes a data storage device in which information, once written, cannot be modified.

This write protection affords the assurance that the data cannot be tampered with once it is written to the device.



Use-Case - Ransomware

Ransomware also blackmail trojans , blackmail software are malicious programs with the help of which an intruder can prevent the computer owner from accessing data, its use or the entire computer system.

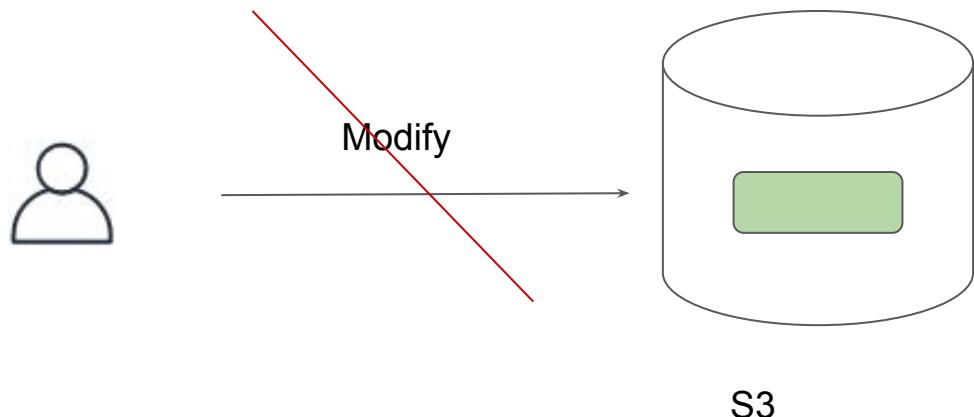
Private data on the foreign computer is encrypted or access to it is prevented in order to demand a ransom for decryption or release.



S3 Object Lock

With S3 Object Lock, you can store objects using a write-once-read-many (WORM) model.

You can use it to prevent an object from being deleted or overwritten for a fixed amount of time or indefinitely.



Retention Modes

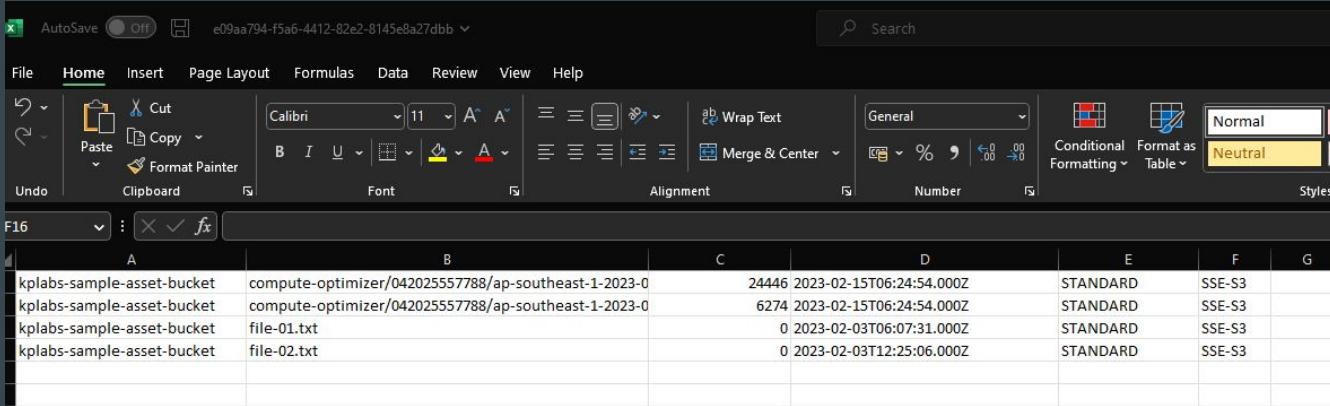
| Retention Mode | Description |
|-----------------|--|
| Governance Mode | When deployed in Governance mode, AWS accounts with specific IAM permissions are able to remove object locks from objects. |
| Compliance Mode | In Compliance Mode, the protection cannot be removed by any user, including the root account. |

Amazon S3 Inventory



Understanding the Basics

Amazon S3 Inventory provides comma-separated values (CSV) of output files that list your objects and their corresponding metadata on a daily or weekly basis for an S3 bucket



The screenshot shows a Microsoft Excel spreadsheet titled "e09aa794-f5a6-4412-82e2-8145e8a27dbb". The ribbon menu is visible at the top, showing tabs for File, Home, Insert, Page Layout, Formulas, Data, Review, View, and Help. The "Home" tab is selected. The main area displays a table of data with columns A through G. The data represents S3 inventory items:

| A | B | C | D | E | F | G |
|----------------------------|--|-------|--------------------------|----------|--------|---|
| kplabs-sample-asset-bucket | compute-optimizer/042025557788/ap-southeast-1-2023-0 | 24446 | 2023-02-15T06:24:54.000Z | STANDARD | SSE-S3 | |
| kplabs-sample-asset-bucket | compute-optimizer/042025557788/ap-southeast-1-2023-0 | 6274 | 2023-02-15T06:24:54.000Z | STANDARD | SSE-S3 | |
| kplabs-sample-asset-bucket | file-01.txt | 0 | 2023-02-03T06:07:31.000Z | STANDARD | SSE-S3 | |
| kplabs-sample-asset-bucket | file-02.txt | 0 | 2023-02-03T12:25:06.000Z | STANDARD | SSE-S3 | |

Inventory List

Following is some of the list of metadata for each listed object that Inventory list contains:

- Bucket name
- Key name
- Version ID
- IsLatest
- Delete marker
- Size
- Last modified date
- Storage class
- Encryption status

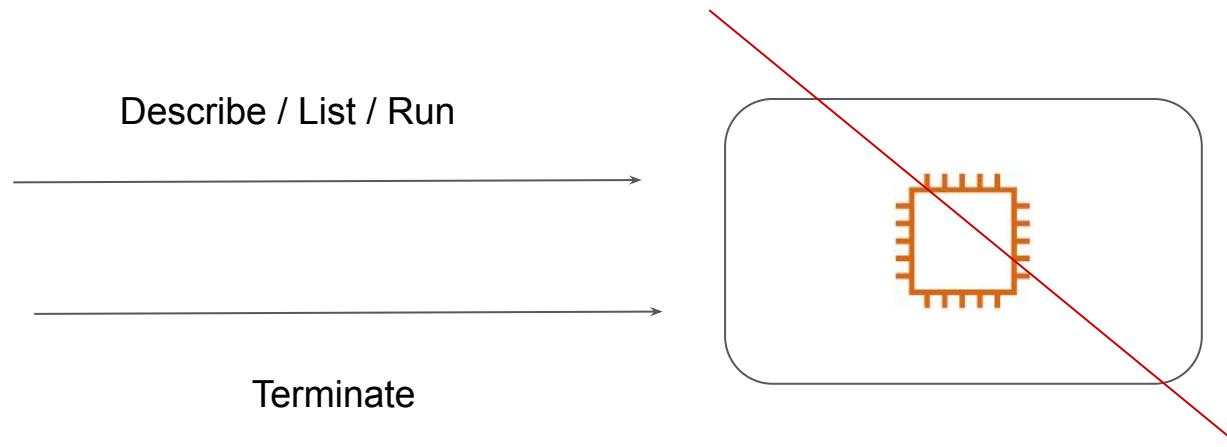
MFA Protected API Access

Enhanced Authentication

Overview of Protected API Access

With IAM policies, you can specify which API operations a user is allowed to call.

For additional security, you can mandate MFA for certain API operation.



Sample MFA based IAM Policy

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Deny",  
            "Action": [  
                "ec2:StopInstances"  
                "ec2:TerminateInstances"  
            ],  
            "Resource": [  
                "*"  
            ],  
            "Condition": {  
                "BoolIfExists": {  
                    "aws:MultiFactorAuthPresent": "false"  
                }  
            }  
        }  
    ]  
}
```

IAM Permissions Boundaries

Advanced IAM

Getting Started

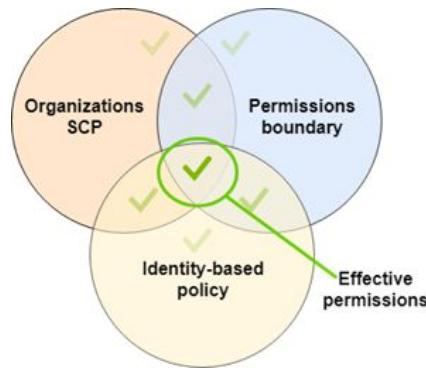
A permissions boundary is an advanced feature in which you use a managed policy to set the maximum permissions that an identity-based policy can grant to an IAM entity.

When you set a permissions boundary for an entity, the entity can perform only the actions that are allowed by both its identity-based policies and its permissions boundaries.

Evaluating Effective Permission with Boundaries

The **effective permissions** for an entity are the permissions that are granted by all the policies associated with the user/role/account.

Within an AWS account, the permissions for an entity **can be affected** by identity-based policies, resource-based policies, permissions boundaries, Organizations SCPs, or session policies.



IAM & S3

Mastering IAM

Overview of S3 Actions

IAM policies are primarily applied at a bucket level and object level.

| Policy Levels | Sample ARN | Description |
|----------------------|-------------------------|----------------------------|
| Bucket Level | ["arn:aws:s3:::demo"] | Operation at bucket level. |
| Object Level | ["arn:aws:s3:::demo/*"] | Operation at object level |

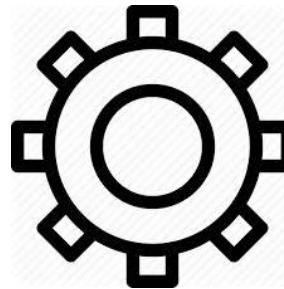
Troubleshooting IAM Policies

Mastering IAM

Let's Troubleshoot

The purpose of this video is to take list of IAM Policies and troubleshoot them to understand why they do not work.

For our demo purpose, we will take example of 5 policies which does not work as intended.



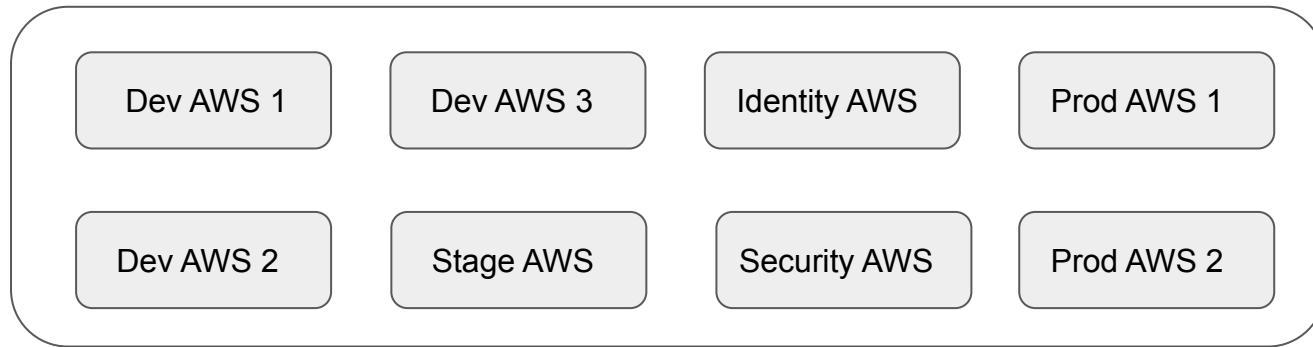
AWS Control Tower

Agility and Governance

Challenges with Multi-Account Environments

Most of the organizations follow a multi-account based architecture.

When the amount of AWS account increases, it leads to own set of challenges.

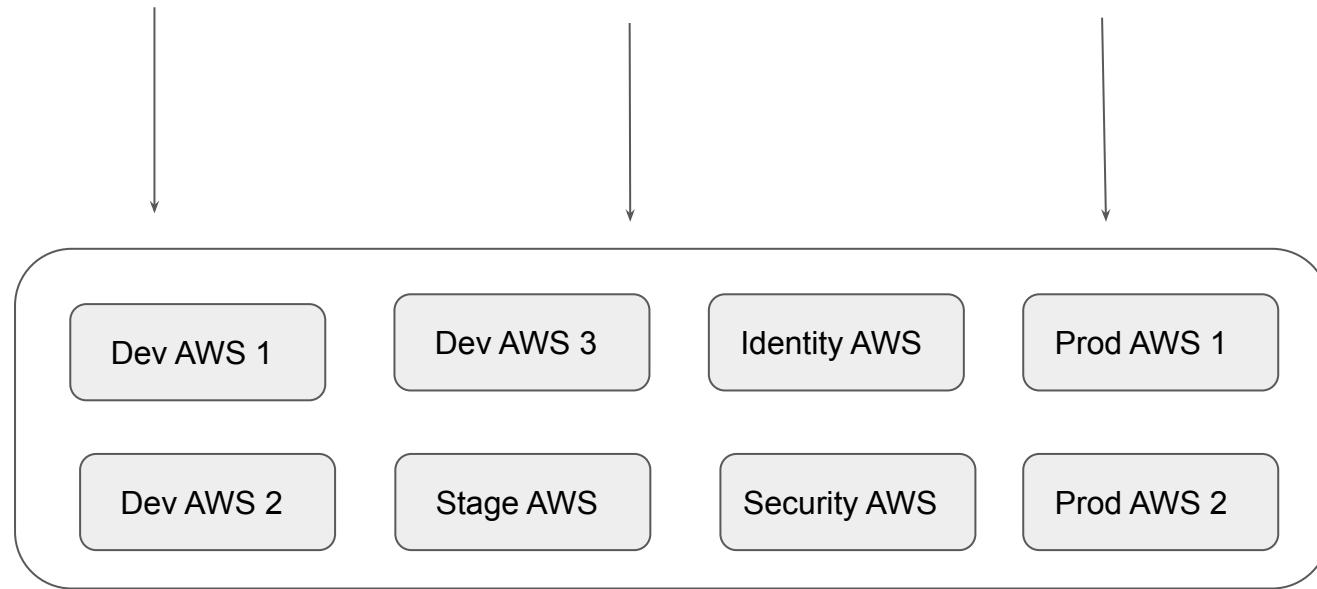


Challenge 1 - Identity Management

username1, password1

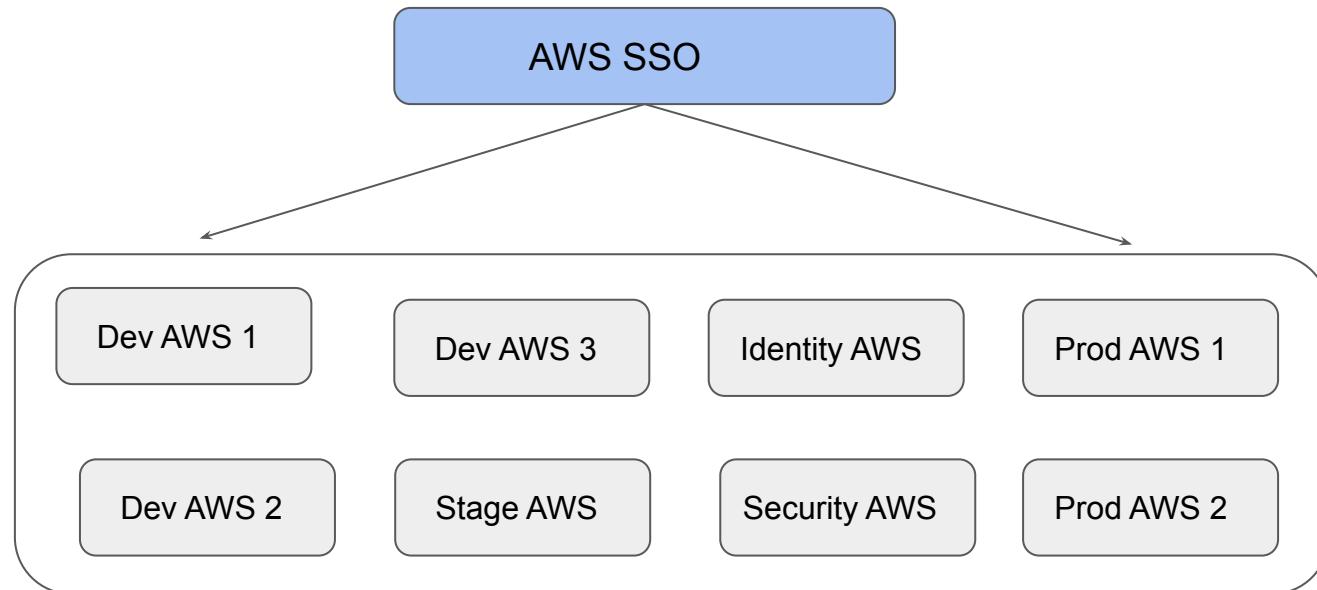
username2, password2

username3 password3



Solution 1 - Single Sign On

Single sign-on (SSO) is an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials.

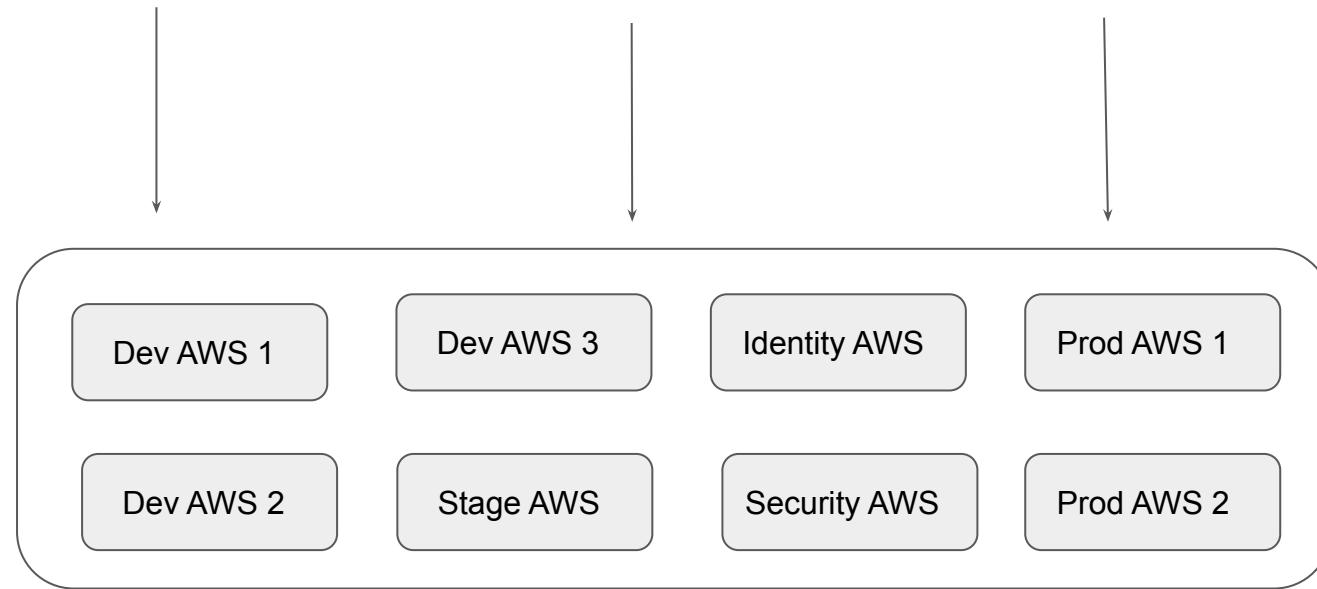


Challenge 2 - Security Hardening

Enable AWS Config

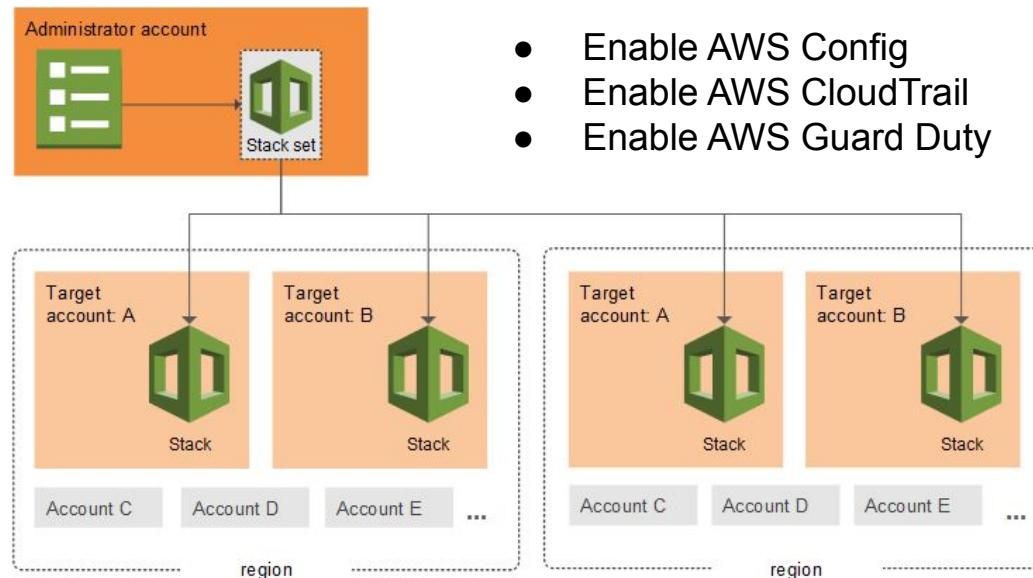
AWS Organizations & SCP

Centralized Logging



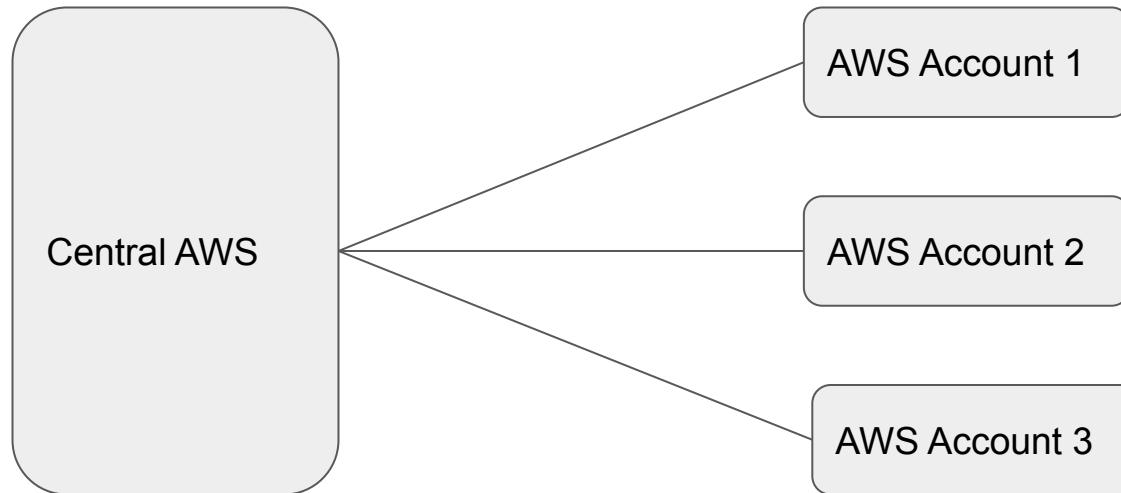
Solution 2 - Security Automation

AWS CloudFormation StackSets allows you to create, update, or delete stacks across multiple accounts and Regions with a single operation



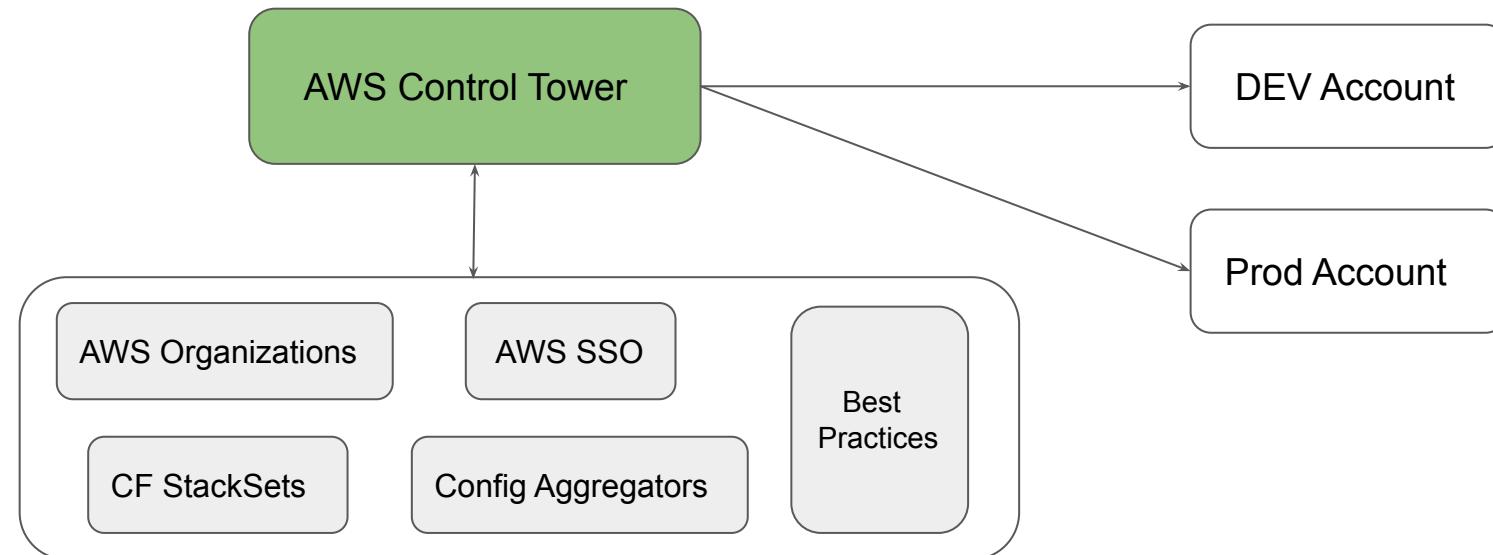
Challenge 3 - Centralized Console

We need to have a centralized console that shows details of all AWS accounts, their security compliance level, and other information



AWS Control Tower

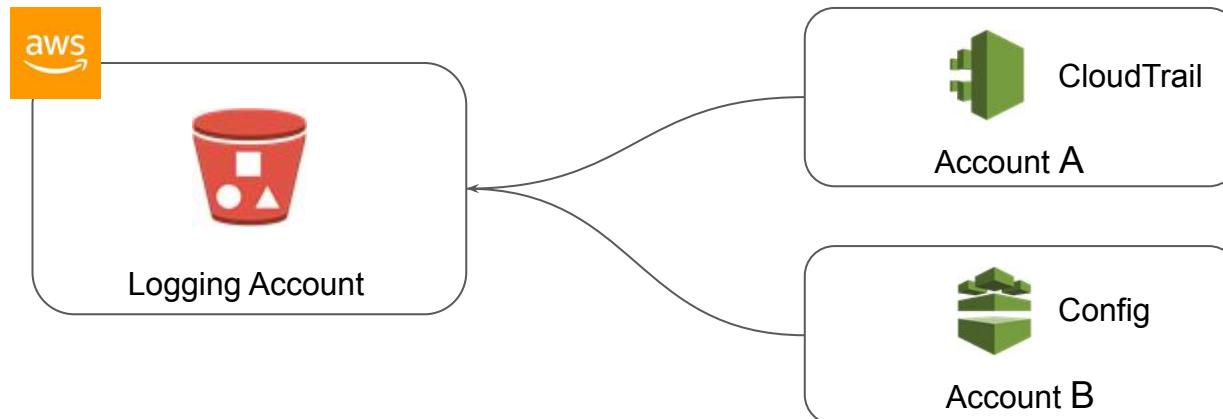
AWS Control Tower offers a straightforward way to set up and govern an AWS multi-account environment, following the best practices.



Centralized Logging

A comprehensive log management and analysis strategy is mission critical in an organization.

It enables the organizations to understand the relationship between operational, security, and change management events and maintain a comprehensive understanding of their infrastructure.

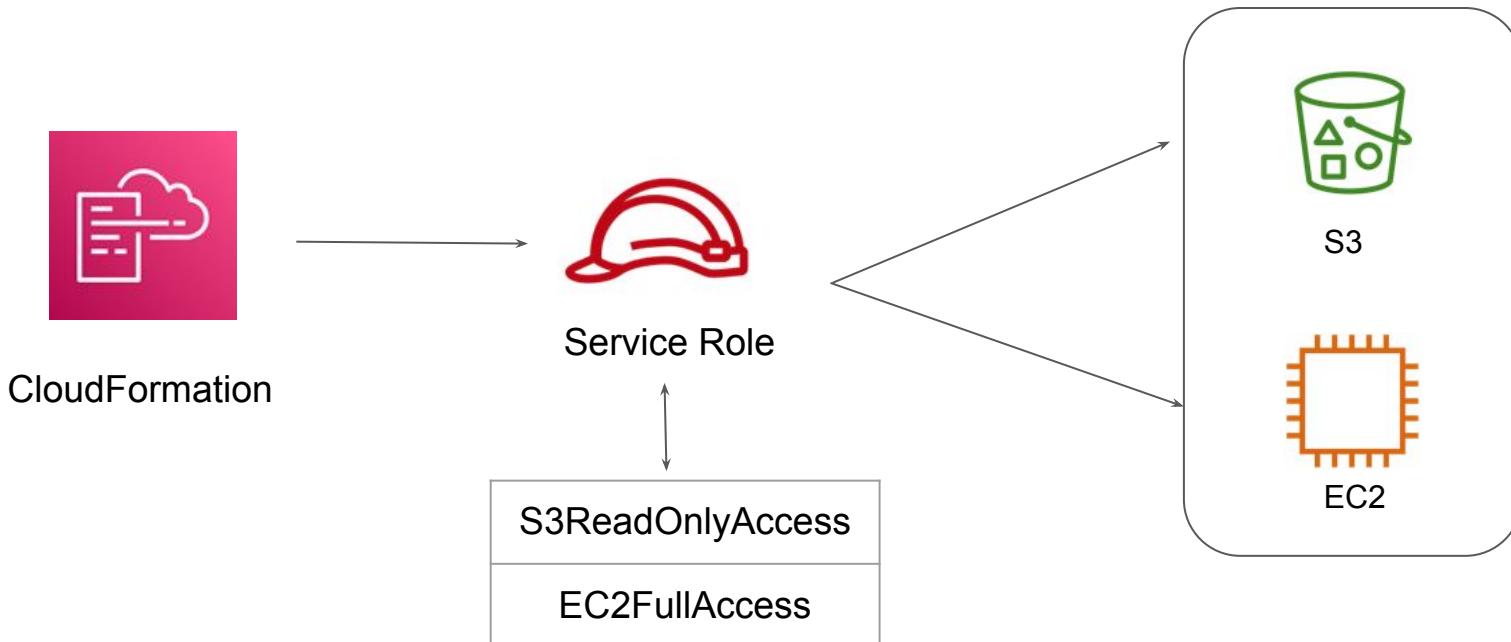


Service Role & Pass Role

[Back to IAM](#)

Overview of Service Roles

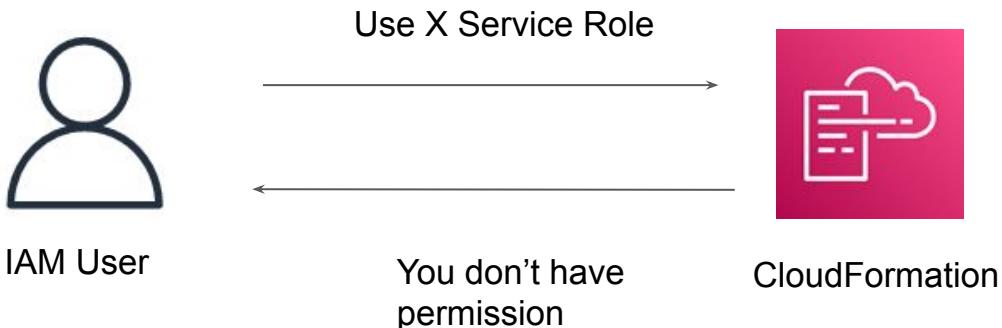
A service role is a role that an AWS service assumes to perform actions on your behalf.



Overview of PassRole

Pass Role allows the service to assume the role and perform actions on your behalf.

To pass a role (and its permissions) to an AWS service, a user must have permissions to pass the role to the service.

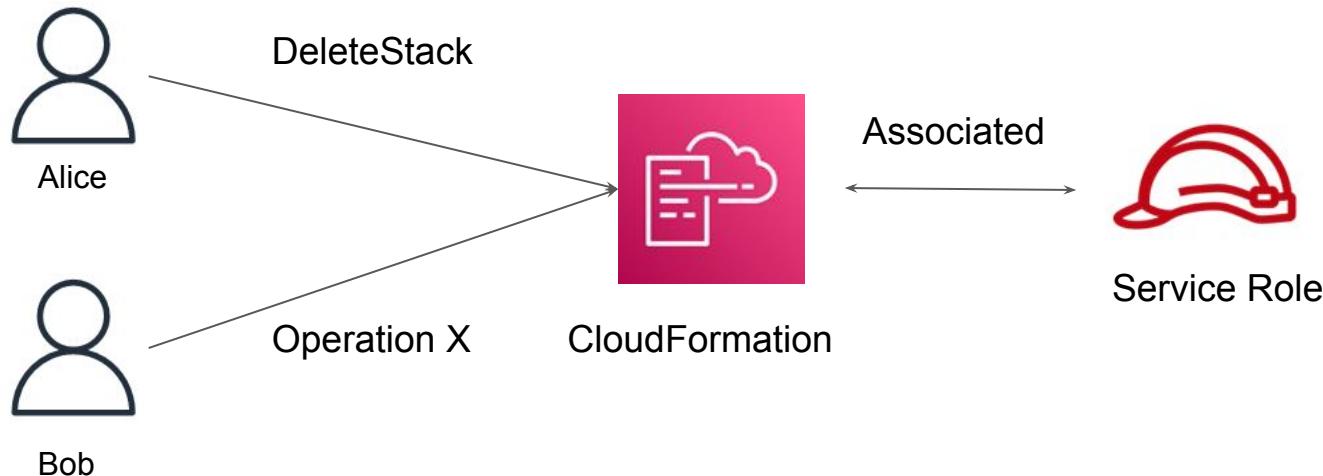


Sample PassRole Policy

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": [  
            "iam:GetRole",  
            "iam:PassRole"  
        ],  
        "Resource": "arn:aws:iam::<account-id>:role/EC2-roles-for-XYZ-*"  
    }]  
}
```

Important Pointer

Once the Role is associated with CloudFormation, other users that have permissions to operate on this stack will be able to use this role, even if they don't have permission to pass it. Ensure that this role grants least privilege.



Policy Example

CloudFormation - iam.yaml

```
Resources:  
  Demo:  
    Type: 'AWS::IAM::Group'  
    Properties:  
      GroupName: DemoGroup
```

Pass Role Policy

```
{  
  "Version": "2012-10-17",  
  "Statement": [{  
    "Effect": "Allow",  
    "Action": [  
      "iam:GetRole",  
      "iam:PassRole"  
    ],  
    "Resource": "arn:aws:iam:<account-id>:role/EC2-roles-for-XYZ-*"  
  }]
```

Amazon Workmail

Mail For AWS

Challenges with Managing Mail Server

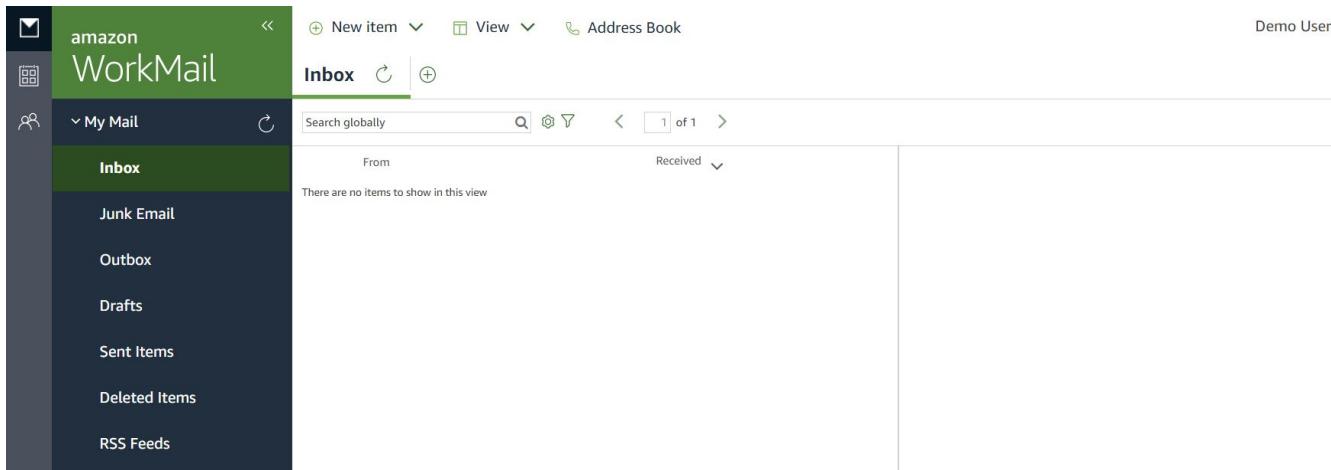
Configuring a Email Server for entire organization is a challenging task.

Various aspects related to Mail Server Configuration, SPAM Detection, Security, High-Availability comes into play.

The screenshot shows a Zimbra webmail interface. The left sidebar contains a navigation menu with links like Mail, Contacts, Calendar, Tasks, Briefcase, and Preferences. Under 'Mail Folders', it lists 'Inbox (3)', 'Sent (2)', 'Drafts', 'Junk (2)', 'Trash', 'Activity Stream (279)', 'Customer Road Trip', 'Personal Info', 'Review Information', 'RSS Feeds', 'Zimbra & S Update', and 'Donna's Inbox (54)'. Below this are sections for Searches, Unread Email, Tags, and Zimlets. The main content area shows an 'Inbox (3)' with three messages from 'Ann Foster' and 'Sam Sample'. One message is selected, showing a detailed view of the email body, attachments, and recipient list. The message body includes several attachments and a link to a Google Doc. The right side of the screen shows a list of 12 messages in the 'Customer Road Trip' folder, dated from August 11, 2014, to August 9, 2014. The messages discuss travel plans, assignments, and meeting locations for a road trip.

