

**IT'S DANGEROUS TO  
AWS ALONE, TAKE THIS**



**[HTTPS://SESSIONS.MINNESTAR.ORG/SESSIONS/1576](https://sessions.minnestar.org/sessions/1576)**

imgflip.com

# Amazon Primer

Things I wish they'd have  
told me before I got started

Kisha Delain  
&  
Levi McCormick

# Outline

- Services
- Tutorials
- Know before you go:  
words of caution
- \$\$\$\$
- Q&A

I am a tiny potato

And I believe in you



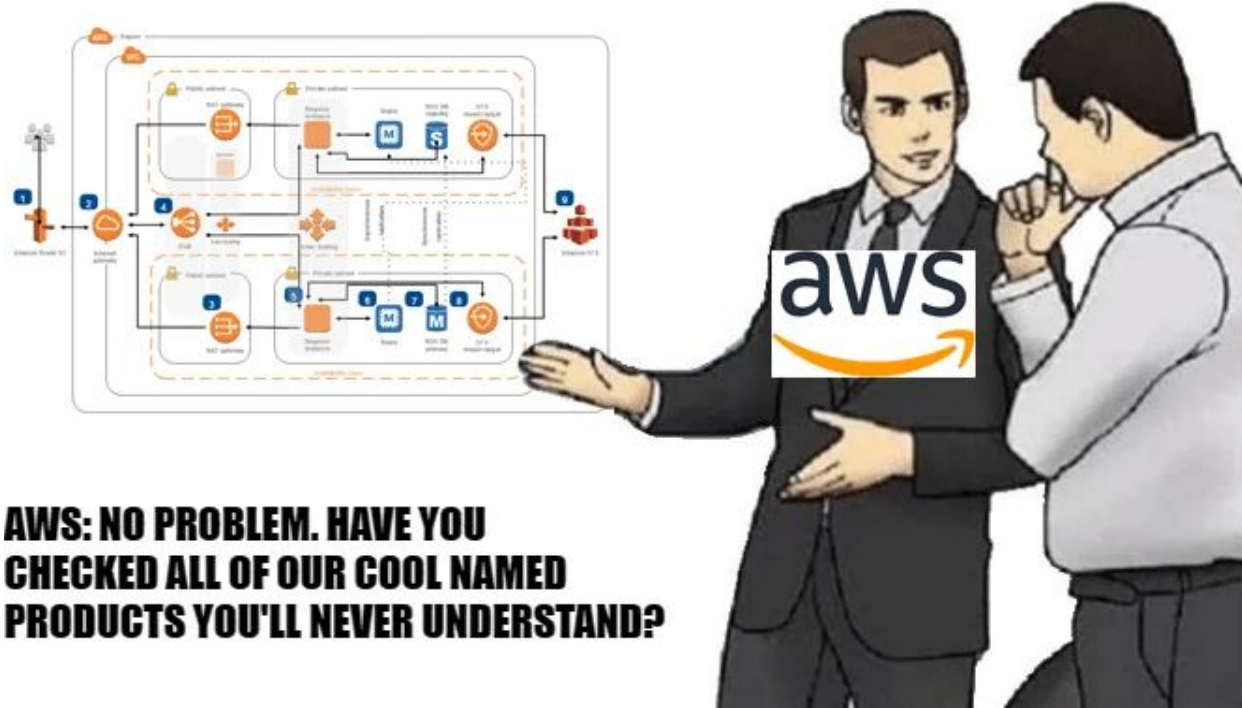
YOU CAN DO THE THING

# 200+ Services

- Elasticache
- RDS
- SQS queueuuueueueuee
- kinesis
- ECS/EKS
- EC2
- lamba
- IAM
- S3
- Cloudfront
- Cloudwatch
- Api gateway

