

AWS Multi-Account Networking: A Guide to Connecting VPCs Across Accounts



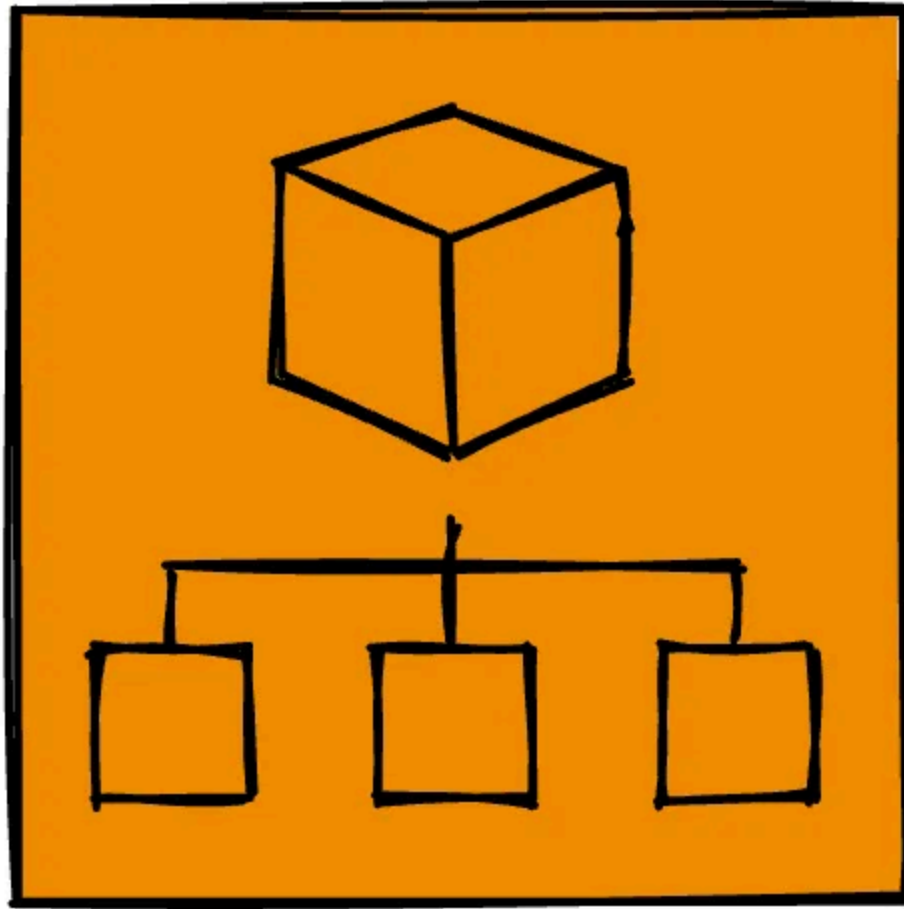
Kawin Promsopa · [Follow](#)

Published in AWS in Plain English · 5 min read · Oct 8, 2024



152





AWS Multi-Account Networking

In this article, I'll explain how to manage VPC connectivity in AWS multi-account setups, where one of the most important options is **AWS Transit Gateway**.

