

Startup Day with AWS and kreuzwerker

21.03.23, Berlin, Alte Münze

PROJECT
BLUEPRINT BERLIN

DRAWING NAME
CLIMB THE WALL

DESIGNED BY
O.U. STUDIO
Lin-Fee Chang 打明聯合
Chen-Hsiao-Tzu
Wu-Yi-Lin
Tsai-Pai-Huan

SCALE
1/1

DATE 2009/6/4

SHEET NO
1





DRAWING NO
A1-1

Build a multi-account setup with superwerker

Manuel Vogel, kreuzwerker

About me

- Coding since 2008
- In love with DevOps and automation
- Surfing and Yoga since 2015
- Minimalism and mindfulness

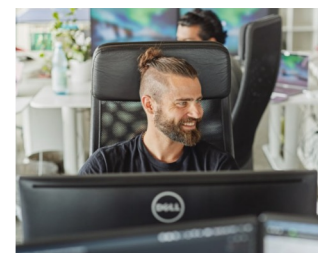
 certified, Cloud-native Engineer 
FinOps Practitioner , Kubernetes 
Terraform, cdk

Talking about things that inspire me,
Coding, Boxing, Yoga, dancing



Manuel Vogel
Head of Solution Architecture


manuel.vogel@kreuzwerker.de



Agenda

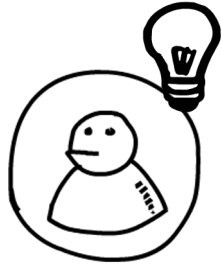
Why a solid foundation
or *Landing Zone (LZ)*

superwerker jumpstart (LZ)
benefits
design principles
internals

This sounds very
amazing, so let's start
building on AWS 



Expectation



1. Idea

aws



2. Create AWS
Account



3. Start
building!



Expectation zoomed in

Periodic Table of Amazon Web Services



But in reality ...

How to ensure a secure AWS setup?

How to keep up to date with the pace of AWS?

Multi-account or not?



How to keep costs under control?

How to detect incidents and events, how to handle them?

Which foundational AWS services should be enabled?

Manual governance in AWS at scale ... ⚡

? Account management

- how to automate policies?
- how to automate identity federation?
- how to do account automation?