... and many more

# ME: I JUST NEED TO HOST 'HELLO WORLD' ON THE CLOUD.

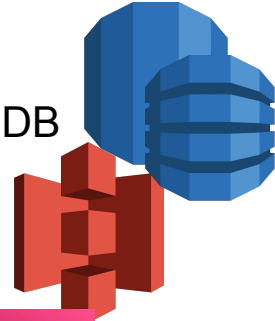


## AWS: NO PROBLEM. HAVE YOU CHECKED ALL OF OUR COOL NAMED PRODUCTS YOU'LL NEVER UNDERSTAND?

# What are you trying to do?

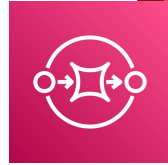
## Store Some Stuff

- Databases: RDS, DynamoDB
- Blobs: S3
- Cache: Elasticache



## Transfer Stuff (Information)

- SQS queueueueuees
- API Gateway
- Cloudfront



## Compute Some Stuff

- Event-driven, small: Lambdas + Step functions
- Too big? Too long?: EC2 / Fargate



## Containerize Your Stuff

- ECS / EKS

## Manage Your Stuff

- AWS Identity Center
- IAM

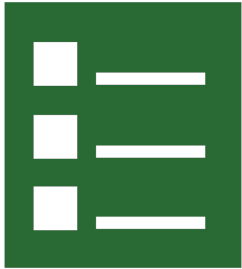
## Watch Your Stuff

- CloudWatch

Machine Learning, Analytics, etc: there are a bunch here we won't touch



# Services - Unsung Heroes



**AWS IAM**

**Permissions**



**VPC**

**Networking**

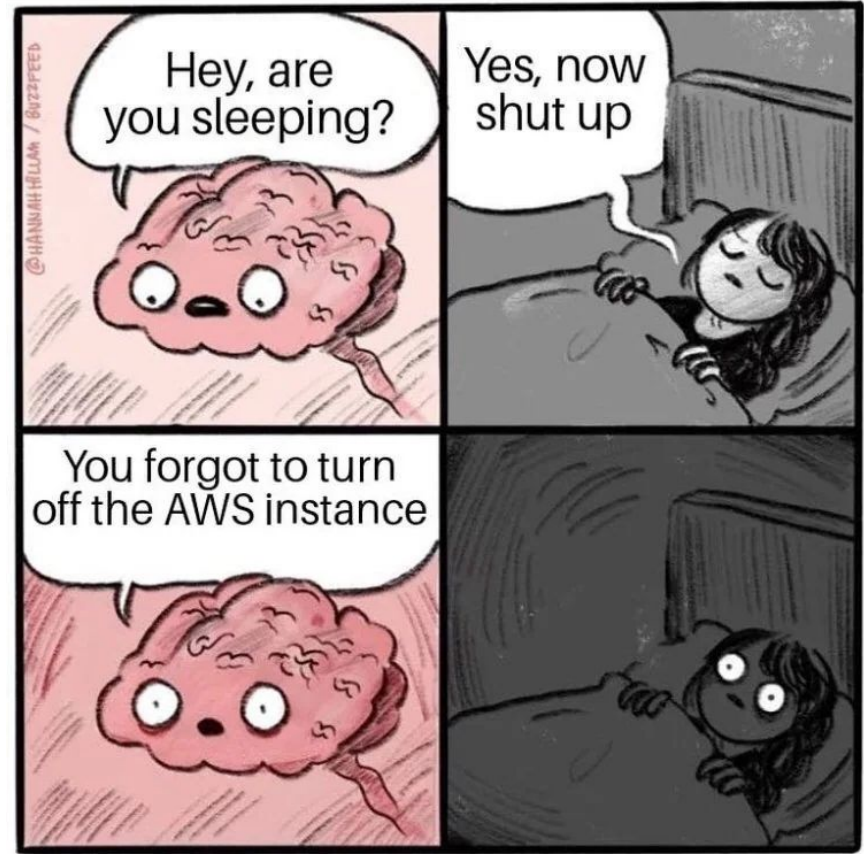


