
aws
SUMMIT
WASHINGTON DC |

SEC201

Scaling automated governance with Landing Zone Accelerator on AWS

Mark Burr
Global Leader - Technology, Solutions and Delivery,
AWS Professional Services
Amazon Web Services

Randy Domingo
Principal Engineer, AWS Professional Services
Amazon Web Services

AWS gets customers at least 60% along their compliance journey in terms of security controls

Compliance requirements

- ✓ Personnel
- ✓ Incident response
- ✓ Boundary protection
- ✓ Identity and access control
- ✓ Disaster recovery
- ✓ Configuration management
- ✓ Highly available architecture
- ✓ System management & monitoring
- ✓ Log management & monitoring
- ✓ Compute and storage
- ✓ Networking
- ✓ Virtualization
- ✓ Data center

Organizations need better visibility and security to optimize their next-gen cloud applications

Increase operational efficiency for your cloud-based workloads and applications

Improve visibility

Enhance security posture

Use AWS services to achieve operational excellence in securing your cloud environment

- Centralize threat detection and monitoring
- Improve security posture assessment
- Optimize vulnerability management
- Streamline root cause analysis
- Improve sensitive data discovery
- Initiate and route workflows to existing systems
- Prioritize critical findings
- Automate remediation
- Scale deployments

AWS security, identity, and compliance solutions

Identity & access management

AWS Identity & Access Management (IAM)

AWS Single Sign-On

AWS Organizations

AWS Directory Service

Amazon Cognito

AWS Resource Access Manager (AWS RAM)

Detection

AWS Security Hub

Amazon GuardDuty

Amazon Inspector

Amazon CloudWatch

AWS Config

AWS CloudTrail

VPC flow logs

AWS IoT Device Defender

Infrastructure protection

AWS Firewall Manager

AWS Network Firewall

AWS Shield

AWS WAF – web application firewall

Amazon Virtual Private Cloud (Amazon VPC)

AWS PrivateLink

AWS Systems Manager

Data protection

Amazon Macie

AWS Key Management Service (AWS KMS)

AWS CloudHSM

AWS Certificate Manager

AWS Secrets Manager

AWS VPN

Server-side encryption

Incident response

Amazon Detective

CloudEndure Disaster Recovery

AWS Config rules

AWS Lambda

Compliance

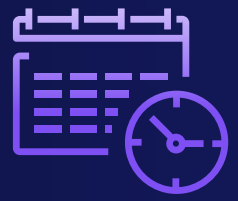
AWS Artifact

AWS Audit Manager

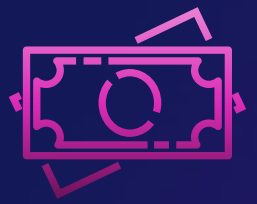
Now, more than ever, organizations need strong foundational architectures

High performing

Secure



Reliable



Cost-efficient

Sustainable

The architectural best practices portfolio

ACCELERATE CLOUD ADOPTION WITH CONFIDENCE

EXPERTISE

AWS Well-Architected

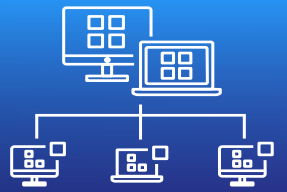
Improve operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability

Sustainable architecture

Enhance sustainability in the cloud via energy reduction and workload efficiency

AWS solutions

Deploy turnkey solutions or kick-start the building process with preconfigured architecture patterns



Architecture center

Access a robust content library, including reference architecture diagrams, best practices, and more

AWS SERVICES

Build a secure foundation

You need a landing zone

- A secure, scalable, multi-account AWS environment based on AWS best practices
- A starting point for net new development and experimentation
- A starting point for migrating applications
- An environment that allows for iteration and extension over time