Overview of Amazon WorkMail

Amazon Workmail is a secure and managed business email service.



IAM Access Analyzer



Understanding the Basics

AWS IAM Access Analyzer provides the following capabilities:

- IAM Access Analyzer helps identify resources in your organization and accounts that are shared with an external entity.
- IAM Access Analyzer validates IAM policies against policy grammar and best practices.
- IAM Access Analyzer generates IAM policies based on access activity in your AWS CloudTrail logs.

Capability 1 - Identify Shared Resource

IAM Access Analyzer helps you identify the resources in your organization and accounts, such as Amazon S3 buckets or IAM roles, **shared with an external entity**.



Supported Resource Types

IAM Access Analyzer analyzes the following resource types:

- Amazon Simple Storage Service buckets
- AWS Identity and Access Management roles
- AWS Key Management Service keys
- AWS Lambda functions and layers
- Amazon Simple Queue Service queues
- AWS Secrets Manager secrets
- Amazon Simple Notification Service topics
- Amazon Elastic Block Store volume snapshots
- Amazon Relational Database Service DB snapshots
- Amazon Relational Database Service DB cluster snapshots
- Amazon Elastic Container Registry repositories
- Amazon Elastic File System file systems

Points to Note

For each instance of a resource shared outside of your account, IAM Access Analyzer generates a finding

You can review findings to determine if the access is intended and safe or if the access is unintended and a security risk

| Active findings | | | | | | |
|---|---------------------------------------|---|-----------------------------|---------------------------|----------------|-------------------|
| Account ID 042025557788 | | | | | | |
| <input type="text"/> Filter active findings | | | | | | |
| <input type="checkbox"/> | Finding ID | Resource | External principal | Condition | Shared through | Access level |
| <input type="checkbox"/> | 95a5821b-bb83-4dd... | EC2 Snapshot snapshot/snap-02e015523dca9a4de | AWS Account 004417287555 | - | - | Write, Read, List |
| <input type="checkbox"/> | 17834d48-adda-407... | IAM Role Cross-Account-Role | AWS Account 004417287555 | - | - | Write |
| <input type="checkbox"/> | 8bf8920b-36ef-4a65... | S3 Bucket cross-account-demo-s3-bucket | All Principals | Source IP 101.0.63.213/32 | Bucket policy | Read |

Capability 3 - Generate IAM Policy

IAM Access Analyzer analyzes your AWS CloudTrail logs to identify actions and services that have been used by an IAM entity (user or role) within your specified date range.

It then generates an IAM policy that is based on that access activity.

Generate policy for demo-user
Generate a policy based on the CloudTrail activity for this user.

Time period and permissions to analyze CloudTrail events

Select time period

Last 1 day(s)

Specific dates
Choose a range of up to 90 days.

CloudTrail access

CloudTrail trail to be analyzed
Specify the CloudTrail trail that logs events for this account

US East (N. Virginia)

To analyze this role's access activity, IAM uses the service role below on your behalf to access the specified trail.

Create and use a new service role

Use an existing service role
There are no suitable roles existing.

[View permission details](#)

[Cancel](#)

Capability 3 - Generate IAM Policy

IAM Access Analyzer analyzes your AWS CloudTrail logs to identify actions and services that have been used by an IAM entity (user or role) within your specified date range.

It then generates an IAM policy that is based on that access activity.

Generate policy for demo-user
Generate a policy based on the CloudTrail activity for this user.

Time period and permissions to analyze CloudTrail events

Select time period

Last 1 day(s)

Specific dates
Choose a range of up to 90 days.

CloudTrail access

CloudTrail trail to be analyzed
Specify the CloudTrail trail that logs events for this account

US East (N. Virginia)

To analyze this role's access activity, IAM uses the service role below on your behalf to access the specified trail.

Create and use a new service role

Use an existing service role
There are no suitable roles existing.

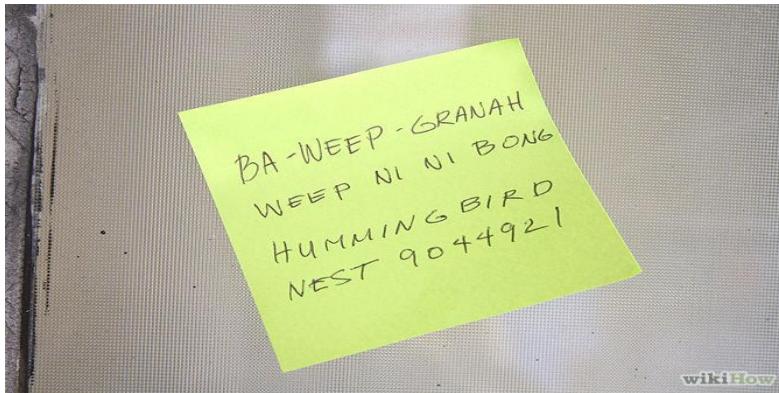
[View permission details](#)

[Cancel](#)

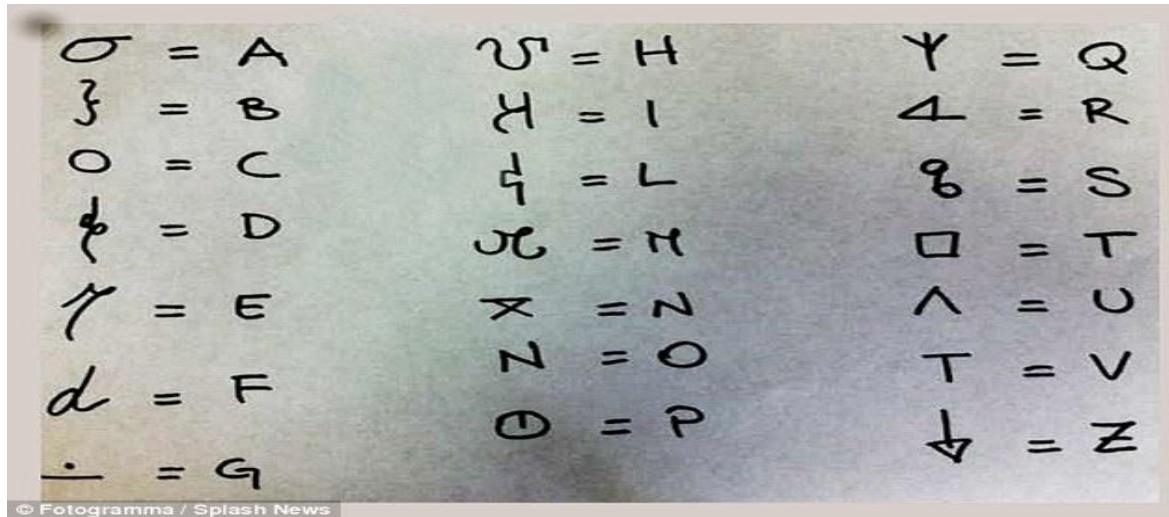
Cryptography

Time to Secret Out

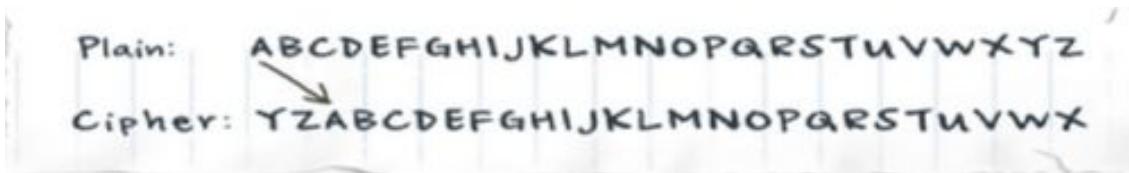
Secret Code Word among Friends



Designing simple encryption



Designing simple encryption



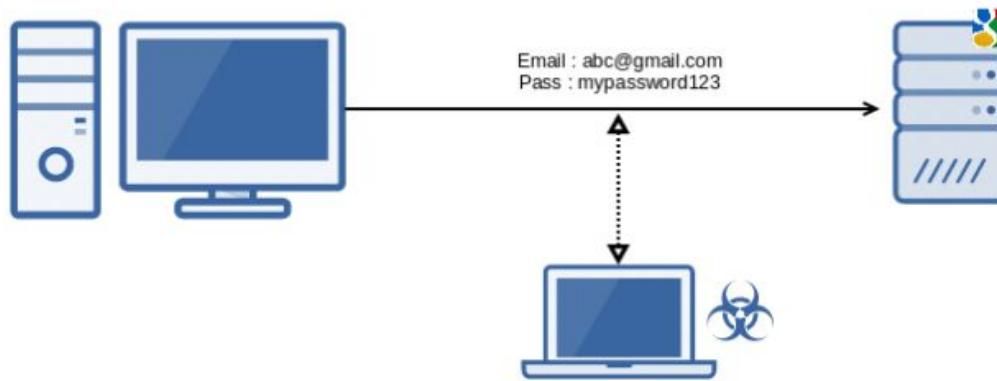
- Normal Password :- MYPASSWORD
- Encrypted PWD :- KWNYQQUMPB

During War times, secret data were always sent in encrypted format.

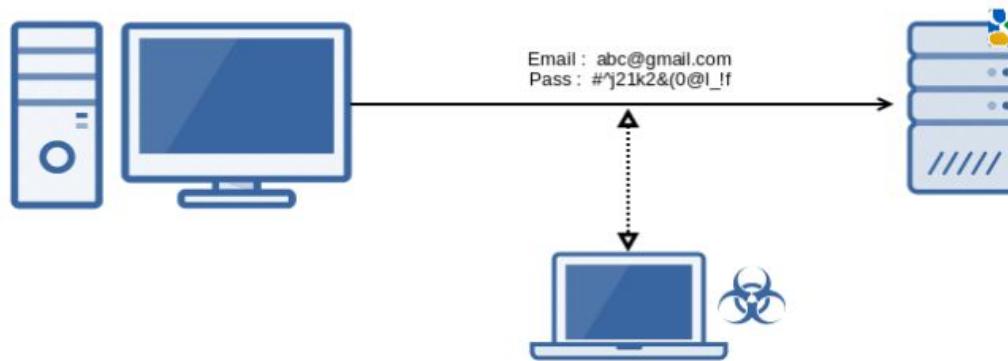
Symmetric Key Encryption



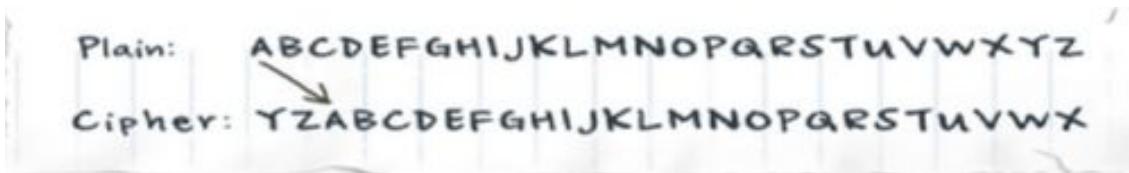
Why Encryption ?



After Encryption



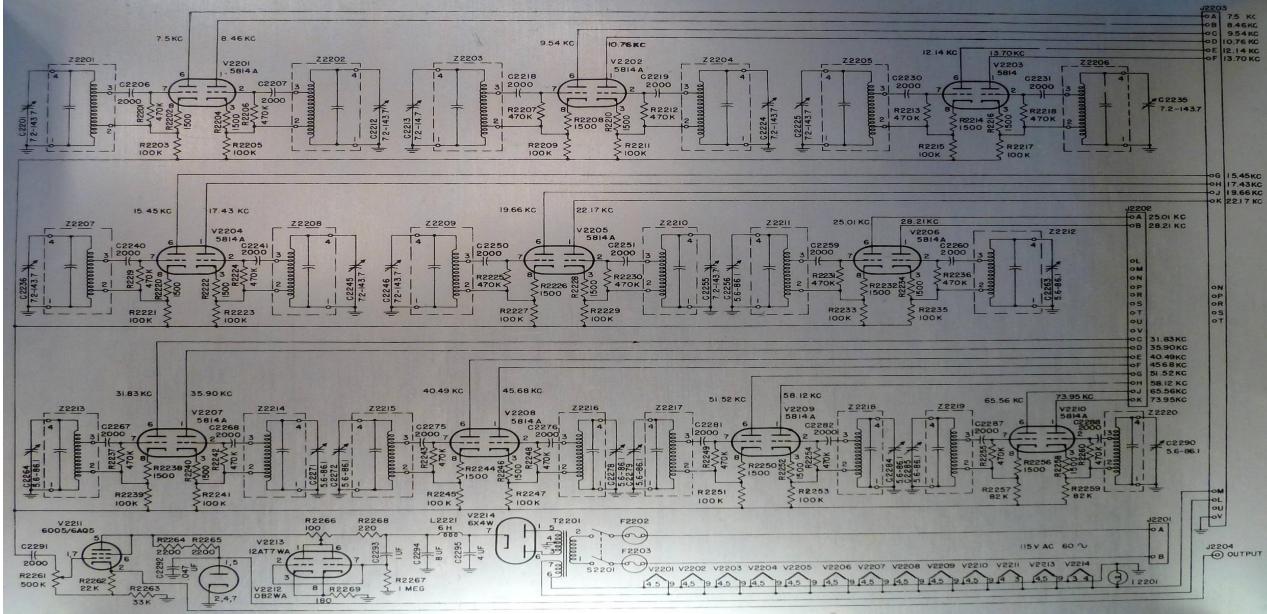
Designing simple encryption



- Normal Password :- MYPASSWORD
- Encrypted PWD :- KWNYQQUMPB

During War times, secret data were always sent in encrypted format.

Algorithms are quite complex

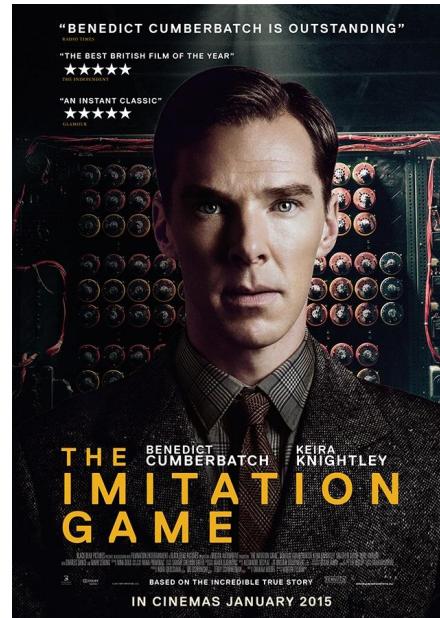


Encryption used during wars - Famous Enigma



Good Movie to watch

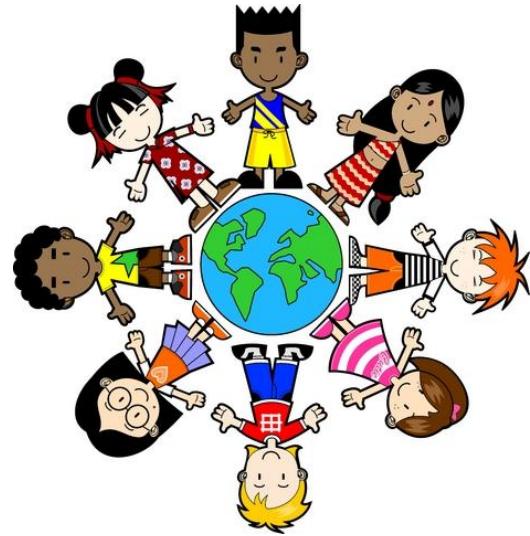
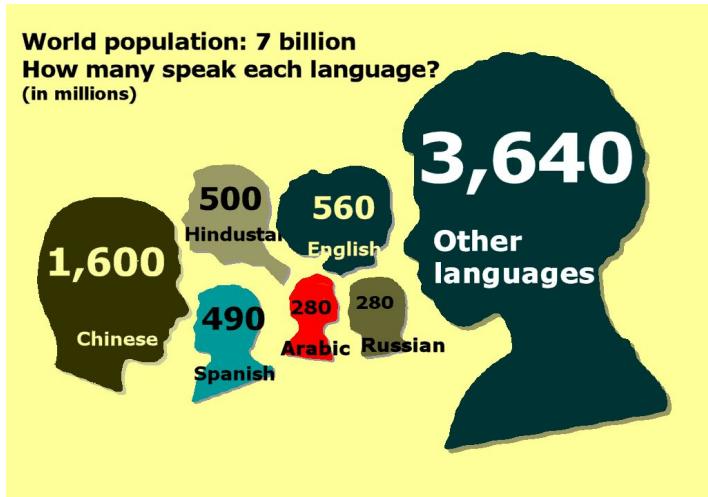
- It is a story about a British mathematician Alan trying to build a machine that would break the german encryption codes.



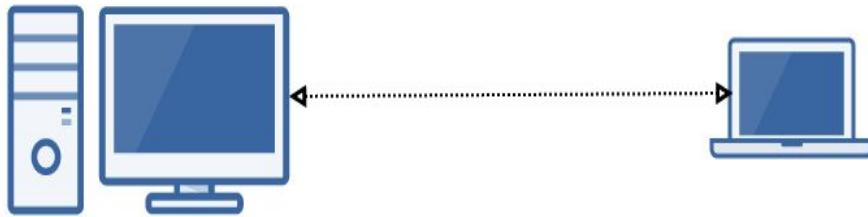
Protocols

Communication

Humans have language to communicate



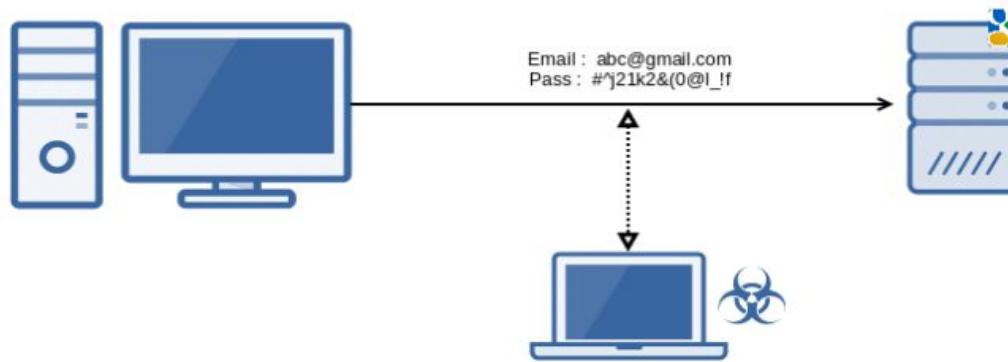
2 computers want to talk to each other







After Encryption



Relax and Have a Meme Before Proceeding

**12-year-old me making
an email I will use
for the rest of my life**



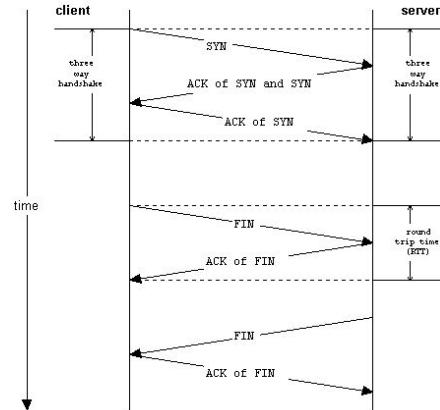
Plain Text vs Encrypted Protocols

Communication

Various Protocols

There are various protocols actively used :

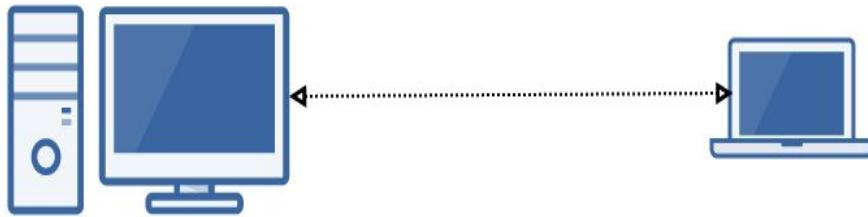
- File Transfer Protocol (FTP)
- Domain Name System Protocol (DNS)
- Transmission Control Protocol (TCP)
- Secure File Transfer Protocol (SFTP)
- Hyper Text Transfer Protocol (HTTP)
- Internet Protocol (IP)



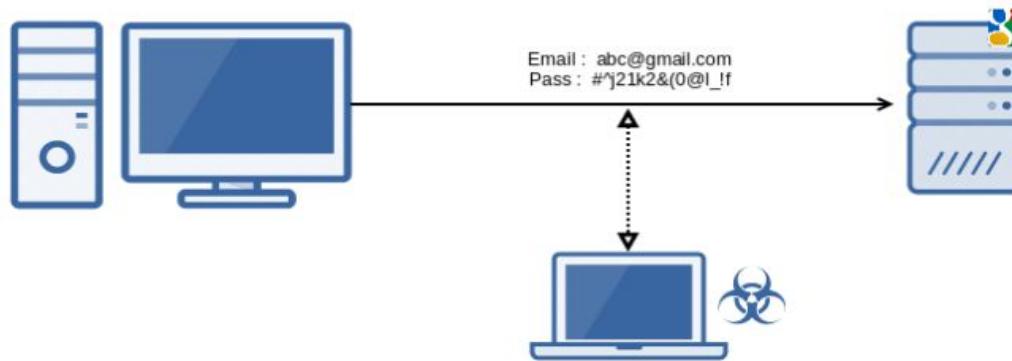
Time line of TCP client-server connection establishment and termination.



2 computers want to talk to each other



After Encryption



CloudHSM

Secure Storage

Amazon CloudHSM

Secure storage for AWS Lambda

Amazon CloudHSM

Storing Expensive House Hold Items

You have an expensive jewellery in your house and you are planning to go on a long vacation.

Where will you prefer to store the jewellery?



Cupboard



Bank Locker

Storing Sensitive Digital Keys

You have sensitive encryption keys that needs to be stored

Where will you prefer to store the keys?



Notepad



Special Security Devices

Special Security Device - HSM

A hardware security module (HSM) is a physical device that provides extra security for sensitive data

This type of device is used to provision cryptographic keys for critical functions such as encryption, decryption and authentication for the use of applications, identities and databases.



Tamper Resistant

- These devices are **tamper resistant**, that means if anyone tries to tamper, they will automatically delete the keys stored.

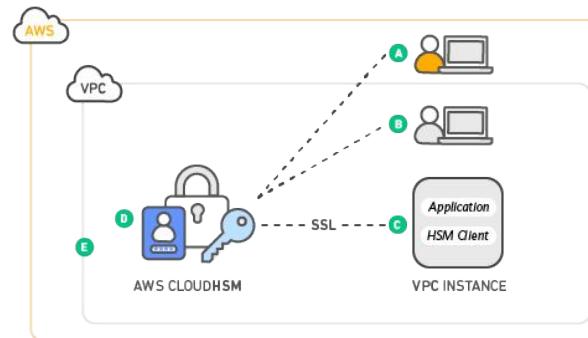


CloudHSM

AWS CloudHSM is a cloud-based hardware security module (HSM).

With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs.

Prior to this, company's had to store HSM on-premise and if infrastructure was on AWS, there were lot of latency involved.



Important Points for Exams

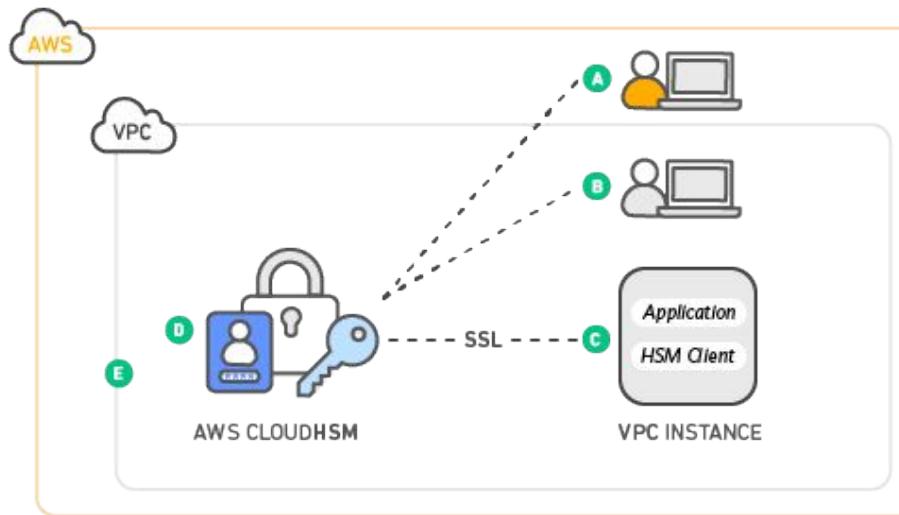
- Cloud HSM is Single Tenanted (Single Physical Device only for you)
 - It must be used within a VPC.
 - We can integrate Cloud HSM with RedShift & RDS for Oracle.
 - For fault tolerance, we will need to build cluster of 2 Cloud HSM.
 - AWS uses Safenet Luna SA HSM appliance for Cloud HSM.
 - They are FIPS validated.
-
- It generally has 2 partitions, one for AWS to monitor and second is cryptographic partition which you have access to and has stored keys.

Important Pointers - CloudHSM

Good For Exams!

Secure VPC Access

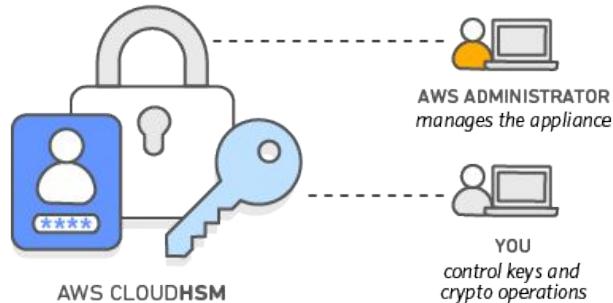
AWS CloudHSM runs in your own Amazon Virtual Private Cloud (VPC), enabling you to easily use your HSMs with applications running on your Amazon EC2 instances



Separation of Duties

Separation of duties and role-based access control is inherent in the design of the AWS CloudHSM.

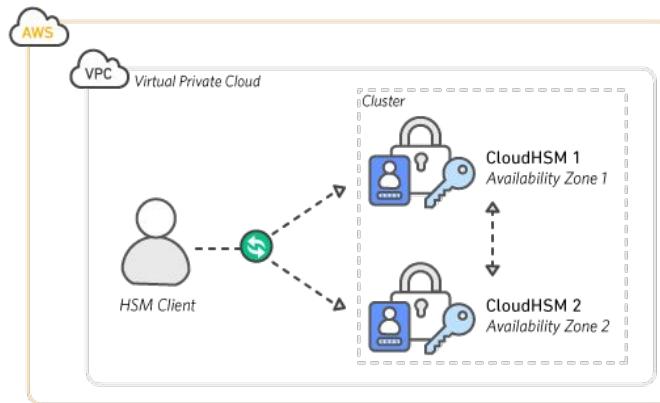
AWS monitors the health and network availability of your HSMs but is not involved in the creation and management of the key material stored within your HSMs.



Load balancing and high availability

AWS CloudHSM automatically load balances requests and securely duplicates keys stored in any HSM to all of the other HSMs in the cluster.

Using at least two HSMs across multiple AZs is Amazon's recommended configuration for availability and durability.



More Important Points

- Cloud HSM is Single Tenanted (Single Physical Device only for you)
- It must be used within a VPC.
- We can integrate Cloud HSM with RedShift & RDS for Oracle.
- They are FIPS validated.

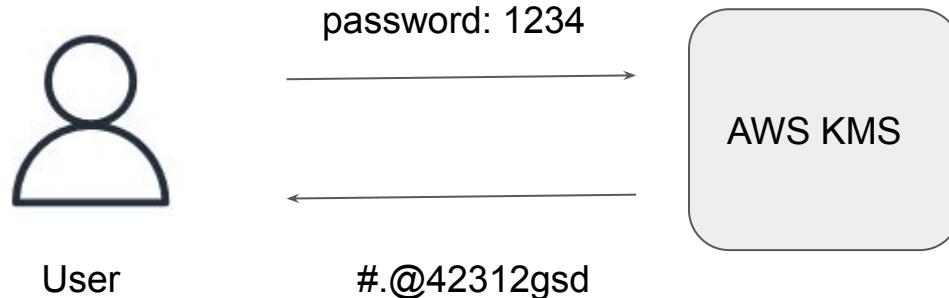
AWS KMS

Do things the right way

Basics of KMS

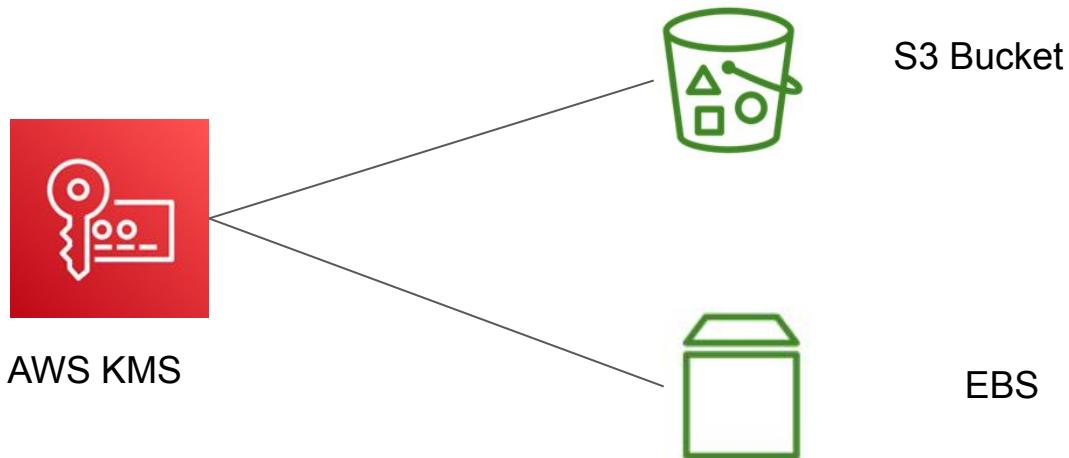
AWS KMS stands for AWS Key Management Service.

This service provides capability to encrypt and decrypt the data.



Integration of KMS

AWS KMS also integrates with various AWS services like S3, DynamoDB, EBS and others.



KMS Practical

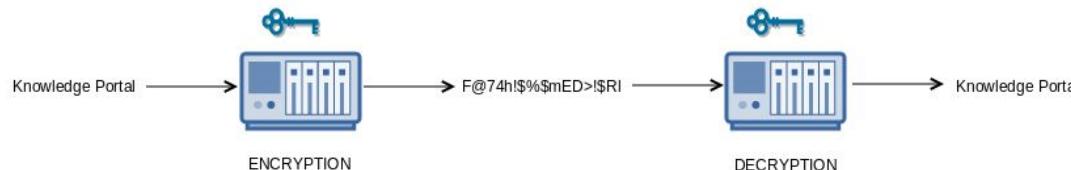
Time to Defend Easily

Revising Cryptography Concepts

Plaintext can refer to anything which humans can understand and/or relate to. This may be as simple as English sentences or even Python code.

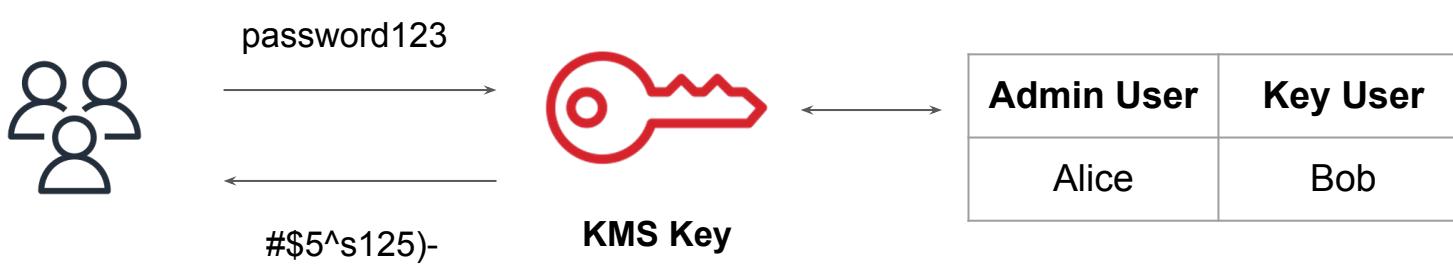
Ciphertext, or encrypted text, is a series of randomized letters and numbers which humans cannot make any sense of.

An encryption algorithm is step by step approach that tells on how the PT will be converted to the CipherText.



KMS Practical Workflow

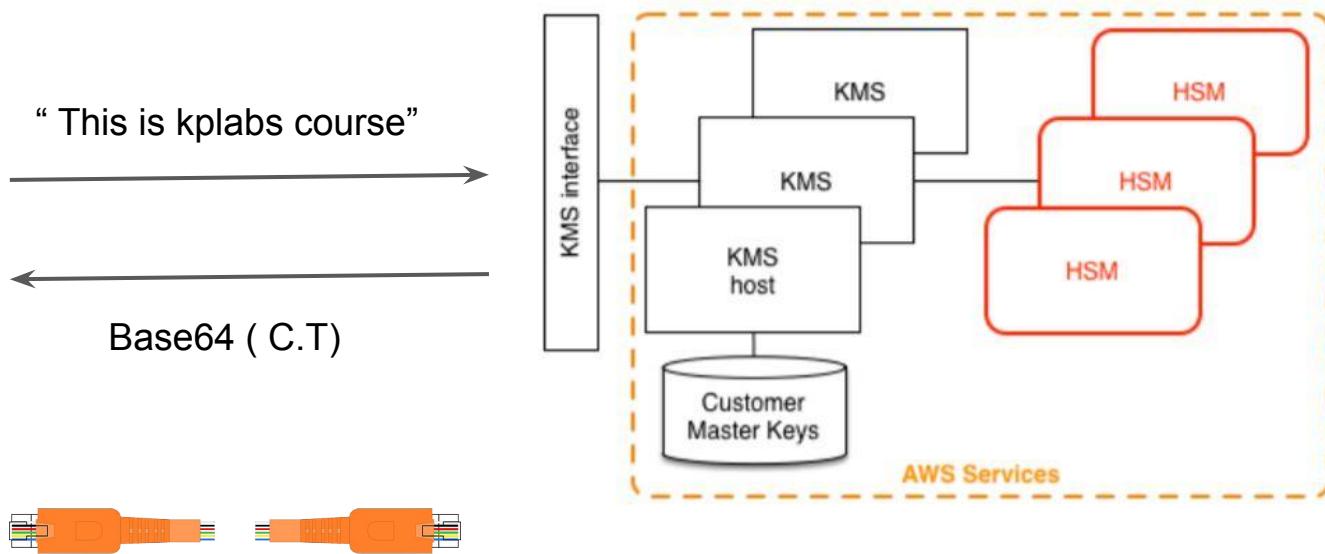
1. Create a Customer Managed Key (CMK)
2. Define the Administrative User & Key User.
3. Encrypt and Decrypt data with the CMK.



KMS Architecture

Let's Scramble

AWS KMS Architecture



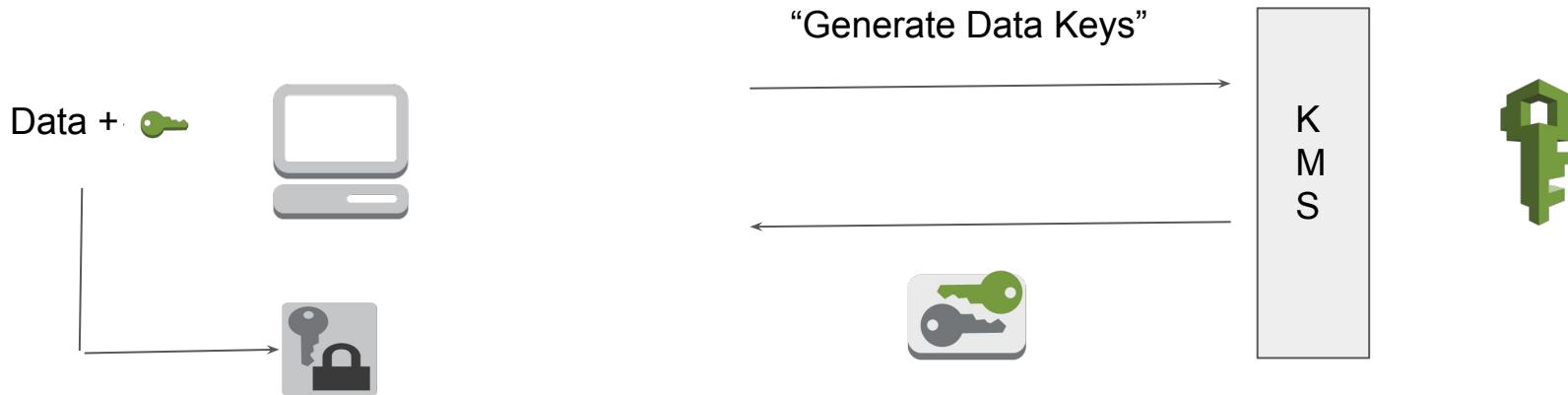
Some of Caveats

- We can encrypt of maximum 4 KB of data with CMK.
- Since data travels over network, there can be latency issue.
- AWS suggested the Customer Master Key + Data Key based approach.



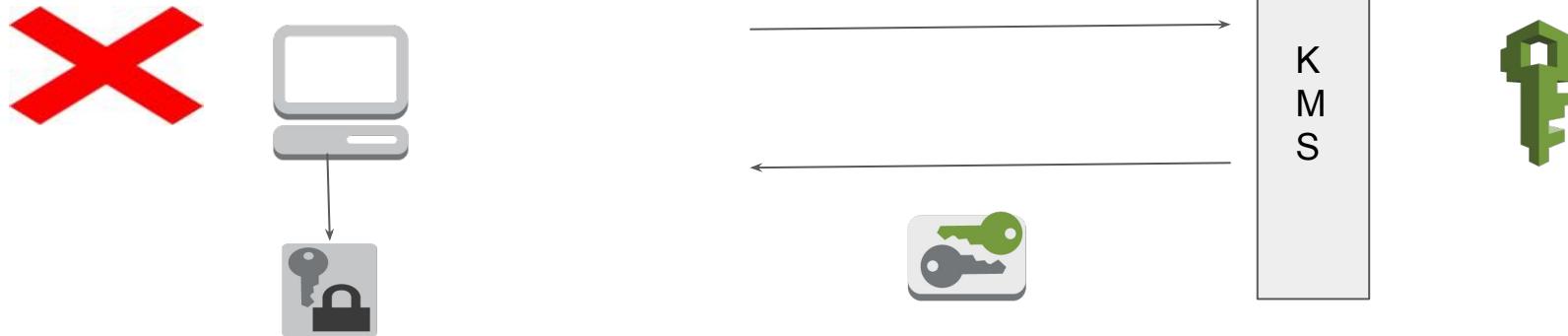
Envelope Encryption

- We generate 1 CMK.
- We then generate the Data Key. AWS returns PT & CT version of it.
- We use the PlainText data key to encrypt the files in server.
- We then store CipherText Data Key along with Encrypted file.