**CloudWatch**

**Logging/Metrics**

# Where To Learn

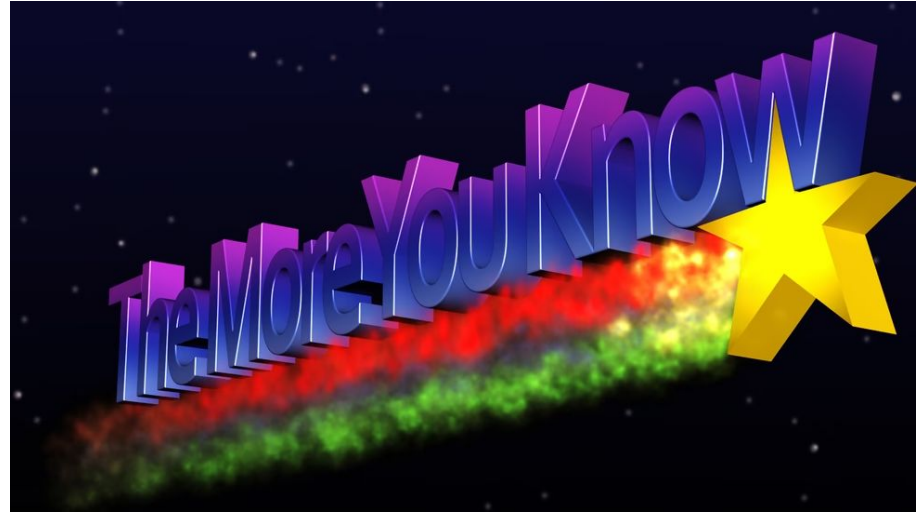
- [AWS Tutorials](#)
- [Cloud Resume Challenge](#)
- [100 Days of Cloud](#)
- [AWS Cloud Institute](#)



Original comic by **Hannah Hillam**

# Know Before You Go

- Don't use Root Creds
- Don't trust AWS IAM examples
- Multi-account
- Budgets
- Why is it so expensive?
- Well Architected Framework



# Don't Use Root Creds

Basically God Mode in the Cloud

Most Reddit posts of compromised accounts are due to people exposing root credentials on Github.

Use restricted IAM users and/or role assumption instead.

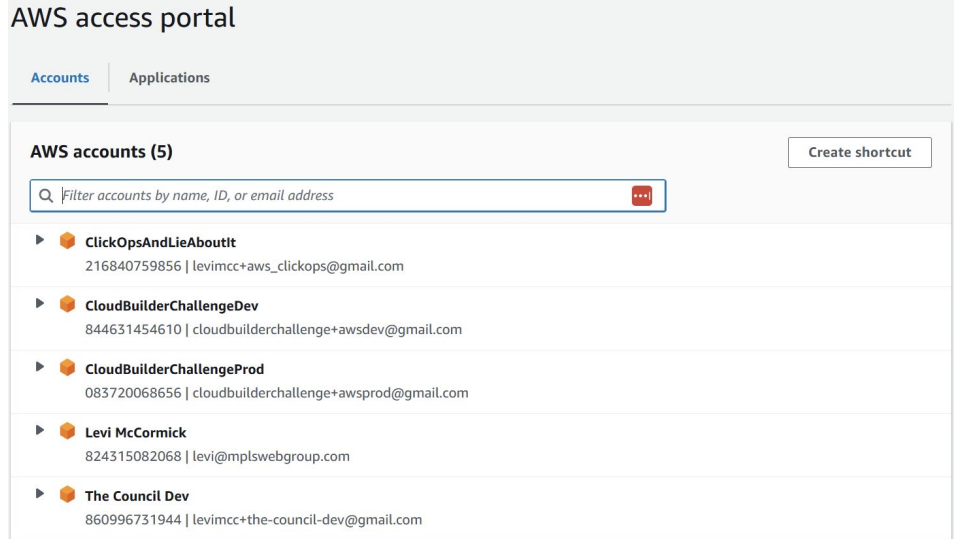




# AWS Identity Center

Service formerly known as AWS SSO.  
Manages Permission Sets and  
assigns them to users across  
accounts in an AWS Organization.

If you can't/won't use SSO, use IAM  
users with limited permission sets.