? Security and compliance

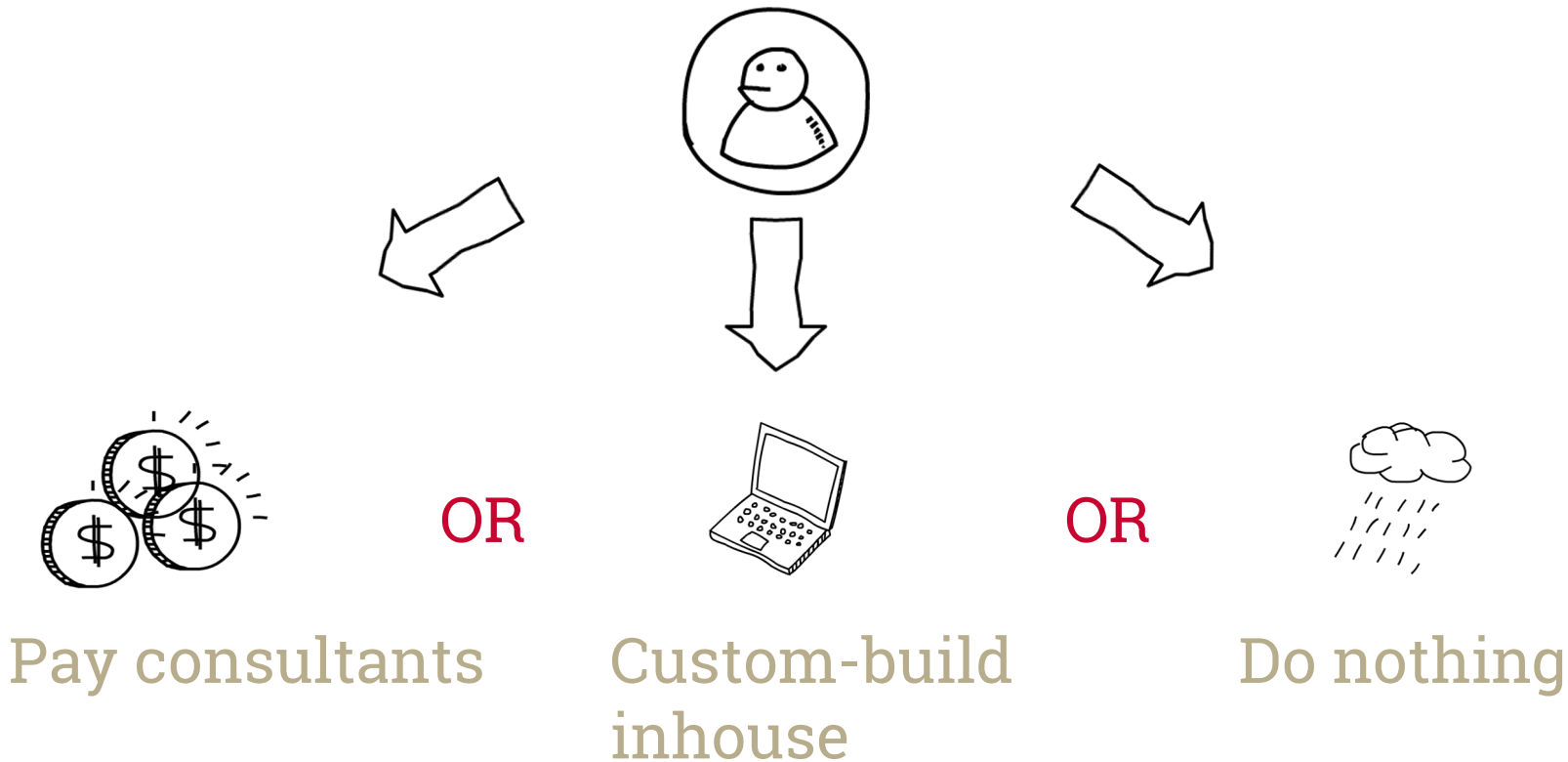
- identity & access automation?
- security automation?
- policy enforcement?

? Budget & Cost management:

- planning and enforcement? 🍷

Building an AWS Foundation usually ends up

...



Problems with custom-built AWS foundations



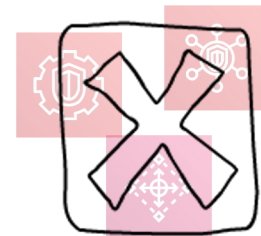
Expensive



“Time to
AWS”
slowed
down



Best
practices
not known



Insecure: Easy
to overlook
basic security
services

Comparison

	Consultants / custom-built	Do nothing	superwerker
Zero upfront cost	✗	✓	✓
Immediate start	✗	✓	✓
Near-zero maintenance costs	✗	✗	✓
Open source	✗	✗	✓
Security controls enabled	?	✗	✓
Stay up-to-date with best practices	?	✗	✓

Landing Zone with **super****werker**



What exactly is a **Landing Zone**? 🤔

A **Landing Zone** is a well-architected multi-account AWS environment that is scalable and secure ✅

The superworker open source solution **automates** the setup of an AWS Cloud environment with **prescriptive AWS Best Practices**.

It enables Startups and SMBs to **focus on their core business**. By **saving** setup and maintenance **time and money**

superworker benefits



Off-the-shelf AWS
experience
(fully automated
setup)



Secure AWS
environment
in hours
instead of
weeks

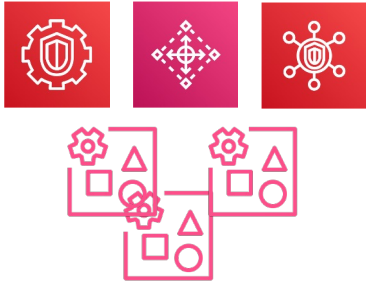


Free and
open-source
official AWS
Quick Start



Bundled &
codified XP of
two AWS
Advanced
Partners

superworker design guidelines



End-to-end tests with real AWS accounts and resources



Documented with Architecture Design Records (ADR)



Low total cost of ownership: only serverless AWS services are used



Forward compatibility and adoption

What's included in superwerker?