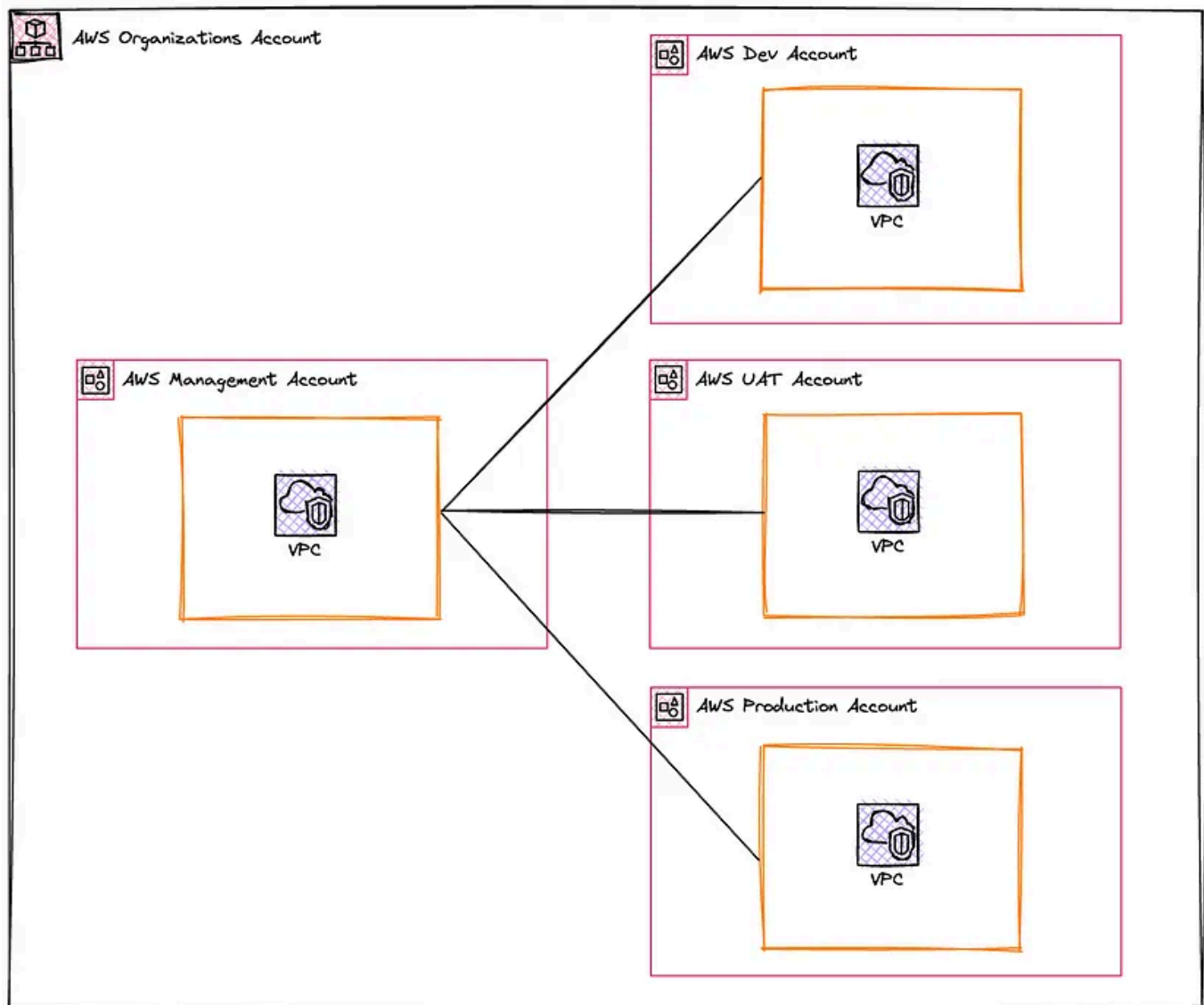
If you'd like to learn more about AWS Transit Gateway in detail, I recommend checking out my previous article "[AWS Transit Gateway 101: How it Works and When to Use It](#)".

TL;DR

AWS Transit Gateway is a service that simplifies network management by connecting multiple VPCs, AWS accounts, and even on-premises networks through

a single gateway. It enables centralized routing, reduces the complexity of managing VPC peering, and enhances security in isolated environments.

...



AWS Multiple Accounts

Why do we need VPC connectivity in Multiple Accounts?

A multiple accounts AWS environment is scaleable and secure, providing the highest level of resource and security isolation.

