TRIANZ℠ | ACCELERATING DIGITAL EVOLUTION

Cloud foundation discussion

- Landing Zone

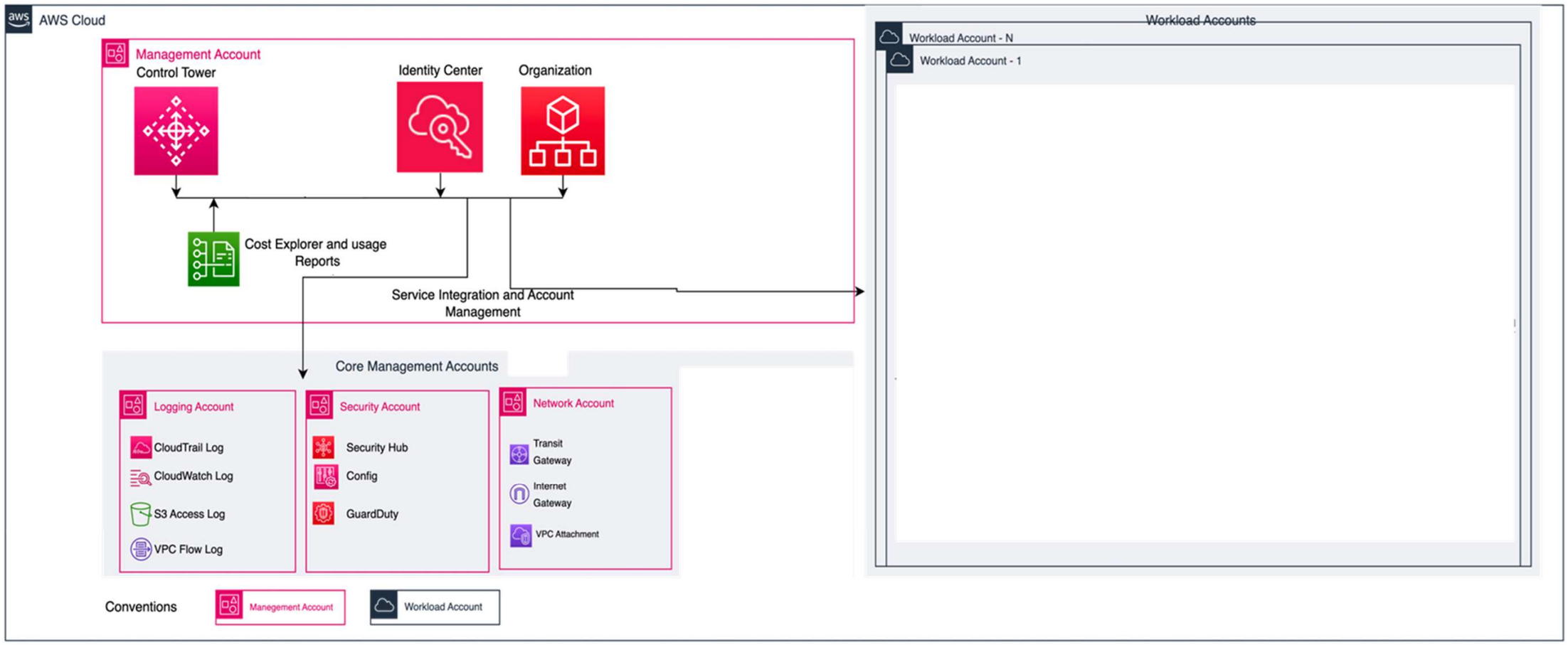
This document is created to provide the context for AWS landing zone creation. While some of the details are included, further detailed are available at the link given below.
https://aws.amazon.com/solutions/implementations/landing-zone-accelerator-on-aws/

www.trianz.com

AWS Recommended Landing zone accelerator

Landing Zone Accelerator on AWS solution deploys a foundational set of capabilities that is designed to align with AWS best practices and multiple global compliance frameworks. With this AWS Solution, you can better manage and govern your multi-account environment that have highly-regulated workloads and complex compliance requirements.