Landing zone elements

Secure and compliant

Meets the organization's security and auditing requirements

Scalable and resilient

Ready to support highly available and scalable workloads

Adaptable and flexible

Configurable to support evolving mission requirements

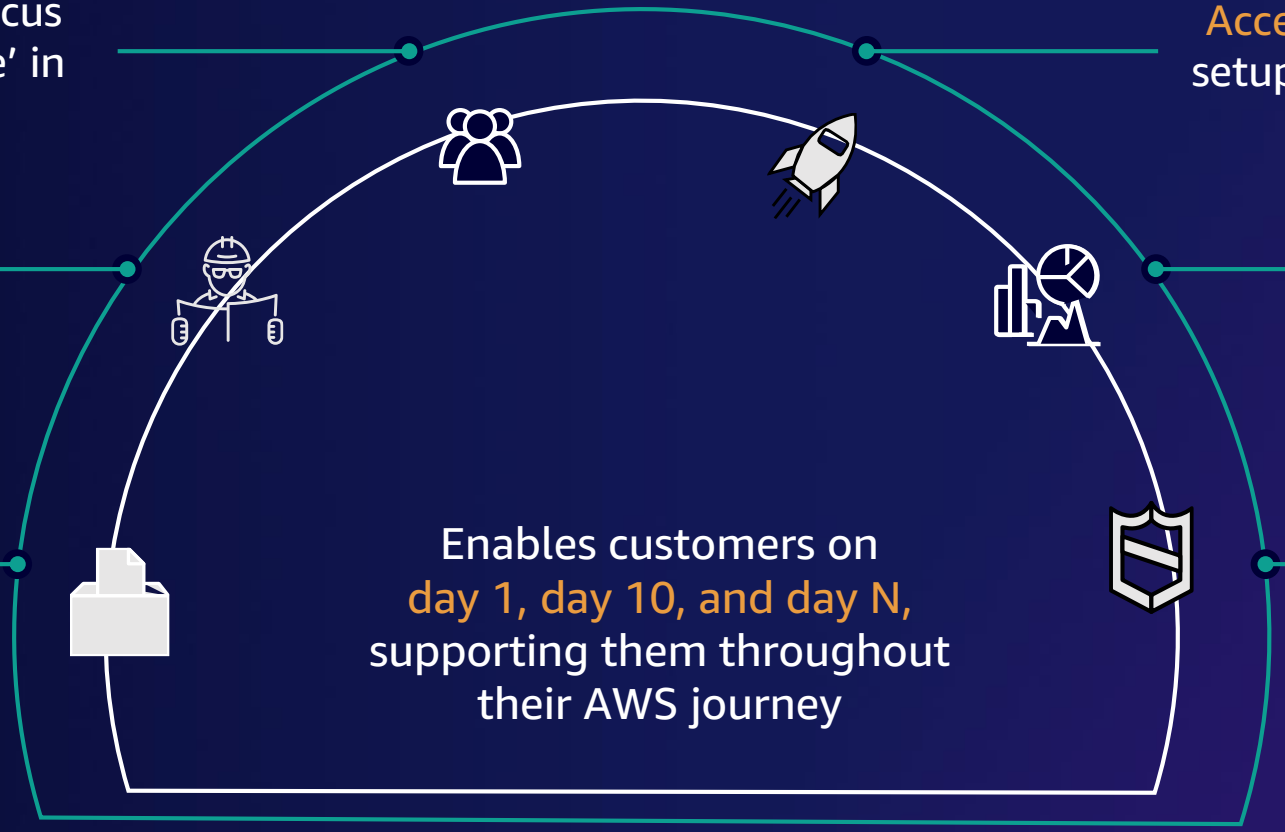
The Landing Zone Accelerator on AWS is an open source software solution that accelerates the implementation of a customer's technical security controls and infrastructure foundation on AWS