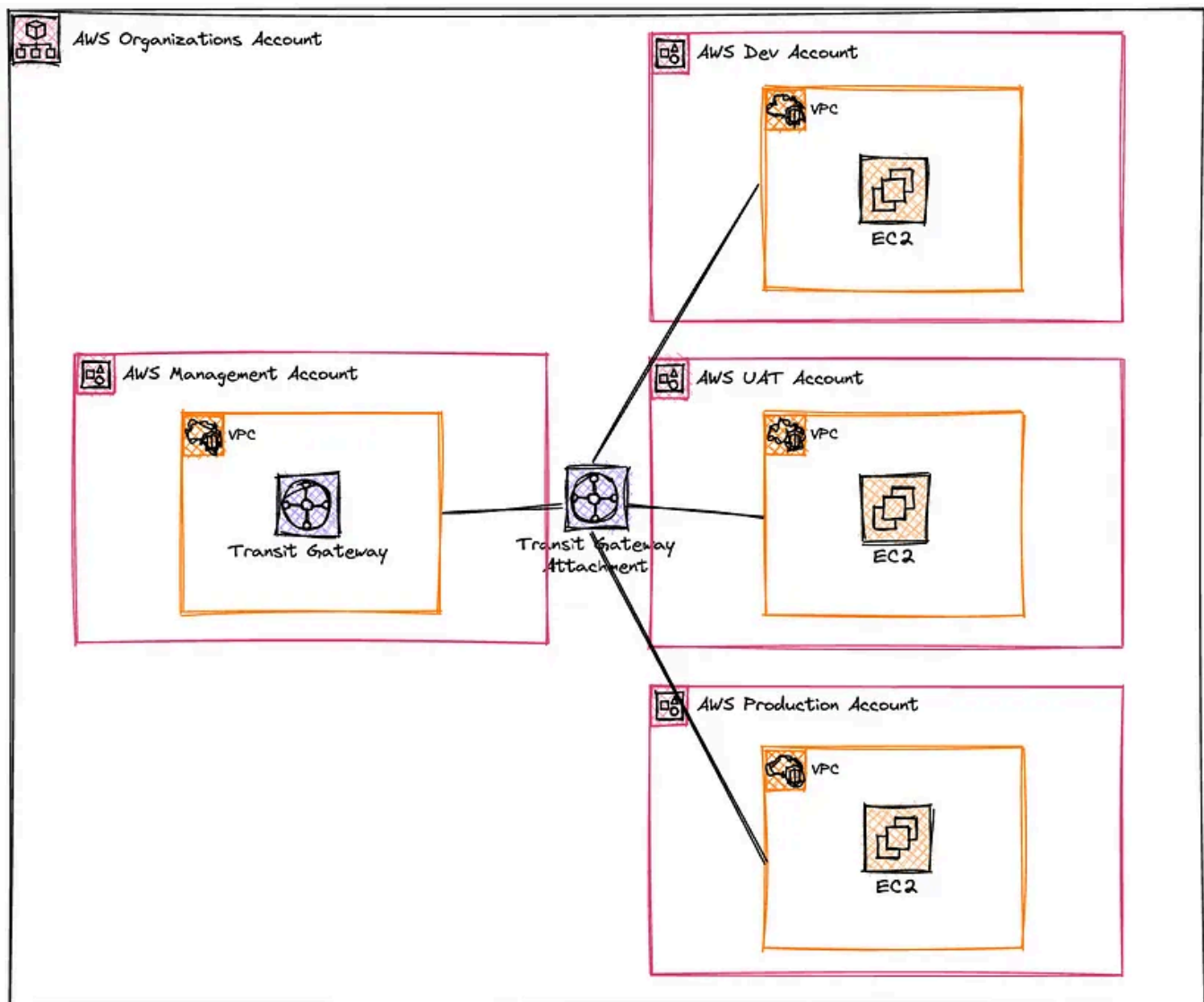
Here are some reasons why a single account might not be enough:

- **Access Management:** Multiple accounts enable organizations to implement more granular access controls, ensuring that only authorized users can access specific resources.
- **Billing:** Resource isolation by account allows for clearer tracking of usage and costs associated with different projects or teams.
- **Compliance:** Different accounts can be configured to meet specific compliance requirements for different business units.
- **Development Environments:** Isolated accounts can be used for testing and development without impacting production environments, reducing the risk of disruptions.
- **Security Control:** Isolating resources into separate accounts reduces the risk of unauthorized access and enhances overall security.

VPC Connectivity Options in Multi-Account Setups

In a multi-account AWS environment, there are several options available to connect VPCs across accounts.

Two of the most commonly used methods are **Transit Gateway** and **VPC Peering**. Both have their advantages, but they serve different use cases and offer varying levels of scalability and complexity.