Reference: https://aws.amazon.com/solutions/implementations/landing-zone-accelerator-on-aws/

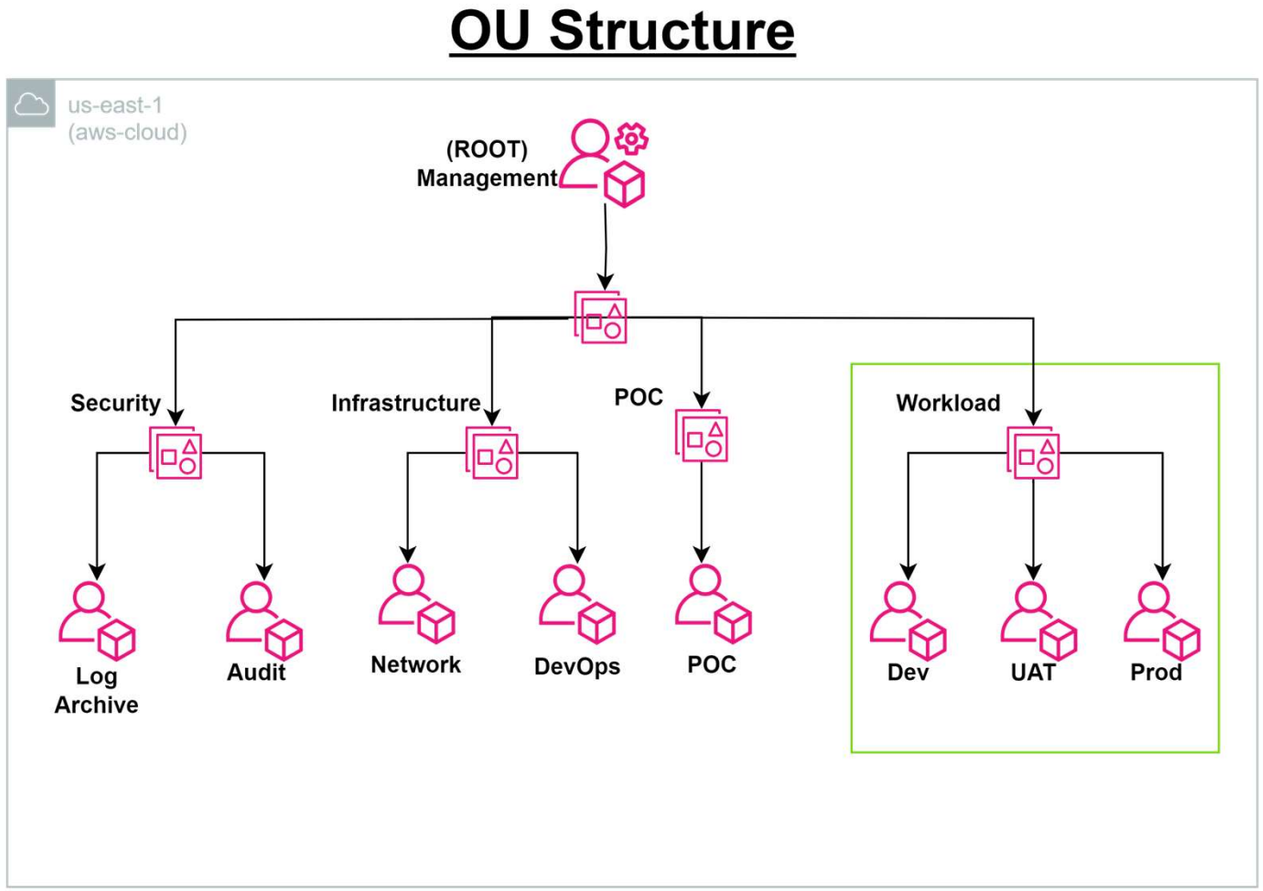


Account OU structure

The AWS landing zone employs an Account Organizational Unit (OU) structure with following functions:

- **Unified Management:** OUs provide a systematic approach to manage accounts collectively, enhancing administrative efficiency.
- **Security Consistency:** Service Control Policies (SCPs) applied to OUs ensure uniform security measures across all accounts.
- **Hierarchical Control:** Security controls cascade from the top-level OU down to subordinate OUs, guaranteeing organization-wide policy adherence.
- **Organizational Alignment:** The root OU encapsulates the entire organization's accounts, while sub-OUs reflect specific business segments, allowing for tailored security controls.