Landing Zone Accelerator Benefits

Customer resources focus on learning to 'operate' in the cloud

Leverages AWS expertise

Flexibility to integrate with other management tools

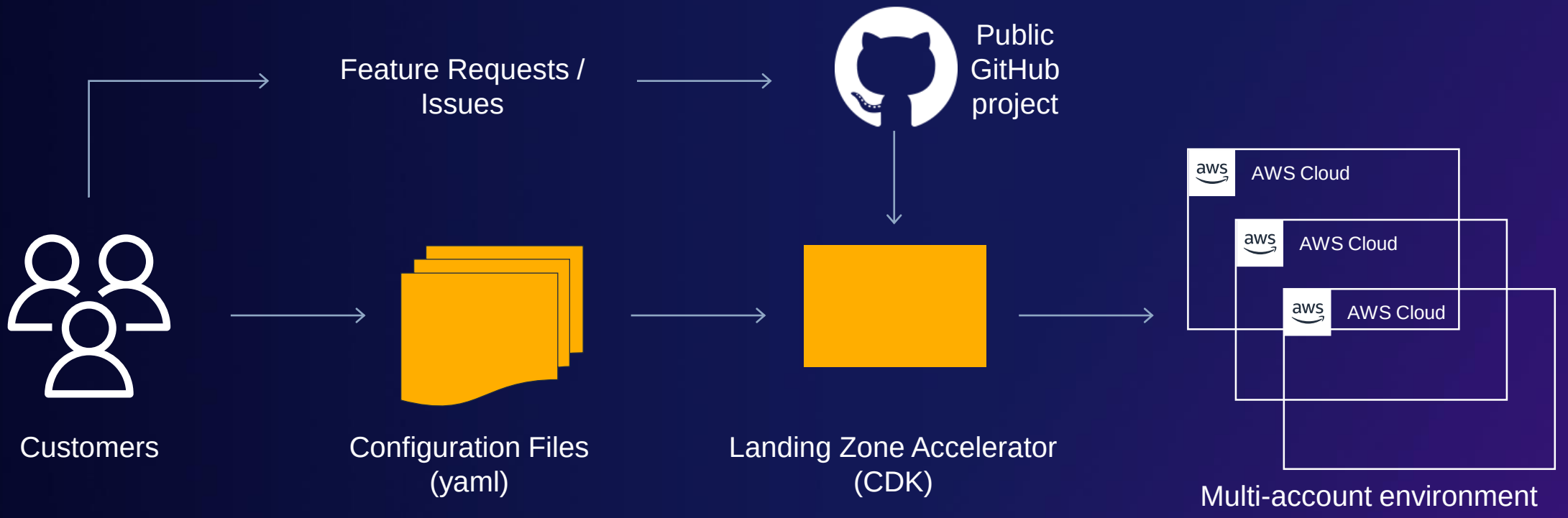


Accelerate environment setups in days, not weeks

Innovate through open source model

Establish a compliant and improved security posture

Architecture



Landing Zone Accelerator on AWS

1. 

Installation Template
(AWS CloudFormation)

2. 

Configuration Files
(yaml)

3. 

AWS CodePipeline

4. 

AWS Cloud
Development Kit

Landing Zone
Accelerator

Landing Zone Accelerator on AWS

1. 

Installation Template
(AWS CloudFormation)

2. 

Configuration Files
(yaml)

3. 

AWS CodePipeline

4. 

AWS Cloud
Development Kit

Landing Zone
Accelerator

```yaml
enable: true
organizationalUnits:
  - name: Security
  - name: Infrastructure
  - name: Dev
  - name: Test
  - name: Prod
serviceControlPolicies:
  - name: AcceleratorGuardrails1
    description: Accelerator GuardRails 1
    policy: service-control-policies/guardrails-1.json
    type: customerManaged
    deploymentTargets:
      organizationalUnits:
        - Infrastructure
        - name: AcceleratorGuardrails2
taggingPolicies:
  - name: TagPolicy
    description: Organization Tagging Policy
    policy: tagging-policies/org-tag-policy.json
    deploymentTargets:
    organizationalUnits:
      - Root
backupPolicies:
  - name: BackupPolicy
    description: Organization Backup Policy
    policy: backup-policies/org-backup-policies.json
    deploymentTargets:
    organizationalUnits:
      - Root
```

```yaml
mandatoryAccounts:
  - name: Management
    email: example-management-root-account@amazon.com
    organizationalUnit: Root
  - name: LogArchive
    email: example-log-archive-account@amazon.com
    organizationalUnit: Security
  - name: Audit
    email: example-audit-account@amazon.com
    organizationalUnit: Security
workloadAccounts:
  - name: SharedServices
    email: example-shared-service-accounts@amazon.com
    organizationalUnit: Infrastructure
  - name: Network
    email: example-network-account@amazon.com
    organizationalUnit: Infrastructure
```

Landing Zone Accelerator on AWS

1. Installation Template (AWS CloudFormation)

2. Configuration Files (yaml)

3. AWS CodePipeline

4. AWS Cloud Development Kit

Landing Zone Accelerator

Landing Zone Accelerator on AWS

1. 

Installation Template
(AWS CloudFormation)

2. 

Configuration Files
(yaml)

3. 

AWS CodePipeline

4. 

