

AWS Control Tower

centrally manage multi-account
environment

Lukas Pour
CTO & AWS Architect @ trustsoft.eu

 partner
network

Advanced
Consulting
Partner

Public Sector Partner
Amazon RDS

AGENDA



01

LANDING ZONE

using
AWS Control Tower

02

MULTIPLE ACCOUNTS

governance and
segmentation

03

SECURITY

across whole AWS
infrastructure

04

DEMO

AWS Control Tower -
first steps and setup



01

LANDING ZONE

using AWS Control Tower



What you expect from AWS services?



BUILD - focus on what
matters



MOVE FAST - from idea to
production



STAY SECURE - easily
without thinking

What do you need to achieve?



SECURE & COMPLIANT

Meet organisation or audit requirements



SCALABLE & RESILIENT

Support highly-available and scalable workload



ADAPTABLE

You never know what business needs :)



KISS

Keep it stupid simple

AWS Landing Zone



Secure and Scalable
multi-account AWS
infrastructure



Based on AWS best practices,
tested by thousands



Starting point for new
development, experiments,
migrations,...

One AWS account is not enough?



SECURITY

Centrally managed and simple auditability



MULTIPLE TEAMS

Separation of work and responsibility



ISOLATION

Account does not share anything with another one



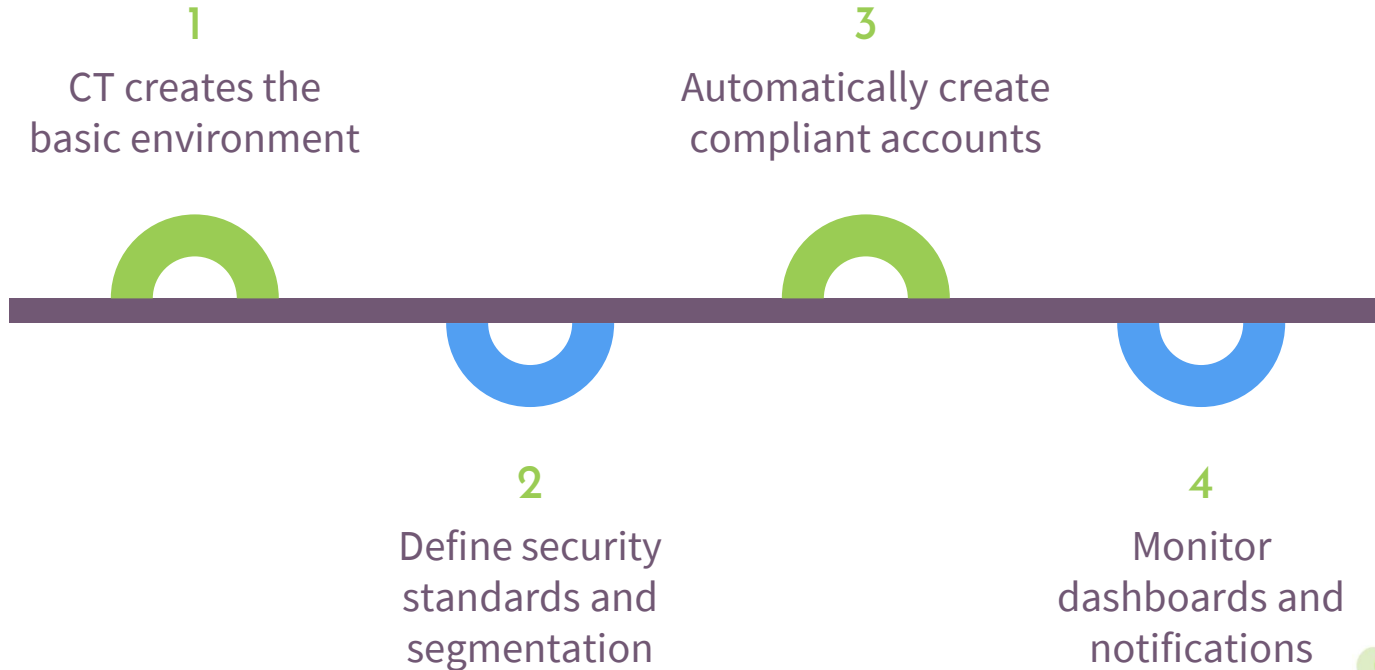
COST MANAGEMENT

Know how much each team, environment, app etc. is spending

“AWS Control Tower provides the easiest way to set up and govern a secure, multi-account AWS environment, called a landing zone.”

–AWS

AWS CONTROL TOWER



What CT Service does for me?