The screenshot displays the 'AWS access portal' interface. At the top, there are two tabs: 'Accounts' (selected) and 'Applications'. Below the tabs, the main content area is titled 'AWS accounts (5)' and includes a search bar with the placeholder text 'Filter accounts by name, ID, or email address'. To the right of the search bar is a 'Create shortcut' button. The list of accounts is as follows:

Name	ID	Email Address
ClickOpsAndLieAboutt	216840759856	levimcc+aws_clickops@gmail.com
CloudBuilderChallengeDev	844631454610	cloudbuilderchallenge+awsdev@gmail.com
CloudBuilderChallengeProd	083720068656	cloudbuilderchallenge+awsprod@gmail.com
Levi McCormick	824315082068	levi@mplswebgroup.com
The Council Dev	860996731944	levimcc+the-council-dev@gmail.com

# Don't Trust AWS IAM Examples

```
s3_client = boto3.client(  
    "s3",  
    aws_access_key_id=AWS_ACCESS_KEY_ID,  
    aws_secret_access_key=AWS_SECRET_ACCESS_KEY,  
)
```

# AWS SDK Credential Chain Resolution

SDKs automatically resolve AWS credentials following a predictable pattern, prioritizing environment variables, then credential files, then a metadata API when running in the cloud.

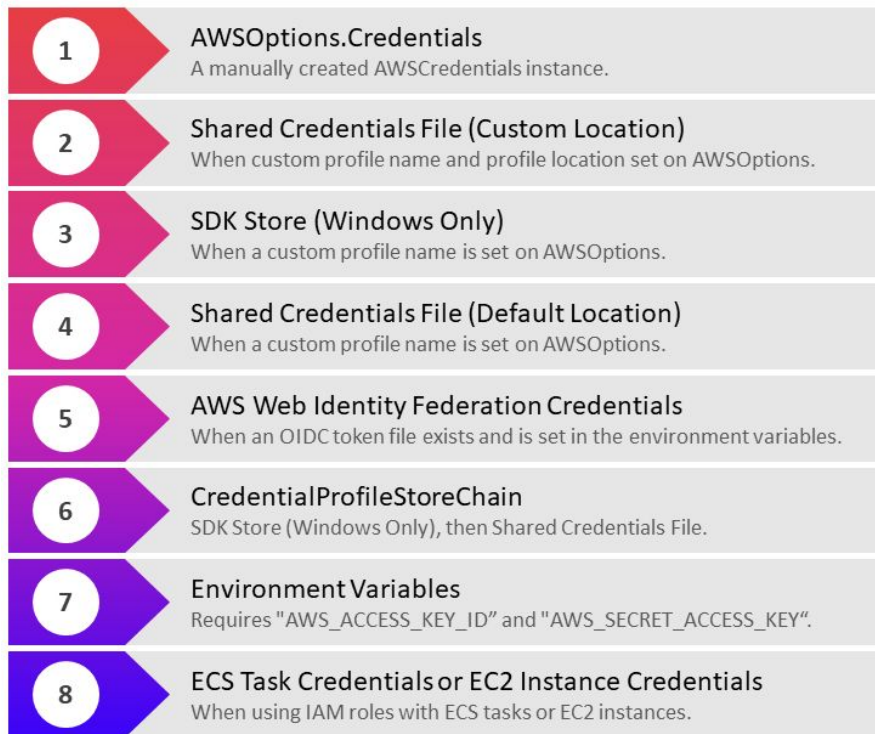
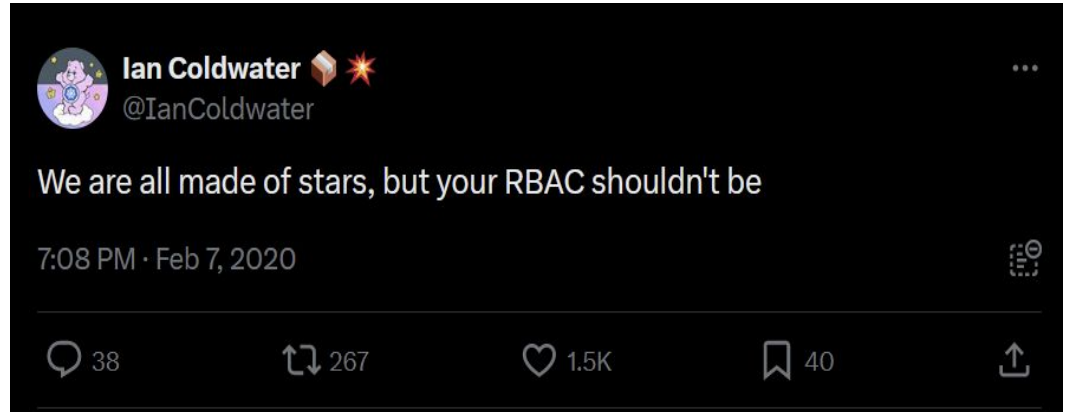


Image courtesy of Steve Gordon

<https://www.stevejgordon.co.uk/credential-loading-and-the-aws-sdk-for-dotnet-deep-dive>

# Not everything needs to be admin

Scoped roles are good policy and prevent you from contributing to someone's bitcoin wallet.