AWS Cloud
Development Kit

Landing Zone
Accelerator

```yaml
homeRegion: &HOME_REGION us-east-1
centralSecurityServices:
delegatedAdminAccount: Audit
ebsDefaultVolumeEncryption:
  enable: true
  excludeRegions: []
s3PublicAccessBlock:
  enable: true
  excludeAccounts: []
macie:
  enable: true
  ...
guardduty:
  enable: true
  ...
securityHub:
  enable: true
  regionAggregation: true
  excludeRegions: []
  standards:
    - name: AWS Foundational Security Best Practices v1.0.0
      enable: true
      controlsToDisable:
        - IAM.1
        - EC2.10
        - Lambda.4
ssmAutomation:
  ...
accessAnalyzer:
  enable: true
  ...
```

```yaml
iamPasswordPolicy:
  allowUsersToChangePassword: true
  hardExpiry: falserequireSymbols: true
  requireNumbers: true
  minimumPasswordLength: 14
  passwordReusePrevention: 24
  maxPasswordAge: 90
awsConfig:
  enableConfigurationRecorder: true
  enableDeliveryChannel: true
  ruleSets:
    - deploymentTargets:
        organizationalUnits:
          - Root
      rules:
          - name: accelerator-iam-user-group-membership-check
            complianceResourceTypes:
              - AWS::IAM::User
            identifier: IAM_USER_GROUP_MEMBERSHIP_CHECK
          - name: accelerator-securityhub-enabled
            identifier: SECURITYHUB_ENABLEDcloudWatch:
  metricSets:
    - regions:
        - *HOME_REGION
      deploymentTargets:
      organizationalUnits:
          - Root
      metrics:
        # CIS 1.1 - Avoid the use of the "root" account
        - filterName: RootAccountMetricFilter
          logGroupName: aws-controltower/CloudTrailLogs
          filterPattern: '{$.userIdentity.type="Root"'
          metricNamespace: LogMetrics
          metricName: RootAccount
          metricValue: "1"
```

Landing Zone Accelerator on AWS

1. Installation Template (AWS CloudFormation)
2. Configuration Files (yaml)
3. AWS CodePipeline
4. AWS Cloud Development Kit

Landing Zone Accelerator

Root OU

Management (Root) Account

AWS Control Tower

AWS Organizations

AWS Single Sign-On

Infrastructure OU

Network Account

Shared Services Account

*For illustration only to demonstrate where these additional capabilities and resources can be deployed

Security OU

Log Archive Account

Amazon CloudWatch

AWS CloudTrail

AWS Config

Centralized Logs Bucket

Audit / Security Tooling Account

AWS Security Hub

Amazon GuardDuty

AWS KMS

Amazon Macie

Dev / Test / Prod OU (Workload Ous)

Workload Account 1 … N

Landing Zone Accelerator on AWS

1. 

Installation Template
(AWS CloudFormation)

2. 

Configuration Files
(yaml)

3. 

AWS CodePipeline

4. 

