Architecting security & governance across your landing zone

Sam Elmalak
WW Tech Leader, Enterprise Greenfield
Amazon Web Services
Agenda

Why a landing zone?

How to think about it?

The framework

The services

How does it all fit together?
Have you seen this before? // reinvent 2018

Multi-account approach

- **Orgs**: Account management
- **Log Archive**: Security logs
- **Security**: Security tools, AWS Config rules
- **Shared services**: Directory, limit monitoring
- **Network**: Direct Connect
- **Dev Sandbox**: Experiments, Learning
- **Dev**: Development
- **Pre-Prod**: Staging
- **Prod**: Production
- **Team SS**: Team Shared Services, Data Lake

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
What do customers want to do on AWS?

**Build**
- focus on what differentiates

**Move Fast**
- ideation to instantiation

**Stay Secure**
- secure and compliant environment
Customers need an environment that is

- **Secure & compliant**
  Meets the organization’s security and auditing requirements

- **Scalable & resilient**
  Ready to support highly available and scalable workloads

- **Adaptable & flexible**
  Configurable to support evolving business requirements
Why?

- Many teams
- Security / compliance controls
- Billing
- Isolation
- Business process
Customers Need

Resource Container

AWS Account

Security/Resource Boundary

API Limits/Throttling

Billing Separation
Isolation with IAM and VPC in one account?

“Gray” boundaries
Complicated and messy over time
Difficult to track resources
People stepping on each other
Resource containers over time
Resource Containers Grouping
You Need... Orchestration Framework

Account Metadata: Owner, function, policies, BU, SDLC, cost center, etc ...
With capabilities...

- Billing Management
- Identity and Access Management
- Immutable Security Logs
- Shared Infrastructure
- Resource Isolation
- Support Dev Lifecycle
- Central Network Connectivity
- Security Tooling
Goals

- Automated
- Scalable
- Self-service
- Guardrails NOT blockers
- Auditable
- Flexible
You need a “landing zone”

• A configured, secure, scalable, multi-account (multiple resource containers) AWS environment based on AWS best 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, AWS Landing Zone, AWS Control Tower

**landing zone:**
- Secure pre-configured environment for your AWS presence
- Scalable and flexible
- Enables agility and innovation

**AWS Landing Zone Solution:**
- Implementation of a landing zone based on multi-account strategy guidance

**AWS Control Tower:**
- AWS Service version of AWS Landing Zone
The Architecture
Service Control Policies (SCPs)

- Enables you to control which AWS service APIs are accessible
  - Define the list of APIs that are allowed – whitelisting
  - Define the list of APIs that must be blocked – blacklisting
- SCPs are:
  Invisible to all users in the child account, including root
  Applied to all users in the child account, including root
- Permission:
  intersection between the SCP and IAM permissions
  IAM policy simulator is SCP aware
Disable Service APIs you Won’t be Using

```json
{
    "version": "2012-10-17",
    "Statement": [
    {
        "Effect": "Deny",
        "Action": "<Insert unwanted service prefix here>:*",
        "Resource": "*"
    }
    ]
}
```

- **NotAction** (Optional) List the AWS actions exempt from the SCP. Used in place of the Action element.
- **Resource** List the AWS resources the SCP applies to.
- **Condition** (Optional) Specify conditions for when the statement is in effect.
Organizational Units

- Grouping of AWS Accounts
- Service Control Policies (SCP) to the groups
- Use permission grouping (NOT corporate structure)

How likely is the group to need a set of similar policies?
AWS Organizations Master

No connection to DC

Organizational Units

Service control policies

Consolidated billing

Minimal resources

Limited access

Restrict Orgs role!
Foundational OUs

Foundational Organizational Units (OU)

- Security
- Infrastructure

- Foundational
- Building blocks
- Once per organization
- Security & Infrastructure
- Have their own development life cycle (dev/qa/prod)
Log Archive

AWS Cloud

AWS Organizations
Master

Foundational Organizational Units (OU)

Security
Infrastructure

Versioned Amazon S3 bucket
Restricted
MFA delete

AWS CloudTrail logs
Security logs
Single source of truth
Alarm on user login
Limited access
Security Accounts

Owned by security team
Enable security operations
Limited access

AWS Cloud

AWS Organizations Master
SCP
OU

Foundational Organizational Units (OU)

Security
Infrastructure

Log Archive

Security Read Only
Security Break Glass
Security Tooling
Security Accounts // Read Only