In the **initial release**, superwerker enables the following AWS services and features in a **fully automated** way:



Control Tower

Base for a future-proof multi-account setup



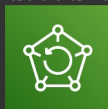
Security Hub

Org-wide ensure established security standards



GuardDuty

Org-wide automatic detection of possible threats breaches



AWS Backup

Org-wide automated backups



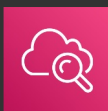
Billing/Budget Setup

Budget Alarms



Preventive Guardrails

protect the infrastructure



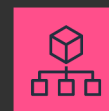
Quick-start dashboard

Quick-Links to e.g. services, SSO setup, notification center



SSM OpsCenter/Items

For notifications / incident response handling



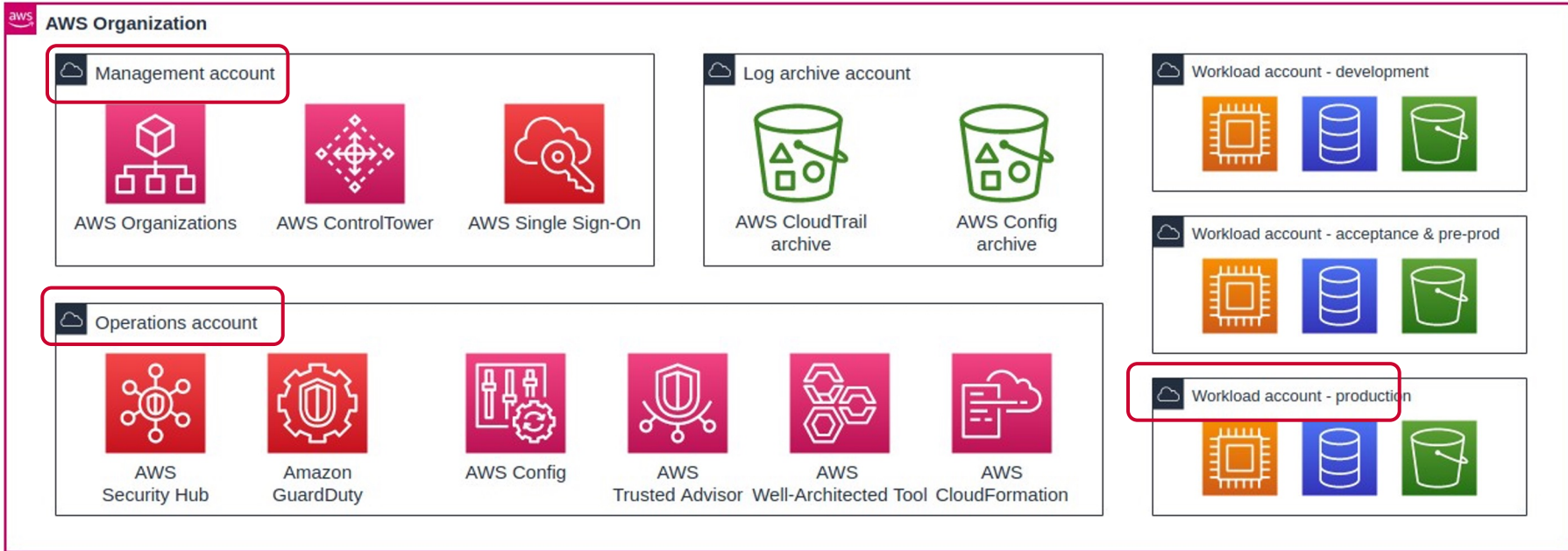
Secure AWS Account Mailboxes

Configure dedicated secure mail domain for AWS Accounts

The Concept of a Landing Zone



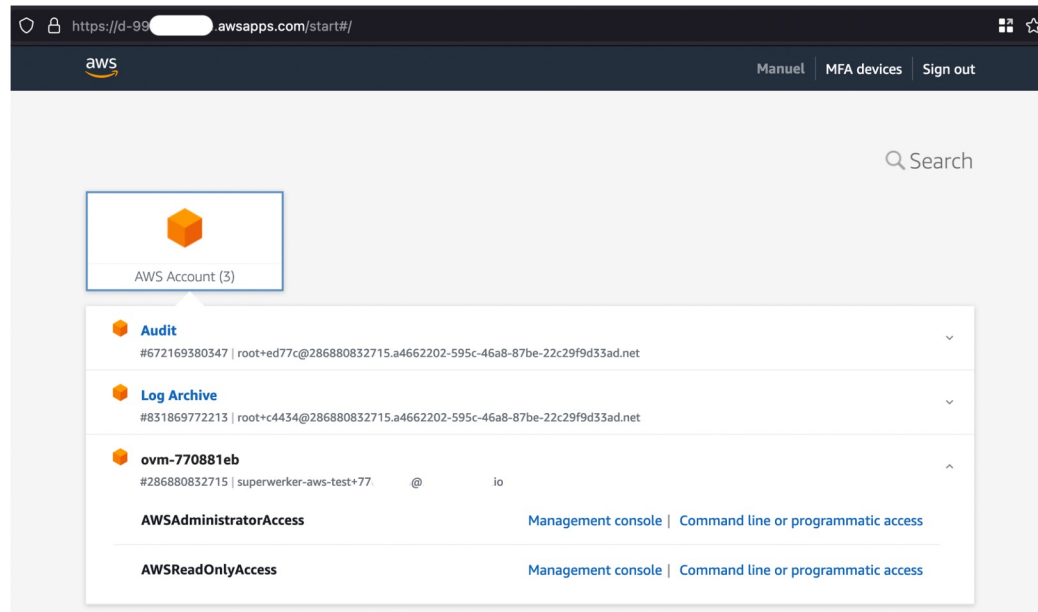
A **well-architected** multi-account AWS environment that is **scalable** and **secure**