AWS Cloud
Development Kit

Landing Zone
Accelerator

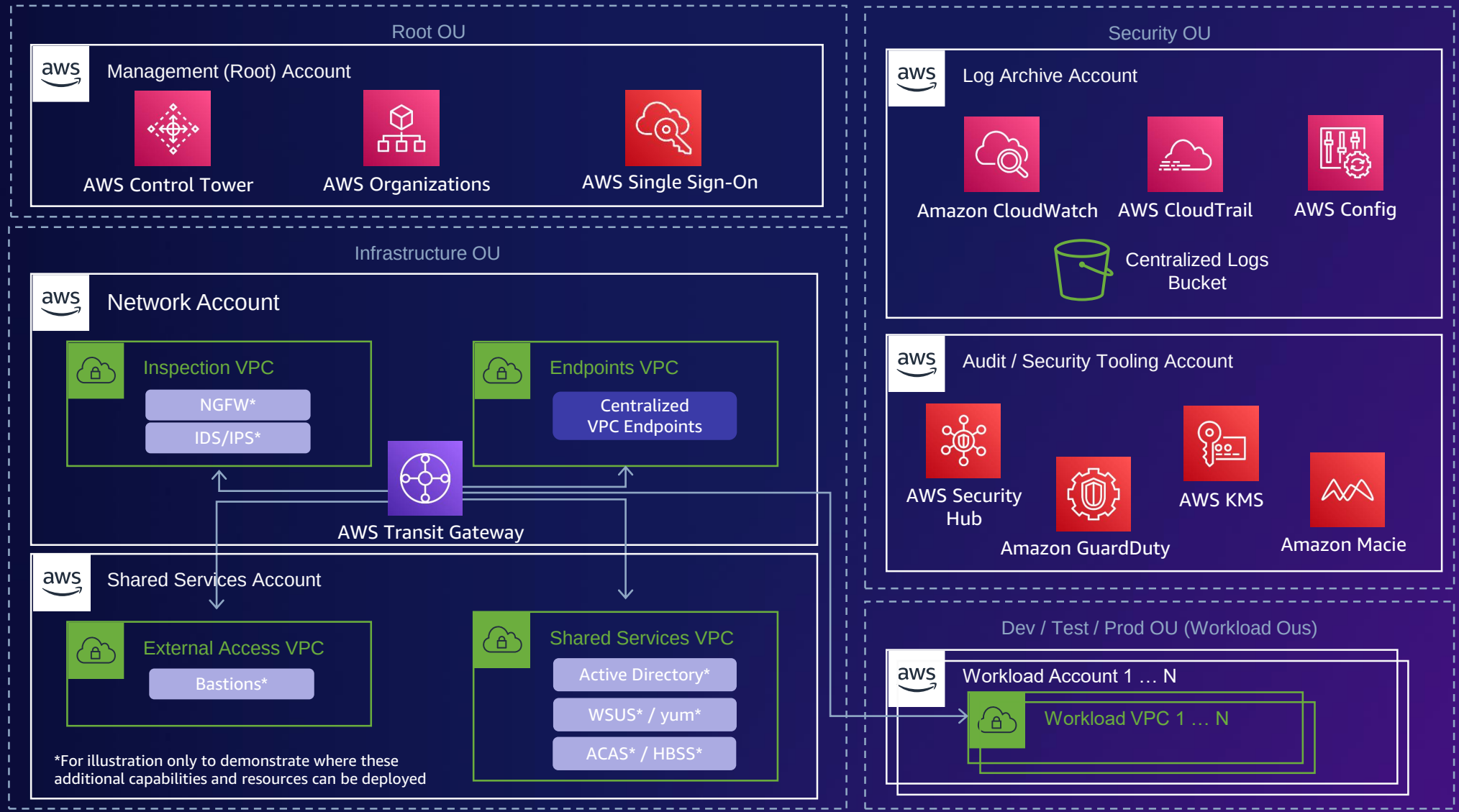
```yaml
homeRegion: &HOME_REGION us-east-1
defaultVpc:
  delete: true
  excludeAccounts: []
transitGateways:
  - name: Network-Main
    account: Network
    region: *HOME_REGION
    shareTargets:
      organizationalUnits:
        - Infrastructure
    asn: 65521
    dnsSupport: enable
    vpnEcmpSupport: enable
    defaultRouteTableAssociation: disable
    defaultRouteTablePropagation: disable
    autoAcceptSharingAttachments: enable
    routeTables:
      - name: Network-Main-Core
        routes: []
      - name: Network-Main-Segregated
        routes: []
      - name: Network-Main-Shared
        routes: []
      - name: Network-Main-Standalone
        routes: []
```

```yaml
vpcs:
  - name: Network-Endpoints
    account: Network
    region: *HOME_REGION
    cidrs:
      - 10.1.0.0/22
    internetGateway: false
    enableDnsHostnames: true
    enableDnsSupport: true
    instanceTenancy: default
    routeTables:
      - name: Network-Endpoints-Tgw-A
        routes: []
      ...
    subnets:
      - name: Network-Endpoints-A
        availabilityZone: a
        routeTable: Network-Endpoints-A
        ipv4CidrBlock: 10.1.0.0/24
        ...
    transitGateway:
      name: Network-Main
      account: Network
    gatewayEndpoints:
      defaultPolicy: Default
      endpoints:
        - service: s3
        - service: dynamodb
    interfaceEndpoints:
      central: true
      defaultPolicy: Default
      endpoints:
        - service: ec2
        - service: ec2messages
```

Landing Zone Accelerator on AWS

1. Installation Template (AWS CloudFormation)
2. Configuration Files (yaml)
3. AWS CodePipeline
4. AWS Cloud Development Kit

Landing Zone Accelerator



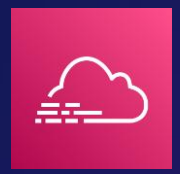
Features - Security


AWS Control Tower


AWS Organizations


Amazon CloudWatch


AWS Config


AWS CloudTrail


AWS Service Catalog


AWS Systems Manager


AWS Security Hub


Amazon GuardDuty


Amazon Inspector


Amazon Macie


AWS Firewall Manager


AWS Resource Access Manager


AWS Key Management Service (AWS KMS)


AWS Identity and Access Management (IAM)


AWS Network Firewall

Features - Networking

Amazon Virtual Private Cloud (Amazon VPC)

Amazon Route 53

AWS Transit Gateway

AWS Direct Connect

Features - Operations

AWS Budgets

AWS Cost & Usage Report

AWS Cost Explorer

AWS Tools and SDKs

AWS Cloud Development Kit (AWS CDK)