- Prepares landing zone based on AWS best practices
 - Core account structure - Master, Log Archive a Audit
 - Single-sign-on
 - Centralized CloudTrail a Config logging to Log Archive account
 - Auditability across whole infrastructure
- Prepared set of guardrails
- Prepared Account Factory
- Control Tower Dashboards
- Monitoring and Notifications

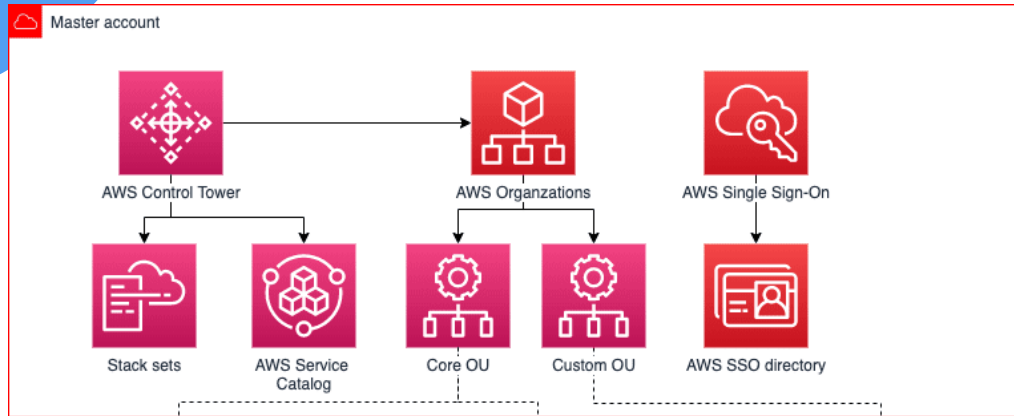


02

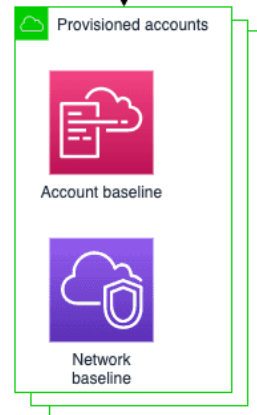
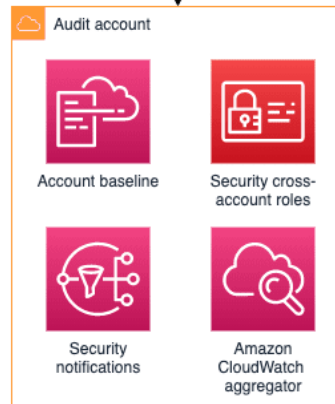
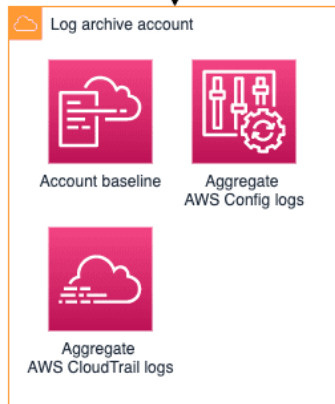
MULTIPLE ACCOUNTS