# Multi-account

AWS best practices recommend using Accounts as a strong boundary to define service domains.

Environments should live in separate Accounts.



# Budgets

Set a budget alert to let you know when exceed your comfort threshold. Then, TAKE ACTION.

## Create Alarm

### Billing Alarm

You can create a billing alarm to receive e-mail alerts when your AWS charges exceed a threshold you choose. Simply:

1. Enter a spending threshold
2. Provide an email address
3. Check your inbox for a confirmation email and click the link provided

When my total AWS charges for the month

exceed: \$  USD

send a notification to:  [New list](#)

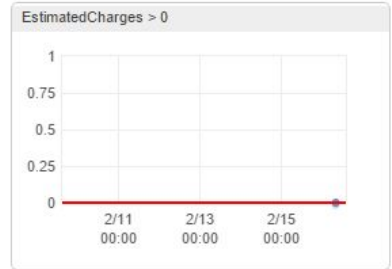
([add email address](#))

**Reminder:** for each address you add, you will receive an email from AWS with the subject "AWS Notification - Subscription Confirmation". Click the link provided in the message to confirm that AWS may deliver alerts to that address.

showing simple options [show advanced](#)

### Alarm Preview

This alarm will trigger when the blue line goes above the red line



### More resources

[AWS Billing console](#)

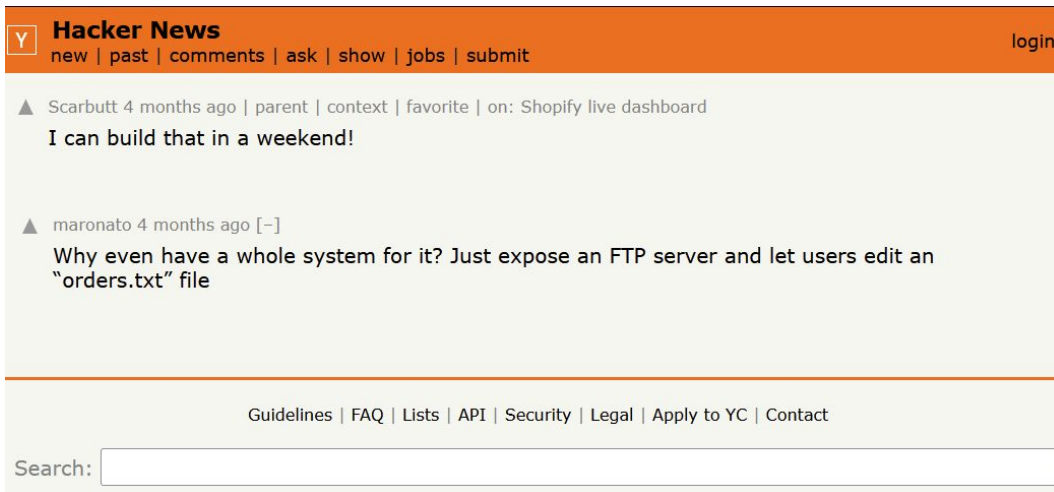
[Getting started with billing alarms](#)

[More help with billing alarms](#)

[AWS Billing FAQs](#)

# Why Is It So Expensive?

You're paying for scaled operations. AWS is far better at replacing failed hard drives than you are.



The image is a screenshot of the Hacker News website. At the top, there is an orange header bar with the text "Y Hacker News" on the left and "login" on the right. Below the header, there is a navigation bar with links: "new | past | comments | ask | show | jobs | submit". The main content area shows two posts. The first post is by "Scarbutt" from 4 months ago, with the title "I can build that in a weekend!". The second post is by "maronato" from 4 months ago, with the title "Why even have a whole system for it? Just expose an FTP server and let users edit an 'orders.txt' file". At the bottom of the page, there is a footer with links: "Guidelines | FAQ | Lists | API | Security | Legal | Apply to YC | Contact". Below the footer is a search bar with the text "Search:" and an empty input field.