AWS CodePipeline

AWS CodeCommit

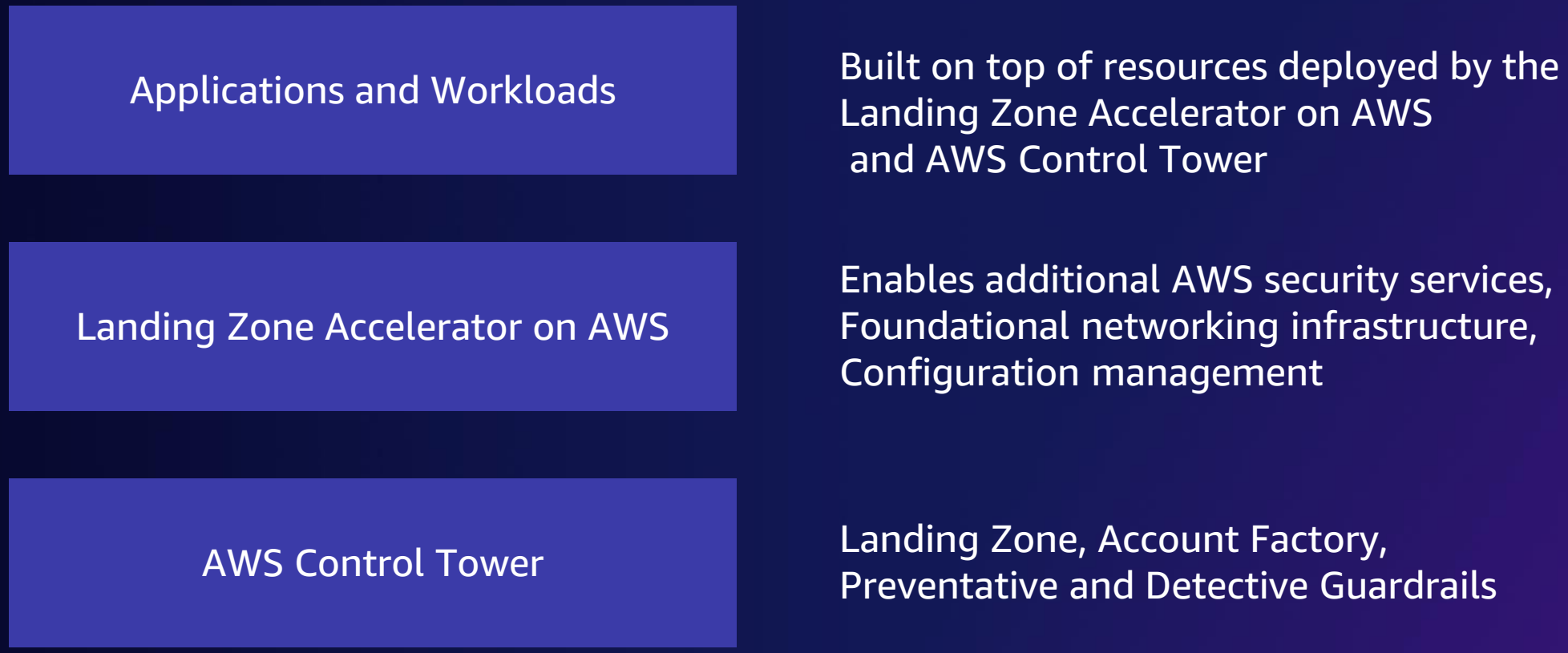
AWS CodeBuild

AWS Managed Services

AWS Professional Services

AWS Support

Integrates with AWS Control Tower



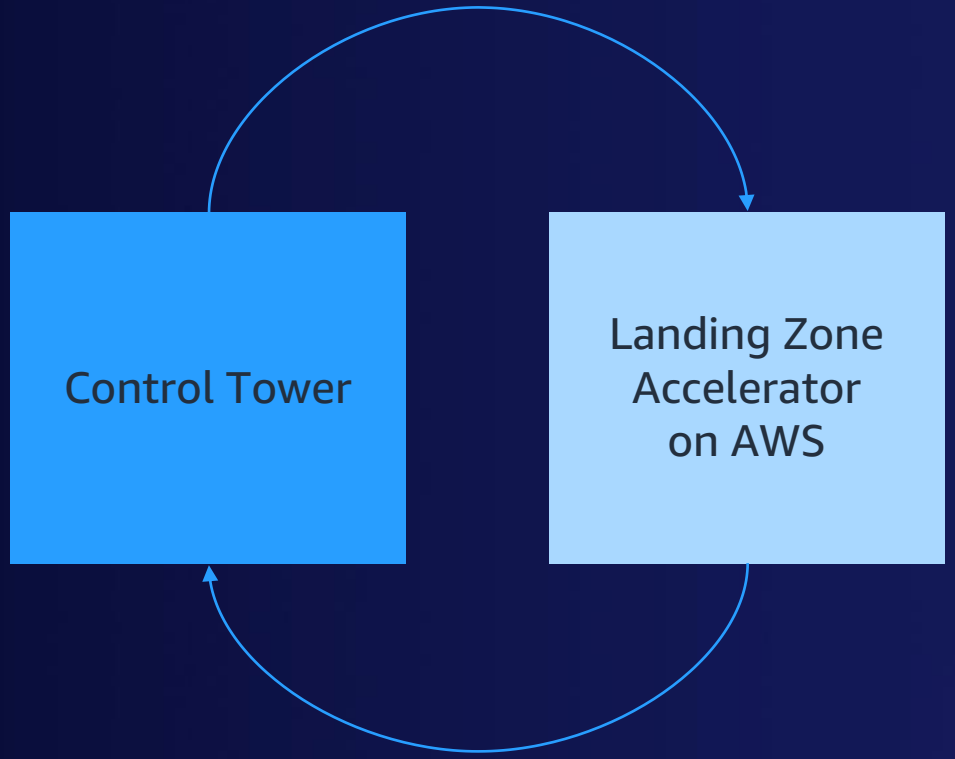
Built on top of resources deployed by the Landing Zone Accelerator on AWS and AWS Control Tower