The Concept of a Landing Zone

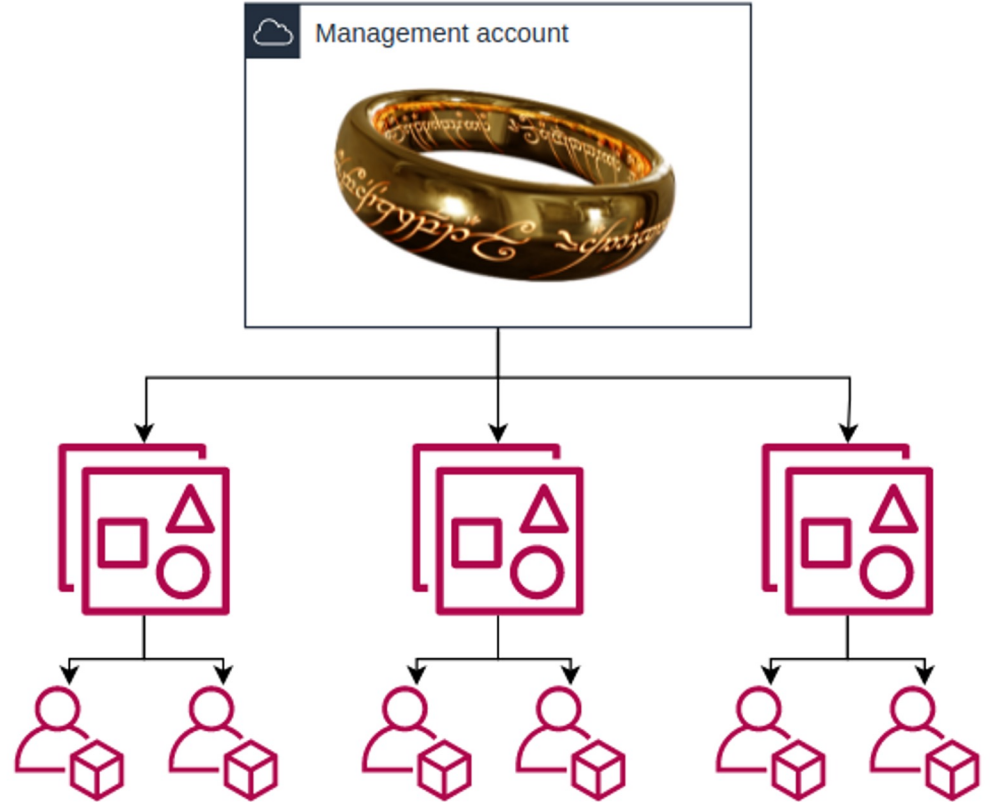


Logging into your accounts via the AWS SSO portal



Organization Management account

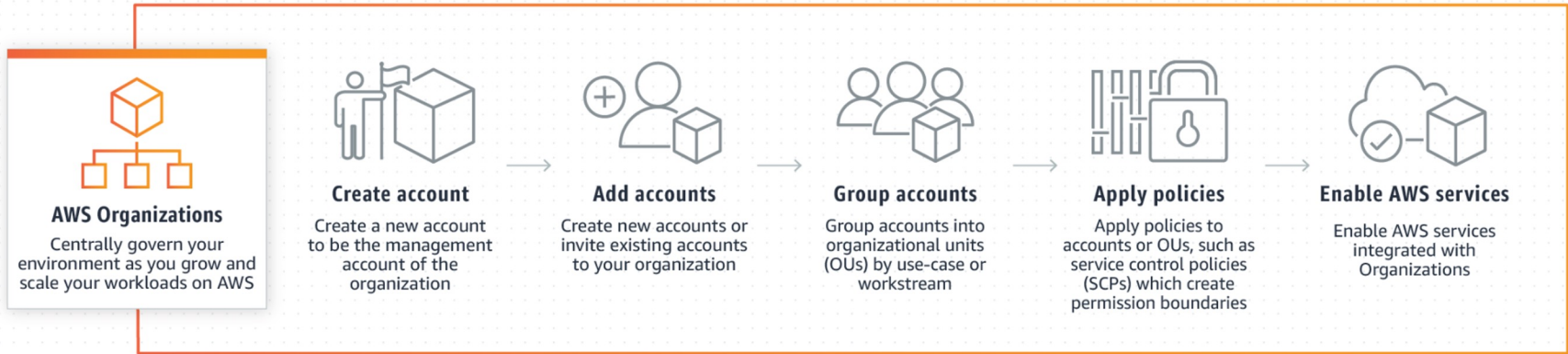