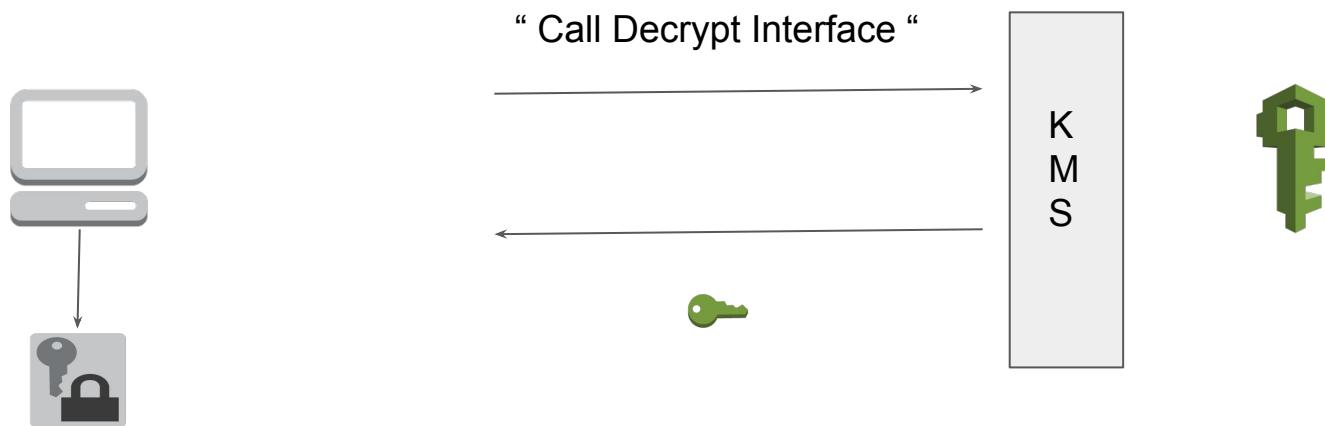
Envelope Encryption

- We generate 1 CMK.
- We then generate the Data Key. AWS returns PT & CT version of it.
- We use the PlainText data key to encrypt the files in server.
- We then store CipherText Data Key along with Encrypted file.



Decryption Steps

- Use the decrypt operation to decrypt the encrypted data key into a plaintext copy of the data key.
- Use the plaintext data key to decrypt data locally.



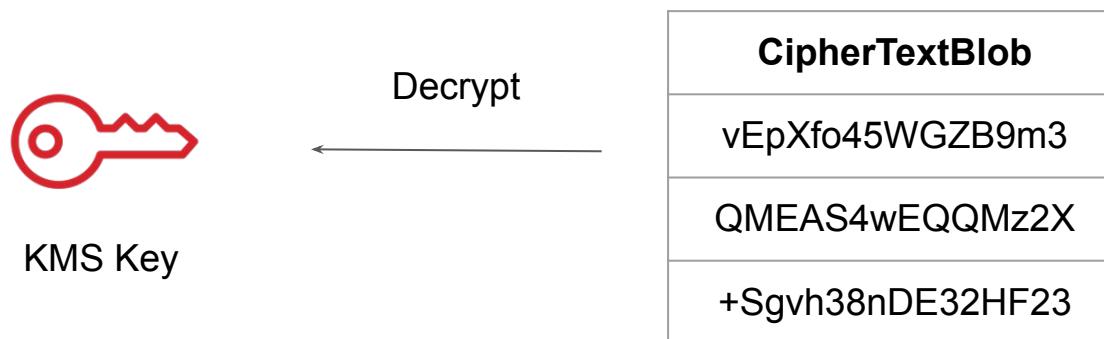
Schedule Key Deletion

Delete the KMS Key

Deleting Key in KMS

Deleting KMS key is destructive and potentially dangerous and an irreversible process.

After a KMS key is deleted, you can no longer decrypt the data that was encrypted under that KMS key, which means that data becomes unrecoverable.



Important Note

You should delete a KMS key only when you are sure that you don't need to use it anymore.

If you are not sure, consider disabling the KMS key instead of deleting it.

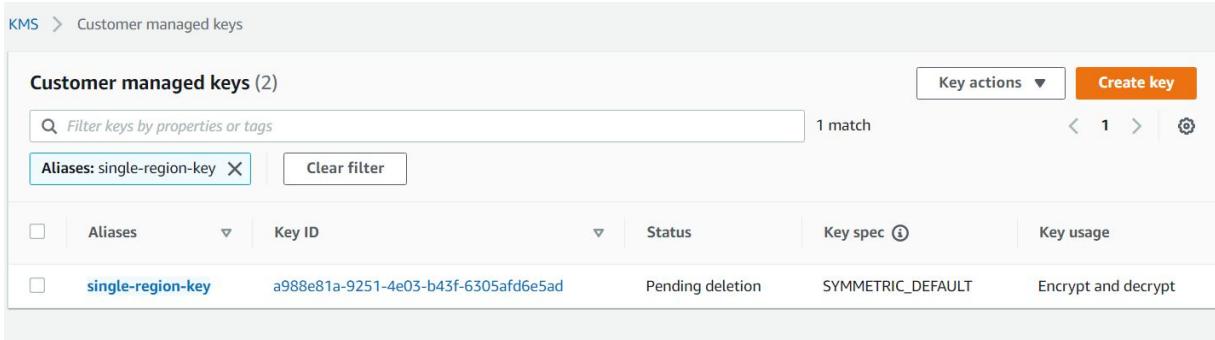
If you disable a KMS key, it cannot be used to encrypt or decrypt data until you re-enable it.

You can re-enable a disabled KMS key if you need to use it again later

Waiting Period for Key Deletion

Because it is destructive and potentially dangerous to delete a KMS key, AWS KMS requires you to set a waiting period of 7 – 30 days. The default waiting period is 30 days.

During the waiting period, A KMS key pending deletion cannot be used in any cryptographic operations.



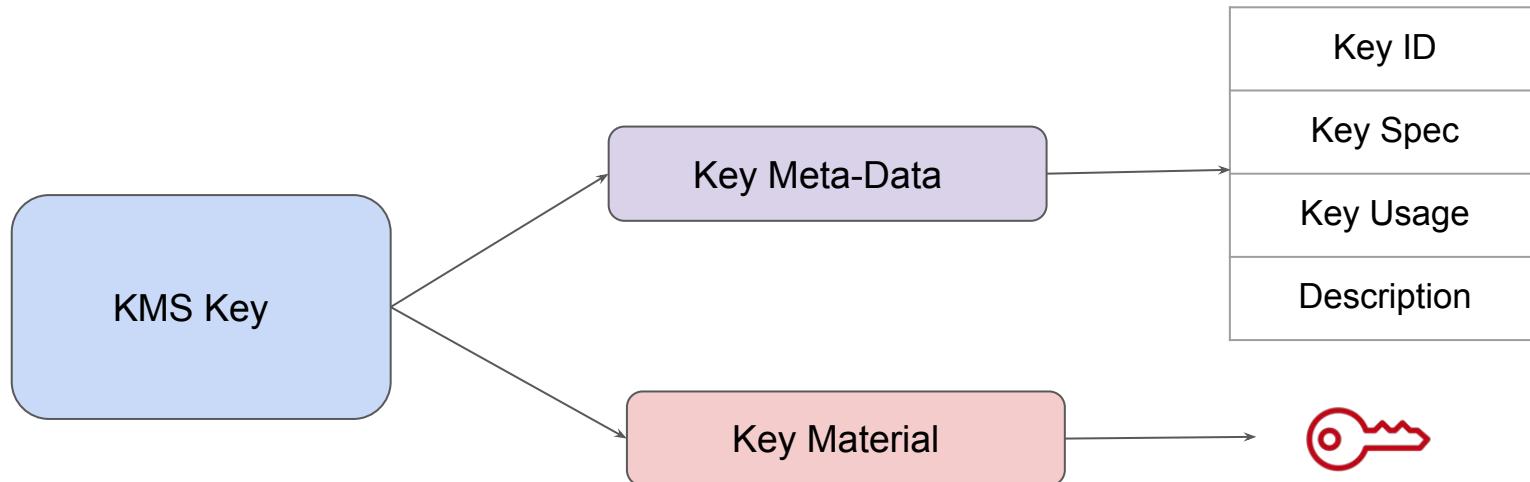
The screenshot shows the AWS KMS console interface. The top navigation bar has 'KMS' and 'Customer managed keys'. Below the navigation is a search bar with 'Filter keys by properties or tags' and a dropdown menu. To the right are 'Key actions' and a 'Create key' button. A pagination indicator shows '1 match' and '1'. Below the search bar is a filter section with 'Aliases: single-region-key' and a 'Clear filter' button. The main table has columns: 'Aliases', 'Key ID', 'Status', 'Key spec', and 'Key usage'. One row is visible: 'single-region-key' (Key ID: a988e81a-9251-4e03-b43f-6305af6e5ad), Status: 'Pending deletion', Key spec: 'SYMMETRIC_DEFAULT', and Key usage: 'Encrypt and decrypt'.

AWS KMS Keys

Categories Of Keys

Basics of KMS Keys

KMS key contains **metadata** and a **reference** to the key material that is used when you run cryptographic operations with the KMS key.



Importance of Key Material

By default, AWS KMS creates the key material for a KMS key.

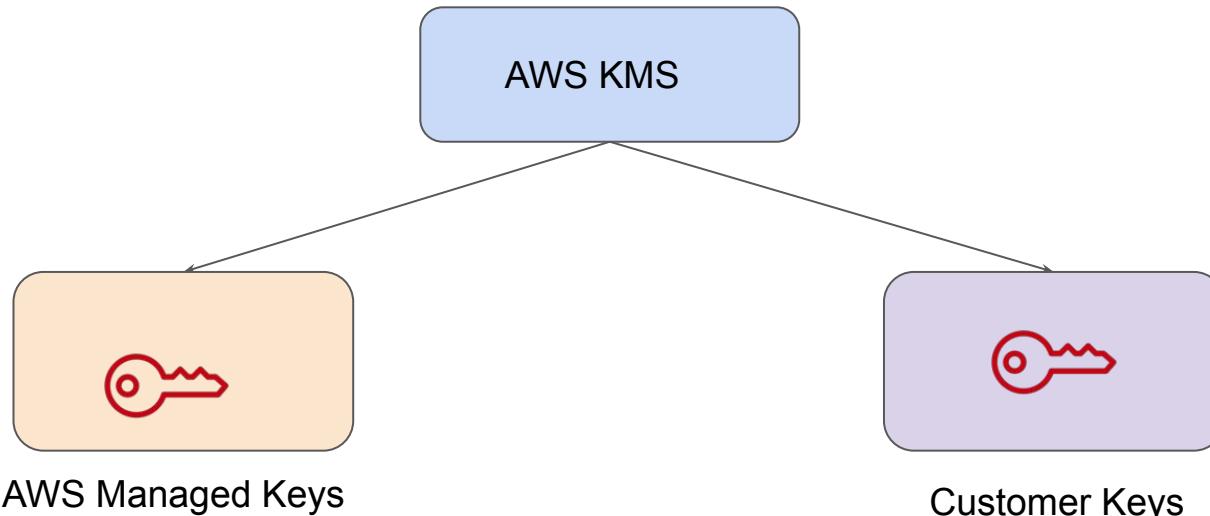
You cannot extract, export, view, or manage this key material.

However, you can import your own key material into a KMS key or create the key material for a KMS key in the AWS CloudHSM cluster associated with an AWS KMS custom key store.

2 Primary Categories of Keys

There are two primary key categories in AWS KMS.

Depending on the type of key that is created, the operations and permissions will change.



AWS Managed Key

AWS managed keys are KMS keys in your account that are created, managed, and used on your behalf by an AWS service integrated with AWS KMS to protect your resources in the service.

Example: S3 with Server Side Encryption

Limited Permissions: Cannot change properties, delete keys,



S3 Bucket



AWS Managed Keys

Customer managed keys

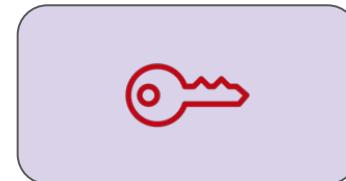
The KMS keys that you create are customer managed keys.

Customer managed keys are KMS keys in your AWS account that you create, own, and manage.

You have full control over these KMS keys



S3 Bucket



Customer Keys

Differences

| Type of KMS Key | View KMS Key Meta-Data | Manage KMS Key | Monthly Fee | Rotation |
|----------------------|------------------------|----------------|-------------|---|
| AWS Managed Key | Yes | No | No | Required. Every year (approximately 365 days) |
| Customer Managed Key | Yes | Yes | Yes | Optional. Every year (approximately 365 days) |

Question Based on This Lecture

There is a requirement from Auditor that the organization must have control over the encryption key including enabling/disabling key at will, modify permissions and delete when necessary.

What is the type of key that is recommended?

1. AWS Managed Key
2. Customer Managed Key.

Asymmetric Key Encryption

Right Architecture is the Key

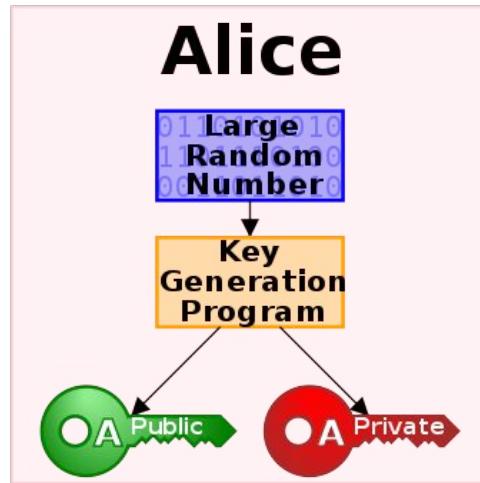
Overview of Asymmetric Key Encryption

Asymmetric cryptography, uses public and private keys to encrypt and decrypt data.

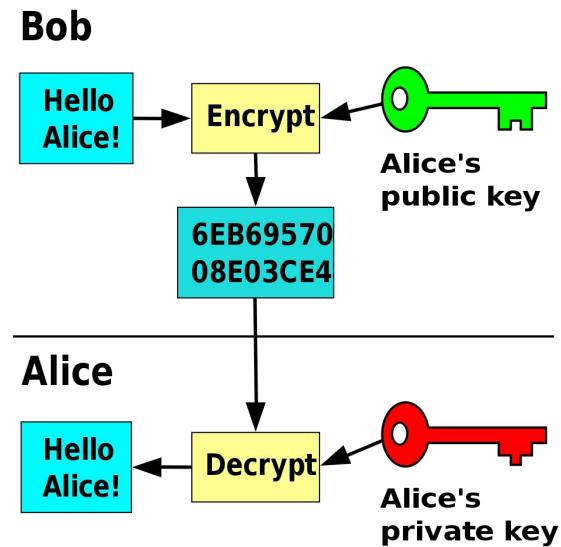
One key in the pair can be shared with everyone; it is called the public key. The other key in the pair is kept secret; it is called the private key.

Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.

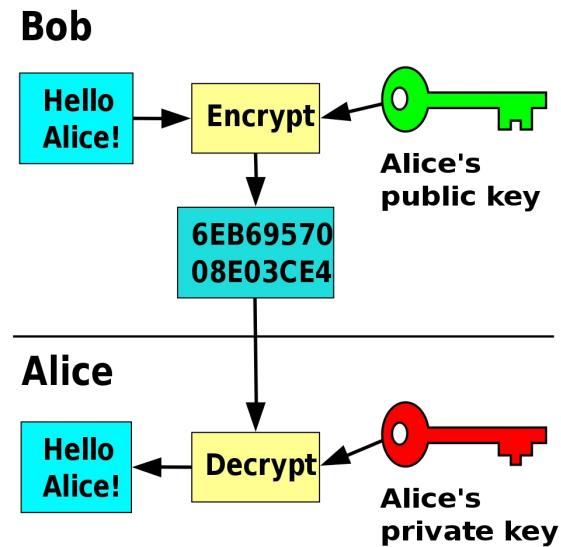
Step 1: Generation of Keys



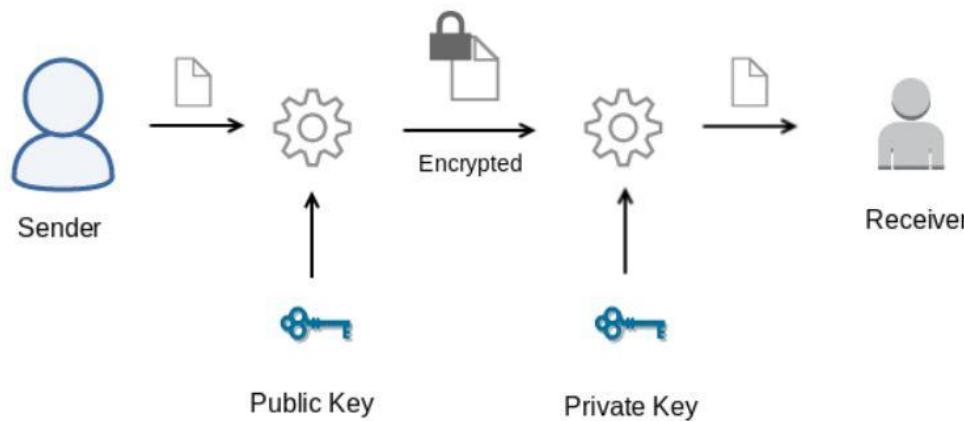
Step 2: Encryption and Decryption



Step 2: Encryption and Decryption

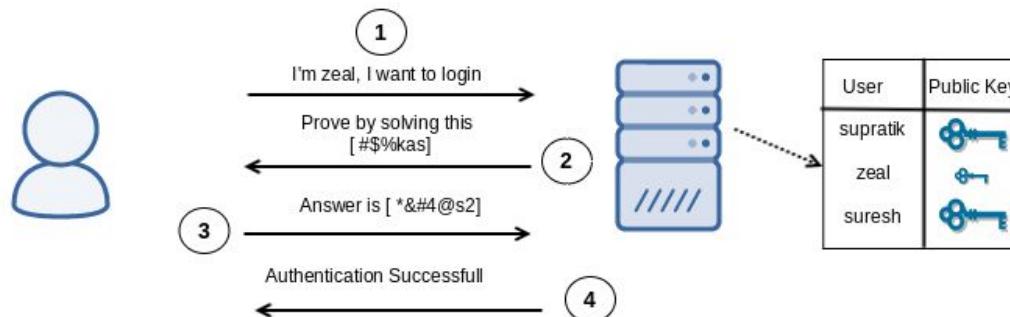


Step 2: Encryption and Decryption



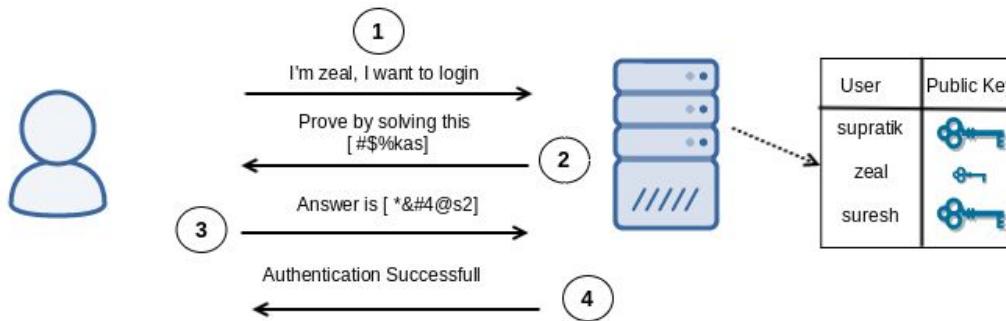
Use-Case of Asymmetric Key Encryption - Step 1

User zeal wants to log in to the server. Since the server uses a public key authentication, instead of taking the password from the user, the server will verify if the User claiming to be zeal actually holds the right private key.



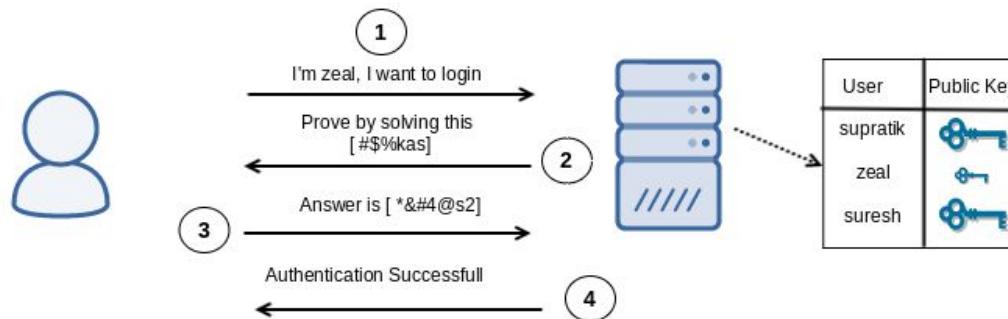
Use-Case of Asymmetric Key Encryption - Step 2

The server creates a simple challenge, $2+3=?$ and encrypts this challenge with the Public Key of the User and sends it back to the User. The challenge is sent in an encrypted format.



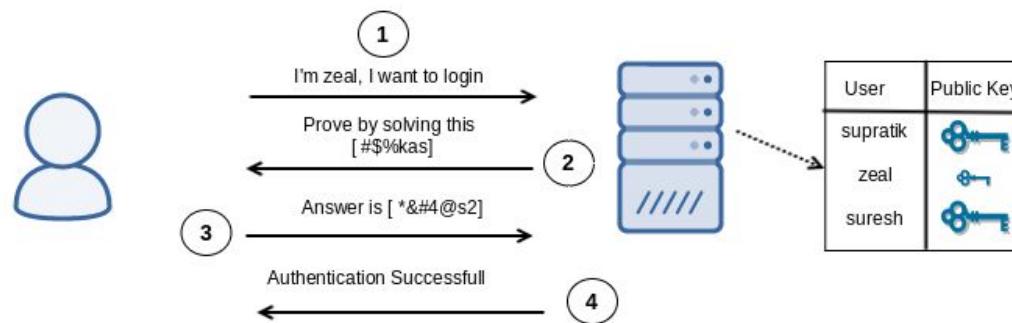
Use-Case of Asymmetric Key Encryption - Step 3

Since the user zeal holds the associated private key, he will be able to decrypt the message and compute the answer, which would be 5. Then, he will encrypt the message with the private key and send it back to the server.



Use-Case of Asymmetric Key Encryption - Step 4

The server decrypts the message with the user's Public Key and checks if the answer is correct. If yes, then the server will send an Authentication Successful message and the user will be able to log in.



Protocols

Because of the advantage that it offers, Asymmetric key encryption is used by variety of protocols.

Some of these include:

- PGP
- SSH
- Bitcoin
- TLS
- S/MIME

Asymmetric Keys with AWS KMS

Mastering Cryptography

Supported Key Format

AWS KMS supports both symmetric and asymmetric keys.

| Key Type | Description |
|----------------|---|
| Symmetric Key | Represents a single 256-bit secret encryption key. To use your symmetric CMK, you must call AWS KMS. |
| Asymmetric Key | Represents public and private key pair that can be used for various operations like encryption/decryption, signing. |

Configure key

Key type [Help me choose](#)

Symmetric

A single encryption key that is used for both encrypt and decrypt operations

Asymmetric

A public and private key pair that can be used for encrypt/decrypt or sign/verify operations

► Advanced options

Cancel

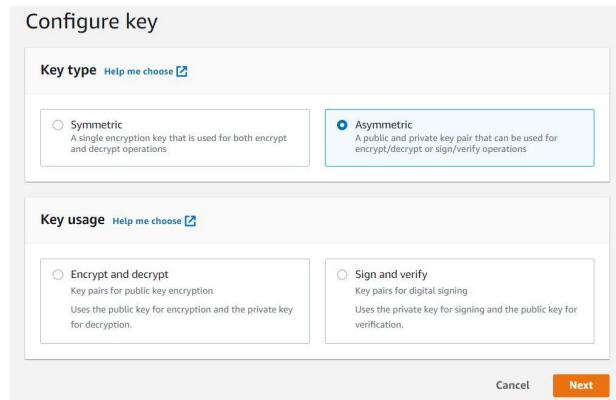
Next

Overview of Asymmetric Key with KMS

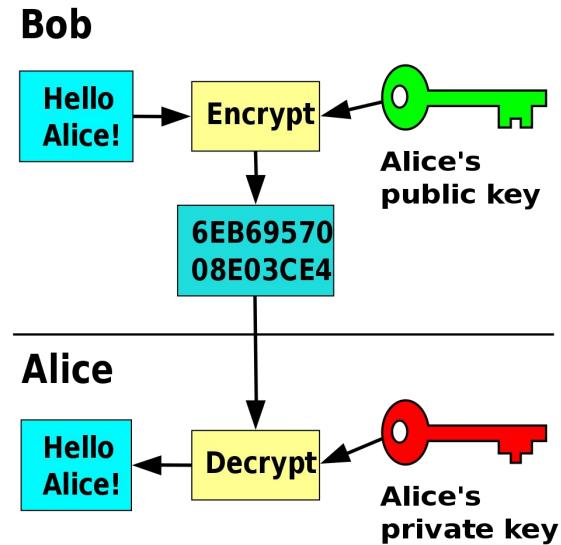
There are two primary use-case where asymmetric keys can be used:

1. Encrypt / Decrypt Data
2. Signing / Verification (Digital Signatures)

You can download the public key of asymmetric key CMK



Workflow 1 - Encryption and Decryption



Digital Signing with KMS

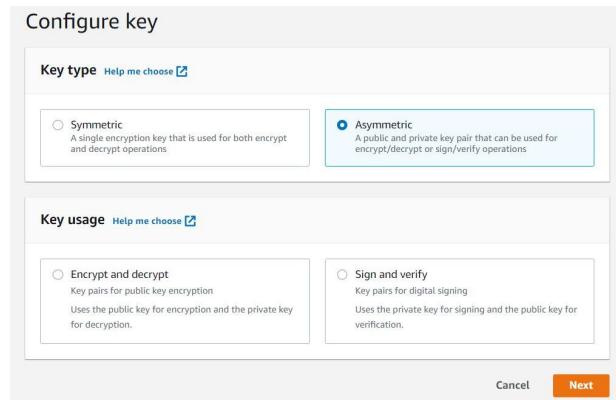
Mastering Cryptography

Overview of Asymmetric Key with KMS

There are two primary use-case where asymmetric keys can be used:

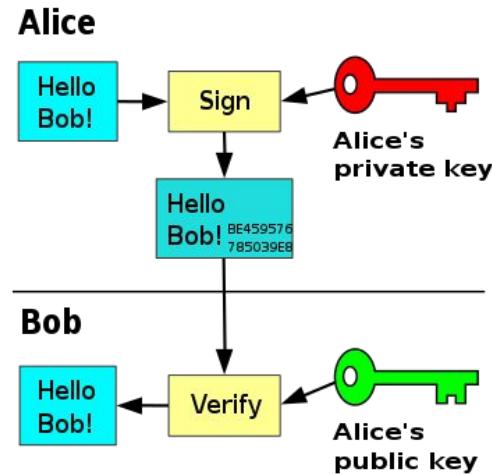
1. Encrypt / Decrypt Data
2. Signing / Verification (Digital Signatures)

You can download the public key of asymmetric key CMK



Overview of Digital Signatures

Non-repudiation systems use digital signatures to ensure that one party cannot successfully dispute its authorship of a document or communication.



Join us in our Adventure

Be Awesome



kplabs.in/twitter



kplabs.in/linkedin

instructors@kplabs.in

Data Key Caching

Optimize for higher workloads

Certain Challenges

There are lot of organizations which use KMS very extensively.

Let's take an example :

I used to work in one of the payments organization (payment gateway) and in such architectures, they used to have **separate data keys** that was used for encrypting of rows of data within the database.

Since there were thousands of rows and for each decrypt operation, we had to send API call to KMS, it used to sometimes create latency and slowness

Data Key Caching

AWS has recently introduced a feature called as “Data Key Caching” in it’s AWS Encryption SDK.

- Data key caching let’s us reuse the data-keys that protects our data, instead of generating new data key for each of the encrypt operation.
- This definitely comes with security tradeoffs, as the encryption best practices discourages extensive re-use of the data-keys.



How it works ?

In AWS Encryption SDK, by default there is a new data key generated for each encrypt operation that is performed.

This is most secure practice. It does bring overhead as well.

| | Generate DataKeys | Clients per region | Total number of requests per second |
|-----------------------------|-------------------|--------------------|-------------------------------------|
| No Cache | 1 | 500 | 500 |
| Local Crypto Material Cache | 1 rps / 100 uses | 500 | 5 |

Important Pointers

Data key caching saves the plaintext and ciphertext of the data keys you use in a configurable cache.

When you need a key to encrypt or decrypt data, you can reuse a data key from the cache instead of creating a new data key.

It is preferred to use data-key caching when there are high frequency needed, latency involved, slow master key operations.

Deleting CMK - Use Case

Interesting Use-Case

Let's take a use-case

A genuine use-case :

Medium Corp is using KMS extensively for EBS encryption. There is one KMS CMK which is used for all EBS encryption. One of the system administrator decided to turn rogue and scheduled deletion of CMK before leaving. You came to know about it once the CMK was deleted. What will happen to your EBS volume data ?

Relax and Have a Meme Before Proceeding

Boss: "Please reply to this email by
the 12th"

Me reading the email on the 15th:

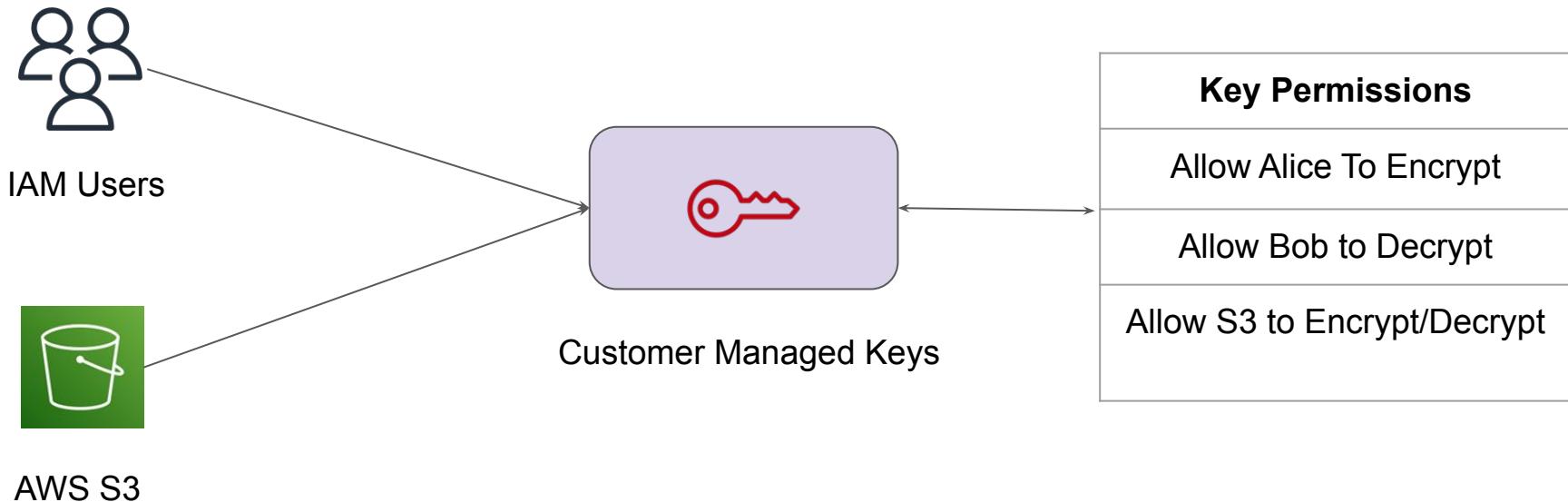


KMS Authentication & Access Control

Security Primer

Importance of Authorization in KMS

AWS KMS can be accessed directly by the IAM Users as well as various AWS services like S3.



Key Policies in AWS KMS

A key policy is a resource policy for an AWS KMS key and are the primary way to control access to KMS keys

No AWS principal, including the account root user or key creator, has any permissions to a KMS key unless they are explicitly allowed



Customer Managed Keys

Default Key Policy

When you create a KMS key, and you don't specify a key policy, AWS KMS applies a very simple default key policy.

This default key policy has one policy statement that gives the AWS account that owns the KMS key permission to use IAM policies to allow access to all AWS KMS operations on the KMS key

```
Key policy

1 {
2     "Id": "key-consolepolicy-3",
3     "Version": "2012-10-17",
4     "Statement": [
5         {
6             "Sid": "Enable IAM User Permissions",
7             "Effect": "Allow",
8             "Principal": {
9                 "AWS": "arn:aws:iam::693331494763:root"
10            },
11            "Action": "kms:*",
12            "Resource": "*"
13        }
14    ]
15 }
```

Key Administrators and Key Users

Key administrators have permissions to manage the KMS key, but do not have permissions to use the KMS key in cryptographic operations.

Key users have permission to use the KMS key directly in all cryptographic operations supported on the KMS key.

Controlling Access to KMS

To control access to your KMS keys, you can use the following policy mechanisms.

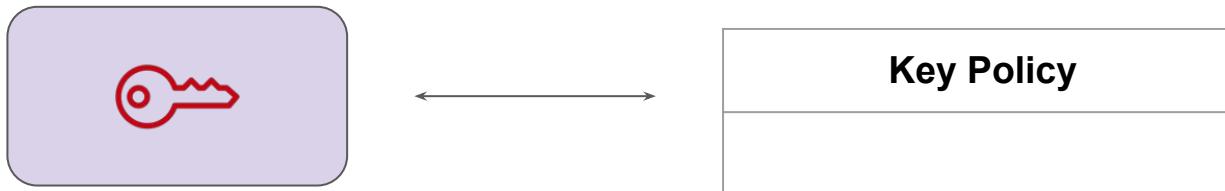
| Access Control | Description |
|----------------|---|
| Key Policy | Every KMS key has a key policy that allows us to define access permissions over the key. |
| IAM Policies | You can use IAM policies in combination with the key policy to control access to a KMS key. |
| Grants | Allows delegating access. |

Importance of Default Policy

KMS Access Control

Setting Base Straight

No AWS principal, including the account root user or key creator, has any permissions to a KMS key unless they are explicitly allowed



Customer Managed Keys

Default Policy

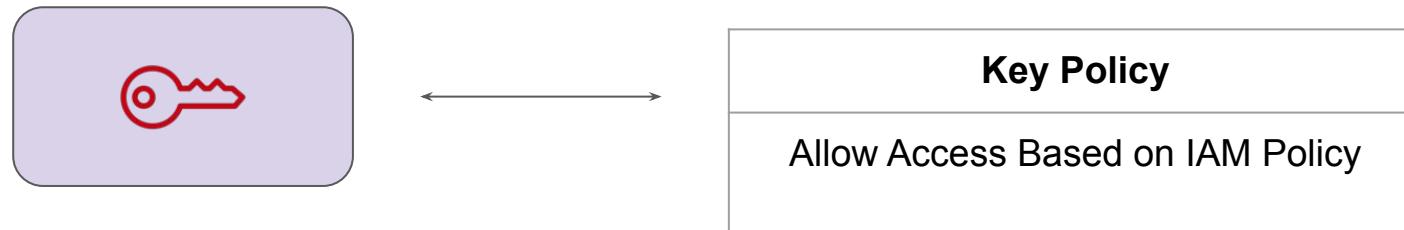
Key policy

```
1 {
2     "Id": "key-consolepolicy-3",
3     "Version": "2012-10-17",
4     "Statement": [
5         {
6             "Sid": "Enable IAM User Permissions",
7             "Effect": "Allow",
8             "Principal": {
9                 "AWS": "arn:aws:iam::693331494763:root"
10            },
11            "Action": "kms:*",
12            "Resource": "*"
13        }
14    ]
15 }
```

Importance of Default Policy

When a default KMS Policy is attached to the key, it enables administrators to define permissions at IAM level.

Note: This policy does not mean all IAM users can perform ALL actions on KMS key.



Customer Managed Keys

Reducing Risk of Unmanageable CMK

Security Primer

Setting the Base

Unless the key policy explicitly allows it, you cannot use IAM policies to allow access to a KMS key.

Without permission from the key policy, IAM policies that allow permissions have no effect.



