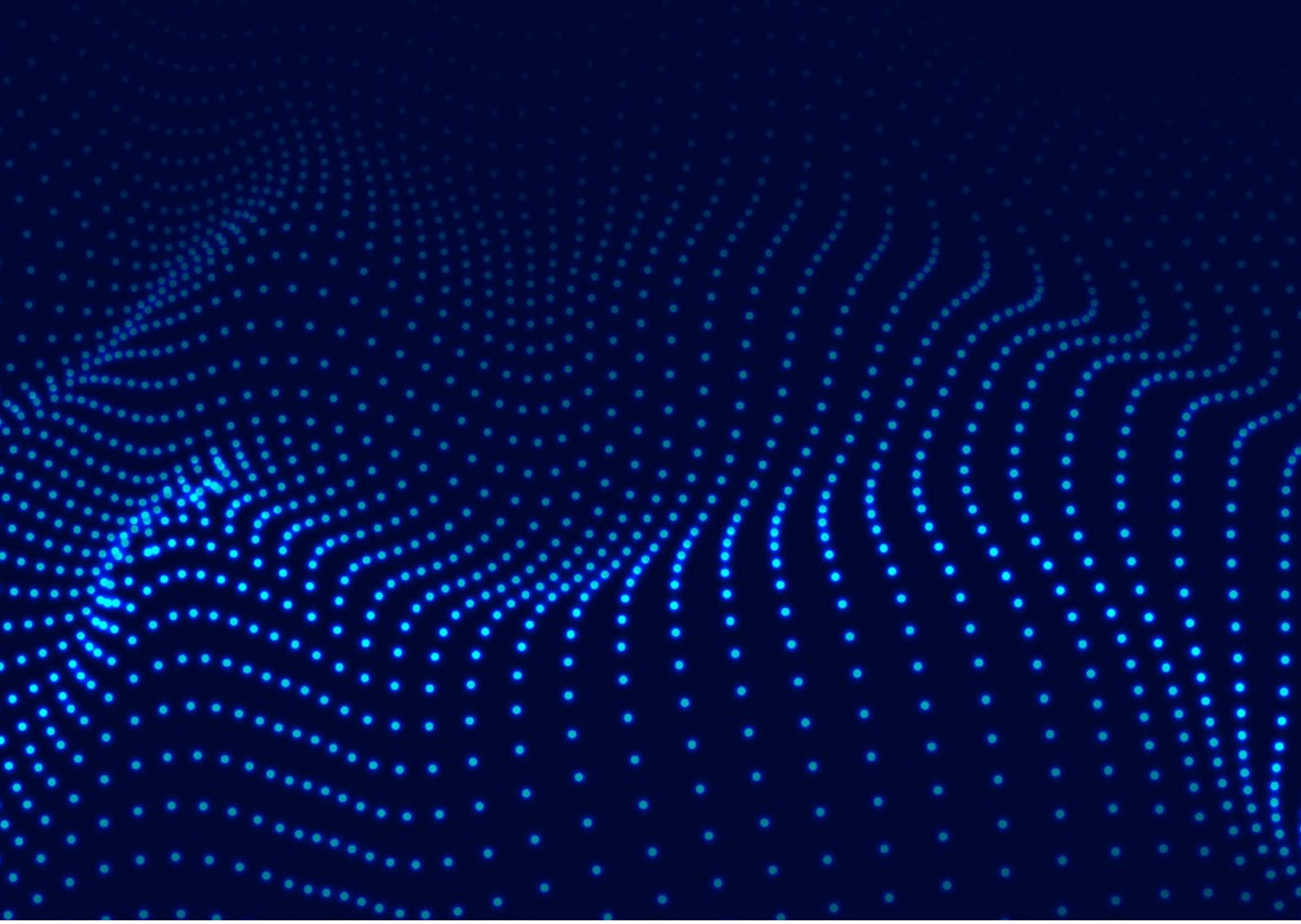


Cloud Foundation

A winning cloud strategy starts with the right foundation

/thoughtworks

Strategy. Design. Engineering.

Cloud Foundation

Our Cloud Foundation Accelerator sets your organization up for success with a landing zone that is a Well-Architected, best practice, secure and flexible, multi-account capable, AWS environment.