One account to rule them all....



Why a **Multi Account strategy**? 🤔

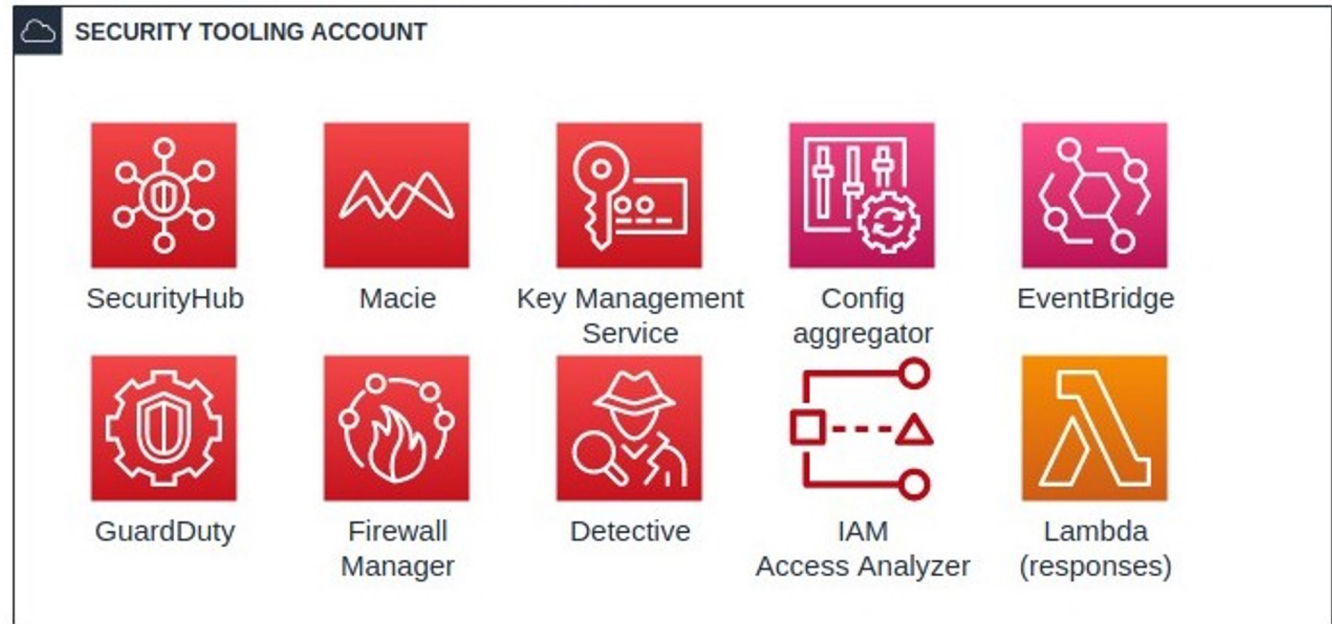
They are like resource containers:
workload categorization, blast radius
reduction, cost allocation and more ✅