# Know Your Billing Dimensions

Application Load Balancers sound simple on the surface, but billing is super complicated.

Google:  
“aws [service] pricing” to find out how a given service is billed before you put it into production.

For Application Load Balancers in the AWS Region:

- \$0.0225 per Application Load Balancer-hour (or partial hour)
- \$0.008 per LCU-hour (or partial hour)
- \$0.005 per hour per Trust Store Associated with Application Load Balancer when using Mutual TLS (or partial hour)

## LCU Details

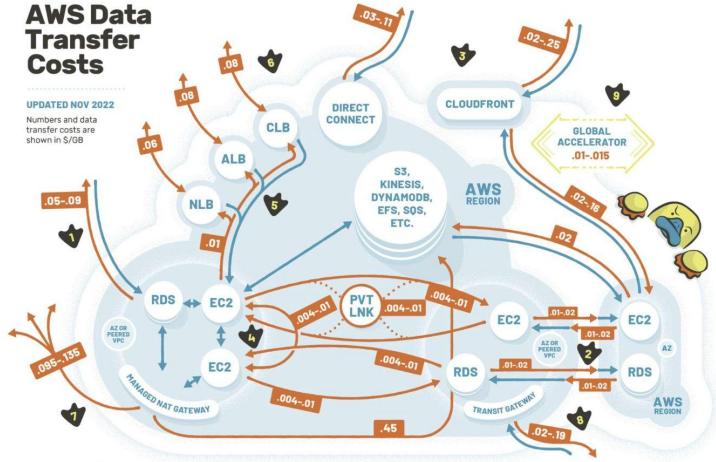
An LCU measures the dimensions on which the Application Load Balancer processes your traffic (averaged over an hour). The four dimensions measured are:

- **New connections:** Number of newly established connections per second. Typically, many requests are sent per connection.
- **Active connections:** Number of active connections per minute.
- **Processed bytes:** The number of bytes processed by the load balancer in GBs for HTTP(S) requests and responses.
- **Rule evaluations:** The product of the number of rules processed by your load balancer and the request rate. The first 10 processed rules are free (Rule evaluations = Request rate \* (Number of rules processed - 10 free rules)).



# Traffic, the Silent Wallet Killer

AWS charges a nearly criminal amount for data transfer, especially out to the internet. Watch for these in high volume applications.



the duckbill group : Still confused as hell? Get help at [duckbillgroup.com](https://duckbillgroup.com)

- 1 Direct outbound data starts at \$90/TB for less than 10TB, and discounts with volume. First 100GB is free.
  - 2 Region-to-region traffic is \$20/TB when it exits a region for indicated services except between us-east-1 and us-east-2, where it's \$10/TB. Even data wants to get out of Ohio.
  - 3 Outbound CloudFront prices are variable by region and usage, but the free tier includes 1TB/month
  - 4 Internal traffic via public or elastic IPs incurs additional fees in both directions.
  - 5 Cross-AZ EC2 traffic within a region costs as much as region-to-region. ELB-EC2 traffic is free except outbound crossing AZs.
  - 6 Elastic Load Balancing: Classic and Network LB is priced per GB. Application LB costs are in LCUs, not \$/GB.
  - 7 Traffic via Managed NAT Gateway – regardless of destination – costs an additional \$45/TB on top of other transfer, including internal transfer (S3, Kinesis, etc.).
  - 8 Variable by port speed and location. Data processing charges apply for each gigabyte sent to the AWS Transit Gateway – whether from a VPC, Direct Connect or VPN.
  - 9 Global Accelerator charges a \$15-\$105/TB charge on top of existing data transfer rates, in whichever direction the data flow is more expensive.
- Inspired by Open Guide to AWS's data transfer diagram  
[github.com/open-guides/og-aws](https://github.com/open-guides/og-aws)

# Free\* Tier(s)

Always Free (First X of usage)