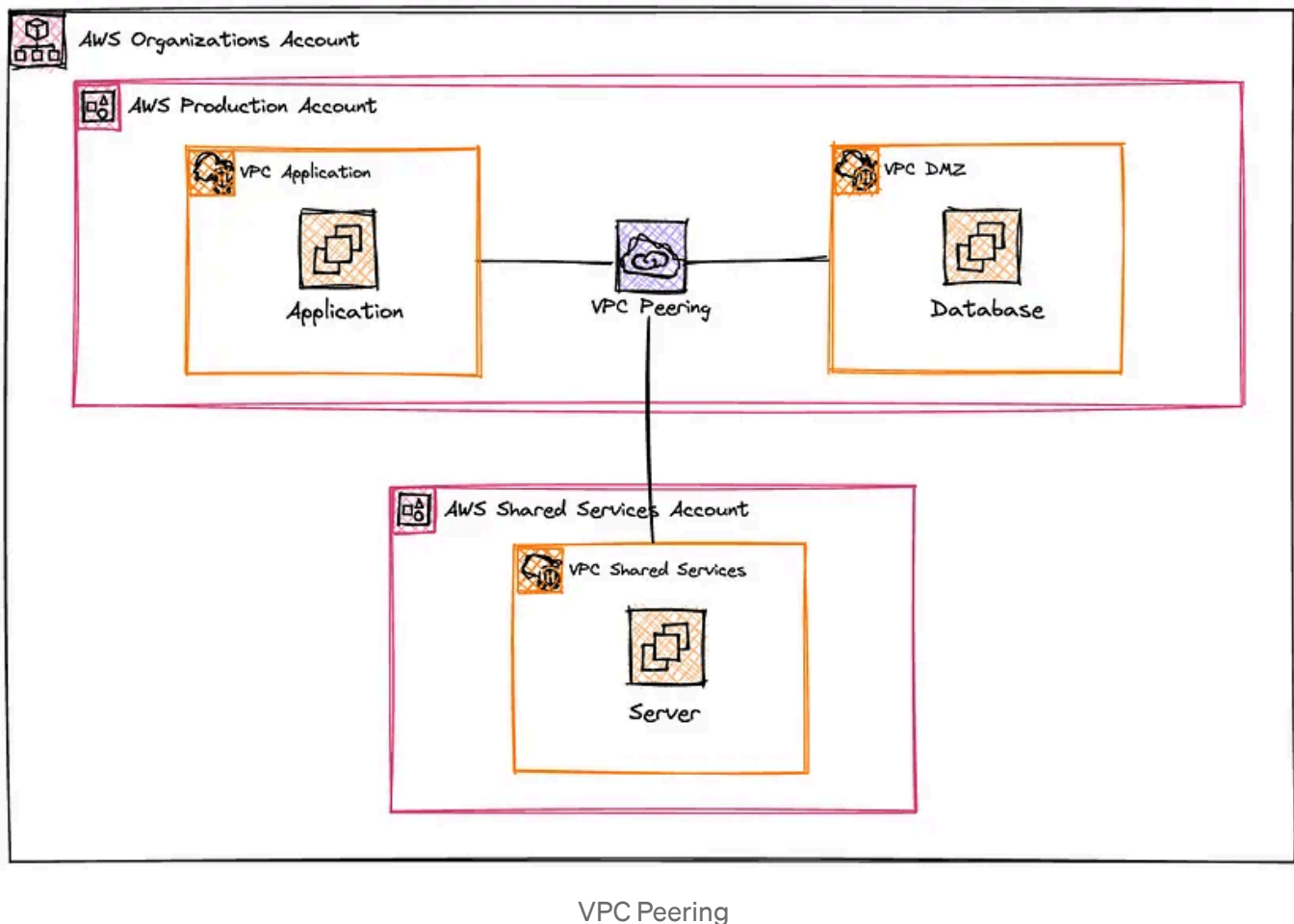
Transit Gateway

Transit Gateway

- **Description:** AWS Transit Gateway is a fully managed service that acts as a central hub connecting multiple VPCs, on-premises networks, and even across AWS regions.
- **Use Cases:**
 - **Centralized Control:** By providing a single point of control for routing and connectivity.
 - **Hybrid Cloud:** Suitable for integrating on-premises networks with AWS through a single connection point.

- **Limitations:**

- **Cost:** Transit Gateway can become expensive with large-scale usage, particularly when handling high volumes of traffic or connecting multiple regions.
- **Single Point of Management:** While centralizing the network, it also means that if there are issues with the Transit Gateway, multiple VPCs could be impacted at once.



VPC Peering

- **Description:** VPC Peering creates a private connection between two VPCs, allowing direct network connectivity in the same AWS account or different accounts.