AWS Organizations



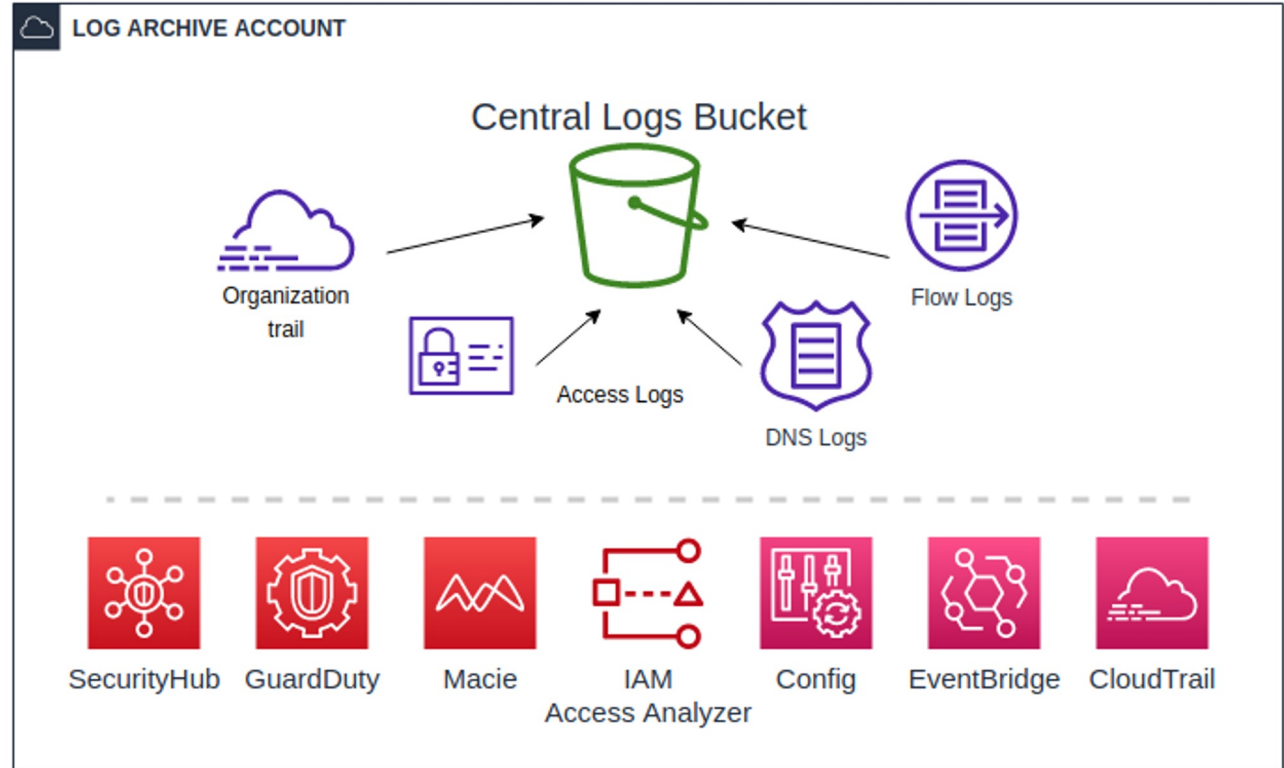
Security OU - Audit (Security Tooling) account

Security Tooling account dedicated to operating security services.