Benefits

- Get AWS right the first time
- Application ready
- Comprehensive security & compliance
- Ready for any workload
- Fully compliant with the AWS Well-Architected Framework
- Inbuilt cost-efficiency & proactive billing alerts
- DevOps ready
- Infrastructure as code & automation
- Comprehensive handover to your team

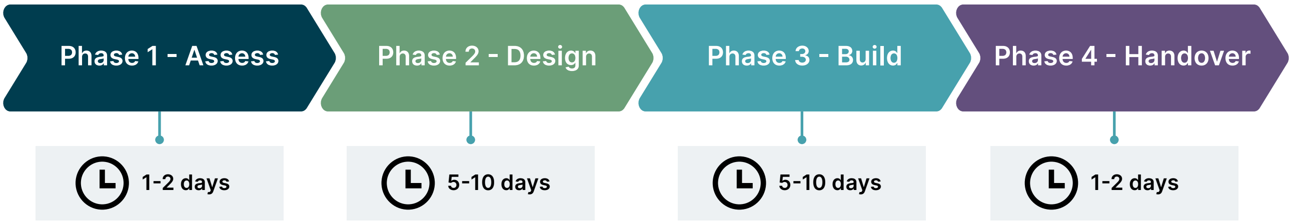
Product overview

Thoughtworks Cloud Foundation Accelerator delivers a best practice, secure and flexible foundation Amazon Web Services(AWS) environment for customers that don't have the capacity internally or the depth of skills yet. Whether you need to replace an outdated AWS solution that doesn't meet best practice or build a new greenfield environment, we'll guide you through every step - prior experience is not necessary.

Based on lessons learned from hundreds of successful engagements and aligned with the AWS Well-Architected Framework, Cloud Foundation brings together everything required with a guaranteed successful outcome. With a typical Cloud Foundation Accelerator taking two to four weeks it's also the shortest path to value on the AWS Cloud.

Our approach

Don't worry if you don't know what you need or how to explain it, we've successfully helped many customers, just like you, build out their foundational AWS environment. Our team of AWS experts will ensure that you de-risk your move to the cloud and get results fast.



Phase 1 - Assess — 1-2 days

Phase 2 - Design — 5-10 days

Phase 3 - Build — 5-10 days

Phase 4 - Handover — 1-2 days

AWS account structure

As part of the Terraform Cloud Foundation, we create a multi-account structure to separate different operating environments from access controls and audit logs.

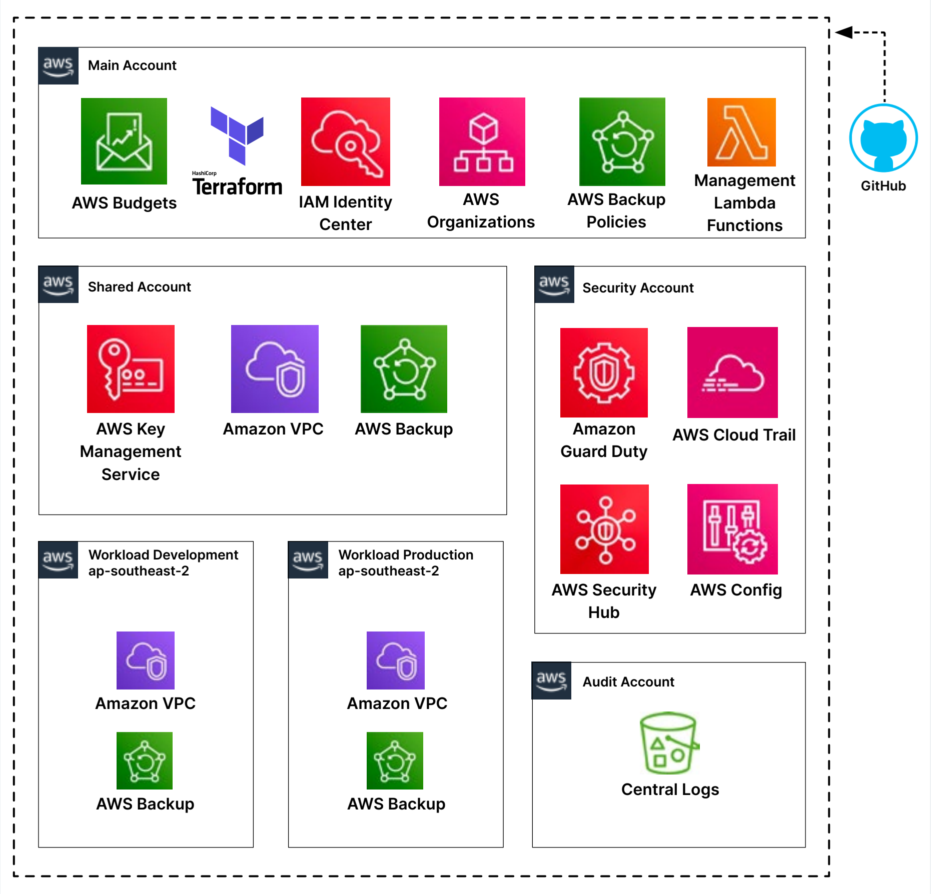
Main: This account is used for consolidated billing, budget control, identity management (via AWS SSO) and administration of your AWS Organisation.