View/Scan resources in other accounts

Exploratory Security Testing

Cross account read-only (security Auditor)

Limited access
Security Accounts // Break Glass

AWS Cloud

AWS Organizations
Master

Foundational Organizational Units (OU)

Security
Infrastructure

△ Log Archive
△ Security Read Only
△ Security Break Glass
△ Security Tooling

Alert on login
Response in case of an event
Should almost never be used
Extremely Limited access
Security Accounts // Tooling

Security tools and audit
Amazon GuardDuty
AWS Security Hub
AWS Config Aggregation
Cross-account roles
Automated Tooling
Automations, not humans
Shared Services

AWS Cloud

AWS Organizations
Master

SCP
OUs

Foundational Organizational Units (OU)

Security
Infrastructure

Log Archive
Sec Read Only
Sec Break Glass
Security Tooling

Shared Services

Connected to DC
DNS
LDAP/Active Directory
Shared Services VPC
Deployment tools
Golden AMI
Pipeline
Scanning infrastructure
Inactive instances
Improper tags
Snapshot lifecycle
Monitoring
Limited access
Network

Managed by network team

Networking services

AWS Direct Connect
AWS Direct Connect Gateway

Shared VPCs

AWS Transit Gateway

Limited access
Additional organizational units
Developer Sandbox

- AWS Cloud
- AWS Organizations
- Master
- Additional OU
  - Sandbox
    - Dev 1
    - Dev 2
- SCP
- OUs
- No connection to DC
- Individual Dev Accounts
- Innovation space
- Fixed spending limit
- Autonomous
- Experimentation
- Fixed spending limit
- Disconnected from network
Workloads

Based on level of needed isolation

Match your development lifecycle

Think Small
Workloads // Dev

AWS Cloud

Additional OU

Workloads

- For software development

Develop and iterate quickly

Collaboration space

Stage of SDLC
Workloads // Pre-Prod

AWS Cloud

- AWS Organizations
- Master
- Additional OU

Workloads

Connected to DC
Production-like
Staging
Testing
Automated deployment
Workloads // Prod

- AWS Cloud
- AWS Organizations Master
- SCP
- OUs

Additional OU

Workloads

- Connected to DC
- Production applications
- Promoted from Pre-Prod
- Limited access
- Automated deployments

- For software development

SDLC

Prod

Pre-Prod

Dev
Starter AWS multi-account framework

AWS Cloud

AWS Organizations

Foundational Organizational Units (OUs)

- Security
  - Δ Log Archive
  - Δ Sec Read Only
  - Δ Sec Break Glass
  - Δ Security Tooling
- Infrastructure
  - Δ Shared Services
  - Δ Network

Additional OUs

- Sandbox
  - Dev 1
  - Dev 2
  - Dev 3
  - - Fixed spending limit
  - - Disconnected from network
- Workloads
  - - For software development
Innovation pipeline

Developer accounts

New initiatives
Experimentation
Innovation

Team/Group accounts

Dev
Pre-Prod
Prod
Shared Services

PoC

Developer accounts

Developer accounts

Developer accounts

Developer accounts
PolicyStaging OU

- Safely test policy changes
- Test Single Account
- Promote to an OU
- Promote to final target OU
- Reduces need for 2nd Org

Additional OU

- Verify & test SCP changes
Suspended OU

- Account closures
- Tag account prior to moving

Deny All SCP
Account Closure
Departures
Tag Account prior to moving
IndividualBusinessUsers OU

Need access for business reasons

Reporting access

S3 bucket to share marketing videos/data

Case by case and pre authorized
Exceptions OU

AWS Organizations
Master

Additional OU

Exceptions OU

- Customized security stance
- SCPs at account level
- Under greater scrutiny

No SCP on OU
SCP on accounts
Strict approval process
SCPs applied to accounts

Account 1
Account 3
Top Secret
Project X
Deployments OU

Build Pipelines

One Account for each Workload

Highly secured

Extremely Limited access
Multi-account framework
Multi-account approach

AWS Organizations

Orgs: Account management
Log Archive: Security logs
Security: Security tools, AWS Config rules
Shared services: Directory, limit monitoring
Network: AWS Direct Connect
Dev Sandbox: Experiments, Learning
Dev: Development
Pre-Prod: Staging
Prod: Production
Team SS: Team Shared Services, Data Lake