Customer Managed Keys

Changing the Key Policy to Allow IAM User

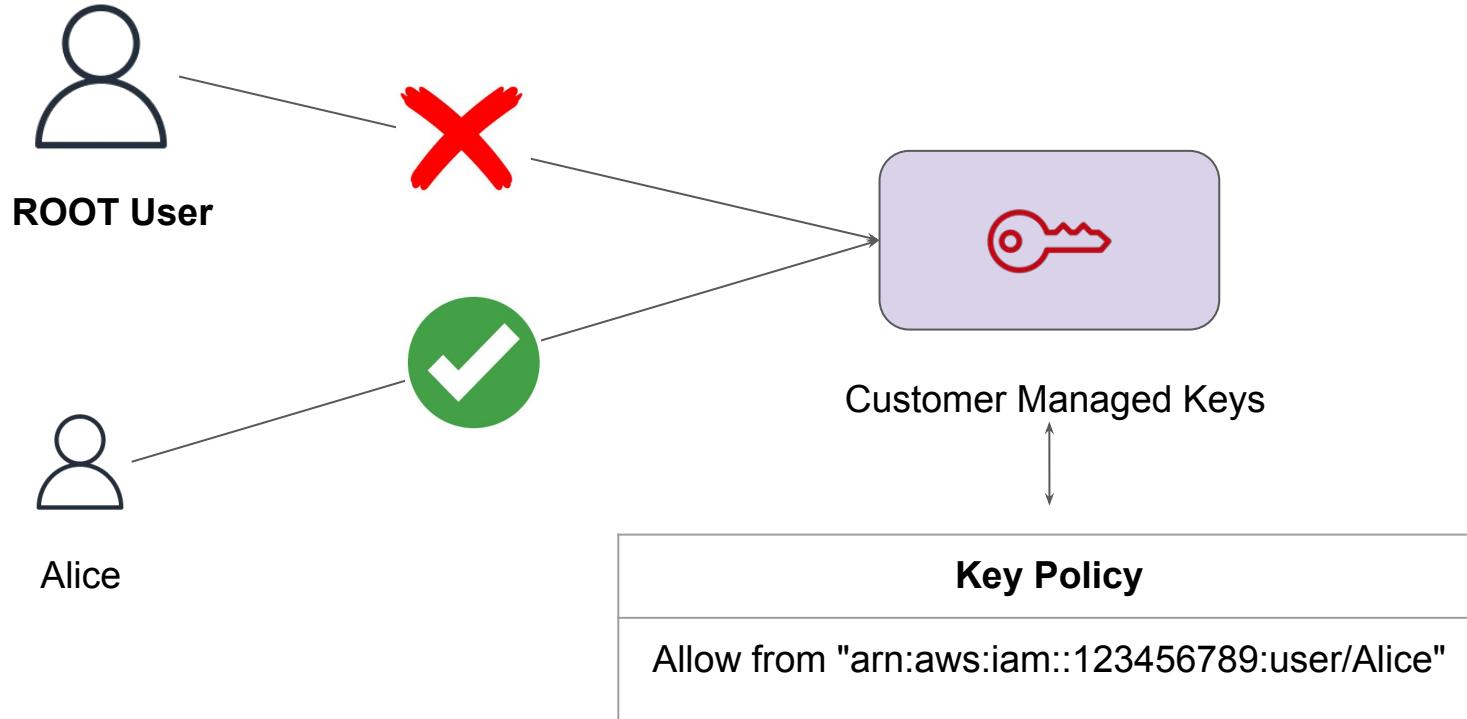
If you change the Key policy to allow specific IAM User, no other users including ROOT will have access to the Key.

Without permission from the key policy, IAM policies that allow permissions have no effect.



Customer Managed Keys

Diagrammatic Representation



Policy Evaluation Logic - Use-Case 1

Understanding KMS Policy Practically

Understanding the Use-Case

Explore the following permission set for Alice user and KMS Key:

| IAM User | IAM Policy | KMS Key Policy |
|----------|--------------------------|--|
| Alice | Allow Encrypt on KMS Key | 1 Allow IAM Policy Access. 2 Allow Decrypt from Alice |

Question:

1. Can Alice Perform Encrypt operation on KMS Key?
2. Can Alice Perform Decrypt operation on KMS Key?

Policy Evaluation Logic - Use-Case 1

Solution Video

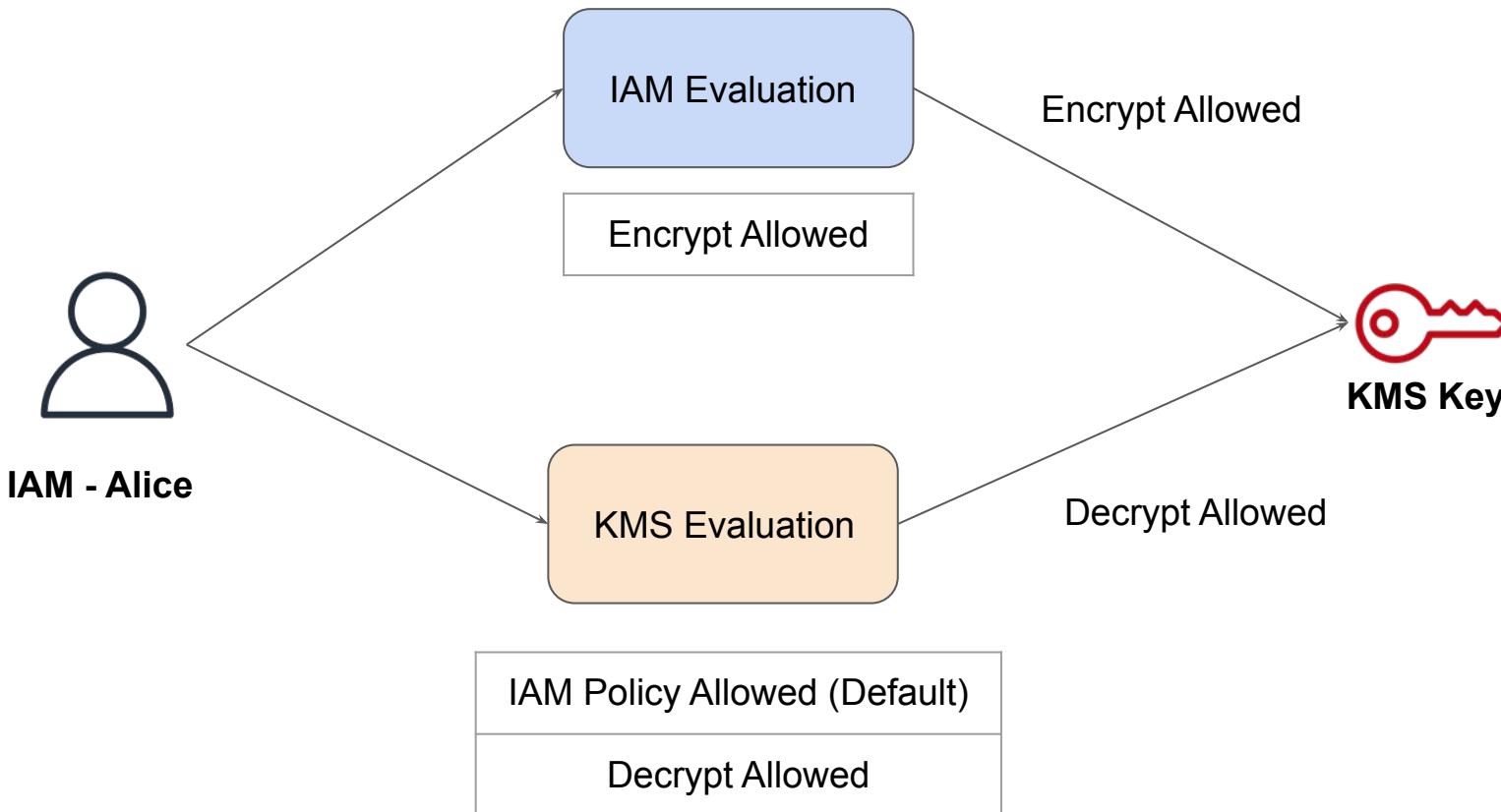
Solution

Based on the following policy:

1. Alice will be able to perform Encrypt Operation.
2. Alice will be able to perform Decrypt Operation

| IAM User | IAM Policy | KMS Key Policy |
|----------|--------------------------|--|
| Alice | Allow Encrypt on KMS Key | <ol style="list-style-type: none">1 Allow AWS Account Access.2 Allow Decrypt from Alice |

Solution Workflow



Policy Evaluation Logic - Use-Case 2

Understanding KMS Policy Practically

Understanding the Use-Case

Explore the following permission set for Alice user and KMS Key:

| IAM User | IAM Policy | KMS Key Policy |
|----------|--------------------------|--|
| Alice | Allow Encrypt on KMS Key | 1 Allow * from Bob 2 Allow Decrypt from Alice |

Question:

1. Can Alice Perform Encrypt operation on KMS Key?
2. Can Alice Perform Decrypt operation on KMS Key?

Policy Evaluation Logic - Use-Case 2

Solution Video

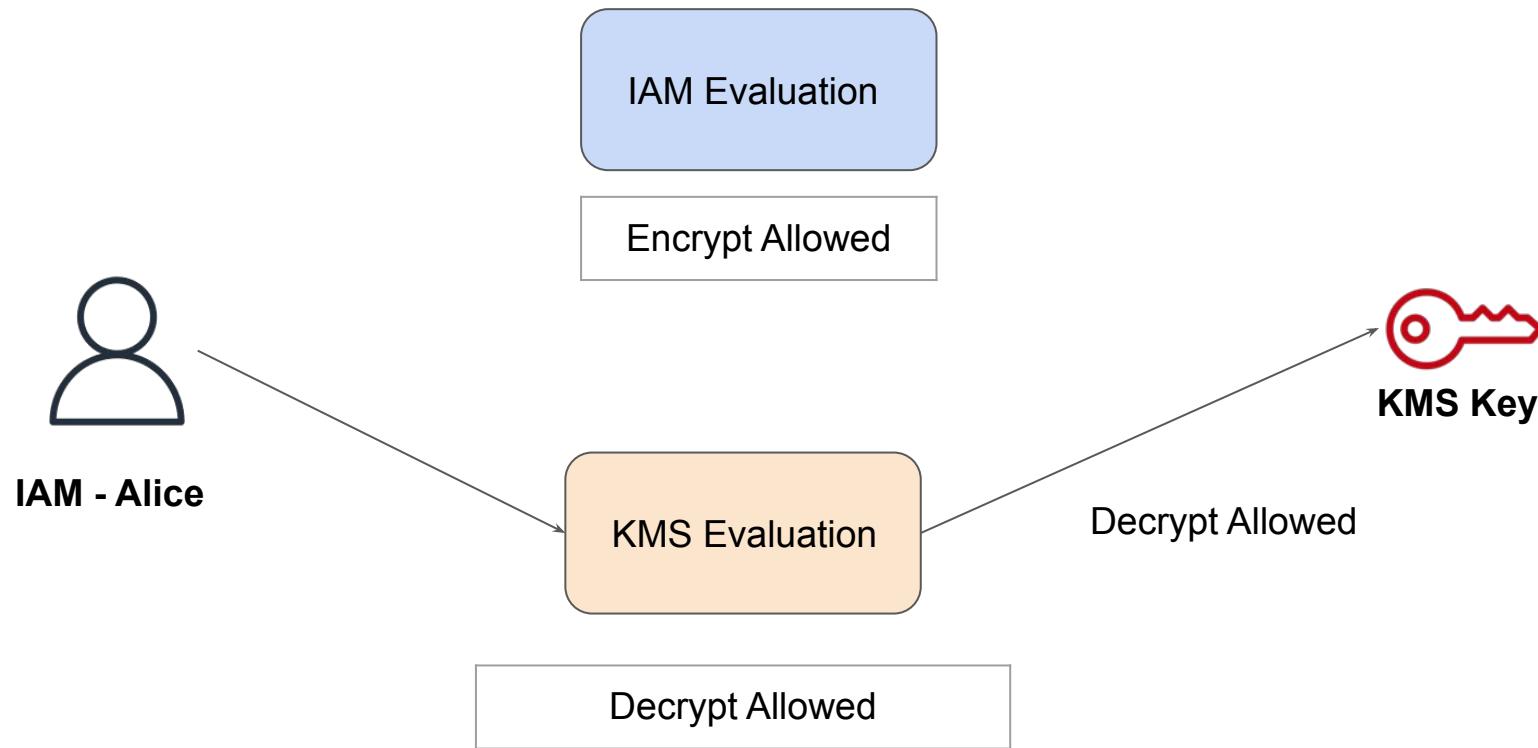
Solution

Based on the following policy:

1. Alice will be **NOT** able to perform Encrypt Operation.
2. Alice will be able to perform Decrypt Operation

| IAM User | IAM Policy | KMS Key Policy |
|----------|--------------------------|--|
| Alice | Allow Encrypt on KMS Key | 1 Allow * from Bob 2 Allow Decrypt from Alice |

Solution Workflow



Policy Evaluation Logic - Use-Case 3

Understanding KMS Policy Practically

Understanding the Use-Case

Explore the following permission set for Alice user and KMS Key:

| IAM User | IAM Policy | KMS Key Policy |
|----------|-------------------------|--|
| Alice | Deny Encrypt on KMS Key | 1 Allow IAM Policy Access. 2 Allow Encrypt & Decrypt from Alice |

Question:

1. Can Alice Perform Encrypt operation on KMS Key?
2. Can Alice Perform Decrypt operation on KMS Key?

Policy Evaluation Logic - Use-Case 3

Solution Video

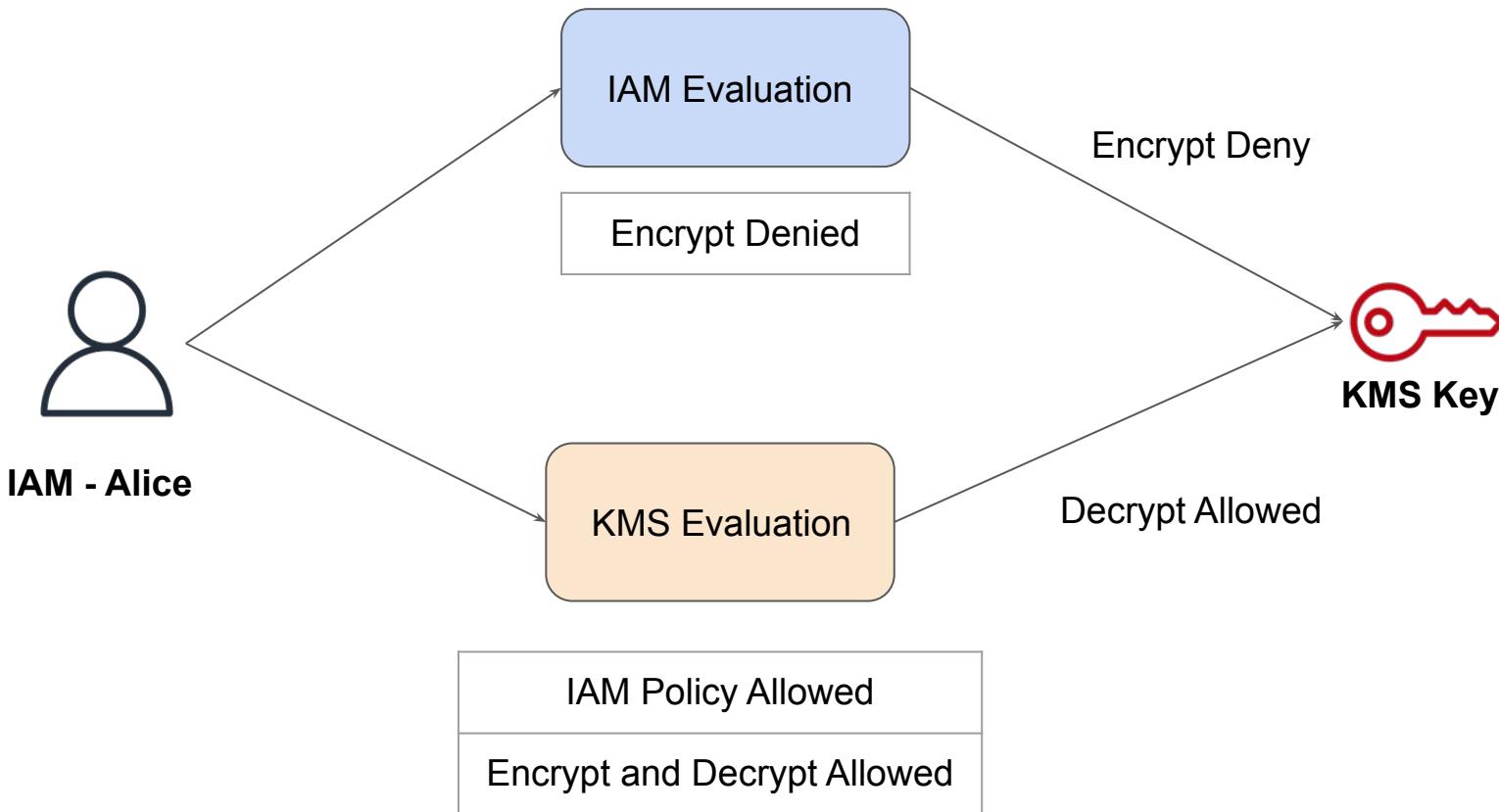
Solution

Based on the following policy:

1. Alice will be **NOT** able to perform Encrypt Operation.
2. Alice will be able to perform Decrypt Operation

| IAM User | IAM Policy | KMS Key Policy |
|----------|-------------------------|---|
| Alice | Deny Encrypt on KMS Key | <ol style="list-style-type: none">1 Allow IAM Policy Access.2 Allow Encrypt & Decrypt from Alice |

Solution Workflow



KMS Grants

Security Primer

Type of Policies

In AWS, there are two types of policies that you will work with:

- i) IAM policies
- ii) Resource Policies

In KMS, by default, all the CMK's have a key policy attached to it.

Importing Key Material in KMS

KMS All The Way!

Getting Started

A customer master key (CMK) contains the **key material** used to encrypt and decrypt data.

When we create a CMK, by default, AWS creates key-material for that CMK. However, we do have an option to create a CMK without key material and then import our key-material into the CMK.

Managing Access to AWS KMS CMK

We can control access to KMS CMK's using following three ways:

- i) Using Key Policies
- ii) Using IAM Policy in combination with key policies
- iii) Using KMS Grants

GRANT Terminology

During the process of Grant, there are two entities which are involved:

Grant user: User which generated the Grant.

Grantee: User who will use the grant generated by the Grant user.

GRANT Process

Grant is like a secret token.

The token has specific permission like encryption, decryption or others.

The Grantee will use this secret token to perform operations on the CMK.

KMS ViaService

Security Angle

Overview of ViaService

The kms:ViaService condition key limits use of an AWS KMS customer master key (CMK) to requests from specified AWS services.

Effect: Allow

```
"Condition": {  
    "ForAnyValue:StringEquals": {  
        "kms:ViaService": [  
            "ec2.us-west-2.amazonaws.com",  
            "rds.us-west-2.amazonaws.com"  
        ]  
    }  
}
```

Migrating KMS Encrypted Data / Regions

Security Angle

Migrating Services using KMS

KMS Keys are region specific.

We cannot call a KMS CMK from one region for services in different region.

During migration, services like AWS EBS has out of box approach to change the CMK to the destination region.

Use-Case - Encrypted RDS Migration

Way Earlier due to limitation of KMS being region specific, RDS used to only support migration of unencrypted RDS snapshots across regions.

Now we can easily migrate even the encrypted RDS snapshots across regions.

Use-Case - Encrypted RDS Migration

Important Points to Remember:

If you copy an encrypted snapshot within the same AWS Region, you can encrypt the copy with the same KMS encryption key as the original snapshot, or you can specify a different KMS encryption key.

For cross-region, we cannot use the same KMS key as snapshot. Instead we must specify a different KMS CMK which belongs to the destination region.

Default Encryption Keys cannot be used while copying of snapshots across AWS regions.

Very Important

Very Important Points to Remember:

If you have been using envelope encryption and have encrypted data with data-keys, then you will have to decrypt all those data before migrating to a different region.

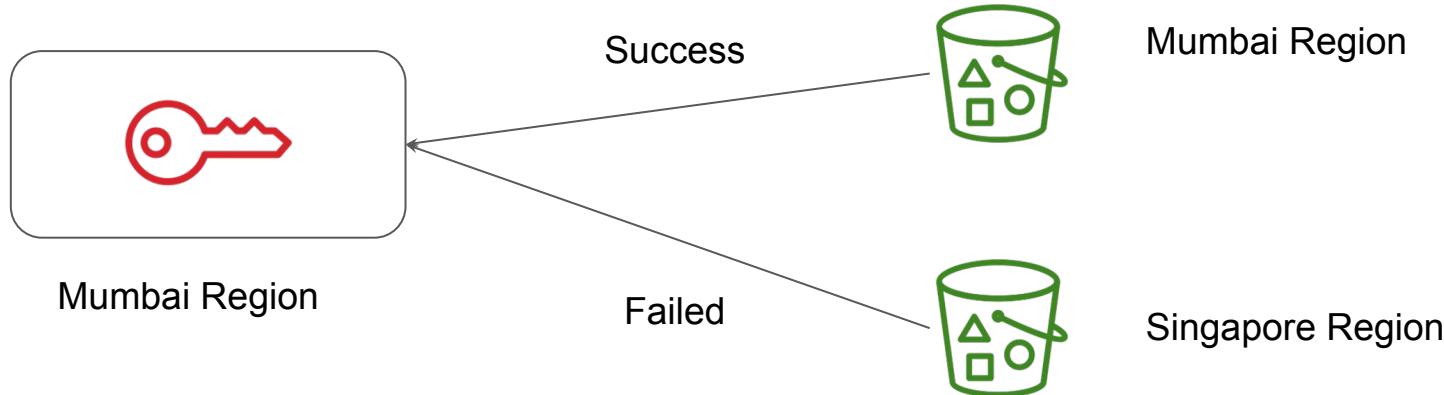
Multi-Region KMS

KMS Across Regions

Challenge with Single Region Keys

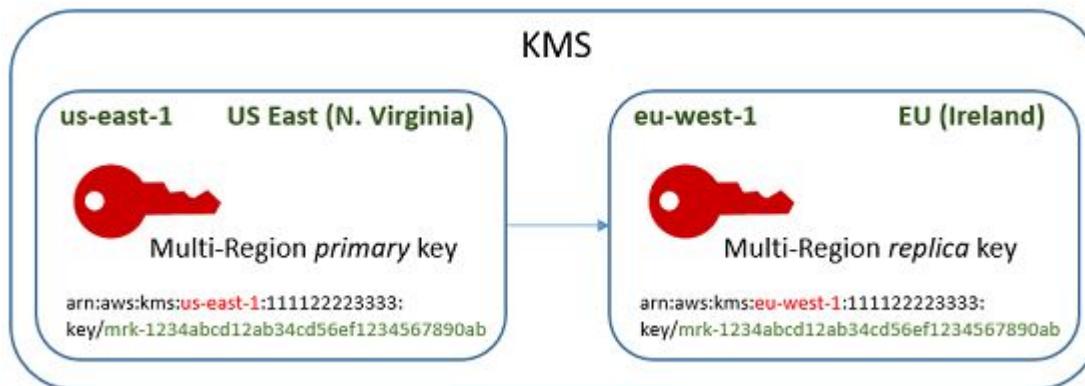
Earlier, the KMS keys were tied to a single AWS region.

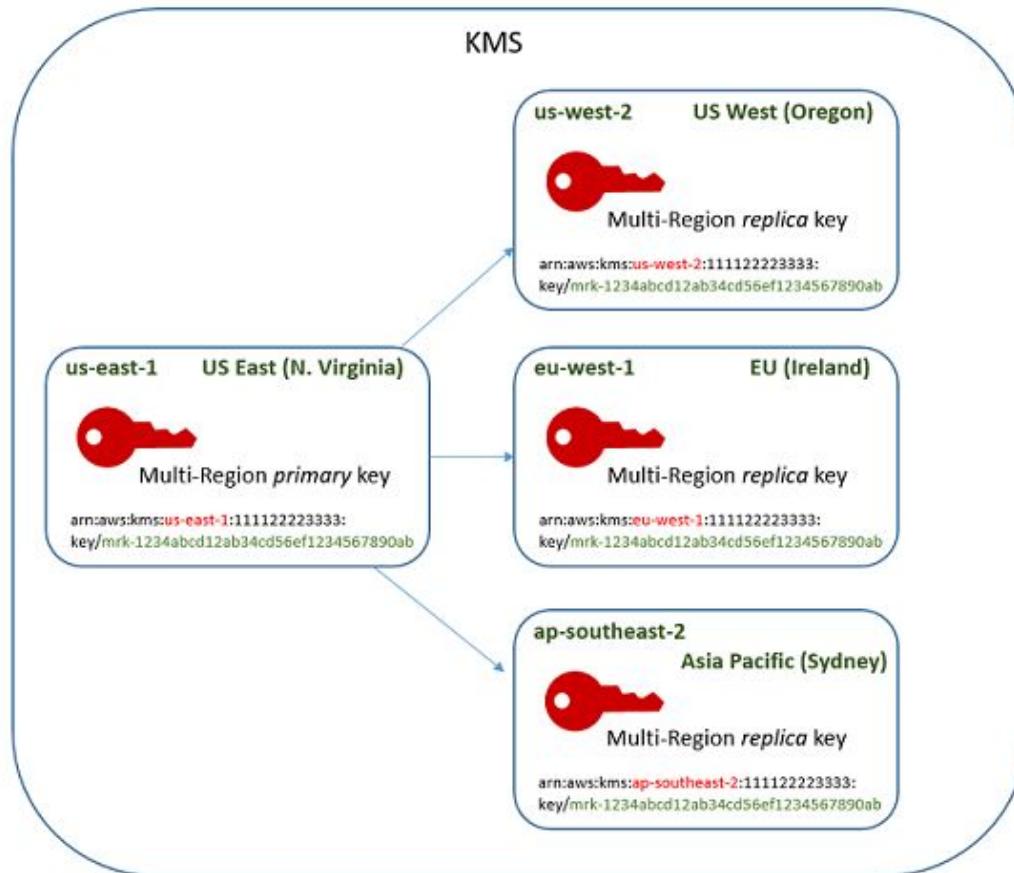
This introduced challenges for multi-region based applications.



Multi-Region KMS Keys

AWS multi-Region keys has the same key material and key ID, so you can encrypt data in one AWS Region and decrypt it in a different AWS Region without re-encrypting or making a cross-Region call to AWS KMS.

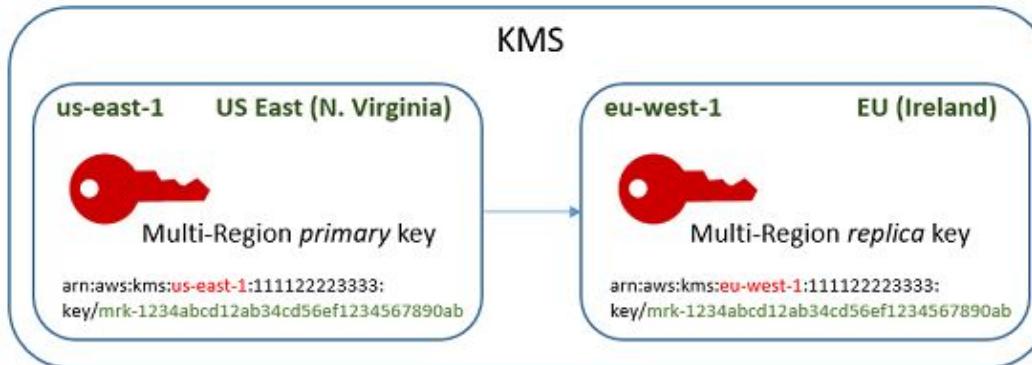




Primary Key and Replica Key

A multi-Region primary key is a KMS key that can be replicated into other AWS Regions

A multi-Region replica key is a KMS key that has the same key ID and key material as its primary key and exists in a different AWS Region.



Shared Properties

Shared properties are properties of a multi-Region primary key that are shared with its replica keys.

AWS KMS creates the replica keys with the same shared property values as those of the primary key.

- Key ID — (The Region element of the key ARN differs.)
- Key material
- Key material origin
- Key spec and encryption algorithms
- Key usage
- Automatic key rotation

Important Pointers

A primary key differs from a replica key in the following ways:

Only a primary key can be replicated.

The primary key is the source for shared properties of its replica keys, including the key material and key ID.

You can enable and disable automatic key rotation only on a primary key.

You can schedule the deletion of a primary key at any time. But AWS KMS will not delete a primary key until all of its replica keys are deleted.

Benefits of CloudHSM over KMS

One over Another!

Benefits of CloudHSM over KMS

When should I use AWS CloudHSM instead of AWS KMS?

Keys stored in dedicated, third-party validated hardware security modules under your exclusive control (only your org team can administer the keys and not AWS)

Integration with applications using PKCS#11, Java JCE, or Microsoft CNG interfaces.

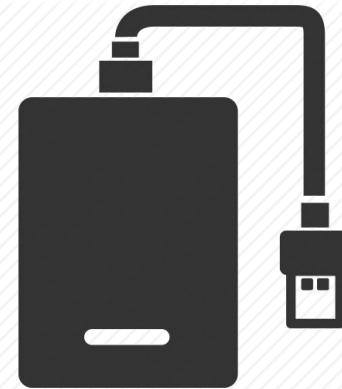
High-performance in-VPC cryptographic acceleration (bulk crypto).

Organization Administrator can export and share keys as needed.

S3 Encryption

S3 is Back

What's the Need ?

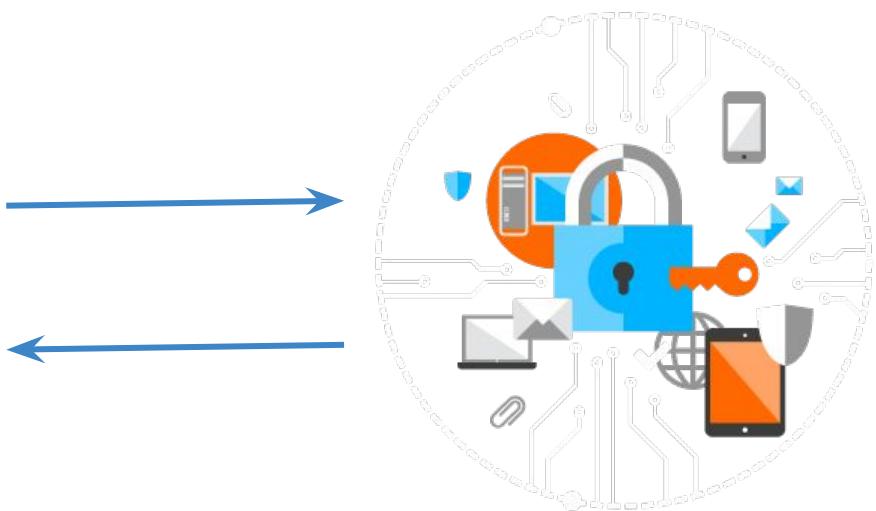


Let's be Proactive

Western Digital external HDs with hardware-based encryption

Aspiring to be a CISSP in 2017? Download the free planning kit!

WD introduced its new **My Book Essential** and **My Book for Mac** desktop external hard drives equipped with the new WD SmartWare software and hardware-based encryption.



S3 also needs Encryption

AWS S3 offers multiple approaches to encrypt the data being stored in S3.

i) Server Side Encryption

- Request Amazon S3 to encrypt your object before saving it on disks in its data centers and then decrypt it when you download the objects.

ii) Client Side Encryption

- Encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

Server Side Encryption

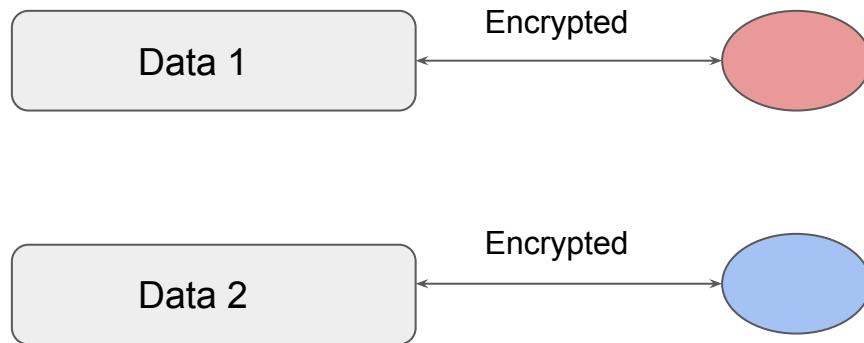
Within Server-Side encryption, there are three options that can be used depending on the use-case.

- Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
- Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS)
- Server-Side Encryption with Customer-Provided Keys (SSE-C)

SSE with Amazon S3-Managed Keys (SSE-S3)

i) Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

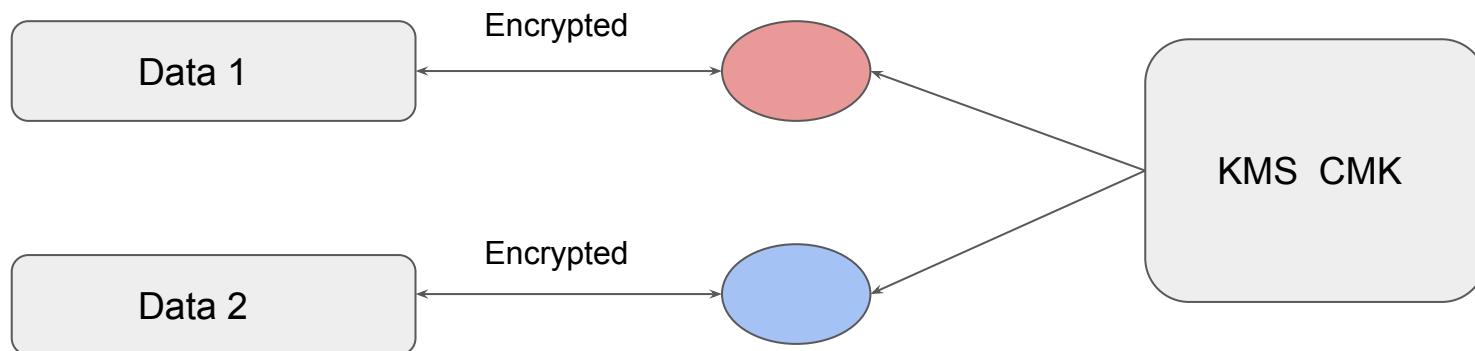
- In this approach, each object is encrypted with a unique key.
- Uses one of the strongest block ciphers to encrypt the data, AES 256.



SSE with CMK (SSE-KMS)

ii) Server-Side Encryption with CMKs Stored in AWS Key Management Service (SSE-KMS)

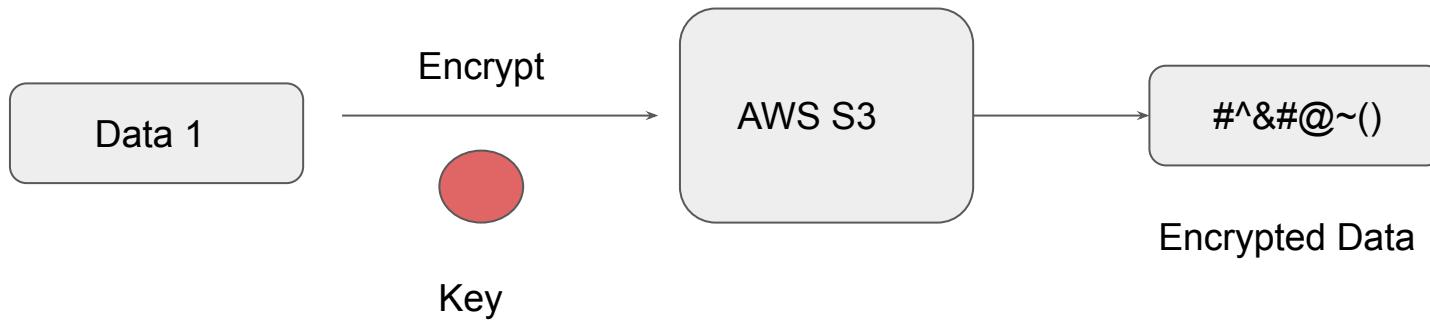
Encrypting data with own CMK allows customers to create, rotate, disable customer managed CMK's. We can also define access controls and enable auditing.



SSE with Customer-Provided Keys (SSE-C)

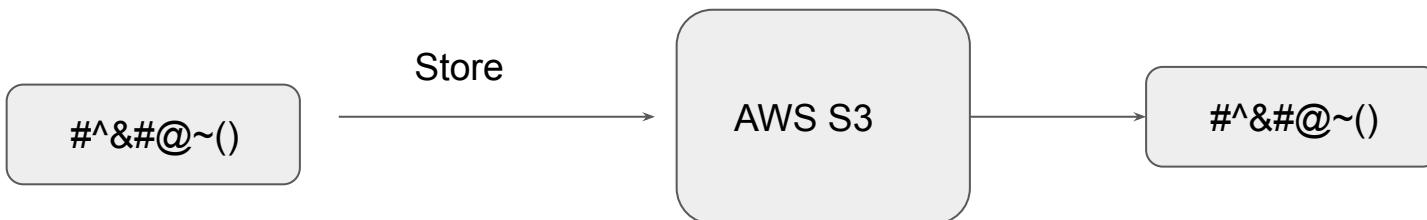
Allows customers to set their own encryption keys.

Encryption key needs to be provided as part of the request and S3 will manage both the encryption as well as the decryption options.



Client Side Encryption

Client-side encryption is the act of encrypting data before sending it to Amazon S3.



Relax and Have a Meme Before Proceeding

me: i'll do it at 6

time: 6:05

me: wow looks like i gotta wait til 7 now



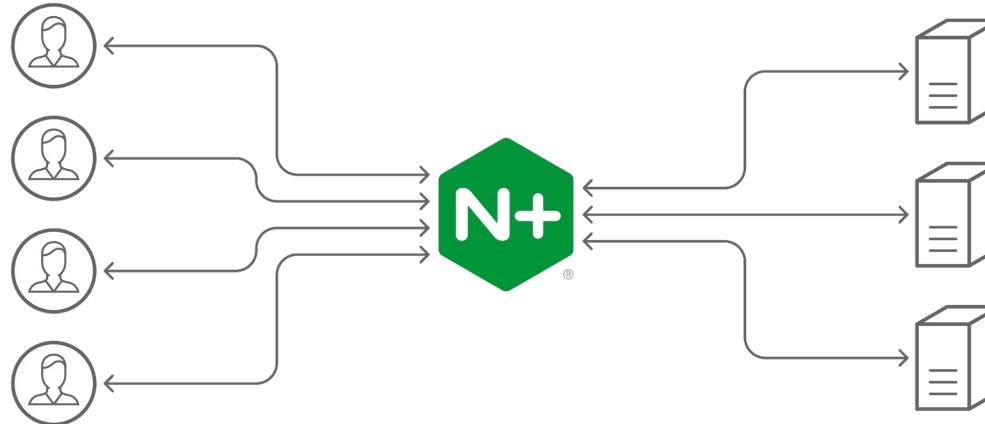
Load Balancing in AWS

Let's Load Balance Traffic in AWS

Basics of Load Balancing

There are multiple software and hardware based load balancing solutions available.