- **Use Cases:**
 - **Simple Connectivity:** Ideal for smaller environments where one or a few VPCs need to communicate with each other within the same or across AWS accounts.
 - **Internal Service Access:** Good for scenarios where one VPC needs to access a specific resource (e.g., database) in another VPC.
- **Limitations:**
 - **No Centralized Management:** Unlink Transit Gateway, each peering connection needs to be manually managed.

Get the full article on Medium: <https://medium.com/@kavinpromsopa/how-to-enable-cross-account-connectivity-865e66df69a5>

Open in app ↗

Medium

Search

Write



How to Enable Cross-Account Connectivity ?

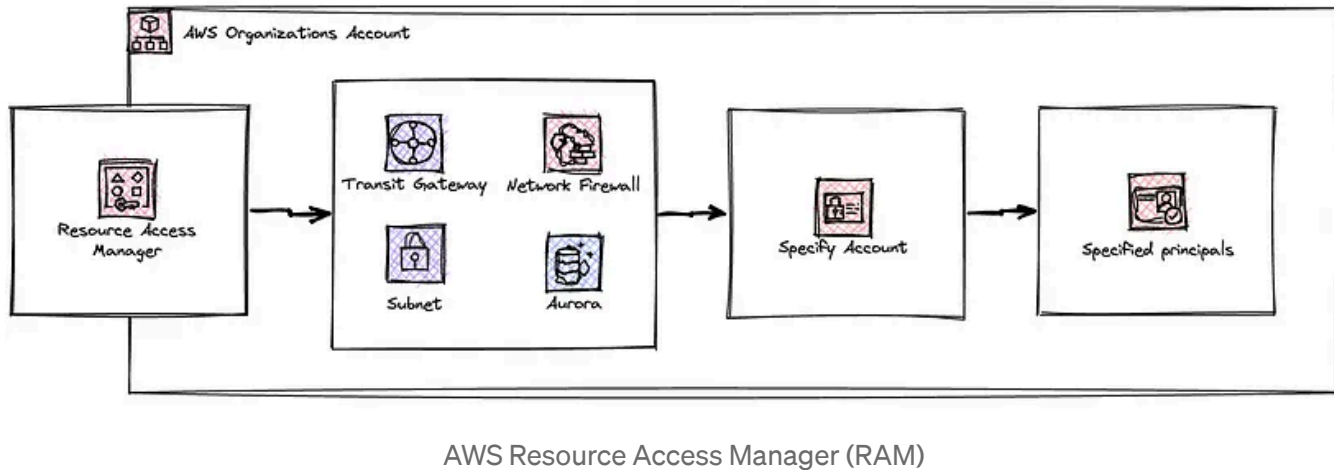
Transit Gateway and VPC Peering simplify cross-account connectivity, especially when used with [AWS Resource Access Manager \(RAM\)](#).

What is AWS Resource Access Manager (RAM)?

AWS Resource Access Manager (RAM) makes it easy to securely share resources across AWS accounts, whether within your organization or with external accounts. With RAM, you can share resources like AWS Transit Gateways, Subnets, Aurora, and Network Firewall without duplicating.

RAM reduces operational overhead for organizations using multiple accounts to improve security or billing isolation. Instead of managing resources separately, you can create them once and share them across accounts in a few simple steps — **create a resource share, select your resources, and specify the accounts.**

And the best part? RAM is available at **NO extra cost!**



Architectural Considerations

When setting up VPC connectivity in a multi-account AWS environment, keep these key factors in mind.

1. Network Segmentation: Decide how to segment your networks for enhanced security and resource isolation.

- Common strategies include:
 - Production and non-production workloads.
 - Different business units or departments.
 - Compliance — sensitive environment.
 - Plan CIDR ranges carefully to avoid any overlaps between VPCs.

2. Routing Complexity: Keep routing simple and efficient, considering how traffic flows across VPCs and external networks.

3. Security & Compliance: Ensure your architecture aligns with security standards and regulatory requirements, including encryption, traffic control, and auditing.

4. Bandwidth & Performance: Assess your bandwidth needs to handle traffic effectively while minimizing latency.

5. Cost Efficiency: Monitor data transfer costs as your network expands, especially with multiple VPCs or regions.

6. Scalability: Design your network for future growth, allowing easy expansion as new accounts or VPCs are added without requiring a redesign.