Shared: Used to house infrastructure that is shared between workload environments (e.g. CI/CD, Active Directory)

Security: Centralised configuration management for all AWS Organisation accounts. It is also the central point of administration for GuardDuty & Security Hub.

Audit: Stores AWS activity logs (CloudTrail), VPC Flow logs, Config logs, Guardduty logs as well as Access Logs

Workload: Separate AWS accounts to house the workloads for each of your operating environments.



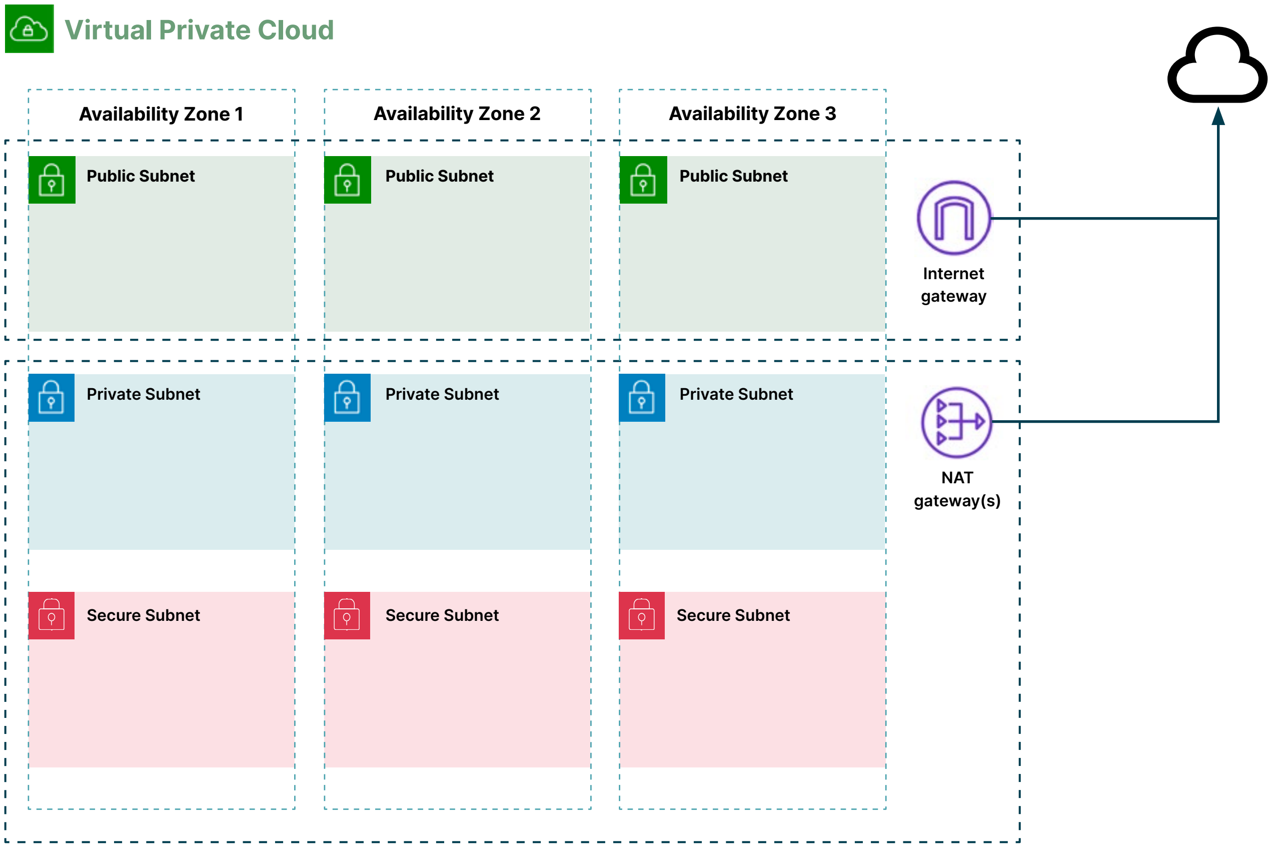
AWS IAM Identity Center

AWS IAM Identity Center (Successor to AWS Single Sign-On) provides a single point of identity management for your multi-account architecture. It contains an internal user database and optionally has the ability to federate against Azure AD and GSuite. As part of the Foundation, Permission Sets will be created for AWS-defined job roles. These job functions include Administrators, Billing, DBA, Developers, Network Administrators, System Administrators, CyberSecurity, and Read-Only access. You can add/modify permission sets if you require additional or altered roles in the future.

Network architecture

Within the Shared account and each Workload account, a VPC containing a 3–tier, highly-available distribution of subnets is created. The three tiers are Public, Private and Secure. These tiers are used to segment workloads; internet access to resources in the Public Subnet is direct, internet access for Private is one-way via NAT gateways and Secure subnet, by default, doesn't have an internet access. Within each tier, a subnet is deployed into each availability zone.

VPC CIDR's are allocated /16 width
Subnet CIDR's are allocated /20 width.



Billing alerts

Billing alerts are configured to send email notifications if a preset budget for your AWS expenditure across all accounts is exceeded, or forecast to be exceeded for the month.

AWS backup policies

Backup policies are configured organisation-wide within the Mainaccount and enforced by AWS Backup for the workloads operating within the Shared and Workload accounts.