Some of the popular ones include Nginx, HA Proxy and others.



Challenges with Maintaining Load Balancing Solution

If you are using a load balancing solution, various responsibilities falls to customer.

Some of these include:

1. High-Availability of Load Balancers.
2. Security.
3. Performance.

Basics of Elastic Load Balancing Service

AWS offers managed load balancing solutions for wide variety of use-cases.

These solutions are offered under the Elastic Load Balancing feature.

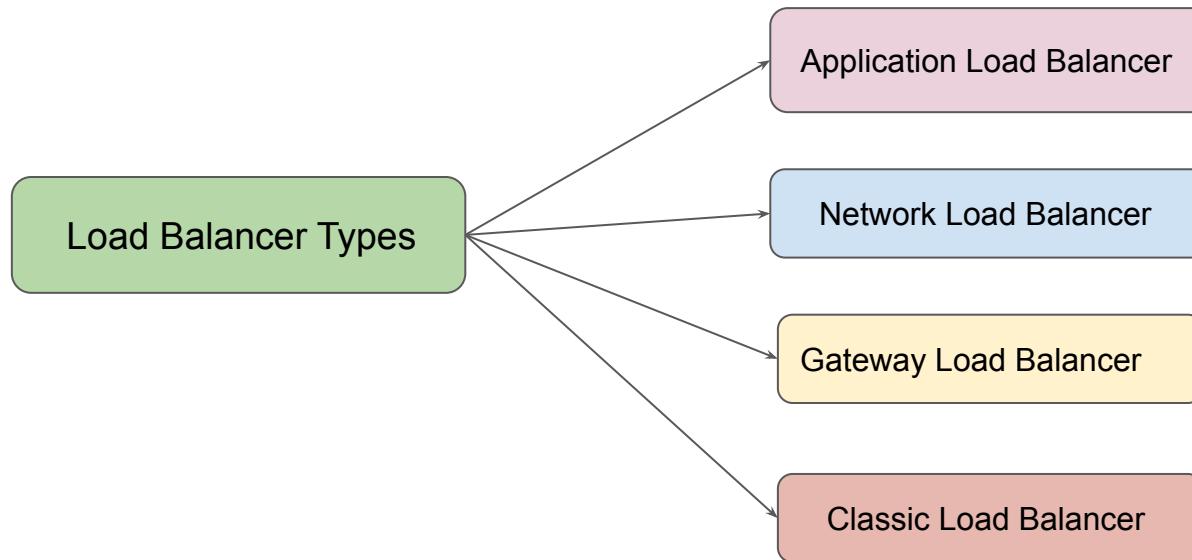
Tight integration with multiple AWS Services.



Elastic Load Balancing

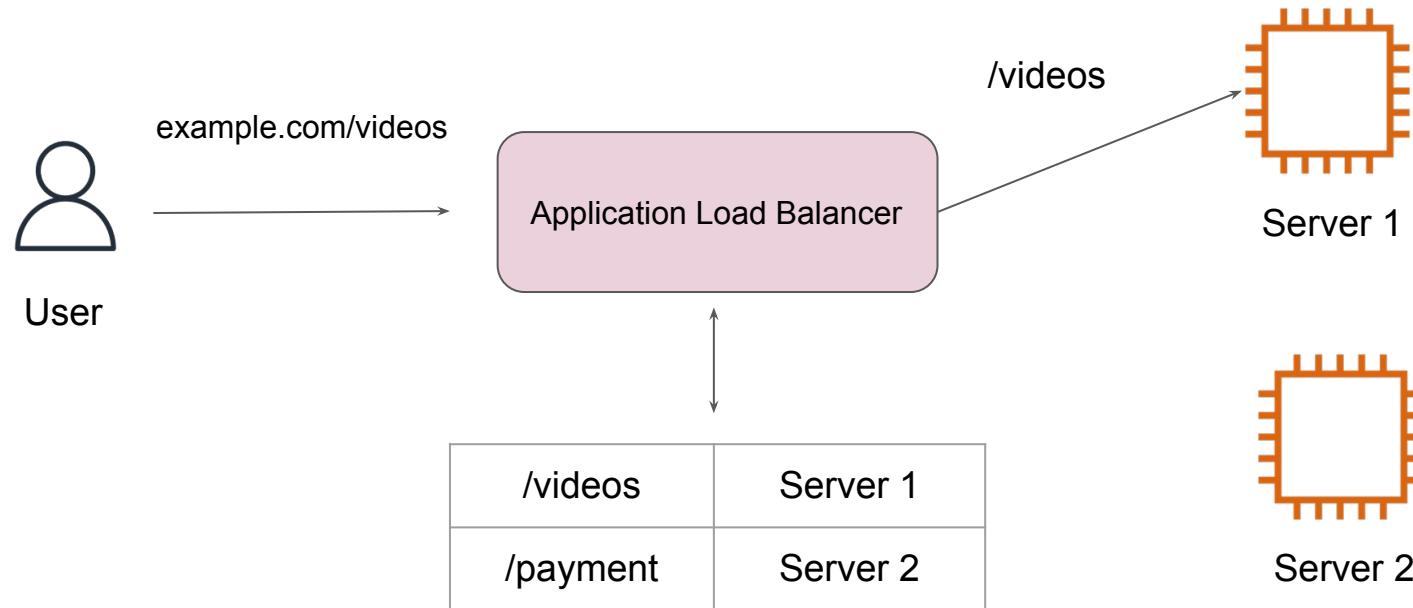
Types of Load Balancers

There are 4 primary type of Load Balancer offerings available.



Application Load Balancers

An Application Load Balancer makes routing decisions at the application layer (HTTP/HTTPS)

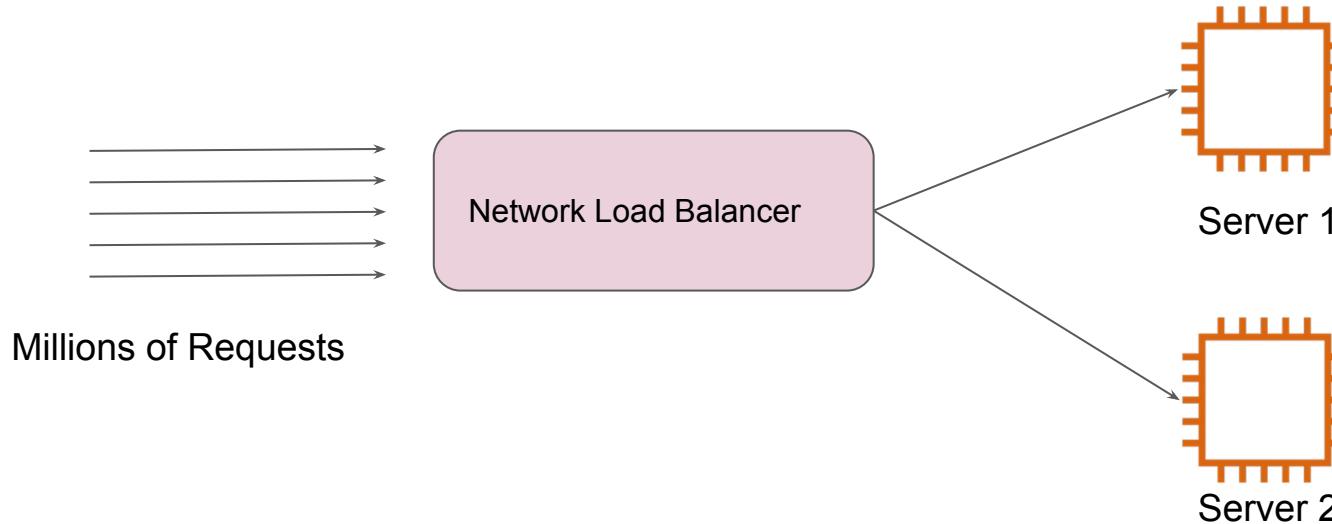


Network Load Balancers

A Network Load Balancer makes routing decisions at the transport layer (TCP/UDP/SSL).

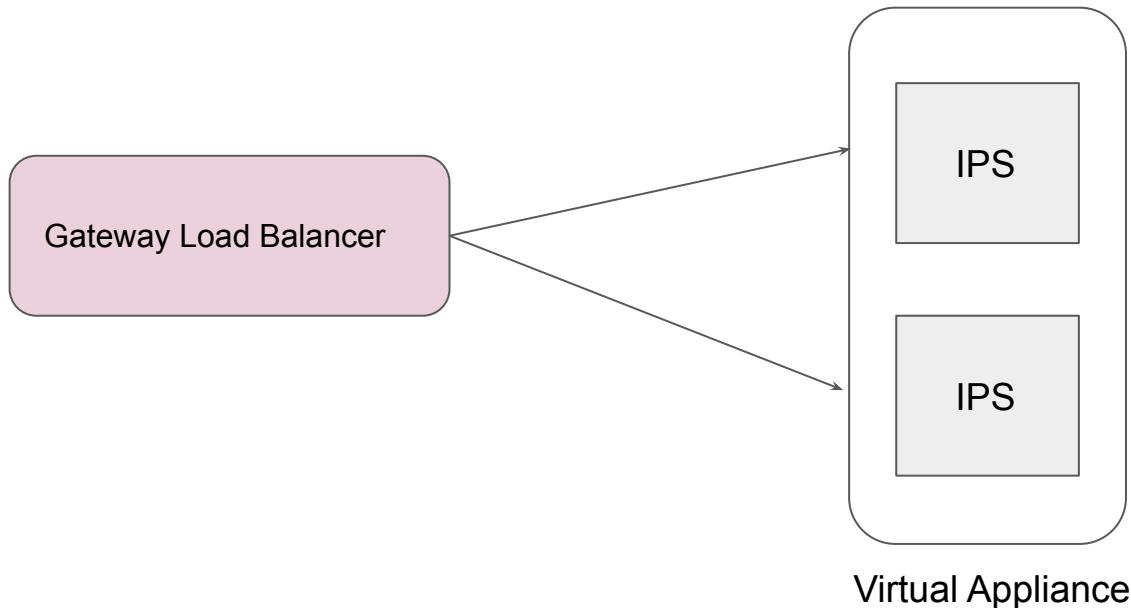
It can handle millions of requests per second.

Not all of the applications work on HTTP/HTTPS protocol.



Gateway Load Balancers

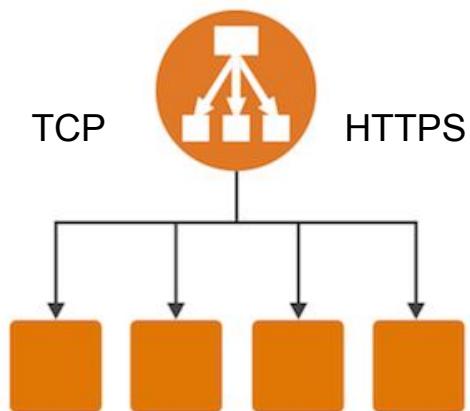
Gateway Load Balancers allow you to deploy, scale, and manage virtual appliances, such as firewalls, intrusion detection and prevention systems, and deep packet inspection systems



Classic Load Balancers

A Classic Load Balancer makes routing decisions at either the transport layer (TCP/SSL) or the application layer (HTTP/HTTPS).

Previous Generation Load Balancer and not recommended.



Summary Slide

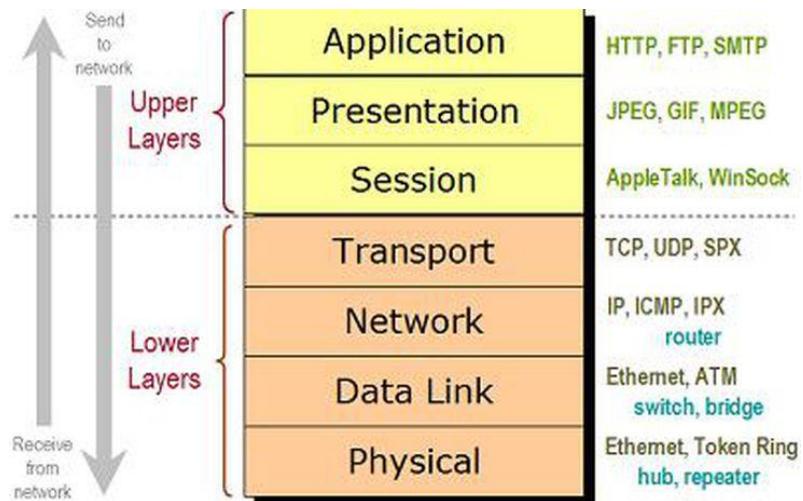
| Load Balancer | Important Notes |
|---------------------------|---|
| Application Load Balancer | Use when you have websites/applications at L7 (HTTP/HTTPS) |
| Network Load Balancers | <p>TCP and UDP based applications.</p> <p>Requirement to handle millions of requests per second.</p> <p>Ultra high performance.</p> |
| Gateway Load Balancer | <p>Use when you have virtual appliances:</p> <p>IDS/IPS Firewalls</p> |

OSI Model & Load Balancers

Revising Networking

Basics of OSI Model

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It



Load Balancer & OSI Layers

Each load balancer operates at a specific layer.

You will only be able to perform operations on requests based on Layer the ELB supports.

| Feature | Application Load Balancer | Network Load Balancer | Gateway Load Balancer | Classic Load Balancer |
|--------------------|---------------------------|-----------------------|--|-----------------------|
| Load Balancer type | Layer 7 | Layer 4 | Layer 3 Gateway + Layer 4 Load Balancing | Layer 4/7 |

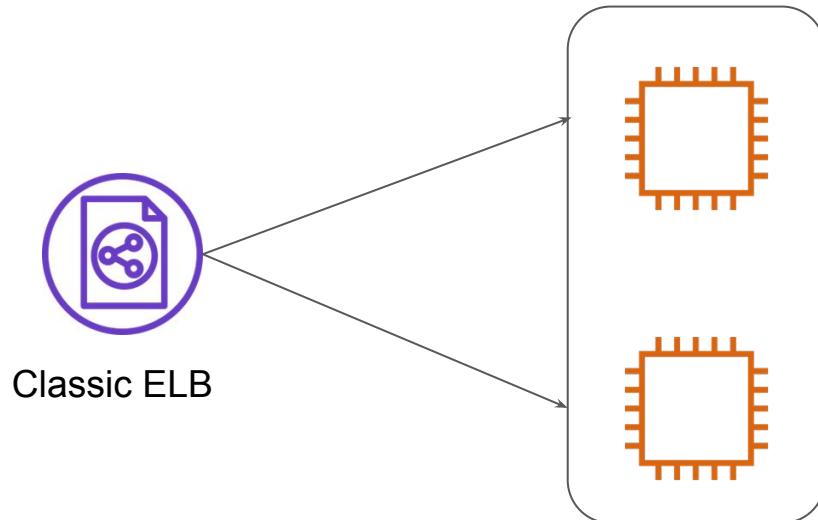
Classic Load Balancers

First generation Load Balancers

Understanding Classic Load Balancers

These are older generation of load balancers.

Provides basic set of features for HTTP, HTTPS, TCP and SSL protocols.



Limitation of Classic Load Balancers

- Does not support native HTTP/2 protocol.
- IP address as targets are not supported.
- Path based routing is not supported. (eg: /images should go to server 1 & /php to server 02)
- Many Many more

Application Load Balancers

Next generation load balancers

Basics of HTTP Headers

HTTP headers let the client and the server pass additional information with an HTTP request or response.

▶ GET http://demo-alb-137613815.us-east-1.elb.amazonaws.com/

| | |
|------------------|-------------------|
| Status | 200 OK ⓘ |
| Version | HTTP/1.1 |
| Transferred | 196 B (35 B size) |
| Request Priority | Highest |

▼ Response Headers (161 B)

- ⓘ Connection: keep-alive
- ⓘ Content-Length: 35
- ⓘ Content-Type: text/plain; charset=utf-8
- ⓘ Date: Thu, 21 Jul 2022 16:49:49 GMT
- ⓘ Server: awselb/2.0

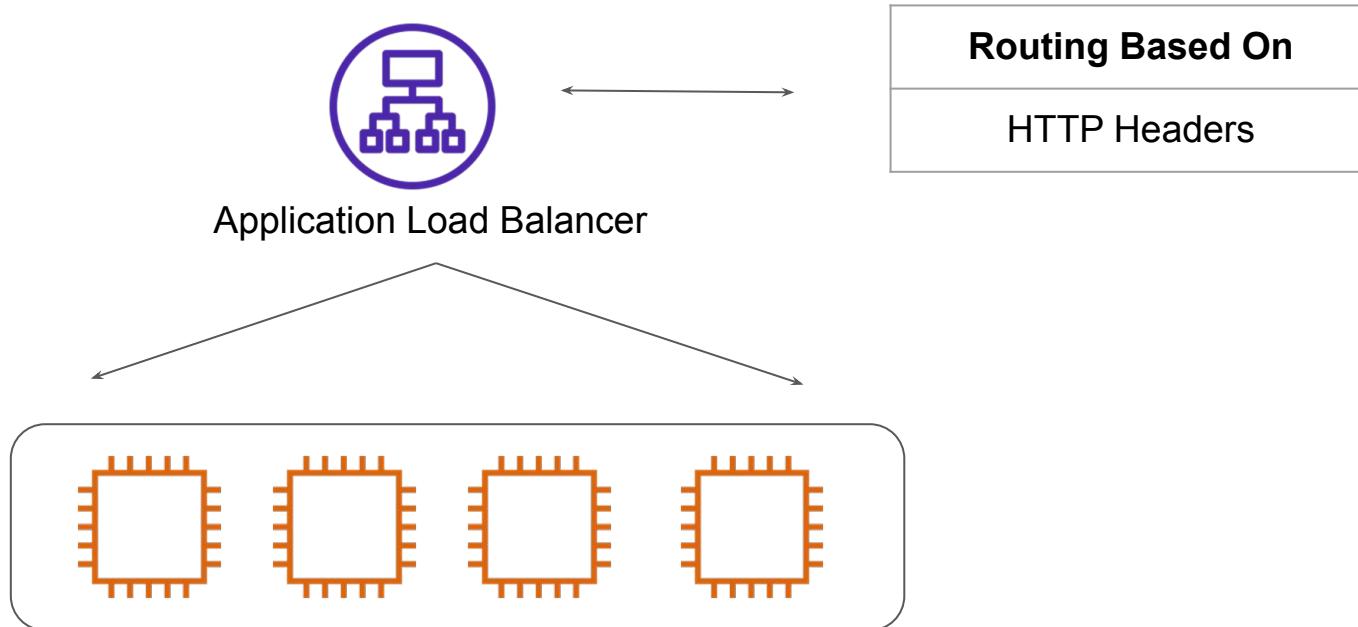
▼ Request Headers (380 B)

- ⓘ Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
- ⓘ Accept-Encoding: gzip, deflate
- ⓘ Accept-Language: en-US,en;q=0.5
- ⓘ Connection: keep-alive
- ⓘ Host: demo-alb-137613815.us-east-1.elb.amazonaws.com
- ⓘ Upgrade-Insecure-Requests: 1

ⓘ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

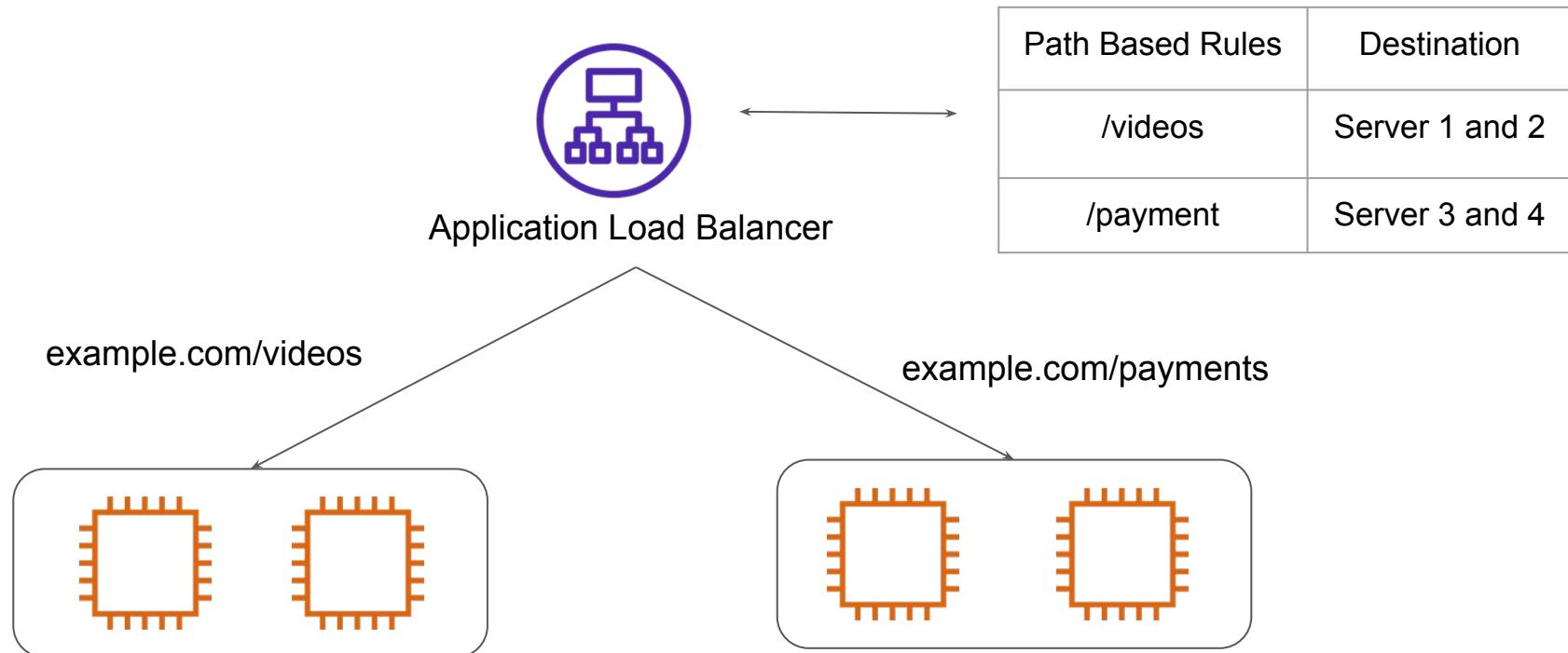
Understanding ALB

Application Load Balancer functions at Application layer and support both HTTP & HTTPS



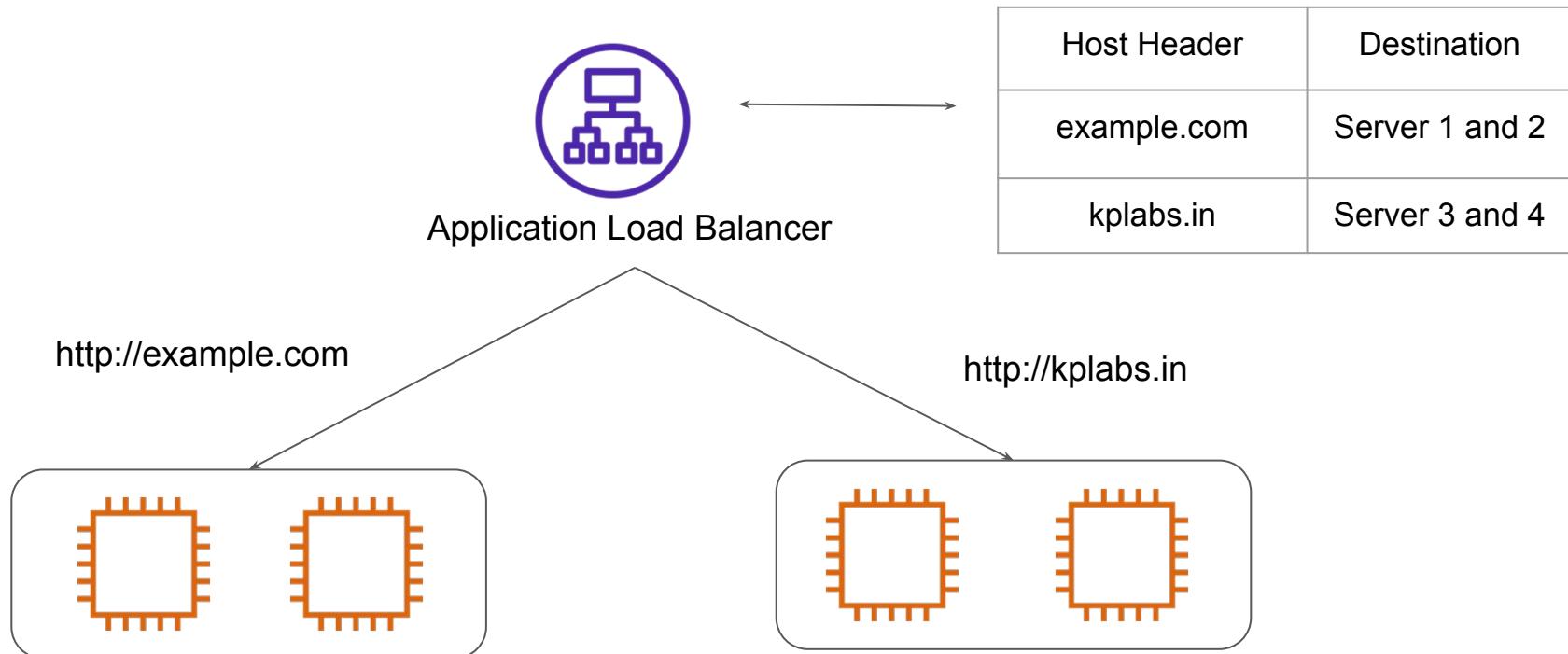
Path Based Routing

The requests are routed based on the URI path.



Routing Using Host Headers

The requests are routed based on the Host Header

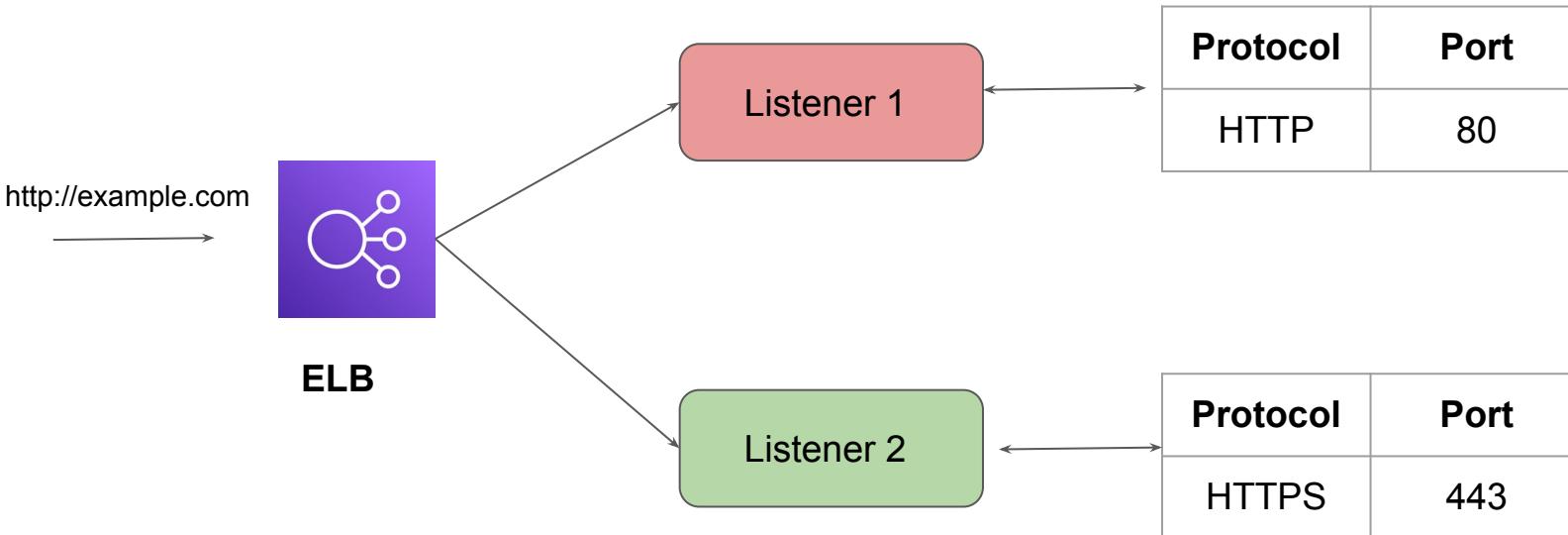


Listener & Target Groups

Next generation load balancers

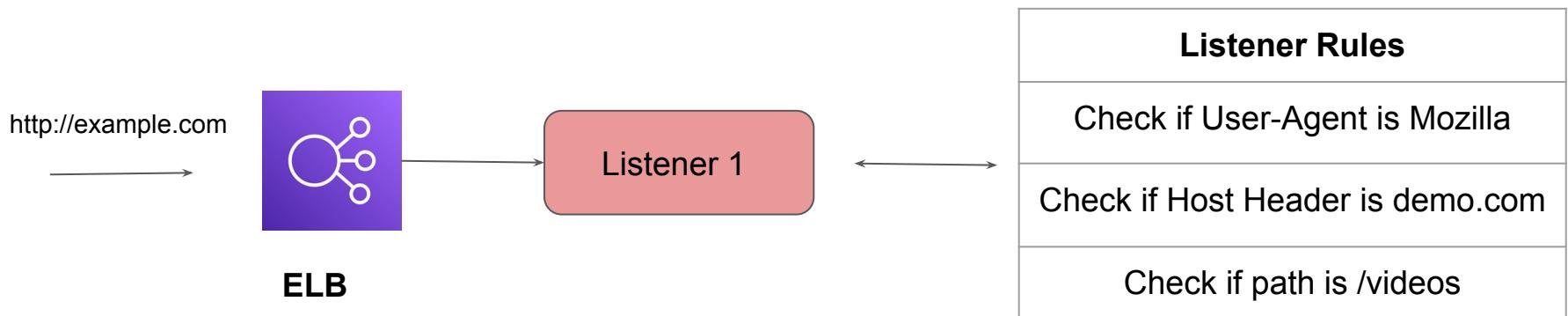
Understanding Listeners

A **listener** is a process that checks for connection requests, using the protocol and port that you configure.



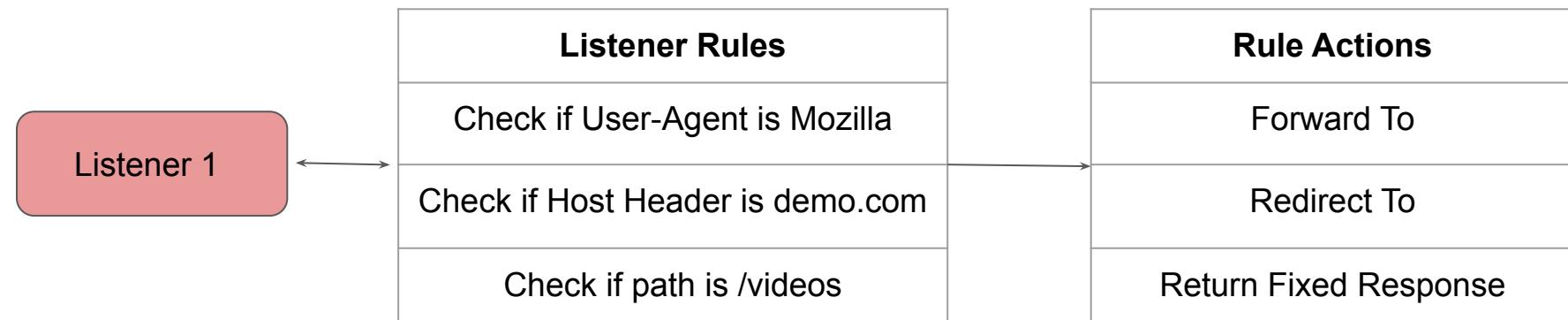
Listener Rules

Each listener has a rule based on which an action is taken based on a request.



Listener Rule Actions

If a request matches a specific rule, what action you want to perform on that request is determined in the Rule Actions.



demo-alb | HTTP:80 (4 rules)

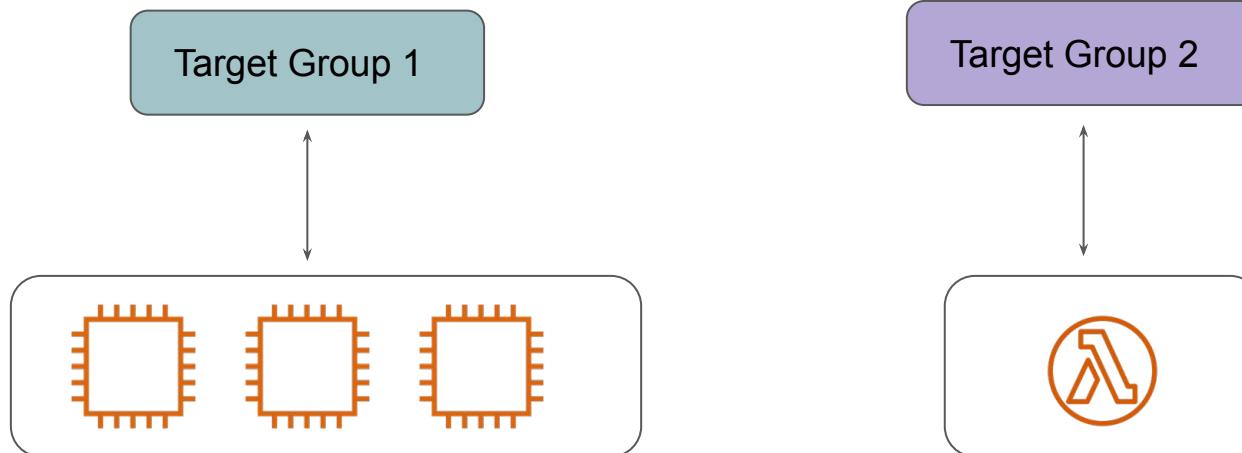
- ▶ Rule limits for condition values, wildcards, and total rules.

| | | |
|-----------------|--|--|
| 1 arn...93720 ▾ | IF ✓ Http header User-Agent is *curl* | THEN Return fixed response 200 Content-Type: text/plain Response body: Hi curl! (less...) |
| 2 arn...c9bc6 ▾ | IF ✓ Http header User-Agent is *Mozilla* | THEN Return fixed response 200 Content-Type: text/plain Response body: Hey Mozilla! You have great addons! (less...) |
| 3 arn...fdb85 ▾ | IF ✓ Http header User-Agent is *wget* | THEN Return fixed response 200 Content-Type: text/plain Response body: Hi There wget! I detected you. (less...) |

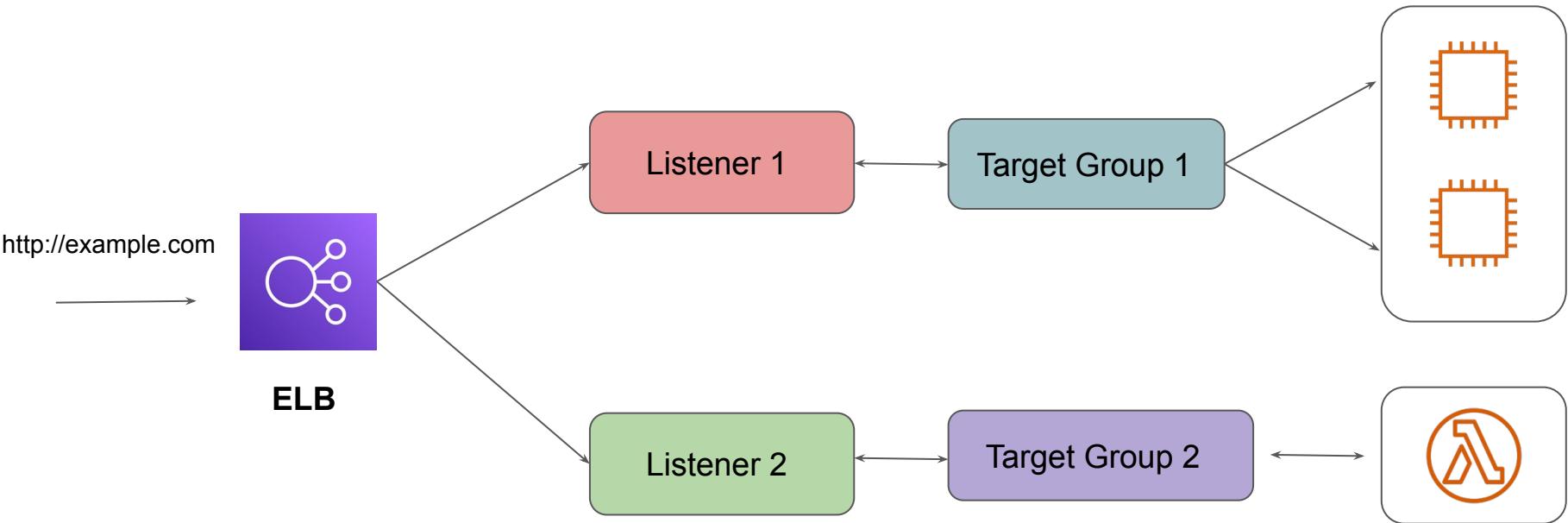
Understanding Target Groups

Target group is used to route requests to one or more registered targets.

These targets can be EC2 instances, Lambda Functions, and others.