Enables additional AWS security services, Foundational networking infrastructure, Configuration management

Landing Zone, Account Factory, Preventative and Detective Guardrails

A future with Control Tower

Accelerator environments use resources and guardrails from the Control Tower Landing Zone



Feature requests are sent to Control Tower (and other AWS service teams)

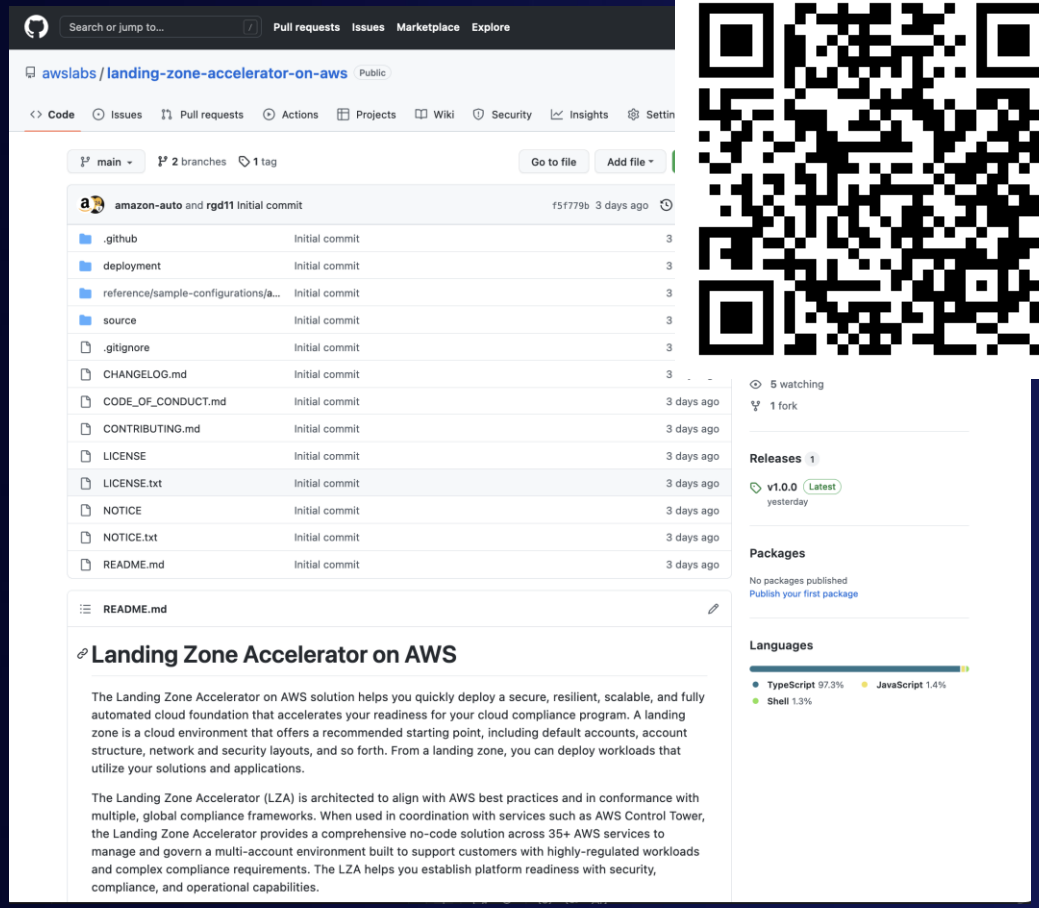
Deprecate accelerator features in favor of a managed service

Landing Zone Accelerator environment can be enrolled into Control Tower, once present in desired home region