Security OU - Log Archive account

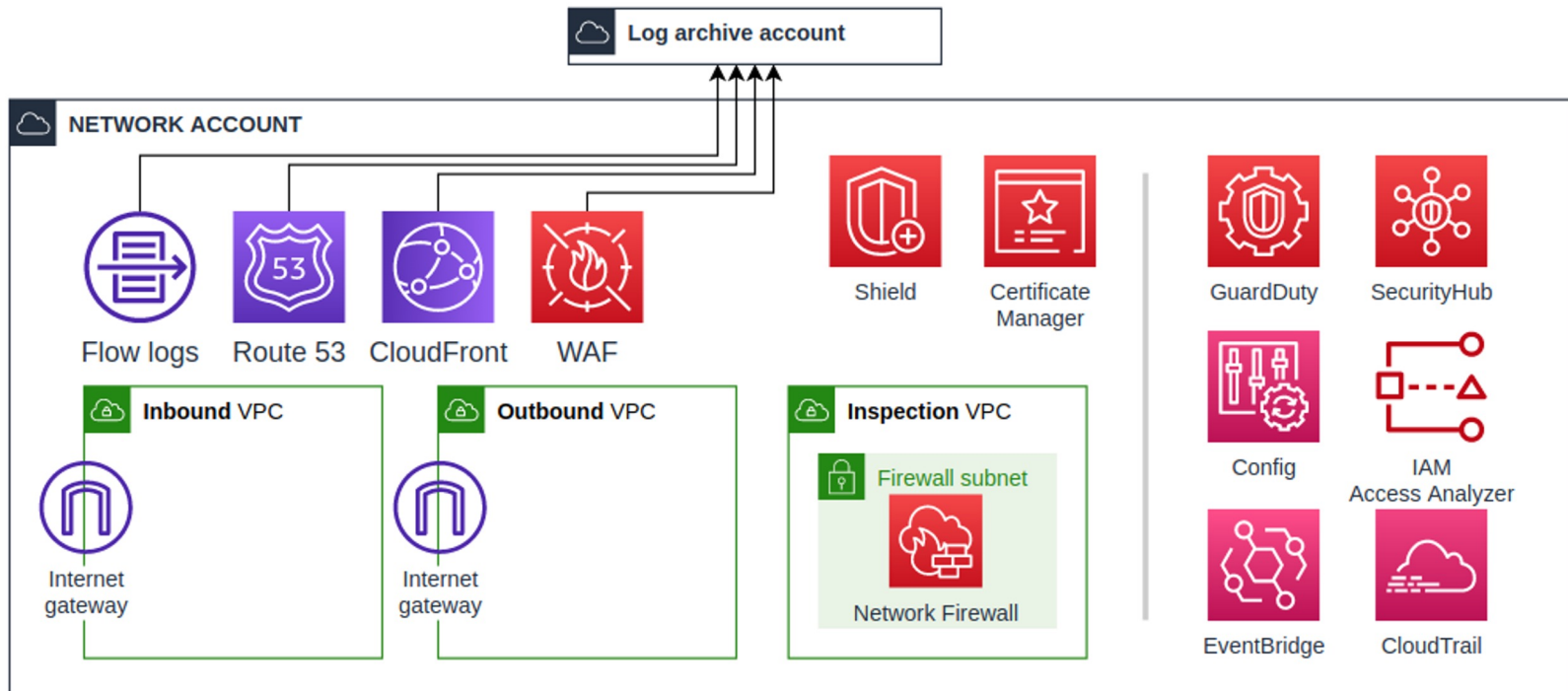
Collect, monitor and audit all security related logs in one central place.



Infrastructure OU - Network account (planned)

The gateway between your business and the broader internet.