Overall Workflow



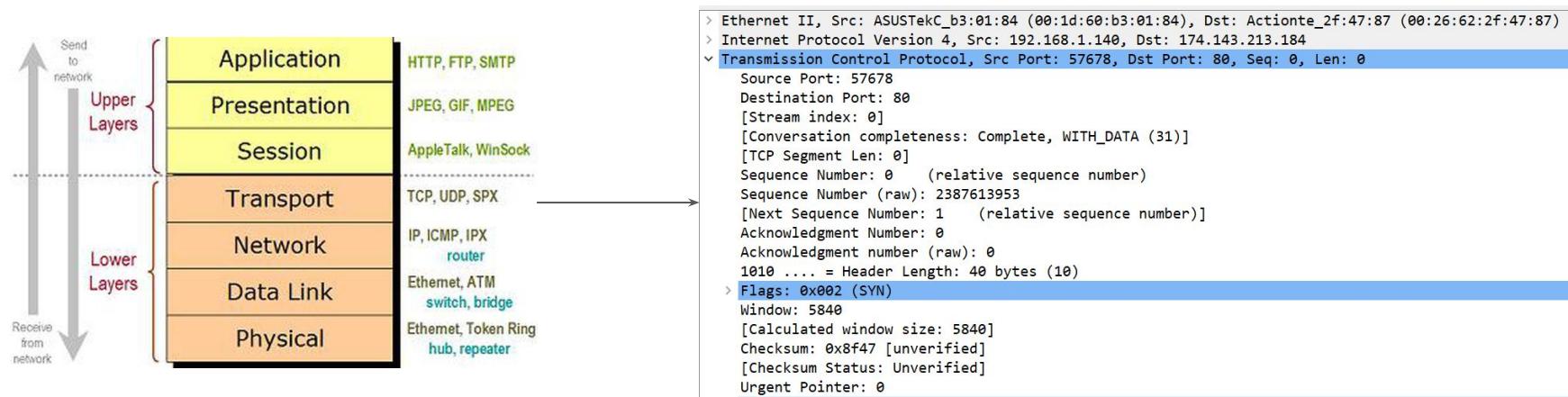
Network Load Balancers

Next generation load balancers

Understanding NLB

Network Load Balancer works on the fourth layer of the OSI model.

It can handle millions of requests per second.



Basic Working

NLB primarily selects a target using a **flow hash algorithm** based on:

Protocol, Source IP address, Source port, Destination IP address, Destination port, and TCP sequence number.

Each individual TCP connection is routed to a single target for the life of the connection.

ELB Access Logs

Who is Visiting Us?

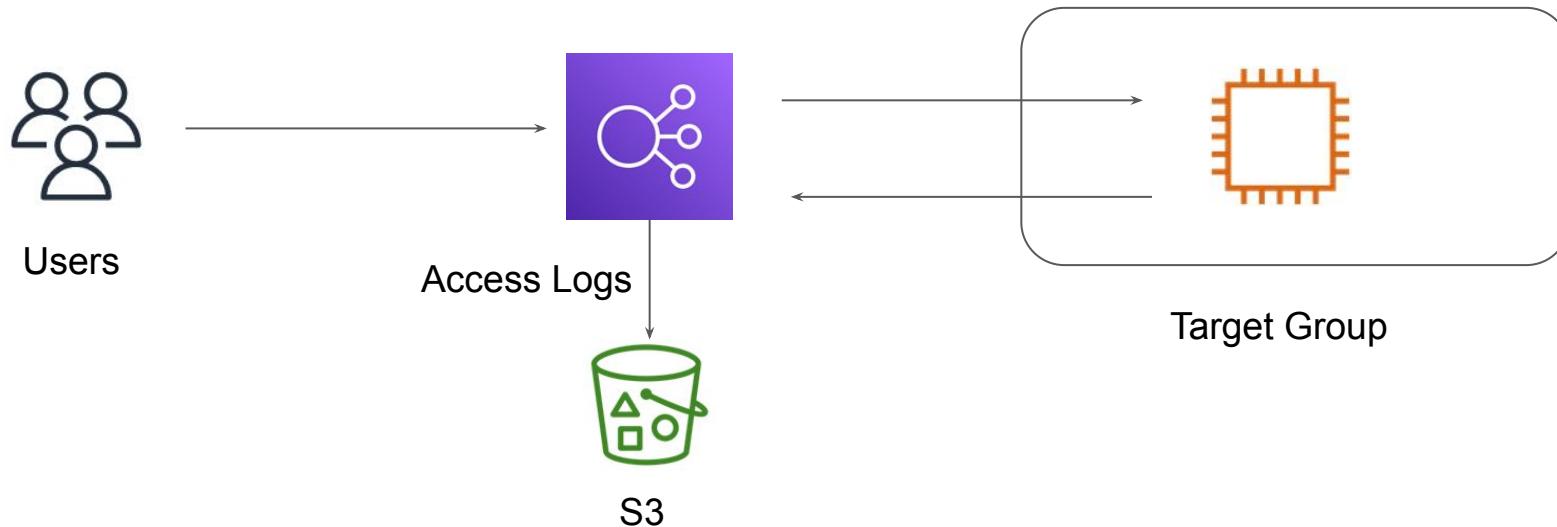
Overview of Access Logs

An access log is a list of all the requests for individual files that people have requested from a Web site

```
[root@ip-172-26-7-135 nginx]# tail -f access.log
128.14.133.58 - - [03/Sep/2021:04:43:10 +0000] "GET / HTTP/1.1" 200 82 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36" "-"
104.149.165.66 - - [03/Sep/2021:04:45:03 +0000] "HEAD /robots.txt HTTP/1.0" 404 0 "-" "-" "-"
92.118.160.57 - - [03/Sep/2021:05:02:42 +0000] "GET / HTTP/1.0" 200 82 "-" "NetSystemsResearch studies the availability of various services across the internet. Our website is netsystemsresearch.com" "-"
114.119.154.115 - - [03/Sep/2021:05:05:14 +0000] "GET /topic/blockchain/ HTTP/1.1" 404 153 "-" "Mozilla/5.0 (Linux; Android 7.0;) AppleWebKit/537.36 (KHTML, like Gecko) Mobile Safari/537.36 (compatible; PetalBot;+https://webmaster.petalsearch.com/site/petalbot)" "-"
135.125.244.48 - - [03/Sep/2021:05:11:08 +0000] "POST / HTTP/1.1" 405 559 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36" "-"
135.125.244.48 - - [03/Sep/2021:05:11:08 +0000] "GET /.env HTTP/1.1" 404 555 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36" "-"
109.49.235.11 - - [03/Sep/2021:05:12:32 +0000] "GET / HTTP/1.1" 200 82 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36" "-"
185.53.90.24 - - [03/Sep/2021:05:20:55 +0000] "GET http://icanhazip.com/ HTTP/1.1" 200 82 "-" "Go-http-client/1.1" "-"
114.119.154.11 - - [03/Sep/2021:05:28:51 +0000] "GET /topic/graphic-design/ HTTP/1.1" 404 153 "-" "Mozilla/5.0 (Linux; Android 7.0;) AppleWebKit/537.36 (KHTML, like Gecko) Mobile Safari/537.36 (compatible; PetalBot;+https://webmaster.petalsearch.com/site/petalbot)" "-"
199.168.150.161 - - [03/Sep/2021:05:39:07 +0000] "GET / HTTP/1.1" 302 145 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36" "-"
```

ELB Access Logs

Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer.



Important Pointers for Access Logs - Part 1

Access logging is an optional feature of Elastic Load Balancing that is disabled by default

Elastic Load Balancing logs requests on a best-effort basis. AWS recommend that you use access logs to understand the nature of the requests, not as a complete accounting of all requests.

Important Pointers for Access Logs - Part 2

The bucket and your load balancer must be in the same Region.

Bucket Policy should be designed so that AWS Account must be able to write to your bucket.

Elastic Load Balancing publishes a log file for each load balancer node every 5 minutes.

Relax and Have a Meme Before Proceeding



alcohol
@Mandac5

What is an extreme sport?



allison
@amazaleax

Doing your homework while the
teacher is collecting it

Capturing Client IP Behind ELB



Understanding the Challenge

In a typical setup, the backend application does not receive the IP address of client.



Points to Note

| Load Balancer Type | Description |
|---------------------------|---|
| Classic Load Balancer | <p>For HTTP based listeners, Client IP is forwarded by default to the servers.</p> <p>For TCP based listeners, Proxy Protocol needs to be enabled.</p> |
| Application Load Balancer | <p>Client IP is passed with the request. Use X-Forwarded-For headers in application to capture the client address.</p> |
| Network Load Balancer | <p>Client IP preservation is enabled (and can't be disabled) for instance and IP type target groups with UDP and TCP_UDP protocols.</p> <p>You can enable or disable client IP preservation for TCP and TLS target groups</p> |

HTTPS

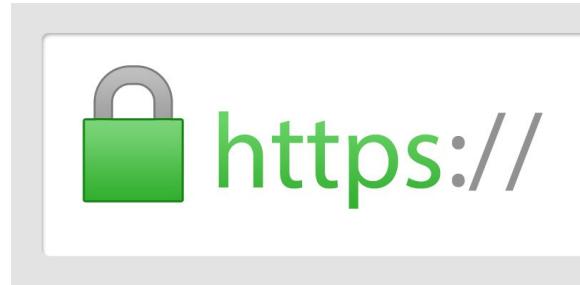
Secure Communication

Overview of HTTPS

HTTPS is an extension of HTTP.

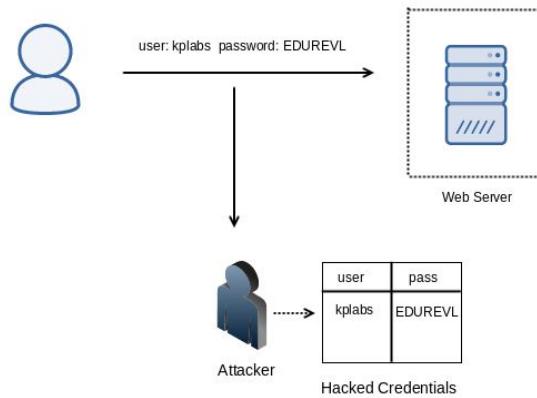
In HTTPS, the communication is encrypted using Transport Layer Security (TLS)

The protocol is therefore also often referred to as HTTP over TLS or HTTP over SSL.



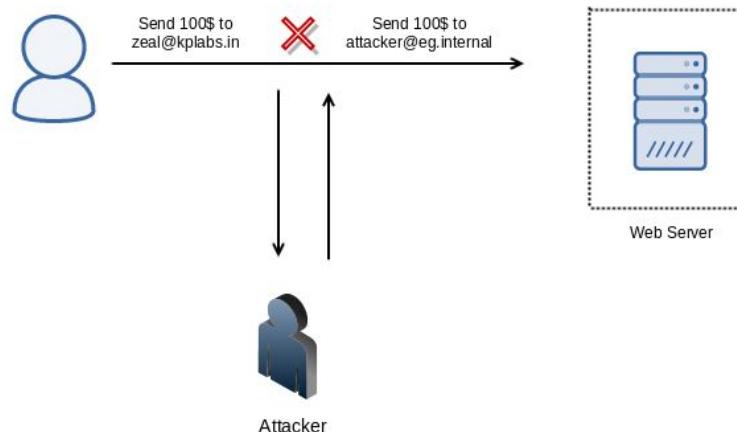
Scenario 1: MITM Attacks

- User is sending their username and password in plaintext to a Web Server for authentication over a network.
- There is an Attacker sitting between them doing a MITM attack and storing all the credentials he finds over the network to a file:



Scenario 2: MITM & Integrity Attacks

- Attacker changing the payment details while packets are in transit.



Introduction to SSL/TLS

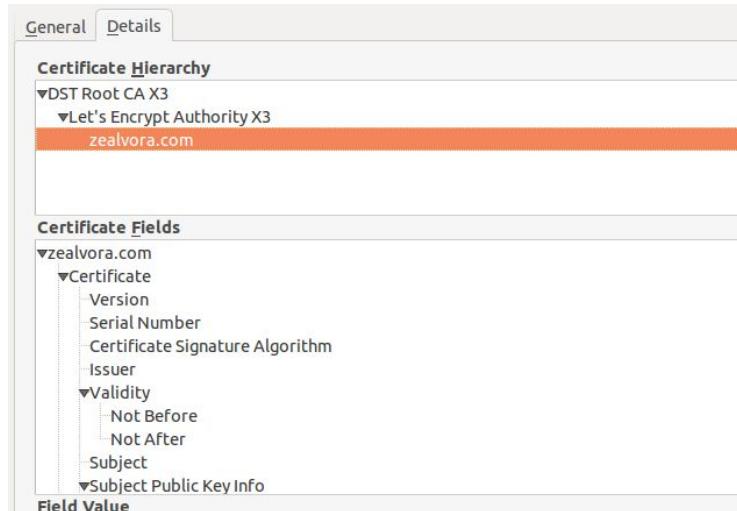
To avoid the previous two scenarios (and many more), various cryptographic standards were clubbed together to establish a secure communication over an untrusted network and they were known as SSL/TLS.

| Protocol | Year |
|----------|------|
| SSL 2.0 | 1995 |
| SSL 3.0 | 1996 |
| TLS 1.0 | 1999 |
| TLS 1.1 | 2006 |
| TLS 1.2 | 2008 |
| TLS 1.3 | 2018 |

Understanding it in easy way

Every website has a certificate (like a passport which is issued by a trusted entity).

Certificate has lot of details like domain name it is valid for, the public key, validity and others.



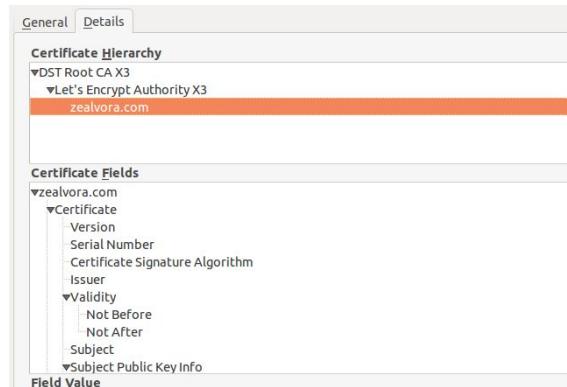
Understanding it in easy way

Browser (clients) verifies if it trusts the certificate issuer.

It will verify all the details of the certificate.

It will take the public key and initiate a negotiation.

Asymmetric key encryption is used to generate a new temporary symmetric key which will be used for secure communication.



Web Server Configuration

```
server {
    listen      80;
    server_name zealvora.com;
    return      301 https://$server_name$request_uri;
}

server {
    server_name zealvora.com;
    listen 443 default ssl;
    server_name zealvora.com;
    ssl_certificate /etc/letsencrypt/archive/zealvora.com/fullchain1.pem;
    ssl_certificate_key /etc/letsencrypt/archive/zealvora.com/privkey1.pem;

    location / {
        root /websites/zealvora/;
        include location-php;
        index index.php;
    }
    location ~ /.well-known {
        allow all;
    }
}
```

AWS Certificate Manager

Certificates Again :)

Earlier Approach

I have a website and I need to use HTTPS. There are two ways, self-signed certificate and the CA signed certificate.



Self Signed Certificate



CA Signed Certificate

Generating Certificates

To generate a certificate for your domain, you will have to go to a Certificate Authority and after required level of validation, you would be issued a certificate.



User

Generate certificate for kplabs.in



Validated for 1 year.

cert

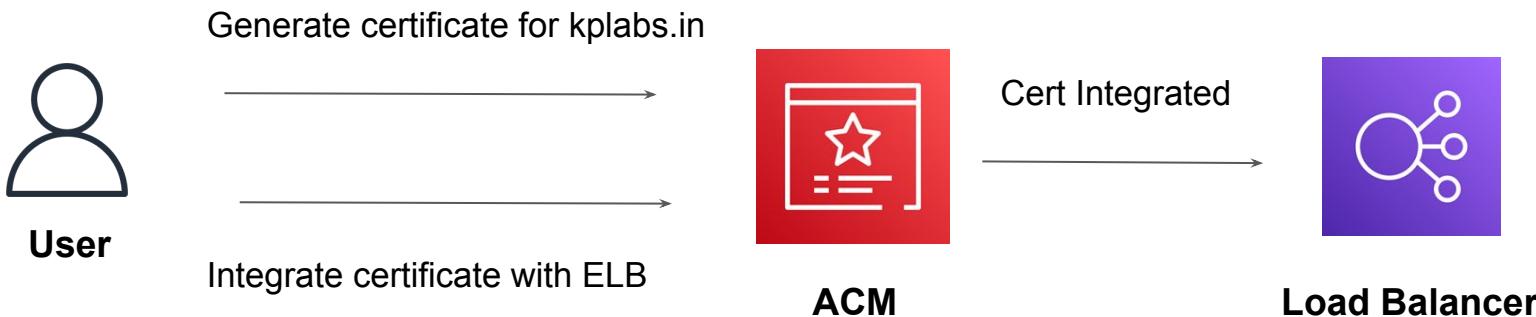
private key



Certificate Authority

AWS Certificate Manager

AWS Certificate Manager (ACM) handles the complexity of creating, storing, and renewing public and private SSL/TLS X.509 certificates and keys that protect your AWS websites and applications.



HTTPS Listener



Understanding the Challenge

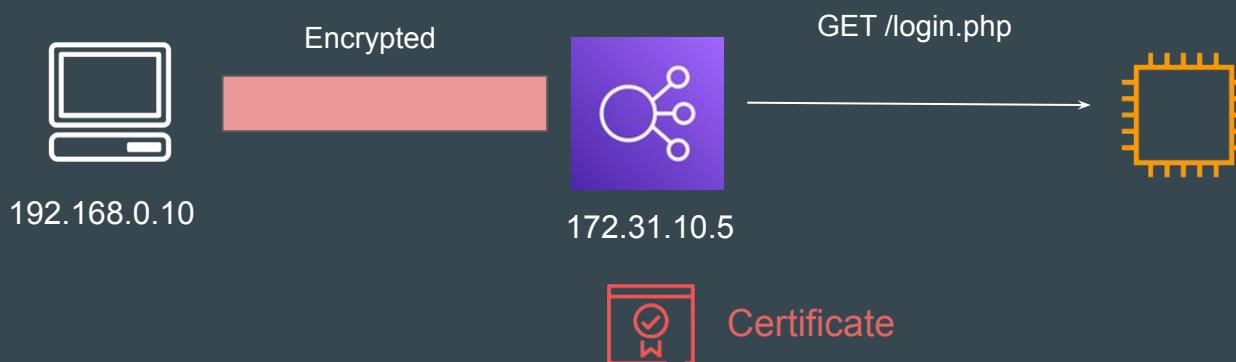
In a typical setup, the end to end connection through ELB remains unencrypted.



Basic Architecture

You can create an HTTPS listener, which uses encrypted connections (also known as SSL offload).

This feature enables traffic encryption between your load balancer and the clients that initiate SSL or TLS sessions.



Points to Note

To use an HTTPS listener, you must deploy at least one SSL/TLS server certificate on your load balancer.

The load balancer uses a server certificate to terminate the front-end connection and then decrypt requests from clients before sending them to the targets.

The screenshot shows the AWS CloudFront Listener configuration page. The top navigation bar includes tabs for Listeners, Network mapping, Security, Monitoring, Integrations, Attributes, and Tags. The 'Listeners' tab is selected, highlighted in blue. Below the tabs, a section titled 'Listeners (1)' is displayed. A descriptive text states: 'A listener checks for connection requests on its port and protocol. Traffic received by the listener is routed according to its rules.' A search bar labeled 'Search' is present. The main table lists one listener entry:

| Protocol:Port | ARN | Security policy | Default SSL cert | Default routing rule |
|---------------|---------------------------|--|--|----------------------|
| HTTPS:443 | ELBSecurityPolicy-2016-08 | kplabsinternal.com (Certificate ID: 4e0b46...) | 1. Forward to <ul style="list-style-type: none">https-target-group: 1 (100%)Group-level stickiness: Off | |

End to End Encryption

With ALB, you can terminate the connection at ALB level and Initiate new encrypted connection to EC2.

If you need to pass encrypted traffic to targets without the load balancer decrypting it, you can create a Network Load Balancer or Classic Load Balancer with a TCP listener on port 443.



Glacier Vault

Security Angle

Overview of AWS Glacier

AWS Glacier is an extremely low-cost storage service which provides secure as well as durable storage for data backup and archival.

With respect to security, there are two things to remember:

- Access to the data in Glacier can be controlled with IAM.
- Data in glacier is also encrypted using SSE (server side encryption).

- For customers who intends to manage own keys, they can encrypt data before uploading it.

Understanding Vault

In Glacier, data is stored as archives.

Vault is a way in which the archives are grouped together in Glacier

We can control who has access to the data by setting up vault-level access policies using IAM.

We also have vault-level policy that we can attach directly to the Glacier Vault.

Glacier Vault Lock

Glacier Vault Lock allows you to easily deploy and enforce compliance controls for individual Glacier vaults with a vault lock policy.

You can specify controls such as “write once read many” (WORM) in a vault lock policy and lock the policy from future edits.

One great thing about Vault Lock policy is that they are **immutable**.

DynamoDB Encryption

Security Primer

Overview of DynamoDB Encryption

If an organization is storing sensitive data in DynamoDB , it is ideal to encrypt the data as close to the origin so that the data remains protected throughout the lifecycle.

We can make use of DynamoDB Encryption Client to protect the data in table even before we send it to DynamoDB.

DynamoDB Client can be used with AWS KMS or even CloudHSM.

The library by itself does not require AWS service, we can use our own crypto Keys and manage them ourselves.

DynamoDB Encryption At Rest

AWS came up with new feature of encryption at rest for DynamoDB.

This allows us to encrypt our data at rest in DynamoDB using AWS KMS.

The table will be encrypted using AES-256.

Encryption Context

Let's Secure

Understanding Challenge - Step 1

E-Commerce website has decided to store the physical address of the customers and associate it with the email address of their accounts.

Every year, E-Commerce decides to send a unique expensive gift to all of their customers.

| Email Address | Physical Address |
|-------------------|------------------|
| alice@example.com | ABC |
| bob@example.com | XYZ |
| john@example.com | DEF |

Understanding Challenge - Step 2

For better security, it was decided to encrypt the physical address with the KMS.

| Email Address | Physical Address |
|-------------------|------------------|
| alice@example.com | #123\$%^ |
| bob@example.com | #9029\$%^ |
| john@example.com | #567\$%# |

Understanding Challenge - Step 3

John is a Developer in the E-Commerce organization and has access to the DynamoDB table.

He decides to replace the cipher text address to that of his for the Alice and bob users.

| Email Address | Physical Address |
|-------------------|------------------|
| alice@example.com | #123\$%^ |
| bob@example.com | #9029\$%^ |
| john@example.com | #567\$%# |

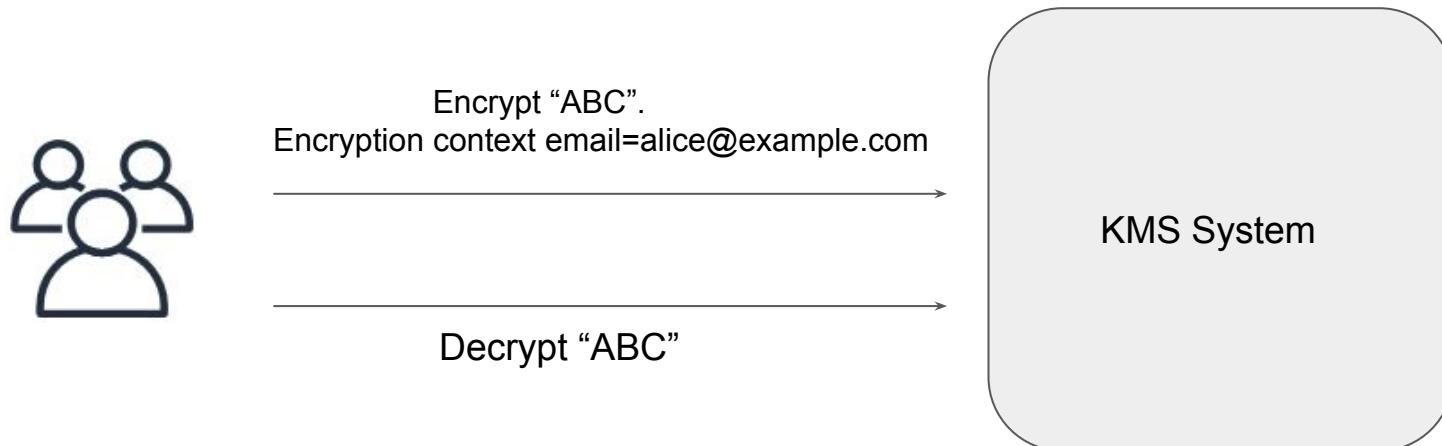


| Email Address | Physical Address |
|-------------------|------------------|
| alice@example.com | #567\$%# |
| bob@example.com | #567\$%# |
| john@example.com | #567\$%# |

Overview of Encryption Context

All AWS KMS cryptographic operations with symmetric CMKs accept an encryption context, an optional set of key-value pairs that can contain additional contextual information about the data.

AWS KMS uses the encryption context as additional authenticated data (AAD) to support authenticated encryption.



Decryption Process



High-Level Overview Solution

| Email Address | Physical Address |
|-------------------|------------------------------|
| alice@example.com | #123\$%^ + alice@example.com |
| bob@example.com | #9029\$%^ + bob@example.com |
| john@example.com | #567\$%^# + john@example.com |

High-Level Overview Solution

| Email Address | Physical Address |
|-------------------|-----------------------------|
| alice@example.com | #567\$%# + john@example.com |
| bob@example.com | #567\$%# + john@example.com |
| john@example.com | #567\$%# + john@example.com |

Decrypt “ABC”

Encryption context email=alice@example.com

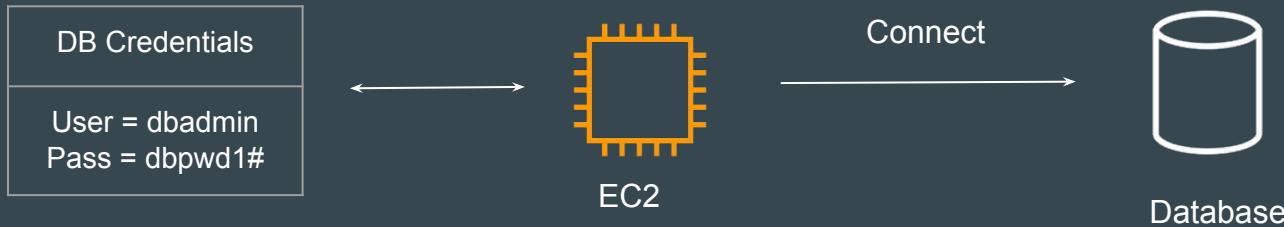
AWS Secrets Manager



Understanding the Challenge

In many organizations, secrets are hard coded directly as part of the application.

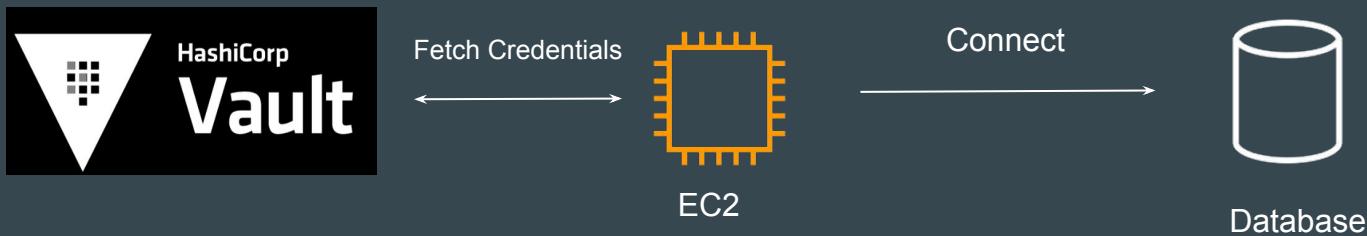
If you want to rotate the secret credential, all the application server needs to be updated. If you miss one, the production can go down.



Introducing Secrets Management

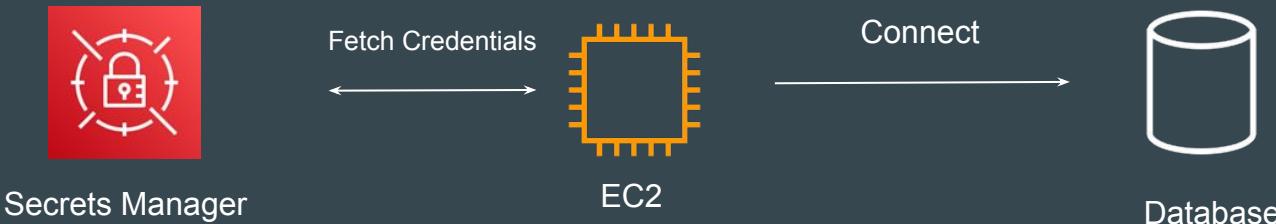
Secret management is a practice that allows developers to securely store sensitive data, such as passwords, keys, and tokens, in a secure environment with strict access controls.

Popular Tools: HashiCorp Vault, AWS Secrets Manager

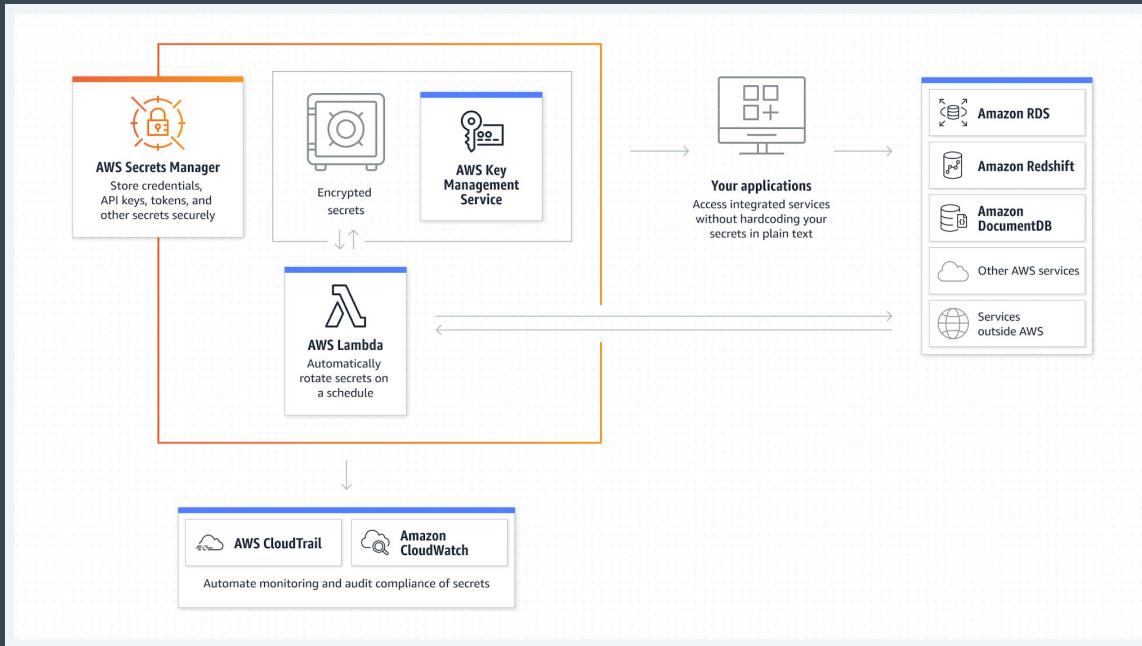


Introduction to Topic

AWS Secrets Manager helps you manage, retrieve, and rotate database credentials, API keys, and other secrets throughout their lifecycles.



Referenced from Docs



Rotate AWS Secrets Manager secrets

Rotation is the process of periodically updating a secret.

Secrets Manager rotation uses an AWS Lambda function to update the secret and the database.

To rotate a secret, Secrets Manager calls a Lambda function according to the schedule you set up. You can set a schedule to rotate after a period of time, for example, every 30 days.

Relax and Have a Meme Before Proceeding



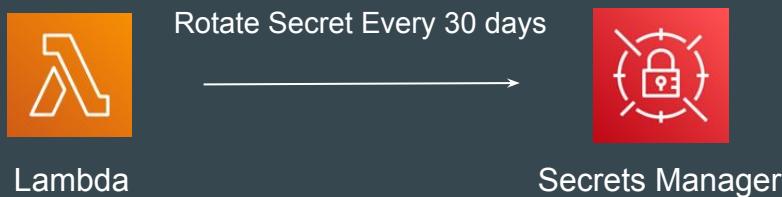
Rotating Secrets



Basics of Rotation

Rotation is the process of periodically updating a secret.

Secrets Manager rotation uses an AWS Lambda function to update the secret and the database.



Points to Note

To rotate a secret, Secrets Manager calls a Lambda function according to the schedule you set up. You can set a schedule to rotate after a period of time, for example, every 30 days.

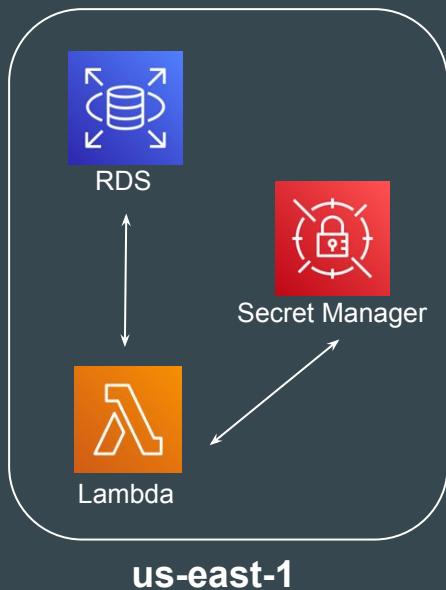
Secrets Manager provides rotation function templates for various use-cases related to RDS, DocumentDB, RedShift etc.

Replicate AWS Secrets Manager secrets



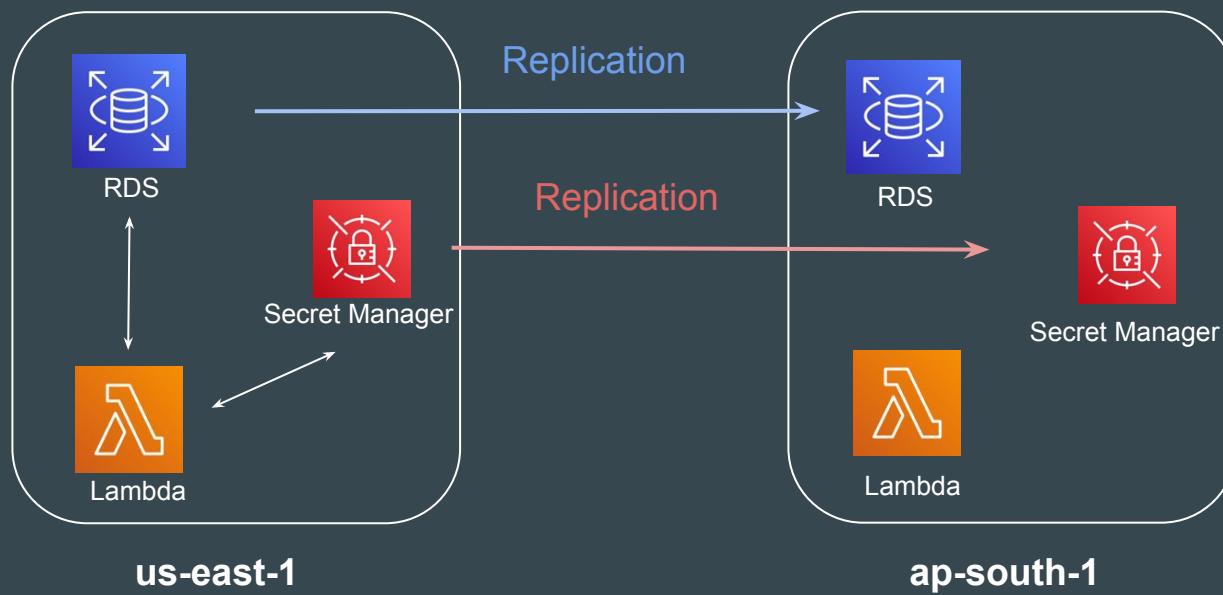
Understanding with Use-Case

In a Disaster Recovery based architecture, it is necessary to setup necessary level of replication across regions for failover.



Replicating Data Across Regions

In this architecture, the data and secrets are replicated across regions.



Points to Note

You can replicate your secrets in multiple AWS Regions to support applications spread across those Regions to meet Regional access and low latency requirements.

If you later need to, you can promote a replica secret to a standalone and then set it up for replication independently.

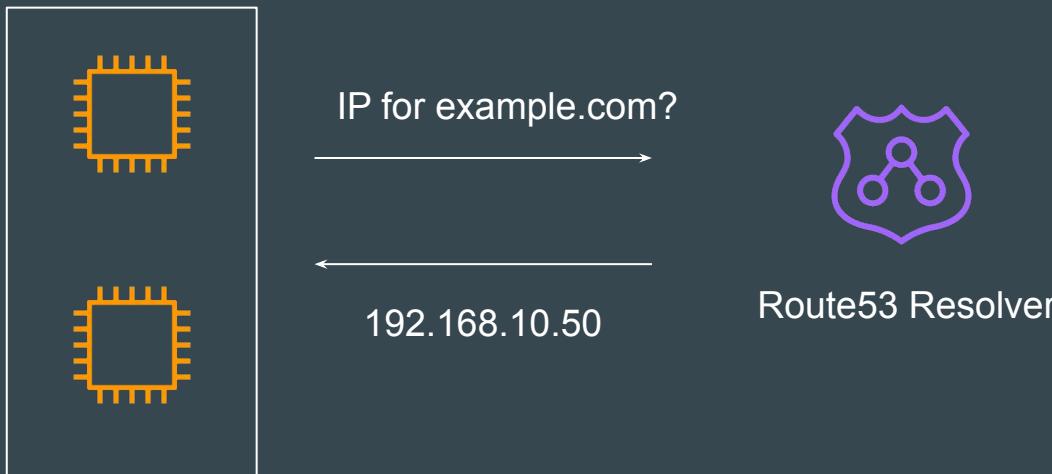
If you turn on rotation for your primary secret, Secrets Manager rotates the secret in the primary Region, and the new secret value propagates to all of the associated replica secrets.

Route53 Resolver



Understanding the Basics

Amazon Route 53 Resolver **responds to DNS queries** from AWS resources for public records, Amazon VPC-specific DNS names, and Amazon Route 53 private hosted zones, and is available by default in all VPCs.



Address of Route53 Resolver

An Amazon VPC connects to a Route 53 Resolver at a **VPC+2** IP address.