Conclusion

When managing multiple AWS accounts, leveraging Transit Gateway and VPC peering can significantly enhance cross-account connectivity.

However, it's important to consider the specific needs of your environment. While Transit Gateway offers centralized control and scalability, VPC Peering may be a simpler, cost-effective alternative for smaller setups or more isolated use cases.

the choice between Transit Gateway and VPC Peering depends on factors like the scale, cost considerations, and complexity of your network architecture.

By understanding the strengths of both Transit Gateway and VPC Peering, you can design a network infrastructure that is efficient, secure, and scalable — customized to meet your organization's specific needs.

If you enjoyed this article, please feel free to leave feedback 🙏, clap 👏, comment 💬, or follow 📌 for more weekly insights and best practices!

• • •

In Plain English

Thank you for being a part of the **In Plain English** community! Before you go:

- Be sure to **clap** and **follow** the writer 🙌
- Follow us: [X](#) | [LinkedIn](#) | [YouTube](#) | [Discord](#) | [Newsletter](#)
- Visit our other platforms: [CoFeed](#) | [Differ](#)
- More content at [PlainEnglish.io](#)

AWS

Networking

Cloud Computing

Security

DevOps



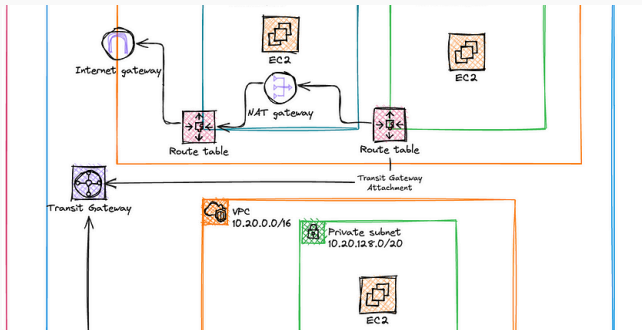
Written by Kawin Promsopa

75 Followers · Writer for AWS in Plain English

[Follow](#)

DevOps | Cloud Architect | Coffee Lover ☕ | Sharing hands-on insights and behind-the-scenes stories on building cloud infrastructure.

More from Kawin Promsopa and AWS in Plain English



Kawin Promsopa in AWS in Plain English

AWS Transit Gateway 101: How It Works and When to Use It

A Hands-On Guide to Implementing AWS Transit Gateway

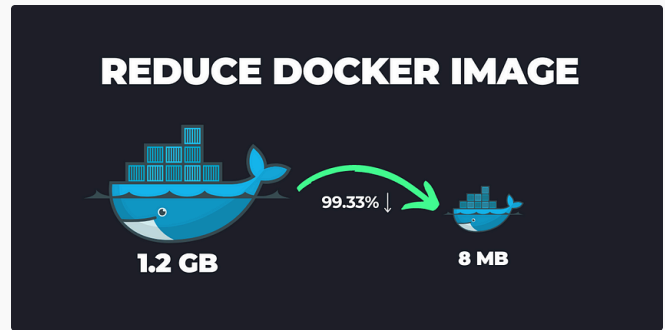
Sep 30



150



3



Dipanshu in AWS in Plain English

Docker pros are shrinking images by 99%: The hidden techniques yo...

Unlock the secrets to lightning-fast deployments and slashed costs—before yo...



Sep 18



3.3K



15



Dipanshu in AWS in Plain English

Why Developers Are Ditching PostgreSQL, MySQL and MongoDB

The Database Revolution Your Project Is Missing Out On



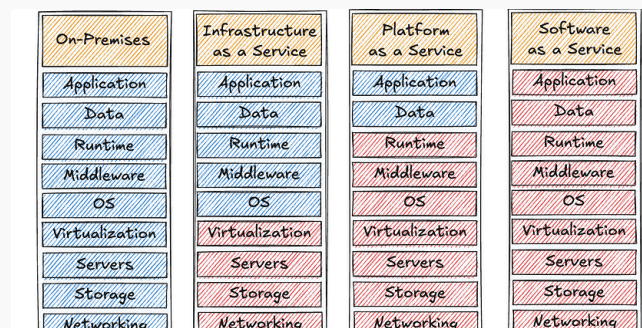
Oct 1



2.1K



47



Kawin Promsopa in AWS in Plain English

A Simple Guide to AWS Cloud Service Models: Which One Work...