governance and segmentation

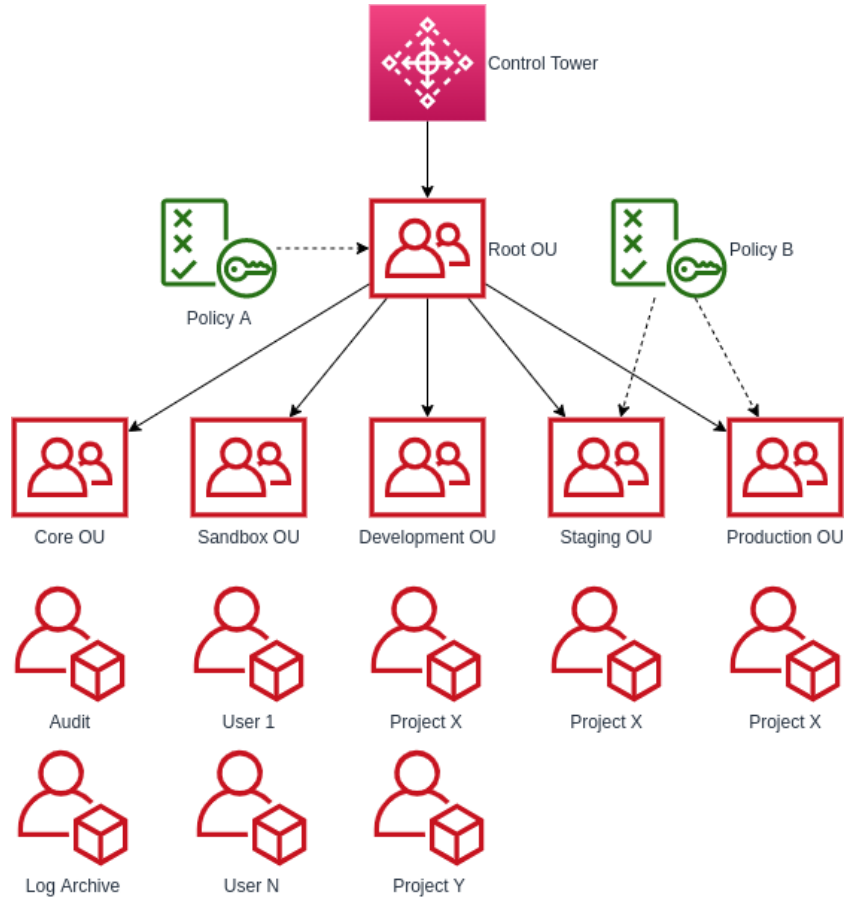




Control Tower basic structure



Control Tower OU structure





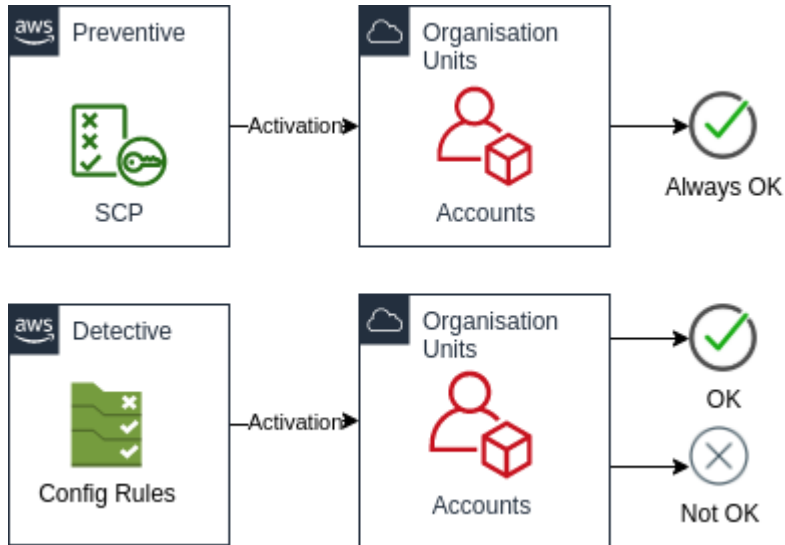
03

SECURITY

across whole AWS infrastructure



Guardrails









- Preconfigured rules in plain english
- Applied on OU level
- Preventive
 - Block and limit functionality
 - Defined using SCP (service control policy)
- Detective
 - Notify or fix functionality
 - Defined using AWS Config rules



Guardrails Examples

- Require MFA for root user
- Blocks public access to AWS S3 Bucket
- Requires encryption of all EBS volumes
- Block deletion of audit logs
- Blocks internet access to SSH port
- Detects whether versioning is enabled in S3 buckets

Key Security Services

	AWS CloudTrail	Tracking of all AWS activity (WEB, CLI, API, ..)
	AWS Config	Comparing configuration with a set of rules
	AWS Security Hub	Central dashboard of security and compliance
	AWS GuardDuty	Detect threads by analyzing network, dns, cloudtrail logs
	AWS Inspector	Analyse application security
	AWS Firewall Manager	Centrally manage AWS firewalls

AWS Security Hub



AWS Security Hub

Quickly assess your high-priority security alerts and security posture across AWS accounts in one comprehensive view



Amazon GuardDuty



Amazon Macie



Amazon Inspector



AWS Firewall Manager



IAM Access Analyzer



AWS Systems Manager

Integrated APN solutions

Continuously aggregate & prioritize

Findings from AWS and partner security services highlight emerging trends or possible issues



Conduct automated security checks

Use industry standards such as the CIS AWS Foundations Benchmark and PCI DSS



Take action

Investigate findings and/or take response and remediation actions

AWS Security Hub

CIS AWS Foundations controls

Security Hub conducts automated checks using the CIS AWS Foundations Benchmark controls.

< 1 2 3 >

<p>2.3 Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible</p> <p>✔ Compliant</p> <p>1 account passed</p>	<p>2.4 Ensure CloudTrail trails are integrated with CloudWatch Logs</p> <p>✘ Non-compliant</p> <p>1 account failed</p>	<p>2.5 Ensure AWS Config is enabled in all regions</p> <p>✔ Compliant</p> <p>1 account passed</p>
<p>2.6 Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket</p> <p>✘ Non-compliant</p> <p>1 account failed</p>	<p>2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs</p> <p>✘ Non-compliant</p> <p>1 account failed</p>	<p>2.8 Ensure rotation for customer created CMKs is enabled</p> <p>No data available</p>



04

DEMO

AWS Control Tower - first steps and setup



Thank you for you attention

We are hiri
**n**