Contents of `/etc/resolv.conf` file of EC2 instance.

```
[ec2-user@ip-172-31-86-117 ~]$ cat /etc/resolv.conf
; generated by /usr/sbin/dhclient-script
search ec2.internal
options timeout:2 attempts:5
nameserver 172.31.0.2
```

Query Resolution

A Route 53 Resolver automatically answers DNS queries for:

1. Local VPC domain names for EC2 instances (for example, ec2-192-0-2-44.compute-1.amazonaws.com).
2. Records in private hosted zones (for example, acme.example.com).
3. For public domain names, Route 53 Resolver performs recursive lookups against public name servers on the internet.

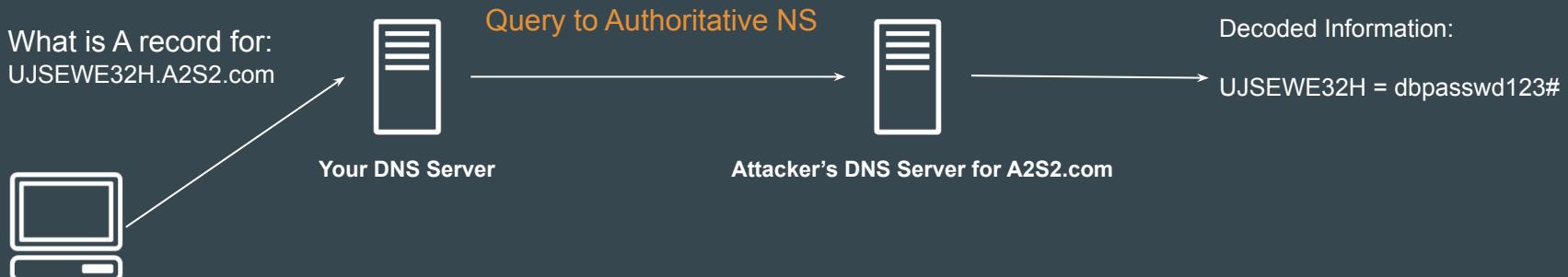
Route 53 Resolver DNS Firewall



DNS Exfiltration Attack

DNS data exfiltration is a way to exchange data between two computers without any direct connection.

The data is exchanged through DNS protocol on intermediate DNS servers.

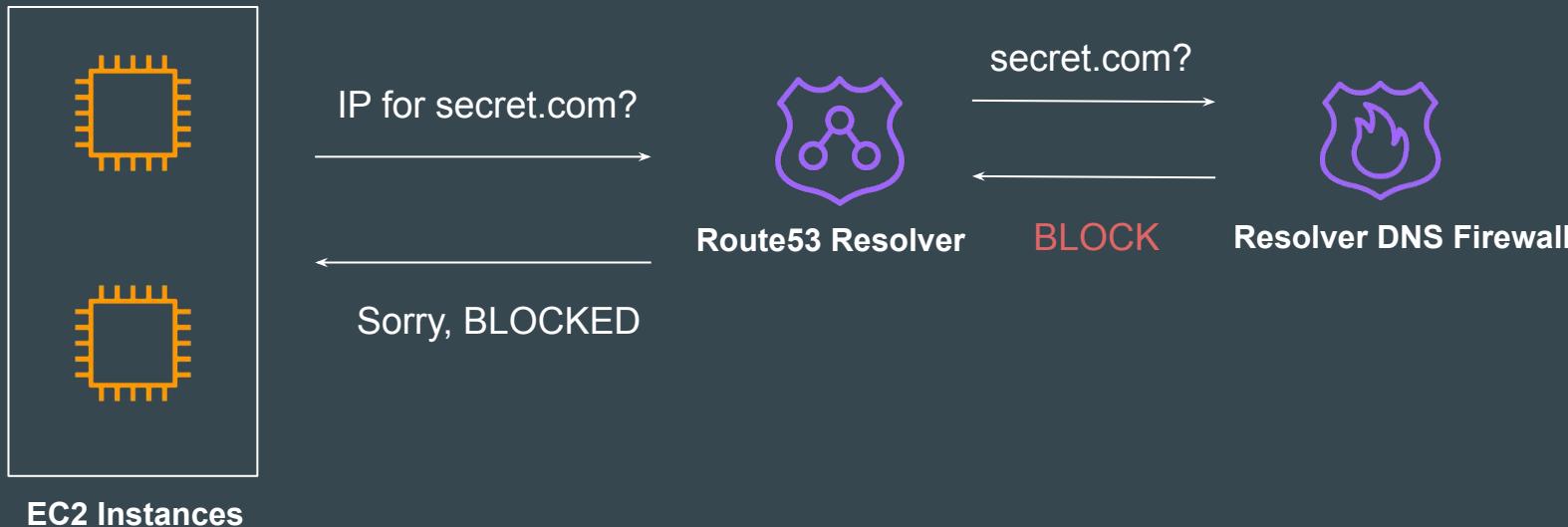


Encoded Stolen Information:

dbpasswd123# = UJSEWE32H

Understanding the Basics

With Route 53 Resolver DNS Firewall, you can **filter and regulate outbound DNS traffic** for your virtual private cloud (VPC).



Points to Note

You can deny access to the domains that you know to be bad and allow all other queries to pass through.

Alternately, you can deny access to all domains except for the ones that you explicitly trust.

You can use Firewall Manager to centrally configure and manage your DNS Firewall rule group associations for your VPCs across your accounts in AWS Organizations

A **primary use of DNS Firewall** protections is to help prevent DNS exfiltration of your data.

AWS Managed Domain List

AWS Managed Domain Lists contain domain names that are associated with malicious activity or other potential threats.

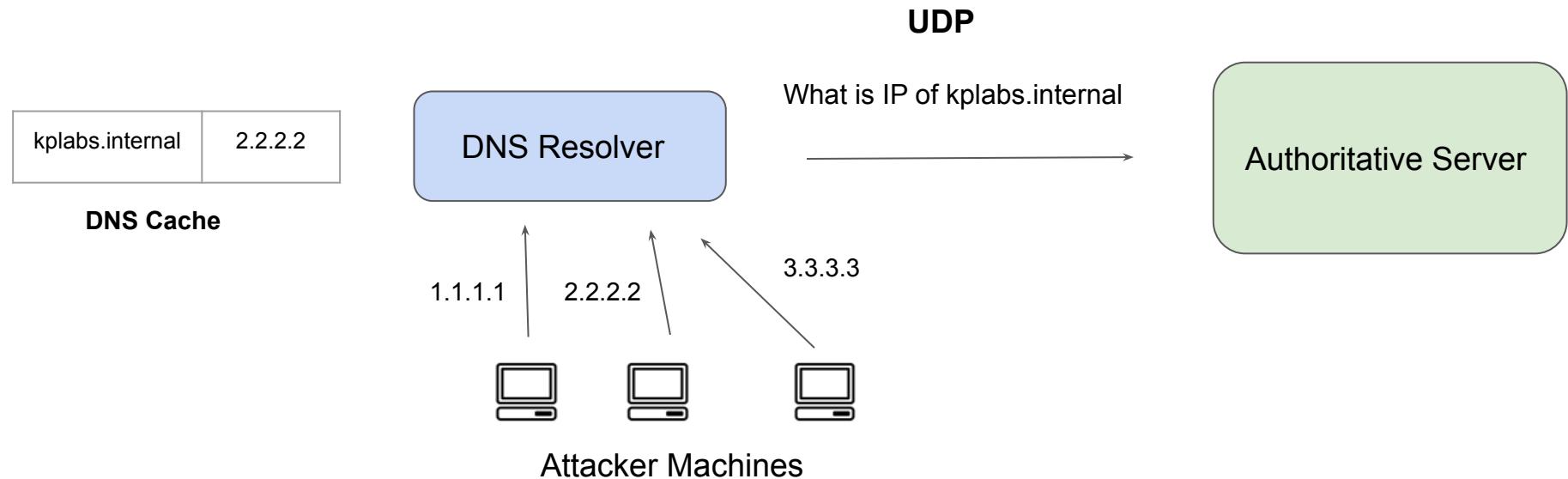
| AWS managed domain lists (3) | | |
|--|---|----------------------------|
| These domain lists are in Region US East (N. Virginia). | | |
| <input type="text"/> <input type="button" value="Search"/> | | |
| Name | ▲ | ID |
| <input type="radio"/> AWSManagedDomainsAggregateThreatList | | rslvr-fdl-15f4860b1ad54ead |
| <input type="radio"/> AWSManagedDomainsBotnetCommandAndControl | | rslvr-fdl-aa970e9eb1ca4777 |
| <input type="radio"/> AWSManagedDomainsMalwareDomainList | | rslvr-fdl-2c46f2ecbfec4dcc |

DNS Cache Poisoning

Compromising DNS

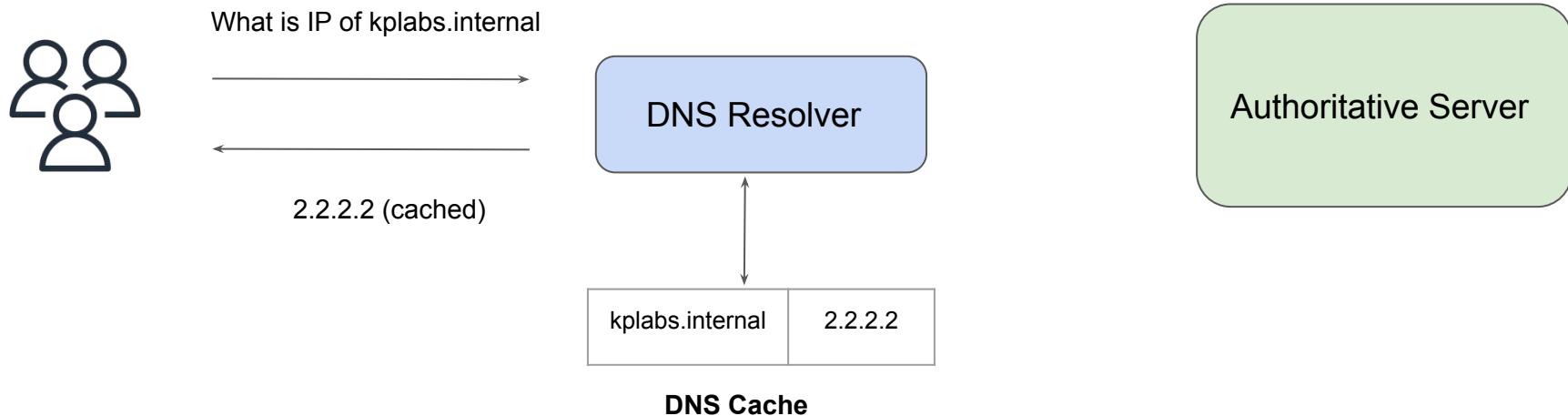
Understanding DNS Cache Poisoning

DNS cache poisoning is a hacking attack in which false information is entered into a DNS cache, so that DNS queries return an incorrect response and users are directed to the wrong websites



Client and DNS Resolver

When the client queries the resolved, they would receive the Cached response.



Important Note

In UDP, since there is no handshake that takes place, it is vulnerable to forging.

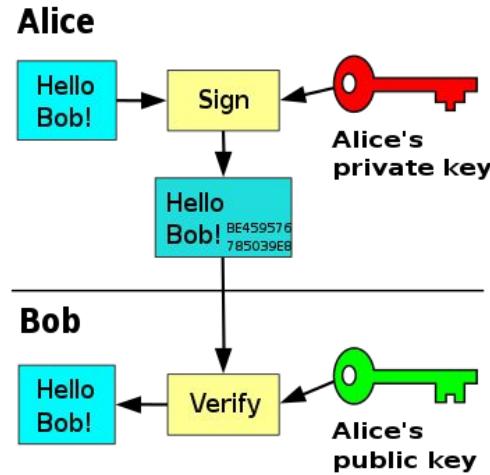
If a DNS resolver receives a forged response, it accepts and caches the data because there is no way to verify if the information is accurate and comes from a legitimate source.

DNSSEC

Securing DNS

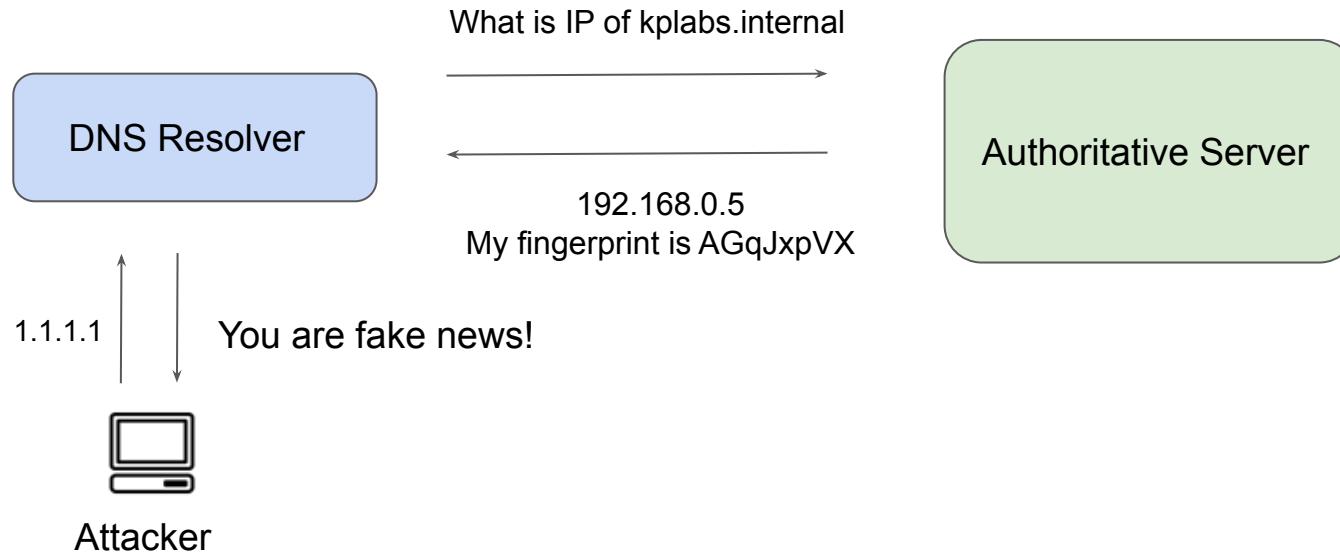
Revising Digital Signatures

Digital signatures are used to ensure that one party cannot successfully dispute its authorship of a document or communication.



Basics of DNSSEC

DNSSEC creates a secure domain name system by adding cryptographic signatures to existing DNS records.



High-Level Pointers

It makes use of Asymmetric key encryption (public and private keys involved)

Public keys are published in the DNS.

Private keys are kept secure and used to digitally sign.

The DNS query response is validated using Public key.

Disadvantages of DNSSEC

It adds complexity both on the client and server side.

Limited support from TLD and DNS servers

Increase in DNS Query Resolution Time

Relax and Have a Meme Before Proceeding

"i have to go home i have so much stuff
to do"
me when i get home:

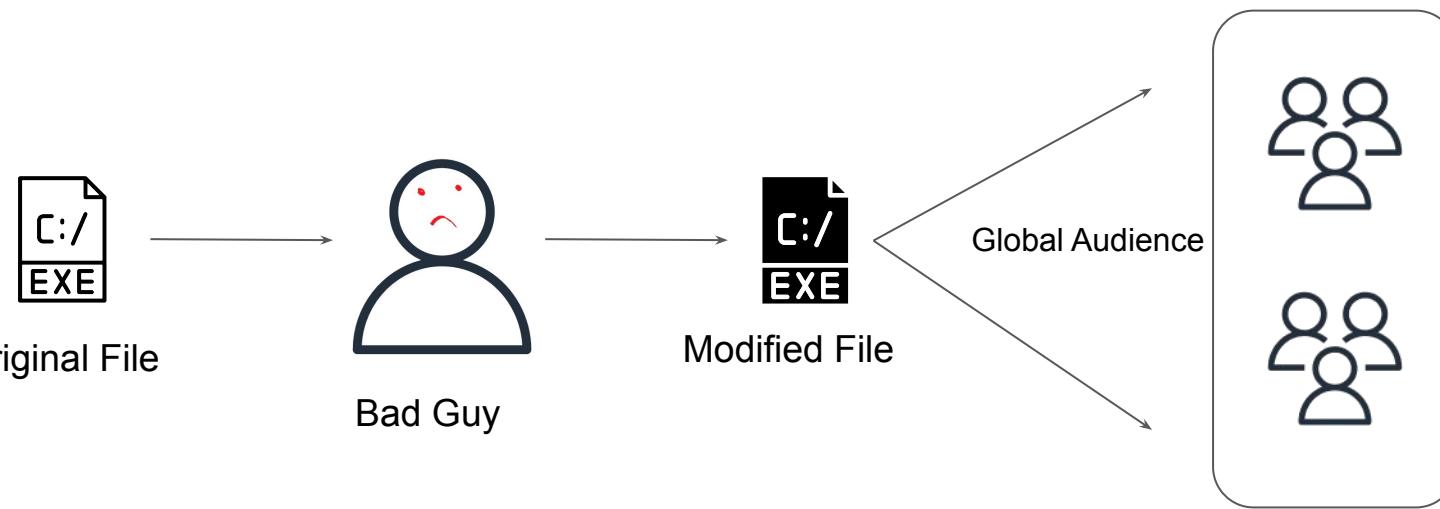


AWS Signer

Code Signing is Important

Understanding the Challenge

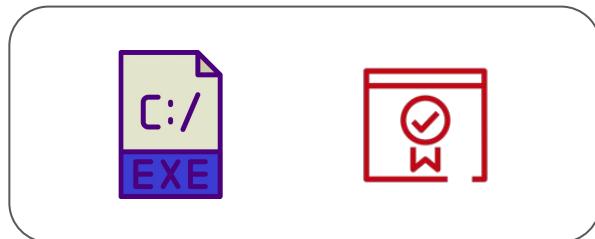
It is very easy to infect a code file to include custom backdoor and distribute it to global audience.



Basics of Code Signing Certificate

Code Signing Certificates are used by software developers to digitally sign applications, drivers, executables and software programs.

Ensures that the code is not altered or compromised.

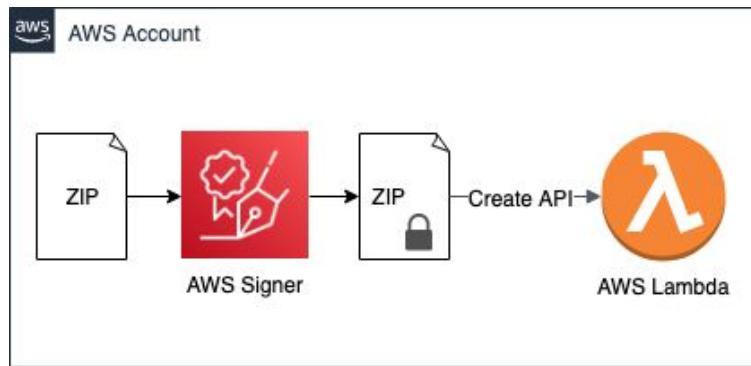


Signed Code

AWS Signer

AWS Signer is a fully managed code-signing service to ensure the trust and integrity of your code.

Organizations validate code against a digital signature to confirm that the code is unaltered and from a trusted publisher.



Supported Services

With Code Signing for AWS Lambda, you can ensure that only trusted code runs in your Lambda functions.

With Code Signing for AWS IoT, you can sign code that you create for IoT devices supported by Amazon FreeRTOS and AWS IoT device management.

Step 1 - Create Signing Profile

A Signing Profile is a trusted publisher and is comparable to the use of a digital signing certificate to generate signatures for your code.

Creating a Profile through the console is only supported for AWS Lambda Platform.

Signing Profile details

Profile name
Enter a unique name for your Signing Profile.

Profile name must contain from 2 to 64 characters. Valid characters are lowercase a-z, uppercase A-Z, 0-9, and _ (underscore).

Signature validity period - optional
Specify the Signature Validity period for the signatures generated by a Signing Profile. The default is 135 months.
 Months

Validity period must be between 1 day and 135 months (11 years and 3 months).

Tags - optional
Assign tags to your AWS resource. You must specify a Tag key and an optional Tag Value. You can manage access to your profiles using Tag-based resource policies.

Tag key Tag value - optional

You can add 49 more tag(s).

Step 2 - Code Signing Configuration

To enable code signing for a function, you create a code signing configuration and attach it to the function

A code signing configuration defines a list of allowed signing profiles and the policy action to take if any of the validation checks fail.

Signing profile and policy configuration

Description
Enter a description to identify this configuration when you view it in a list or add it to a function.

The maximum length is 256 characters.

Signing profiles [Info](#)
Choose or enter a signing profile version ARN. To create a signing profile, use AWS Signer [Create](#)
Signing profile version ARN

[Delete](#)

Add signing profiles
You can add 19 more signing profiles.

Signature validation policy [Info](#)

Warn
Deployments succeed with a warning logged to CloudWatch.

Enforce
Block deployments when code is signed by an unapproved profile, or if the signature is expired or revoked.

[Cancel](#) [Create configuration](#)

Step 3 - Create Signing Job

Create a signing job that can sign a specific code file from destination like S3 bucket.

Start Signing Job

A Signing Job is an asynchronous process to generate a signature for your code. Starting a Job through the console is only supported for AWS Lambda Platform.

Signing Job details

Signing Profile to use
Choose the Signing Profile to perform code signing.

Code asset source location
Specify the S3 location of the code asset to be signed. Only ZIP formatted assets are accepted.

S3Uri Object version

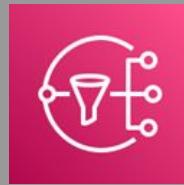
Only buckets in current region are displayed. Cross region signing is not supported.

Signature destination path with prefix
Specify the S3 path to upload the signature. The signature object name will be the provided prefix appended with the Signing Job ID.

S3Uri

Only buckets in current region are displayed. Cross region signing is not supported.

EBS Snapshots



Understanding the Basics

You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots.

You can create a new volume from the snapshot.

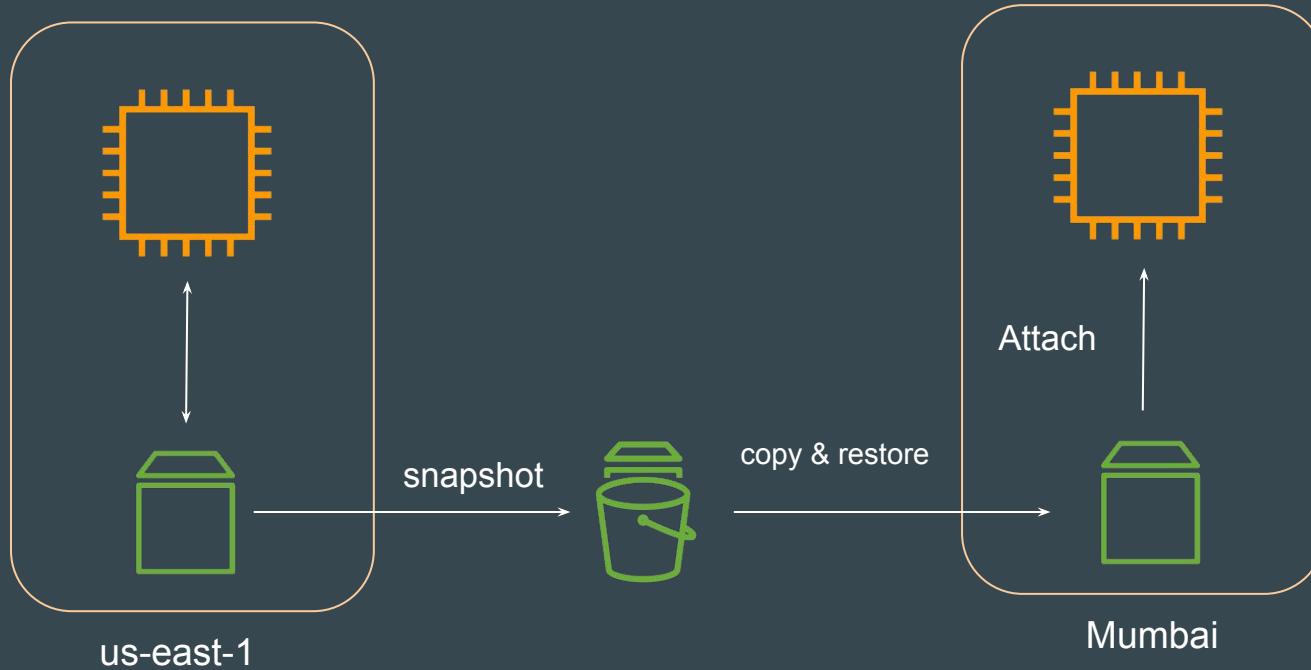


Copying Snapshots

Snapshots can be copied across Availability Zone, Regions and AWS Accounts.



Use-Case: Migrating Data Across Region



Join us in our Adventure

Be Awesome



kplabs.in/twitter



kplabs.in/linkedin

EBS Encryption



Basics of Disk Level Encryption

Disk Level encryption involves encrypting all the files that are part of the storage device.

Multiple Set of Technologies: BitLocker, Apple FileVault and others



EBS Encryption

Amazon EBS encryption uses AWS KMS keys when creating encrypted volumes and snapshots.

For an encrypted EBS volume that is attached to a supported instance type, the following types of data are encrypted:

1. Data at rest inside the volume
2. All data moving between the volume and the instance
3. All snapshots created from the volume
4. All volumes created from those snapshots

Points to Note

Enabling EBS Encryption has minimal effect on latency.

Encryption and decryption are handled transparently, and they require no additional action from you or your applications.

Amazon EBS encrypts your volume using industry-standard AES-256 data encryption

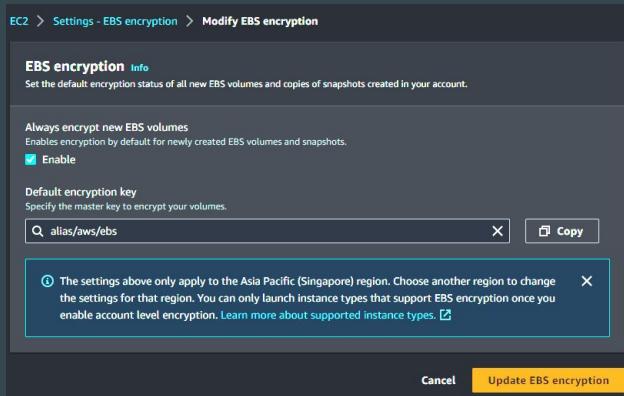
EBS Encryption By Default



Encrypt ALL EBS Volumes

New Amazon EBS volumes aren't encrypted by default.

However, there is a setting in the EC2 console that turns on encryption by default for all new Amazon EBS volumes and snapshot copies created within a specified Region.



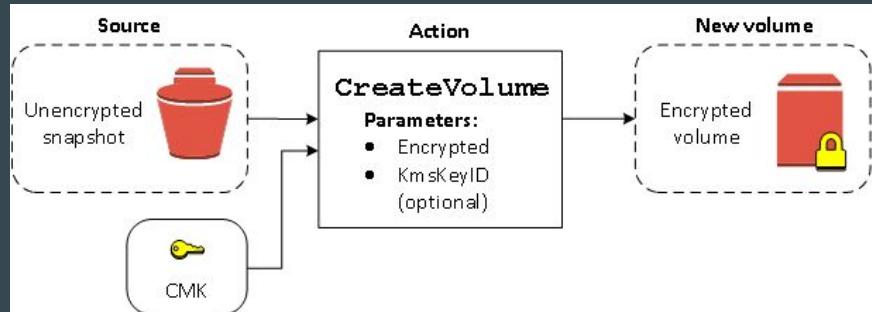
EBS Encryption scenarios



1 - Encrypted Volume from Unencrypted Snapshot

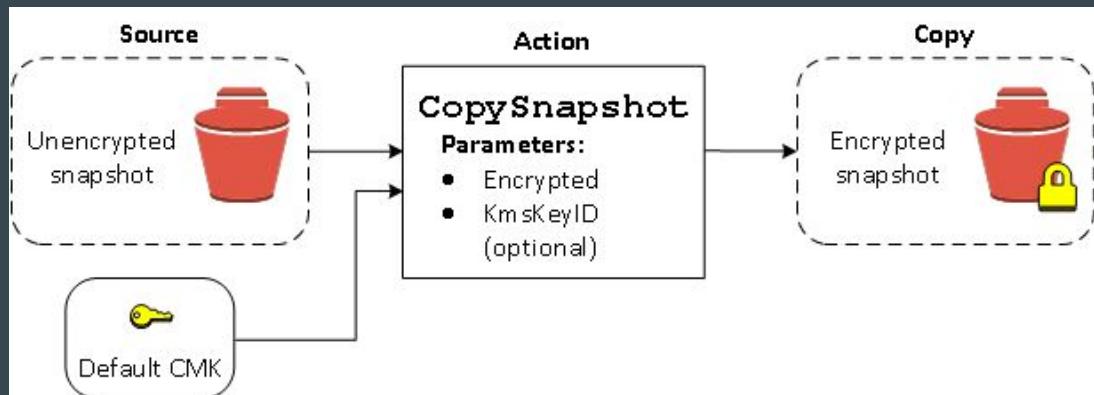
Without encryption by default enabled, a volume restored from an unencrypted snapshot is unencrypted by default.

However, you can encrypt the resulting volume by setting the **Encrypted** parameter



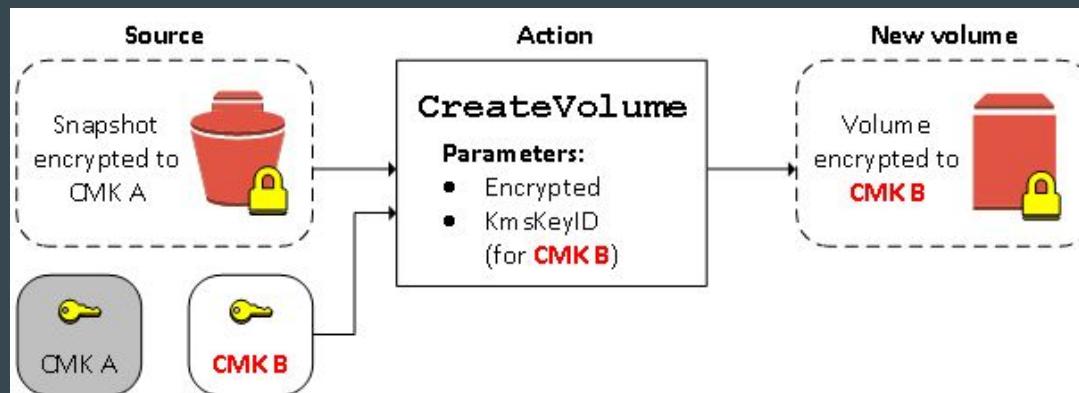
2 - Unencrypted to Encrypted Snapshot

You can encrypt the resulting snapshot by setting the Encrypted parameter.



3 - Re-Encrypt Volume from Encrypted Snapshot

When the CreateVolume action operates on an encrypted snapshot, you have the option of re-encrypting it with a different KMS key.

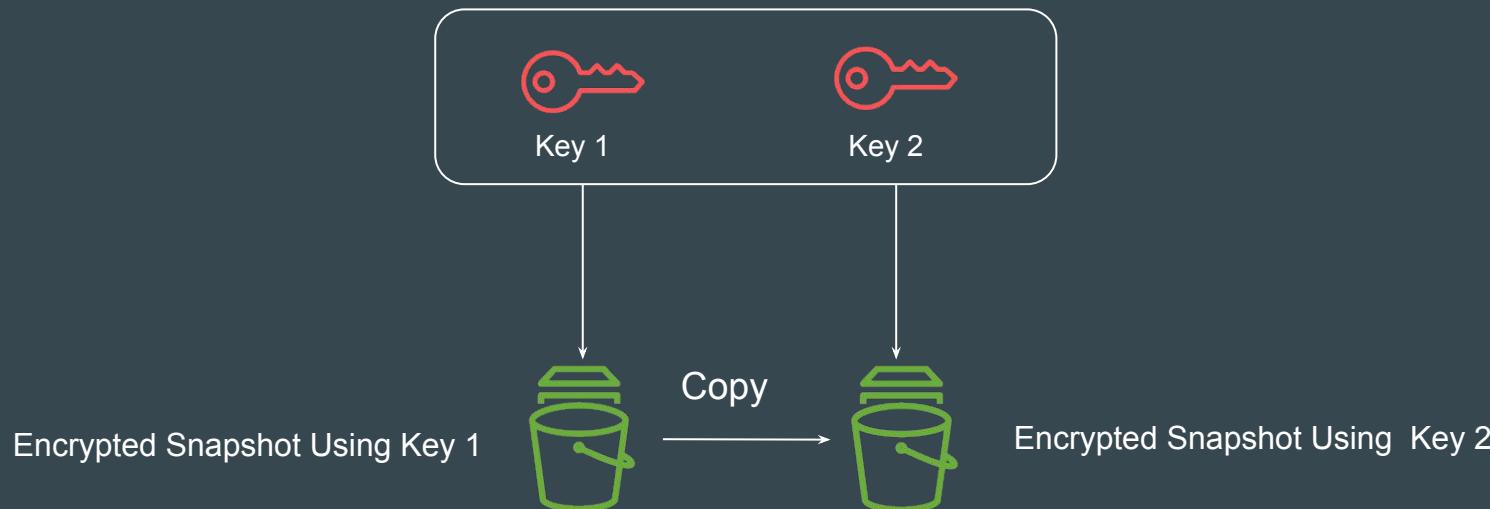


Encrypted Snapshot Sharing



Encrypted Snapshot Copying

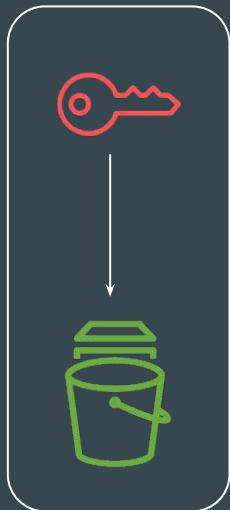
When you copy a snapshot, you can encrypt the copy or you can specify a KMS key that is different than the original, and the resulting copied snapshot uses the new KMS key.



Encrypted Snapshot with AWS Key

You can only share snapshots that are encrypted with a customer managed key with other AWS accounts.

default (aws/ebs)



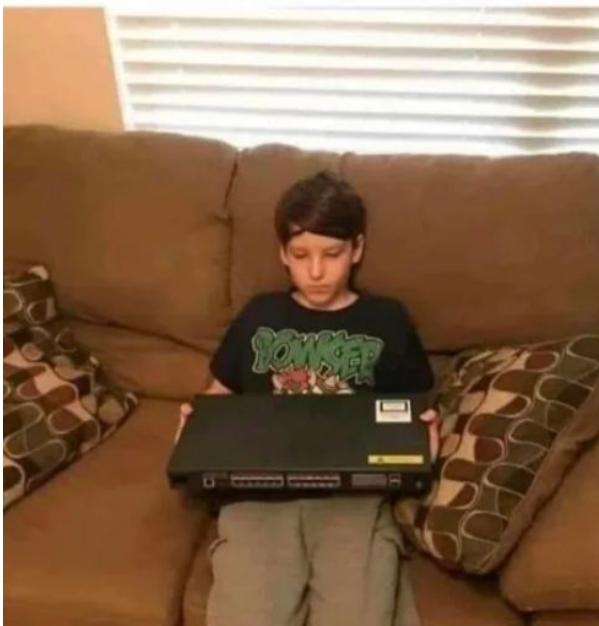
Sharing Not Supported



AWS Account 2

Relax and Have a Meme Before Proceeding

When your kid asks for a switch for Christmas.



Exam Preparation - I

The most favourite section!

Important Pointer 1 - Keys Compromise

Dealing with exposed Access / Secret Keys

- Determine the access associated with those exposed keys.
- Invalidate the exposed keys by making them inactive.
- Add an explicit deny policy with the IAM principal.
- Review the logs to see possible backdoors.

Important Pointer 2 - EC2 Compromise

Dealing with compromised EC2 Instance

- Lock the instance down through the security group, so it remains isolated.
- Take the EBS snapshot.
- Take a memory dump.
- Perform the forensics analysis.

Important Pointer 3 - Guard Duty

If you perform penetration testing from specific EC2, you can whitelist the EIP of EC2 in Guard Duty to avoid unnecessary alerts being generated.

Supported Data Sources: VPC Flow Logs, AWS CloudTrail event logs, and DNS logs.

Important Pointer 3 - Guard Duty

If you are using a 3rd party DNS resolver, for example, OpenDNS or GoogleDNS, or if you set up your own DNS resolvers, then GuardDuty cannot access and process data from this data source.

In an AD environment, the DNS resolved is generally set to that of the AD Server.

Important Guard Duty Findings to Remember;

- CloudTrailLoggingDisabled

Important Pointer 4 - Penetration Test

AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for eight services that include EC2, ELB, RDS, Aurora, CloudFront, and others.

In exams, you can still see older types of questions, so be ready to select an answer based on using the “Pre-Authorized scanning engine from the marketplace.”

Important Pointer 5 - EC2 Abuse Notice

AWS Customer can receive abuse notice on several occasion:

If your AWS workload has being used for the purpose, which does not conform to the acceptable usage policy.

Be aware of the action that you need to take when you receive an Abuse notice.

[similar to when EC2 is compromised, EBS snapshot, memory dump, restrict network]

Important Pointer 6 - Stolen Laptop Use-Case

Let's assume that the laptop of a system administrator is stolen. System Administrator had access to all of the EC2 instances.

How should you deal with such a scenario?

Modify the authorized_key file of all the EC2 instances and remove the key associated with the system administrator.

Important Pointer 7 - CloudTrail Aspects

Investigating Potential Compromise - CloudTrail

CloudTrail console will store all the events for the last 90 days in the even history.

Post 90 days, since CloudTrail Logs will be stored in S3, you can make use of AWS Athena to query.

Exam Preparation - II

The most loved section!