Infrastructure

Security

Workloads

Sandbox

Data Center

Network Path
Log Flow
Optional Network Path
Multi-account approach

**AWS Organizations**

**Orgs:** Account management

**Log Archive:** Security logs

**Security:** Security tools, AWS Config rules

**Shared services:** Directory, limit monitoring

**Network:** AWS Direct Connect

**Dev Sandbox:** Experiments, Learning

**Dev:** Development

**Pre-Prod:** Staging

**Prod:** Production

**Team SS:** Team Shared Services, Data Lake
Multi-account approach // security log flow

- **Orgs:** Account management
- **Log Archive:** Security logs
- **Security:** Security tools, AWS Config rules
- **Shared services:** Directory, limit monitoring
- **Network:** AWS Direct Connect
- **Dev Sandbox:** Experiments, Learning
- **Dev:** Development
- **Pre-Prod:** Staging
- **Prod:** Production
- **Team SS:** Team Shared Services, Data Lake
Multi-account approach // network connectivity

**Orgs:** Account management

**Log Archive:** Security logs

**Security:** Security tools, AWS Config rules

**Shared services:** Directory, limit monitoring

**Network:** AWS Direct Connect

**Dev Sandbox:** Experiments, Learning

**Dev:** Development

**Pre-Prod:** Staging

**Prod:** Production

**Team SS:** Team Shared Services, Data Lake
Implementation
AWS solutions that enable **agility + governance**

**Set up multi-account AWS environments**
- AWS Control Tower
- AWS Organizations
- AWS Service Catalog

**Establish cost controls**
- AWS Budgets
- AWS License Manager
- AWS Marketplace (Private Marketplace)

**Monitor/Manage policies and security configurations**
- AWS CloudTrail
- AWS Config
- AWS Security Hub
- Amazon CloudWatch

**Improve over time – operate and optimize**
- AWS Well-Architected Tool
AWS Organizations

Central governance and management across AWS accounts for a comprehensive multi-account AWS environment

- Manage and define your organization and accounts
- Control access and permissions
- Audit, monitor, and secure your environment for compliance
- Share resources across accounts
- Centrally manage costs and billing

Powers AWS Control Tower and AWS Landing Zone
AWS Control Tower

Self-service solution to automate the setup of **new AWS multi-account environments**

- An AWS service offering account creation based on AWS best practices
- Deployment of AWS best practice Blueprints and Guardrails
- Baseline fundamental accounts to provide standardization of best practices
- Single pane of glass for monitoring compliance to guardrails
AWS Control Tower capabilities

**Account Management**
- Framework for creating and baselining a multi-account environment using AWS Organizations
- Initial multi-account structure including security, audit, & shared service requirements
- An account vending machine that enables automated deployment of additional accounts with a set of managed and monitored security baselines
- A management console that shows compliance status of accounts
- The ability to apply AWS best practice guardrails and Blueprints to accounts at account creation
- The ability to detect and report on any drift / changes that have occurred that deviate from initial configuration options

**Identity & Access Management**
- User account access managed through AWS SSO federation
- **NEW!** Integration options with other 3rd party SSO providers
- Cross-account roles enable centralized management

**Security & Governance**
- Multiple accounts enable separation of duties
- Initial account security and AWS Config rules baseline
- Network baseline
Starter AWS multi-account framework

AWS Cloud

AWS Organizations

Foundational Organizational Units (OUs)

- Security
- Infrastructure

Δ Log Archive
Δ Sec Read Only
Δ Sec Break Glass
Δ Security Tooling

Δ Shared Services
Δ Network

Additional OUs

Sandbox

- Dev 1
- Dev 2
- Dev 3

- Fixed spending limit
- Disconnected from network

Workloads

- For software development
Starter AWS multi-account framework

AWS Cloud

AWS Organizations

Foundational Organizational Units (OUs)
- Security
- Infrastructure
  - \(\Delta\) Log Archive
  - \(\Delta\) Sec Read Only
  - \(\Delta\) Sec Break Glass
  - \(\Delta\) Security Tooling
  - \(\Delta\) Shared Services
  - \(\Delta\) Network

Additional OUs
- Sandbox
  - Dev 1
  - Dev 2
  - Dev 3
  - For software development
  - Fixed spending limit
  - Disconnected from network
- Workloads

Control Tower deploys these automatically
AWS Organizations
or
AWS Control Tower
or
AWS Landing Zone
or ...?
We thought we did this...
But...
Approach on how to setup isolation and security controls in AWS environment...

Isolation through AWS accounts...

Customer/Partner built

AWS Landing Zone

AMS

DevOps/DevSecOps?