Understanding AWS Service Models: How They Work and When to Use Them

Oct 22



65



2



[See all from Kawin Promsopa](#)[See all from AWS in Plain English](#)

Recommended from Medium

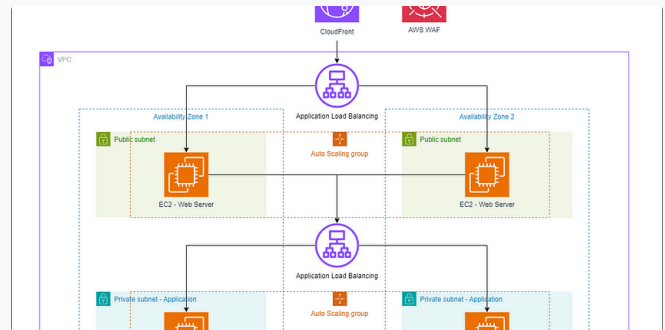


Z Zachary King in DevOps.dev

Practical Terraform: You're Doing it Wrong (Part 1)

We've all written Terraform IaC that we're not proud of before—it happens. These are...

★ Oct 14 🖱️ 62 💬 2 📌 ⋮



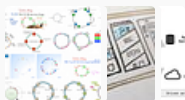
Reynold Nathaniel in AWS Tip

Cloud Architecting—How do you draw professional AWS...

To give you a little background, I have been a Cloud Solutions Architect for 4+ years...

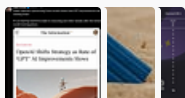
Oct 23 🖱️ 268 💬 5 📌 ⋮

Lists



General Coding Knowledge

20 stories · 1737 saves



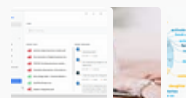
Natural Language Processing

1809 stories · 1424 saves



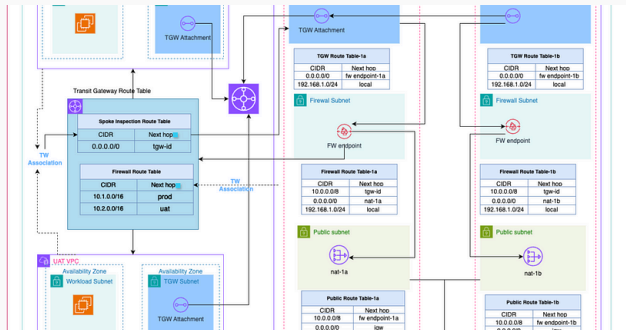
Business 101

25 stories · 1267 saves



Productivity

242 stories · 613 saves



Shivanshu Sharma in Searce

Configuring Traffic Inspection Using a Single Inspection VPC

Step by Step guide to configure centralized VPC for traffic Inspection in AWS

Oct 8 🖱 25

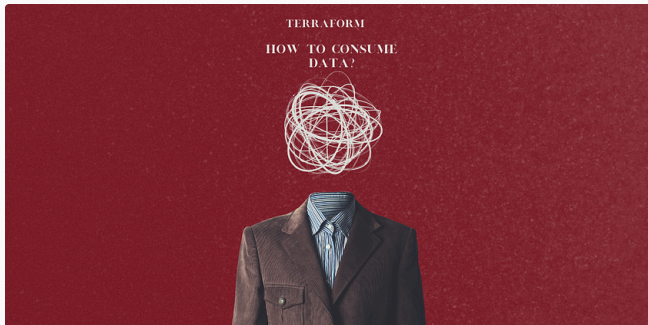


Digger HQ

8 Terraform Best Practices to Prevent Drift

Infrastructure drift occurs when the actual state of your infrastructure diverges from th...

Sep 23 🖱 2



Rahul Sharma in AWS in Plain English

The Terraform Scenario You're Likely to Encounter in Any...

I want to take you through one of the most common problems in terraform:



Sep 23 🖱 215 💬 4



Lio in DevCloud Ninjas

AWS DevOps Project: CI/CD Pipeline with Infrastructure as...

How to build Advanced Automated CI/CD Pipeline with IAC, Microservices, Service...

Oct 7 🖱 59 💬 3



[See more recommendations](#)