Important Pointer 1 - VPC Flow Logs

- version - The VPC Flow Logs Version
- account-id - AWS Account ID
- interface-id - The network interface id
- srcaddr - The source address
- destaddr - Destination Address
- src port - Source Port
- dest port - Destination Port
- protocol - The protocol number
- packets - Number of packets transferred
- bytes - Number of bytes transferred
- start - Start time in unix seconds
- end - End time in unix seconds
- action - ACCEPT or REJECT
- log status - Logging status of flow log

2 7742829482 eni-4d788e3d 115.73.149.218 10.0.5.157 12053 23 6 2 88 1485439809 1485440090 REJECT OK

Important Pointer 2 - AWS Inspector

AWS Inspector scans target based on various baselines that it supports, includes:

- Common Vulnerabilities & Exposures
- CIS Benchmarks
- Security Best Practices
- Network Reachability

To scan the target, we have to provide a “key-value” pair for a tag associated with the target.

Important Pointer 3 - Systems Manager

Run Command:

- Allows running a set of command document on the target instance.

Patch Compliance:

- Allows us to check the compliance status of an EC2 instance with respect to patching activity.

Patch Baseline

- Patch Baseline determines what patches needed to be installed in EC2 instance.
- We can also define approval for the same.

Important Pointer 3 - Systems Manager

Maintenance Window:

- Provides a mechanism for scheduling particular activity on a target instance.

Parameter Store

- Allows us to store secrets.
- Prefer Secure String method.

Important Pointer 4 - AWS Config

AWS Config allows us to record configuration changes, and it also provides a set of compliance with rulesets that allows us to assess our AWS environment.

Can be used for a variety of use-cases, some of these includes:

- Auditing IAM policy assigned to users before and after a specific event / incident.
- Detecting if CloudTrail is disabled
- Verify if all EC2 instances are running from approved AMI.
- Detect security group with open rules (0.0.0.0/0) for ports like SSH, RDP, and others.
- Detect if Internet Gateway is added to a not-authorized VPC.
- Detect if EBS volumes are encrypted.

AWS Config can also be integrated with AWS Lambda for automatic remediation.

Important Pointer 5 - AWS Athena

AWS Athena is generally used for use-case where we want to analyze the logs from S3 like CloudTrail, VPC Flow Logs, and others with simple SQL statements in a serverless manner.

Any use-case that we might find in the exam were an analysis of logs stored in S3 without setting up infrastructure; Athena might be the right option.

Important Pointer 6 - AWS WAF

It can be attached to ALB and CloudFront distribution and API Gateway.

Can block Layer 7 Attacks.

Can also be used to block request based on the User-Agent Headers.

Important Pointer 7 - CloudWatch Logs

CloudWatch Logs can be used to store server and application logs centrally.

Steps:

1. Assign appropriate IAM role to EC2 instance to push logs to CloudWatch.
2. Install the CloudWatch Agent.
3. Configure appropriate configuration and start CloudWatch Agent.

For troubleshooting related aspects, the following approach can be used:

- Verify if awslogs agent is running (can be done manually or via Run Command)
- Verify if appropriate IAM policy is attached to the role associated with EC2.

Important Pointer 8 - CloudWatch Metric Filter

CloudWatch Metric filters can be used to identify the errors, and CloudWatch Alarms can be used when it reaches the threshold.

For use-cases where you need automatic alerts on a specific condition like too many unauthorized API calls, than you can make use of CloudWatch Metric Filter.

Step 1: Define Pattern
Step 2: Assign Metric

Define Logs Metric Filter

Editing Filter "eventName=CreateAccount-userIdentity-userName-ithollow-2" for Log Group "CloudTrail/DefaultLogGroup"

You can use metric filters to monitor events in a log group as they are sent to CloudWatch Logs. You can monitor and count specific terms or extract values from log events and associate the results with a metric. [Learn more about pattern syntax.](#)

Filter Pattern
({\$.eventName = "CreateUser") && (\$.userIdentity.userName != "ithollow")})

Show examples

Select Log Data to Test
201633966051_CloudTrail_us-east-1

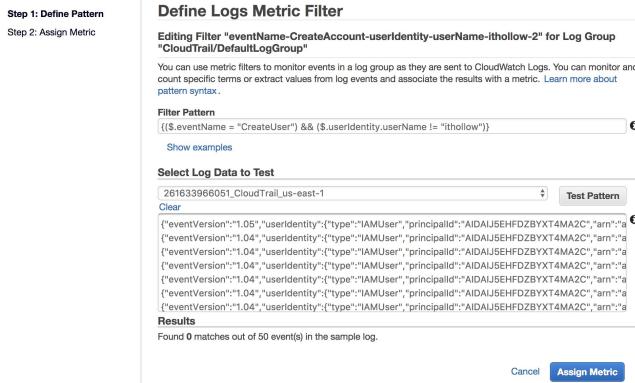
Test Pattern

Clear

Results

Found 0 matches out of 50 event(s) in the sample log.

[Cancel](#) [Assign Metric](#)



Important Pointer 9 - IP Packet Inspection

If you want to inspect contents within an IP packet for certain anomalies, then the following approach can be used:

At a VPC level, create a proxy server for packet inspection. Route all the VPC Outbound traffic through the proxy server.

Install an appropriate agent on the host. Inspect the traffic at the host level.

Note: VPC Flow Logs cannot be used in such use-case.

Important Pointer 10 - CloudTrail

It is important to enable CloudTrail for all the regions and also store the data centrally.

CloudTrail log file integrity validation allows us to determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it.

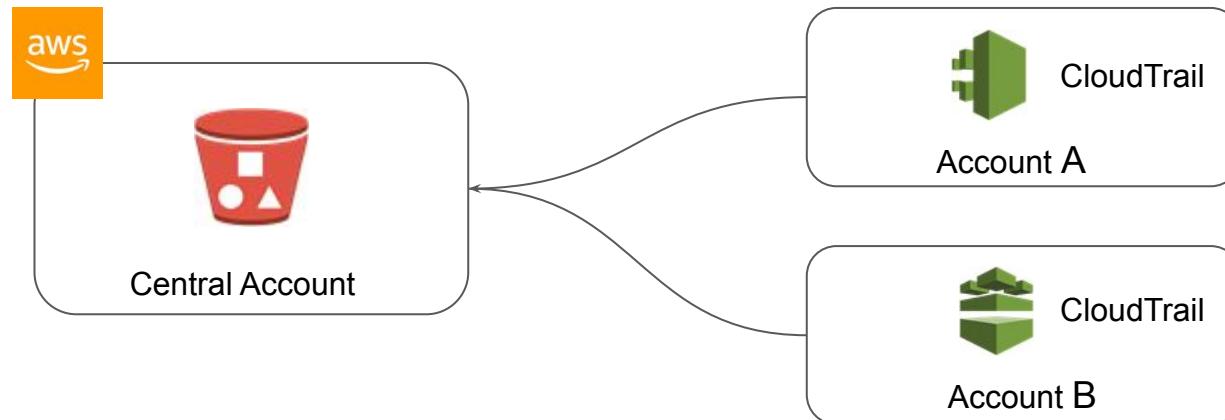
1. CloudWatch Metric filters can be used to identify the errors and CloudWatch Alarms can be used when it reaches the threshold.

If you want to update the log file prefix in CloudTrail, first modify the S3 bucket policy with the new prefix and then update the CloudTrail trail.

Important Pointer 11 - Centralized Logging of CloudTrail

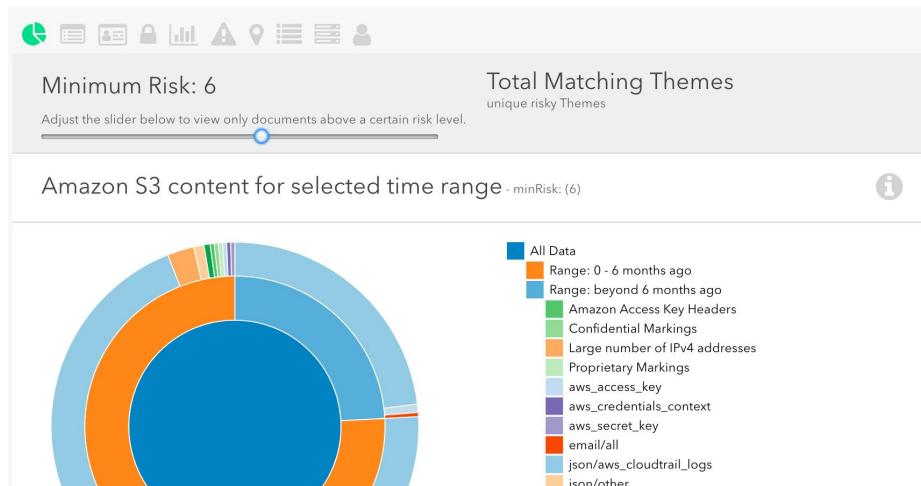
Know all the steps required to perform centralized logging for CloudTrail Logs.

1. Create a S3 bucket in the central account with an appropriate bucket policy.
2. Configure CloudTrail in all accounts to push logs to central S3 bucket.



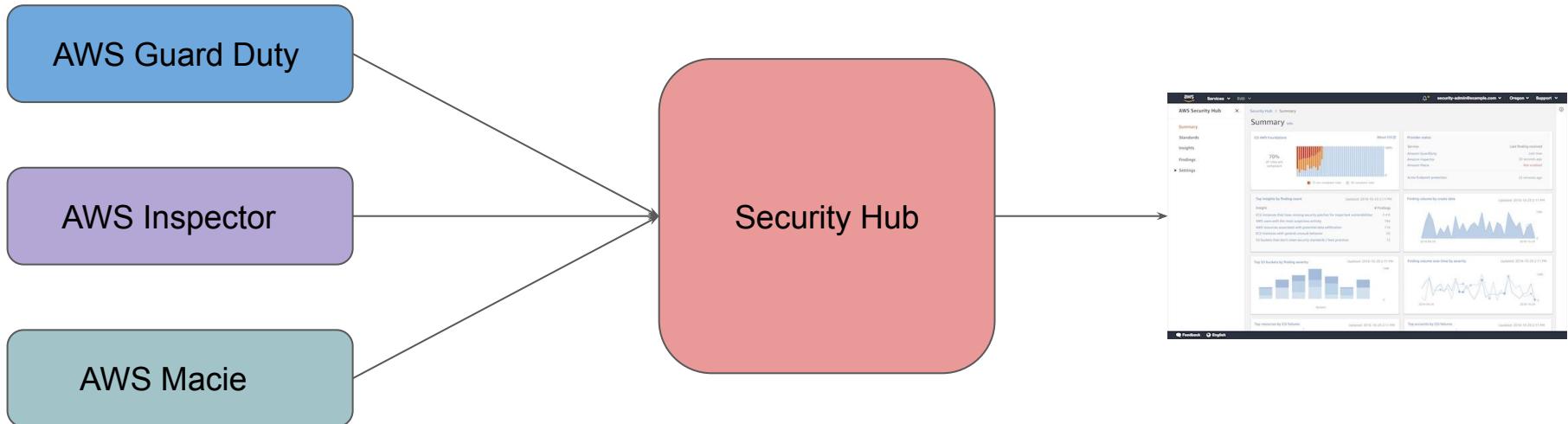
Important Pointer 12 - AWS Macie

AWS Macie can be used to recognize sensitive information like PII data, DB backups as well as data related to intellectual property,



Important Pointer 13 - Security Hub

AWS Security Hub gives you a comprehensive view of your high-priority security alerts and compliance status across AWS accounts.



Important Pointer 14 - Miscellaneous Pointers

CloudWatch Events enables us to respond to changes in our AWS environment in real-time.

If you want to perform real-time analytics on the log files, you can use services like ElasticSearch as well as Kinesis.

Exam Preparation - III

We all like important pointers!

Important Pointer 1 - DDoS Mitigation

Know about AWS services that can help during DDoS attacks:

- AWS Shield [Layer 3, Layer 4, Layer 7]
- CloudFront
- Auto-Scaling
- Route53
- WAF
- CloudWatch

If you are making use of a static website that uses HTML, CSS, you can migrate it to an S3 bucket with CloudFront to protect against DDoS attacks instead of hosting it in EC2 instances.

Important Pointer 2 - Key Pair Use-Case

What happens if you launch an instance and delete the key-pair from AWS?

The keys are always stored in authorized_keys in the Linux server.

If you create AMI of EC2 instance and copy it in different region and launch new EC2 from the AMI, the new EC2 will still have the old .public key in authorized_keys file.

Important Pointer 3 - Direct Connect

Direct Connect is a dedicated connection between your datacenter and AWS.

It is region specific except for the US regions.

The traffic in Direct connect is not encrypted. If encryption is required then we need to use VPN tunnel through the DX connection.

Important Pointer 4 - EBS Secure Data Wiping

AWS wipes the data from EBS before it is made available for reuse.

Before deleting EBS volume, customer can also wipe the data.

When the storage device has reached its end of use, they are decommissioned via detailed steps mentioned via NIST 800-88 or DOD standards.

Read the question very carefully before selecting the answer.

If question states that data must be wiped before EBS is released, then this is not the right answer. You will have to use other tools for that.

Important Pointer 5 - EC2 Tenancy Attribute

EC2 instance launched in VPC has a specific tenancy attribute associated with it.

Shared: EC2 instance runs on shared hardware.

Dedicated: EC2 runs on hardware only shared between instances of same account.

Hosts: Instance runs on dedicated hosts which provides granular level of HW access.

Important Pointer 6 - CloudFront

For the user to access S3 contents only via CloudFront, you can enable CloudFront Origin Access Identity.

Make sure to have an appropriate S3 bucket policy that allows only specific CloudFront distribution to access the bucket.

CloudFront also supports SNI with the help of dedicated IP for compatibility with older browsers.

Important Pointer 7 - CloudFront Signed URLs and Cookies

CloudFront signed URLs and signed cookies provide the same basic functionality: they allow you to control who can access your content.

Use signed URLs in the following cases:

- You want to use an RTMP distribution. Signed cookies aren't supported for RTMP distributions.
- You want to restrict access to individual files, for example, an installation download for your application.
- Your users are using a client (for example, a custom HTTP client) that doesn't support cookies.

Use signed cookies in the following cases:

- You want to provide access to multiple restricted files, for example, all of the files for a video in HLS format or all of the files in the subscribers' area of the website.

Important Pointer 8 - Miscellaneous CloudFront

CloudFront supports custom TLS certificates. If you intend to use that, make sure to import certificate to CloudFront

- You must import the certificate in the US East (N. Virginia) Region.
- Your key length must be 1024 or 2048 bits and cannot exceed 2048 bits.
- Also ensure that certificate, private key and chain are in the PEM encoded format.

Important Pointer 9 - VPC Endpoints

It can be used to connect with AWS resources privately without the need for an Internet connection.

Know both the Gateway Endpoints as well as Interface Endpoints

VPC Endpoints can also be used to whitelist only specific S3 buckets within the genuine account.

VPC Endpoint can also be used with KMS. You can make use of aws:sourceVpc condition key to grant or restrict access to an AWS KMS CMK based on the VPC endpoint along with ensuring Private DNS is enabled.

Important Pointer 10 - Network ACL

Be Aware of the working of stateful and stateless firewalls.

NACL is a Stateless Firewall offering.

Works at a subnet level.

Maximum of 40 rules per Network ACL can be applied. Default is 20.

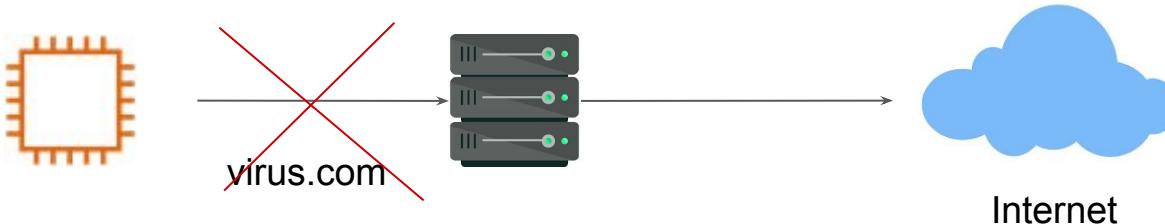
If more rules are needed, you can choose to use host-based firewalls like iptables.

Important Pointer Part 11 - URL WhiteListing

If there is a need to allow application to only access certain URLs outbound, then we need to implement custom proxy server like Squid or some 3rd Party solution from AWS Marketplace.

Example Rule:

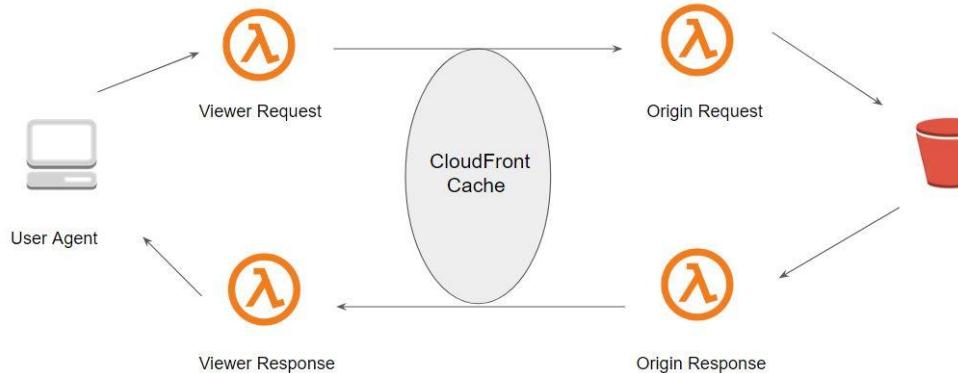
1. Server should only access URL related to OS Package updates (updates.centos.org).
2. All other URLs should be blocked.



Important Pointer - Part 12 - Lambda@Edge

Lambda@Edge lets you run Lambda functions to customize content that CloudFront delivers.

If you want to add additional HTTP headers without modifying the source code of the application, you can make use of Lambda@Edge.



Important Pointer 13 - SES

AWS SES service can be used for sending emails.

TLS can be used for encrypted connection with the SMTP server.

Remember The Important Ports : 25, 587, 2587

Endpoint URL:

email-smtp.us-east-1.amazonaws.com over port 587

Important Pointer - Part 14 - Miscellaneous Pointers 1

If you want that EC2 instances to not use the Amazon-Provided DNS, you can disable the DNS resolution in VPC.

Host Based IDS can be used for file integrity monitoring. You can integrate it with CloudWatch for alerting aspects.

If organization wants to implement IPS, an IPS agent needs to be installed in EC2 instance which scans the traffic and can report to central IPS server.

Important Pointer 15 - Miscellaneous Pointers 2

Virtual Private Networks (VPN) can be used to connect to private AWS resources in VPC. VPN is also a right solution for employees working remotely to connect to AWS resource. You can use VPN appliance from AWS Marketplace like OpenVPN

Know what is Bastion Host and AWS Artifact service.

EC2 Instance Metadata

- EC2 Instance Metadata is available on following IP: 169.254.169.254.
- User can be blocked accessing Metadata through IPTABLES.

Exam Preparation - IV

Everyone likes important pointers!

Important Pointer 1 - IAM

- Prepare for questions related to troubleshooting IAM policies.
- Be aware of IAM Policy Evaluation Logic
- Be aware of IAM Policy variables [\${aws:username}"]

Important Pointer 2 - Federation

You must remember step by step process and the flow when federation is used.

Understand components like Identity Broker, Service Provider, Identity Provider.

External ID with IAM Role

It is important to make use of External ID specifically when creating a cross-account IAM role for the partner account.

Important Pointer 3 - Cross Account IAM Role

Know the step by step process required to create cross-account IAM Role.

Be aware of troubleshooting related scenarios.

If any individual is having trouble accessing certain AWS accounts, the following aspects can be looked upon:

1. Verify if the sts:AssumeRole has been granted.
2. Verify if the appropriate RoleArn is added properly.
3. Verify the External ID.

Important Pointer 4

Web Identity Federation

Web Identity Federation is generally used when user does not belong in the organization.

Example: User signs-in to your web app via public IdP and your mobile app wants to store data to services like DynamoDB, S3 etc.

AWS Directory Service

- Simple AD, Microsoft AD, and AD Connector
- Troubleshooting AD Integration.
- Know that when you integrate with AD, the DNS should point to AD.

Important Pointer 5 - AWS Organizations

Provides two options while enabling :

- Consolidated Billing.
- All Features

Service Control Policies can be used to restrict access to all the users, including ROOT.

Remember that SCP cannot allow access; it can only be used to restrict access.

Important Point 6 - ADFS

Active Directory Federation Services (ADFS) is a Single Sign-On (SSO) solution created by Microsoft.

Supports SAML for authentication.

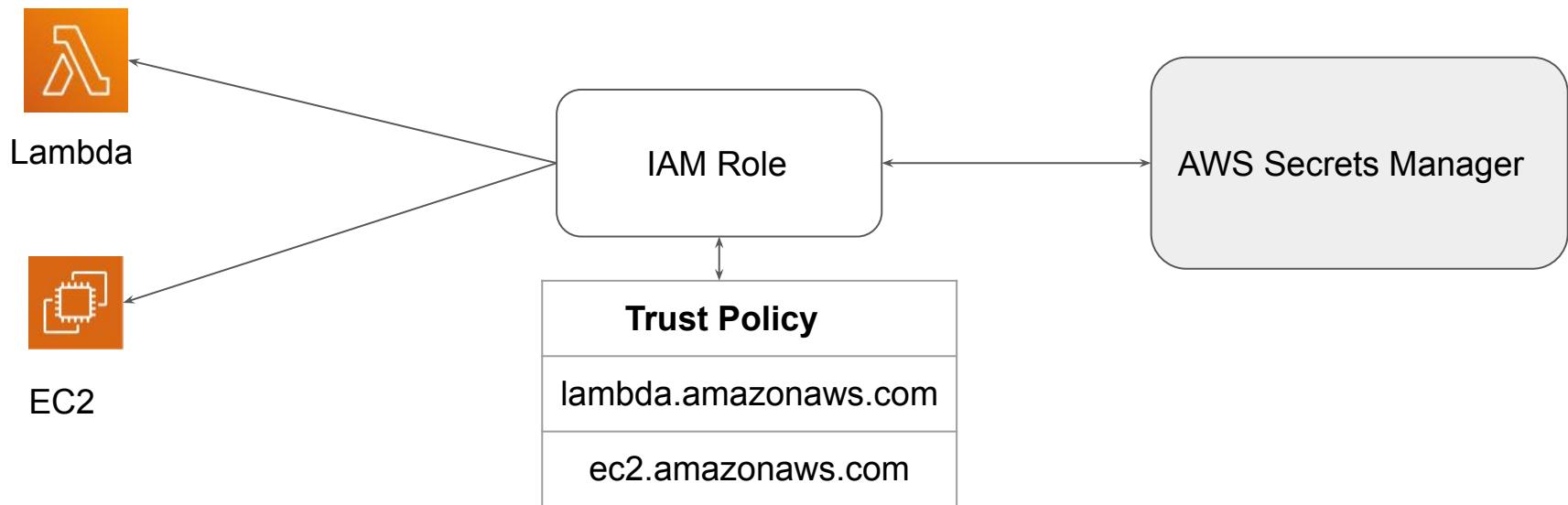
Active Directory groups are associated with IAM roles.

All the users in the AD group can assume the appropriate IAM role.



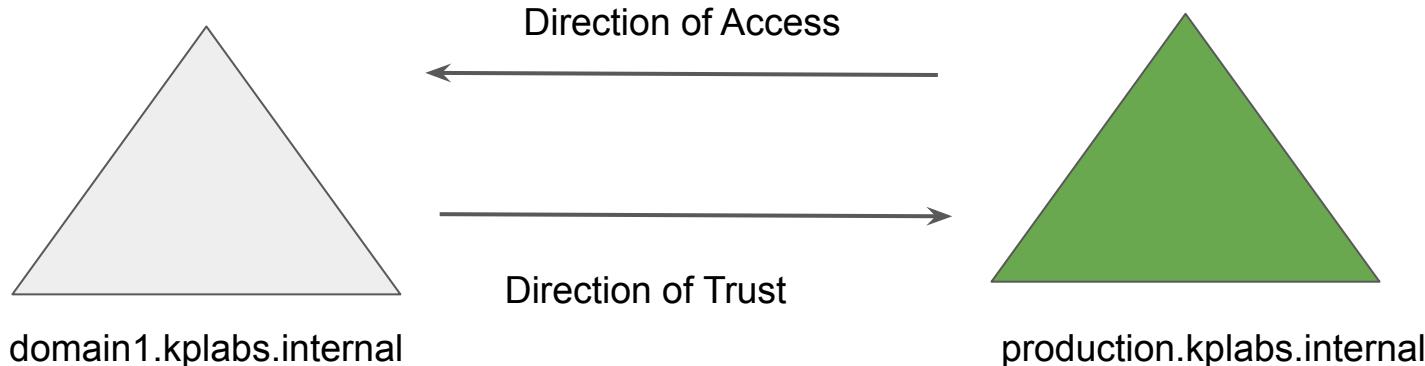
Important Point 7 - IAM Role for Multiple Service

If you want an IAM role to be used by multiple services, you have to modify the Trust Policy.



Important Pointer 8 - Direction of the Trust

- In AD, domain to domain communication can occur through Trusts.
- Trust can either be one-way or two-way.
- In a two-way trust, the domain from either side can access the other side.
- The direction of trust is opposite to the direction of access.



Edit Trust Relationship

You can customize trust relationships by editing the following access control policy document.

Policy Document

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "Service": ["lambda.amazonaws.com", "ec2.amazonaws.com"]  
8       },  
9       "Action": "sts:AssumeRole"  
10      }  
11    ]  
12 }
```

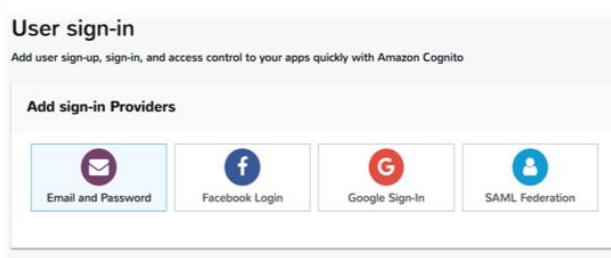
Important Pointer 9 - Cognito

Amazon Cognito provides authentication, authorization, and user management service for your web and mobile apps.

For authentication-related aspects for mobile application, Cognito can be a good choice

Fine-grained access control can be added to users belonging to a different group.

Catch Words: Social Media Website



Important Pointer 10 - Miscellaneous Pointers

You should avoid using ROOT user. In new AWS Account, set a MFA for the root user and switch to the IAM user. Avoid creating Access/Secret keys for the root user.

Important S3 Pointers:

Presign URL's allows us to create time expiry URL for an object within private S3 bucket.

- You should be able to read S3 bucket policies.
- Note difference between arn:aws:s3:::demobucket and arn:aws:s3:::demobucket/*
- Cross-Account bucket policy use-case is key [bucket-owner-full-control]
- 3 ways to assign permission, IAM, S3 ACL and Bucket Policies.

Important Pointer 11 - Identity and Resource Based Policies

Identity-based policies are attached to an IAM user, group, or role.

Resource-based policies are attached to a resource.

We attach these policies directly to a resource like S3 bucket, SQS Queue, KMS keys.

While troubleshooting access issues, always verify the resource-based policy and Identity-based policy.

Exam Preparation - V

Data Protection

Important Pointer 1 - AWS Certificate Manager

Certificates in ACM are regional resources. To use certificate with ELB, you must issue certificate in the same region as ELB.

To use an ACM Certificate with Amazon CloudFront, you must request or import the certificate in the US East (N. Virginia) region

There are two ways in which certificate can be issued:

- Email Verification
- DNS Verification.

Certificate for domain **example.com** will not work for test.example.com.
We need to get wildcard certificate ***.example.com** for the above.

Important Pointer 1 - AWS Certificate Manager

If you ever get question in exam related to exporting ACM certificates, remember following:

- We cannot export public certificates created by ACM.
- We can export private certificate created by ACM and use them in EC2.

Important Pointer 2 - CloudHSM

- CloudHSM is single tenanted (single physical device only for you)
- It must be within VPC.
- We can integrate CloudHSM with RedShift, RDS for Oracle.
- For fault tolerance, we need to build cluster with two CloudHSM.
- AWS uses SafeNet Luna SA 700 HSM appliance for CloudHsm.
- Provides tamper-evident controls.

One benefit of CloudHSM over KMS is that in CloudHSM, only the organization staff can administer the keys while in KMS, AWS staff can also administer the keys.

Important Pointer 3

DynamoDB Security

We can make use of DynamoDB Encryption Client library to encrypt data at origin before it's stored in DynamoDB.

Important Pointer 4

CloudTrail & Encryption

By default, logs file delivered by CloudTrail to S3 bucket is encrypted by AWS server-side encryption.

We also have option for log file encryption using SSE-KMS.

Important Pointer 5 - KMS

KMS is one of the most important topic for the exam.

Be thorough with all the videos we have for KMS.

Be very thorough with KMS Policy (we have three use-cases)

Keys are commonly rotated to limit the impact of potential key compromise.

If your CMKs come from original KMS key material, you can opt to have AWS automatically rotate your CMK every year.

Use KMS Encryption Context for Additional Authenticated Data (AAD) to prevent tampering with the ciphertext.

Important Pointer 6 - Rotating CMK

The “Automated Key Rotation” option for KMS appears for AWS KMS generated key material.

You cannot automatically rotate CMKs with imported key material. You can rotate them manually.

If you choose to import keys to AWS KMS, you can manually rotate them by creating a new CMK and mapping an existing key alias from the old CMK to the new CMK.

Important Pointer 7 - Cross Region KMS

CMKs are region specific and cannot be shared across regions.

If you are replicating certain data across multiple regions, then you can re-wrap the data encryption key from the source region using the CMK.

Important Pointer 8 - Miscellaneous KMS

If you have accidentally deleted the imported key material in CMK, than you can download the new wrapping key and import token and import the original key into the existing CMK.

Important Pointer 9 - Elastic Load Balancer

Know the difference between Classic Load Balancer and Application Load Balancer
ALB can be integrated with AWS WAF for Layer 7 protection.

Understand difference between various ELB listener types. [TCP and HTTP Listeners]

If application is running a custom proprietary protocol, than HTTP/HTTPS listeners cannot be used (in CLB as well as ALB). Make use of TCP based listeners.

ELB supports Perfect Forward Secrecy and we need to enable ECDHE key-exchange.

Have an overview of proxy protocol and backend authentication.

Important Pointer 10 - Glacier Vault

Remember that vault lock feature of Glacier.

Policies are immutable, it helps in compliance.

When you initiate the vault locking process (initiate-vault-lock), the status is InProgress.

If there are any mistakes or typos, you can call the abort-vault-lock operation, fix the appropriate things and call the initiate-vault-lock again.

Important Pointer 11

Classic EBS Use-Case

What happens if EBS is encrypted with CMK and that CMK is deleted ?

EBS will work till it is not unmounted. Backup your data quickly.

Important Pointer 12 - S3 Encryption

If each object in S3 needs to be encrypted with a unique key, than you can make use of multiple Customer Master Keys (CMK).

If you want to encrypt data with CMK, make use of SSE-KMS.

You can also create a two-factor authentication for decryption. For such use-case, you can define a MFA policy with the key policy.

Important Pointer 13 - S3 Transit Encryption

By default, S3 allows both HTTP and HTTPS connections.

This can be a threat if you are uploading sensitive data over HTTP connections.

If you want to enforce encryption in transit, you can create a S3 bucket policy

```
"Condition": {  
    "Bool": {  
        "aws:SecureTransport": "true"  
    }  
}
```

Important Pointer 14 - S3 Server Side Encryption

Within Server-Side encryption, three options can be used depending on the use-case.

- Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
- Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS)
- Server-Side Encryption with Customer-Provided Keys (SSE-C)

Important Pointer 15 - EBS Encryption Use-Case

A user having full access to EC2 cannot start EC2 instances that is using encrypted EBS volumes.

In order to overcome this scenario, following are the two important policy actions that must be attached:

- kms:Decrypt
- kms>CreateGrant

Important Pointer 16 - AWS Secrets Manager

Enabling rotation causes the secret to rotate once immediately when you save the secret.

Before you enable rotation, be sure you update all of your applications using this secret credentials to retrieve the secret from Secrets Manager.

Any applications you fail to update break as soon as the old credentials become invalid.

Important Pointer 17 - Miscellaneous ELB

Specific ELB Security Policies can be used that allows deprecated ciphers for legacy clients.

While migrating from Classic Load Balancer to Application Load Balancer, there can be issues related to connection for the older devices. This is because the cipher suites in ALB are blocking the connection.

Perfect Forward Secrecy is a feature that provides additional safeguards against the eavesdropping of encrypted data, through the use of a unique random session key. This prevents the decoding of captured data, even if the secret long-term key is compromised.

Important Pointer 18 - Parameter Store with CMK

To perform any operation on a secure string parameter, Parameter Store must be able to use the AWS KMS CMK that you specify for your intended operation.

Most of the Parameter Store failures related to CMKs are caused by the following problems:

The credentials that an application is using do not have permission to perform the specified action on the CMK.

The CMK is not found. This typically happens when you use an incorrect identifier for the CMK.

The CMK is not enabled. When this occurs, Parameter Store returns an **InvalidKeyId** exception

Updated Important Pointers

AWS Security Specialty

MFA Protected API Access

With IAM policies, you can specify which API operations a user is allowed to call.

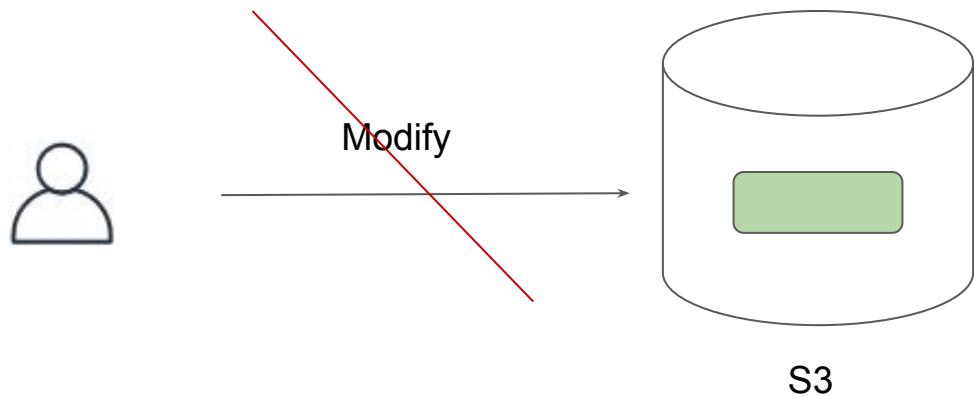
For additional security, you can mandate MFA for certain API operation.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:StopInstances"
                "ec2:TerminateInstances"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "false"
                }
            }
        }
    ]
}
```

S3 Object Lock

With S3 Object Lock, you can store objects using a write-once-read-many (WORM) model.

You can use it to prevent an object from being deleted or overwritten for a fixed amount of time or indefinitely.



Docker Security

There can be various approaches that can be used to enhance the overall security posture while using containers. Some of these include:

Limit resource consumption (CPU, memory), networking connections, ports, and unnecessary container libraries.

Segregating containers by host, function, and data classification.

HTTPS-Only S3

By default, Amazon S3 allows both HTTP and HTTPS requests.

You can explicitly set bucket policy so that only HTTPS connections would be allowed.

Here is a sample condition:

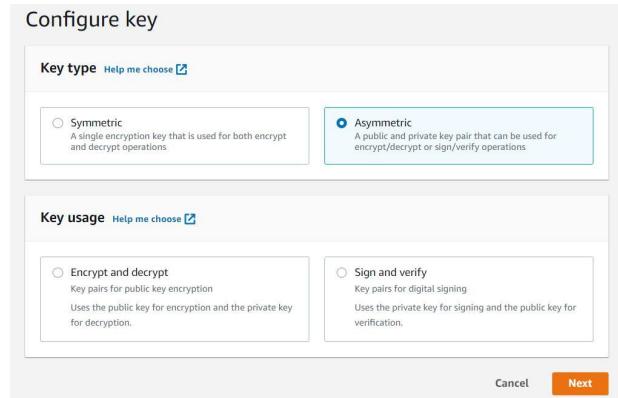
```
"Condition": {  
    "Bool": {  
        "aws:SecureTransport": "false"  
    }  
}
```

Asymmetric Key with KMS

There are two primary use-case where asymmetric keys can be used:

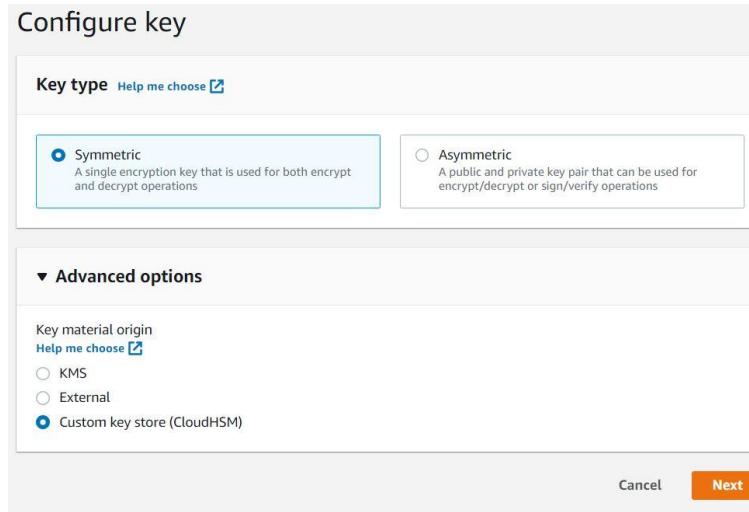
1. Encrypt / Decrypt Data
2. Signing / Verification (Digital Signatures)

You can download the public key of asymmetric key CMK



KMS and CloudHSM Integration

AWS services integrate with AWS Key Management Service, which in turn can be integrated with AWS CloudHSM through the KMS custom key store feature.



CloudHSM over KMS

CloudHSM ensures that only company support staff can administer encryption keys, whereas AWS KMS allows AWS staff to administer keys.

You might need the ability to immediately remove key material from AWS KMS and to prove you have done so by independent means

You might have a requirement to be able to audit all use of your keys independently of AWS KMS or AWS CloudTrail.

Best of Luck with the Exams

Positive Possum believes you can do
the thing