The Foundation is deployed with backup policies for daily, weekly, monthly and yearly backups out-of-the-box.

Organisation governance

CloudTrail logs every API call made to your AWS accounts by the AWS Web Console or via Command Line Interface. Organisation CloudTrails prevents users from disabling this audit trail and ensures logs are centrally stored in the Audit account.

Service Control Policies (SCP’s) are used to enforce restrictions within AWS accounts from the outside in. As part of the Foundation, an SCP is deployed preventing users from disabling the AWS audit controls.

Terraform remote state

The Terraform state for the Foundation is stored remotely within S3 buckets owned by the Main account.

To ensure you are still able to deploy changes in the event of a regional outage, the state for each region is stored in a dedicated S3 bucket within that region.

Technical documentation

Technical documentation describing the infrastructure deployed within each AWS account and all Terraform modules is dynamically generated when the Foundation Terraform stack is run.

This documentation is stored within the Foundation git repository, meaning that the documentation is always kept up-to-date with the infrastructure code (when deployed using the Foundation deployment tooling).

AWS Security Hub

AWS Security Hub integrates with other services like Guard Duty and IAM Access Analyzer to provide a single pane-of-glass view over the security posture of your AWS Organisation, detecting deviations and aggregating findings to a central monitoring point.

As part of the Terraform Foundation, Security Hub is enabled in all workload accounts and configured to aggregate findings into the Audit account.

As you begin using the Foundation to run workloads, AWS Security Hub can be easily expanded to integrate with AWS Systems Manager, AWS Firewall Manager and Amazon Inspector v2 to provide centralised visibility over the security posture of your EC2 instances and firewalls.