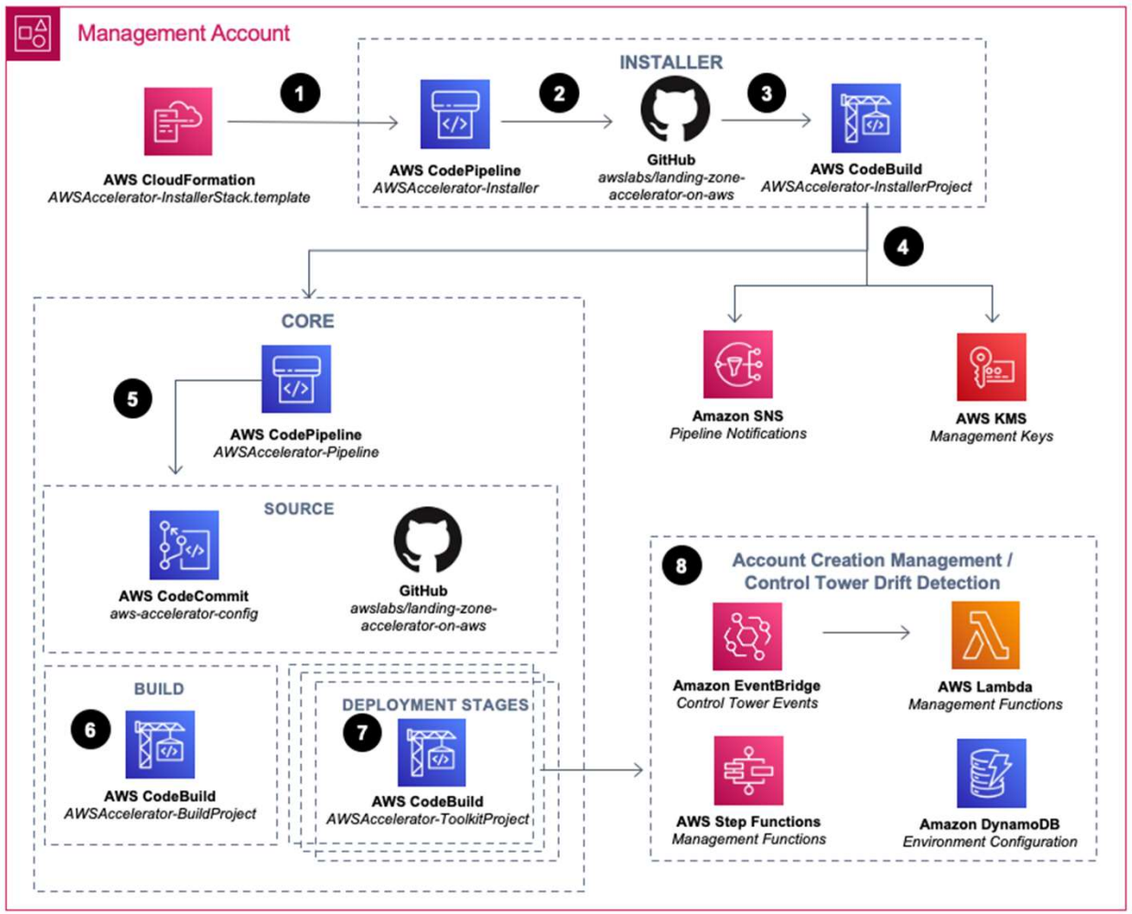
Following OU structure is proposed



Landing zone (Core) and Deployment pipelines

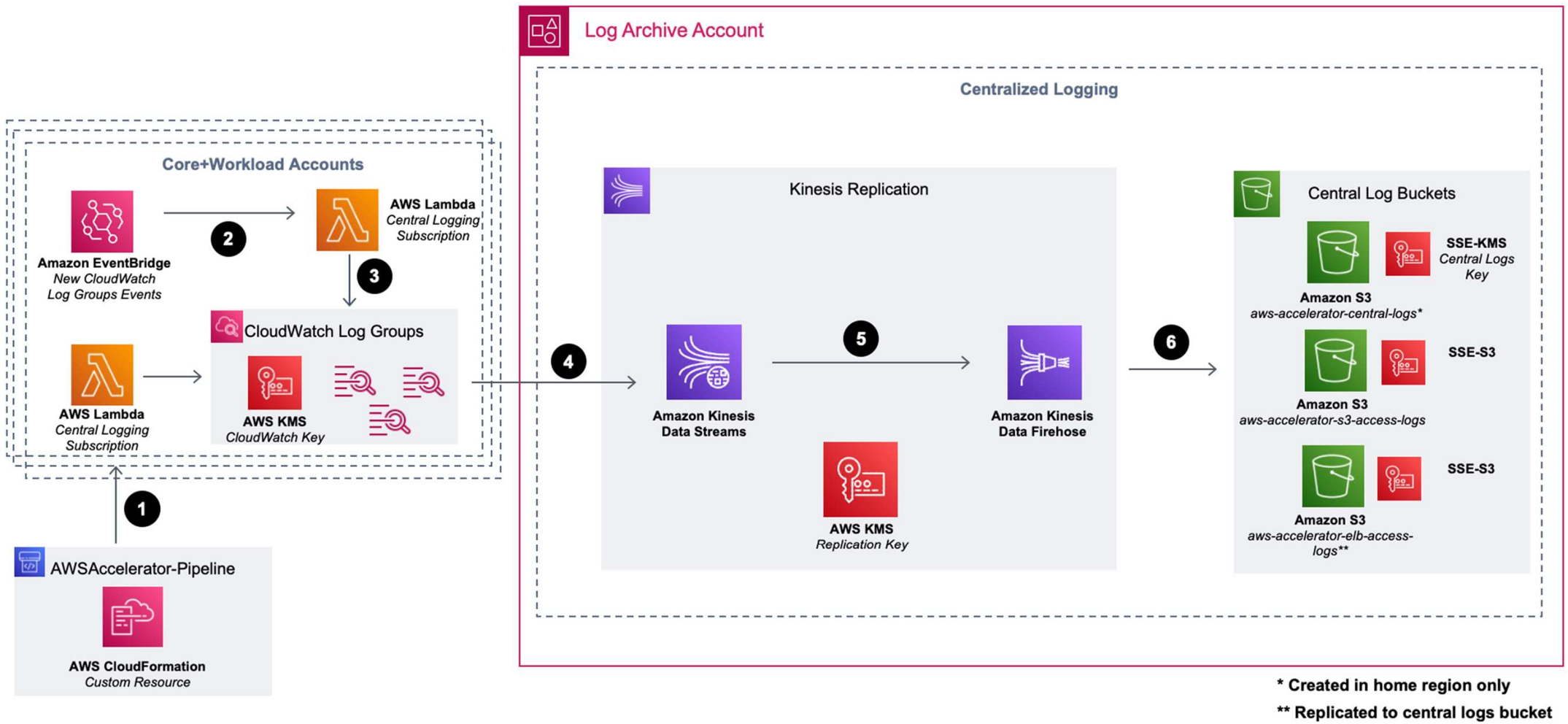
AWS Landing Zone Accelerator (LZA) deployment pipeline is a sophisticated system designed to automate the setup of a secure, multi-account AWS environment. LZA uses AWS CloudFormation to deploy CodePipeline pipelines, an installer, and the core deployment pipeline, along with associated dependencies.