Customer Ops Team

MSP

Security & Governance

MSP

App Operations

Infrastructure Operations

Implementation (SA/PS Advise)

Guidance

Multi-account Strategy

AWS Control Tower

AWS Organizations

Customer Ops Team

MSP

AMS

Customer Ops Team

DevOps/DevSecOps?
Recommendations

New customer:
• Evaluate AWS Control Tower (CT)
• Use out-of-box guardrails and blueprints
• Use CT Account Factory

Existing customer:
• Native CT AWS CloudWatch events and reference implementation
• Beta to use CT in existing AWS Organizations

Current AWS Landing Zone (ALZ) customers:
• New version to upgrade
• Replaces ALZ code with CT functionality
• Extensibility framework with CT
Summary
Multi-account framework

AWS Cloud

AWS Organizations Master
SCP
OUs

Foundational Organizational Units (OU)
- Security
- Infrastructure

- Log Archive
- Sec Read Only
- Sec Break Glass
- Security Tooling
- Shared Services
- Network

Additional OU
- Sandbox
- Workloads
- Policy Staging
- Suspended
- Individual Business Users
- Exceptions
- Deployments

- Fixed spending limit
- Disconnected from network
- For software development
- Verify & test SCP changes
- Account closures
- Tag account prior to moving
- For individual business users
- Customized security stance
- SCPs at account level
- Under greater scrutiny
- For deployment infrastructure
How many landing zones?

Primary production: Yes

Dev/QA/test deployment: Yes
  • Test out new CT/Orgs features
  • Test out orchestration framework/services

Always running pre-prod deployment: Maybe

Forensics: Maybe
<table>
<thead>
<tr>
<th>Session Code</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC325</td>
<td>Architecting security &amp; governance across your landing zone</td>
</tr>
<tr>
<td>ARC344</td>
<td>Understanding the landing zone journey</td>
</tr>
<tr>
<td>GPSTEC203</td>
<td>Control Tower versus AWS Landing Zone</td>
</tr>
<tr>
<td>SEC325</td>
<td>Architect governance at enterprise scale with Goldman Sachs</td>
</tr>
<tr>
<td>MGT307</td>
<td>Governance at scale: AWS Control Tower, AWS Organizations, and more</td>
</tr>
<tr>
<td>MGT302</td>
<td>Enable AWS adoption at scale with automation and governance</td>
</tr>
<tr>
<td>SEC335</td>
<td>How to deploy secure workloads with AWS Control Tower</td>
</tr>
<tr>
<td>GPSTEC324</td>
<td>Automating ISV product deployment in AWS Landing Zone</td>
</tr>
<tr>
<td>GPSTEC325</td>
<td>Control Tower in a nutshell and practice enablement for APN Partners</td>
</tr>
<tr>
<td>ENT214</td>
<td>Cloud migration in the face of data-center eviction</td>
</tr>
<tr>
<td>ENT215</td>
<td>Five steps AMS leverages to accelerate cloud adoption</td>
</tr>
<tr>
<td>SEC324</td>
<td>Deep dive into AWS multi-account strategies</td>
</tr>
<tr>
<td>ARC315</td>
<td>Build end-to-end governance with AWS Control Tower</td>
</tr>
<tr>
<td>SEC347</td>
<td>DNS across a multi-account environment</td>
</tr>
</tbody>
</table>
Ideas and guidance // Multi-account Strategy

• Service control policies strategies and recommendations
• Identify Federation best practices and details
• Steps to migrate into a multi-account environment
• Networking recommendations (Transit gateway, Shared Amazon VPC, Private Link, peering, etc …)
• Security specific tooling and where to run/how e.g. Firewalls, IDS/IPS
• Alerting and alarming recommendations
• Forensics landing zone
• QA/Staging landing zone
• Backup/disaster recovery recommendations at account level
• Cost implications of many accounts vs. few
• CI/CD in a multi-account environment
Thank you!
Please complete the session survey in the mobile app.
Ideas and guidance // Multi-account Strategy

• Service control policies strategies and recommendations
• Identify Federation best practices and details
• Steps to migrate into a multi-account environment
• Networking recommendations (Transit gateway, Shared Amazon VPC, Private Link, peering, etc …)
• Security specific tooling and where to run/how e.g. Firewalls, IDS/IPS
• Alerting and alarming recommendations
• Forensics landing zone
• QA/Staging landing zone
• Backup/disaster recovery recommendations at account level
• Cost implications of many accounts vs. few
• CI/CD in a multi-account environment