Amazon Guard Duty

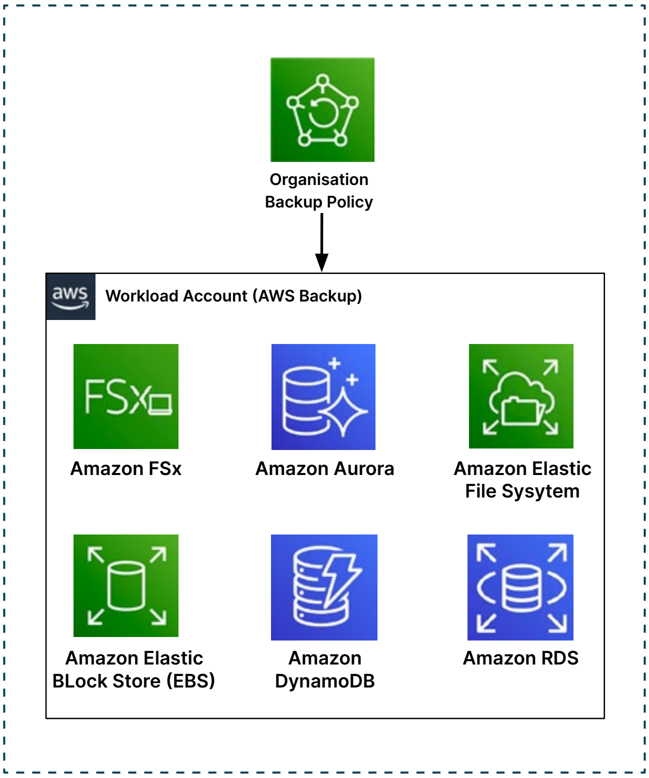
AWS Guard Duty continuously monitors your CloudTrail, VPC Flow Logs and DNS Logs to detect malicious activity and report findings. GuardDuty is enabled in all AWS accounts as part of the Terraform Foundation and configured to consolidate findings into the Audit account. These findings are then shared with AWS Security Hub.

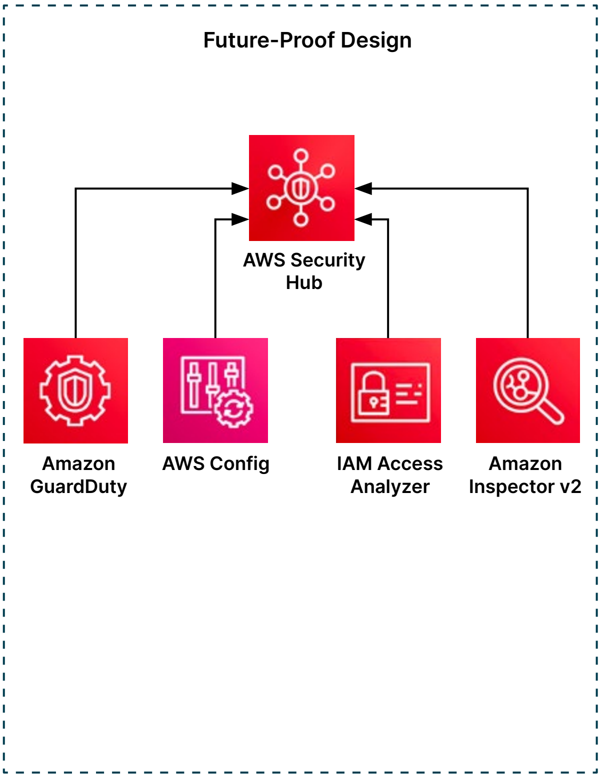
Sustainability

Amazon has pledged to be Net zero carbon by 2040 with a path to achieving 100% renewable energy usage by 2025.

According to research undertaken by 451 Research, workloads operating on AWS infrastructure are 3.6× more energy efficient than the median of the surveyed US enterprise data centres. Due to the dynamic allocation technologies and energy efficiencies built into AWS datacentre infrastructure, tasks operating on AWS have an 88% lower carbon footprint than other US enterprise datacentres.

The Terraform Foundation has been designed in accordance with the AWS Well Architected Framework, meaning that when you begin migrating workloads into your accounts, you will be inherently gaining AWS' work towards sustainability and assisting your organisation in achieving its sustainability goals.


Organisation Backup Policy
aws
Workload Account (AWS Backup)
Amazon FSx
Amazon Aurora
Amazon Elastic File Sysytem
Amazon Elastic BLock Store (EBS)
Amazon DynamoDB
Amazon RDS



Thoughtworks is a global technology consultancy that integrates strategy, design and engineering to drive digital innovation. We are over 11,500 Thoughtworkers strong across 51 offices in 18 countries. For 30 years, we've delivered extraordinary impact together with our clients by helping them solve complex business problems with technology as the differentiator.

thoughtworks.com

/thoughtworks

Strategy. Design. Engineering.

© Thoughtworks, Inc. All Rights Reserved.