For more details: https://docs.aws.amazon.com/solutions/latest/landing-zone-accelerator-on-aws/architecture-diagram.html



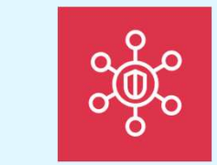
Logging architecture

This architecture enables centralised approach for log management, allowing for unified policies for log management, archiving, retention and deletion processes.



LZA enables core security services needed to meet several compliance requirements

	Key Component Description
A	Security Hub, aggregates and prioritizes security information and alerts from other AWS security services such as Guard Duty, Inspector, and Macie. It integrates with CloudWatch Logs and Events to identify compliance or incident issues and define workflows that can be executed when vulnerabilities are detected.
B	Service Control Policies (SCPs) are a feature of AWS Organizations used to define and enforce permission guardrails across AWS accounts. They help ensure that accounts within an organization comply with the company's security and compliance requirements.
C	CloudWatch, collects operational data from AWS built services and stores them as logs and metrics. It has customizable rules that trigger alarms, allowing for notifications and automated actions to be performed using AWS services like ASG or Lambda. CloudWatch is an important tool for securing your account, and integrating CloudTrail events with CloudWatch rules can help detect critical API usage.
D	CloudTrail, will allow for monitoring of all API calls made across the account, including actions performed in the console, AWS SDKs and command line tools, making it a crucial tool for monitoring account activity. CloudTrail's data can be integrated with other AWS services such as CloudWatch and SNS to send notifications when security-critical APIs are used, making it an important feature for compliance and operational auditing of an AWS account.
E	AWS Config is a service that provides a comprehensive view of the configurations of AWS resources, enabling continuous monitoring and assessment. It facilitates governance, compliance, and resource management by recording and evaluating configuration.
F	Other services of Macie, Inspector, GuardDuty will not be enabled.



AWS Security Hub

Security Control Policy

AWS CloudWatch

AWS CloudTrail

AWS Config

Low Level discussion points

For the deployment of the landing zone, each core account created during the process must have a distinct email address. Here are the examples provided:

- Management = management@prioritywaste.com
- Log archive = log@prioritywaste.com
- Security = security@prioritywaste.com
- Prod = management+prod@ prioritywaste.com
- Dev = management+dev@ prioritywaste.com
- NW = management+nw@ prioritywaste.com
- DevOps = management+devops@ prioritywaste.com

Agreement:

- Account number 236345613440 will serve as the root account, and the landing zone architecture (LZA) will be initiated from this account, as confirmed by Ameet.
- The us-east-1 region will be designated as the primary for all workloads, with us-east-2 as the disaster recovery (DR) site if required.
- Controls from the CIS framework will be implemented in conjunction with the LZA setup.

MAP Tagging:

Following are the map tags assigned by AWS.

Initiative	Tag key	Tag value	Mandatory / Optional
Platform build	map-migrated	migSZUDBD3OY2	Mandatory for PB Resources
Fleet mgmt	map-migrated	mig3W94SJXDED	Mandatory for Fleet / IOT resources

Tags for resource categorization (all mandatory):

Initiative	Tag key	Tag values
Project Name	project	pw
Track	track	lz, devops, fleet, data, etc.
Environment	env	dev, uat, prod

Naming convention:

pw-<resourcetype>-<env>-<purpose>-<instancecount>

e.g. pw-api-dev-user-1

Cost of Landing Zone accelerator:

- Deployment of AWS recommended LZA incurs cost (appr. 400 USD per month) without any resources
- Cost increases once the resources are deployed for the project

https://docs.aws.amazon.com/solutions/latest/landing-zone-accelerator-on-aws/cost.html

TRIANZ℠ | ACCELERATING DIGITAL EVOLUTION

Great Place To Work. Certified 2023 USA | INDIA

Thank you

Yaseen Mohammed
Yaseen.mohammed@trianz.com
+61 451 405 893