12 Months Free (new customers only)

Free Trials (time limited for new services)

<p><b>COMPUTE</b></p> <hr/> <p>Free Tier <span>12 MONTHS FREE</span></p> <p>Amazon EC2</p> <h2>750 Hours</h2> <p>per month</p> <p>Resizable compute capacity in the Cloud.</p> <p>750 hours per month of Linux, RHEL, or SLES</p> <p>▼</p>	<p><b>STORAGE</b></p> <hr/> <p>Free Tier <span>12 MONTHS FREE</span></p> <p>Amazon S3</p> <h2>5 GB</h2> <p>of standard storage</p> <p>Secure, durable, and scalable object storage infrastructure.</p> <p>5 GB of Standard Storage</p> <p>▼</p>	<p><b>DATABASE</b></p> <hr/> <p>Free Tier <span>12 MONTHS FREE</span></p> <p>Amazon RDS</p> <h2>750 Hours</h2> <p>per month of database usage (applicable DB engines)</p> <p>Managed Relational Database Service for MySQL, PostgreSQL, MariaDB, or SQL Server.</p> <p>▼</p>
<p><b>DATABASE</b></p> <hr/> <p>Free Tier <span>ALWAYS FREE</span></p> <p>Amazon DynamoDB</p> <h2>25 GB</h2> <p>of storage</p> <p>Serverless, NoSQL, fully managed database with single-digit millisecond performance at any scale.</p> <p>▼</p>	<p><b>MACHINE LEARNING</b> <span>NEW</span></p> <hr/> <p>Free Tier <span>FREE TRIAL</span></p> <p>Amazon SageMaker</p> <h2>2 Months</h2> <p>free trial</p> <p>Machine learning for every data scientist and developer.</p> <p>250 hours per month of ml.t3.medium on</p> <p>▼</p>	<p><b>COMPUTE</b></p> <hr/> <p>Free Tier <span>ALWAYS FREE</span></p> <p>AWS Lambda</p> <h2>1 Million</h2> <p>free requests per month</p> <p>Run code without thinking about servers or clusters</p> <p>1,000,000 free requests per month</p> <p>▼</p>

# Well Architected Framework

AWS documented guidance on how to build in the cloud.

## AWS Well-Architected and the Six Pillars

### Framework Overview

The AWS Well-Architected Framework describes key concepts, design principles, and architectural best practices for designing and running workloads in the cloud. By answering a few foundational questions, learn how well your architecture aligns with cloud best practices and gain guidance for making improvements.



[HTML](#) | [Labs](#)

### Operational Excellence Pillar

The operational excellence pillar focuses on running and monitoring systems, and continually improving processes and procedures. Key topics include automating changes, responding to events, and defining standards to manage daily operations.

[HTML](#) | [Labs](#)

### Performance Efficiency Pillar

The performance efficiency pillar focuses on structured and streamlined allocation of IT and computing resources. Key topics include selecting resource types and sizes optimized for workload requirements, monitoring performance, and maintaining efficiency as business needs evolve.

[HTML](#) | [Labs](#)

### Security Pillar

The security pillar focuses on protecting information and systems. Key topics include confidentiality and integrity of data, managing user permissions, and establishing controls to detect security events.

[HTML](#) | [Labs](#)

### Cost Optimization Pillar

The cost optimization pillar focuses on avoiding unnecessary costs. Key topics include understanding spending over time and controlling fund allocation, selecting resources of the right type and quantity, and scaling to meet business needs without overspending.

[HTML](#) | [Labs](#)

### Reliability Pillar

The reliability pillar focuses on workloads performing their intended functions and how to recover quickly from failure to meet demands. Key topics include distributed system design, recovery planning, and adapting to changing requirements.

[HTML](#) | [Labs](#)

### Sustainability Pillar

The sustainability pillar focuses on minimizing the environmental impacts of running cloud workloads. Key topics include a shared responsibility model for sustainability, understanding impact, and maximizing utilization to minimize required resources and reduce downstream impacts.

[HTML](#) | [Labs](#)

# Q&A

Levi: <https://www.linkedin.com/in/levimccormick/>

Kisha: <https://www.linkedin.com/in/kishadelain/>



## Slides