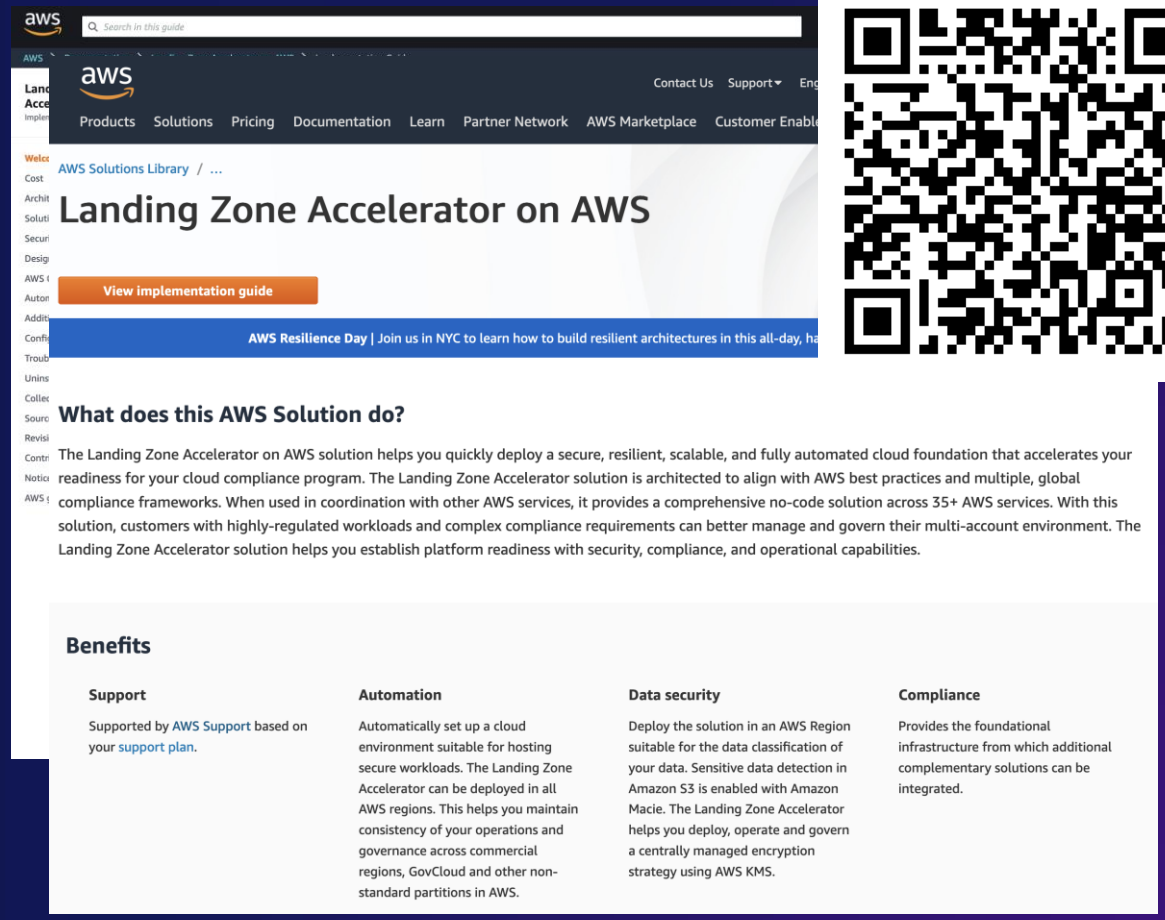
Solution Highlights

- Build secure and compliant AWS environments in days, instead of months or years.
- Focus time and critical budgets on migration, transformation, and innovation.
- Documentation helps demonstrate compliance requirements are met and shortens time to prepare for accreditation of their AWS environment.
- Customers can install the Solution directly from GitHub or have it delivered by AWS Professional Services or Partners.
- Customers can get technical assistance from AWS Support.

Call to Action



https://github.com/awslabs/landing-zone-accelerator-on-aws
GitHub Repository



https://aws.amazon.com/solutions/implementations/landing-zone-accelerator-on-aws/
AWS Solutions
Implementation and Deployment Guide

Learn in-demand AWS Cloud skills

AWS Skill Builder

Access **500+ free** digital courses and Learning Plans

Explore resources with a variety of skill levels and **16+** languages to meet your learning needs

Deepen your skills with digital learning on demand

Train now

AWS Certifications

Earn an industry-recognized credential

Receive Foundational, Associate, Professional, and Specialty certifications

Join the **AWS Certified community** and get exclusive benefits

Access **new** exam guides

Thank you!

Please complete the session survey in the mobile app

Android

iOS