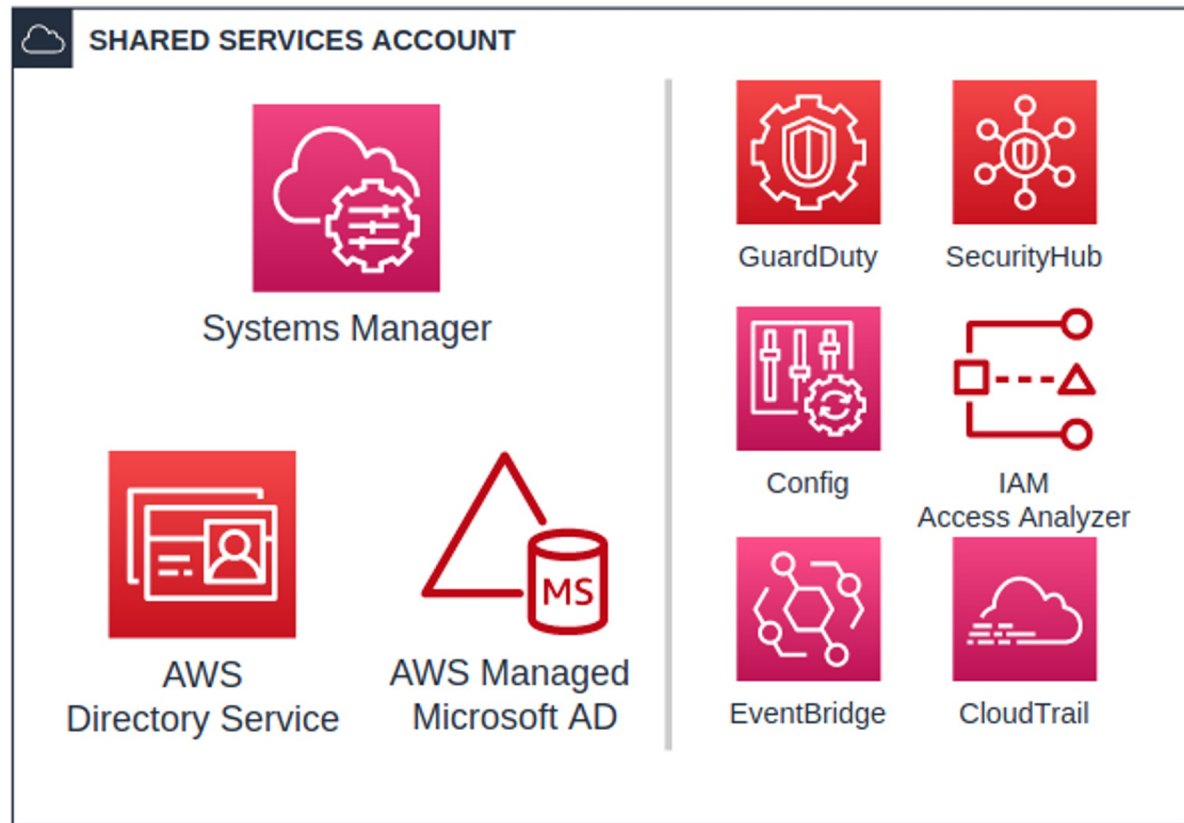
Planned 🧑



Infrastructure OU - Shared Services account

Share services
between teams
and applications.

Also **planned** 



Sandbox OU

Fail fast, fail smart!



AWS Control Tower



AWS Control Tower

The easiest way to set up and govern a secure, compliant multi-account AWS environment



Automate setup of your landing zone based on best-practice blueprints



Apply guardrails for ongoing governance over your AWS workloads



Automate your account provisioning workflow with an account factory



Get dashboard visibility into your organizational units, accounts, and guardrails

Secure multi-accounts setup with Control Tower



AWS Control Tower > Dashboard

► Recommended actions Get personalized guidance

Environment summary

3	6
Organizational units	Accounts

Enabled guardrail summary

24	2
Preventive guardrails	Detective guardrails

Noncompliant resources

< 1 > ⓘ

Resource ID	Resource type	Service	Region	Account name	Organizational unit	Guardrail
No noncompliant resources found						
No noncompliant resources detected on guardrails with a Clear status.						

Registered organizational units

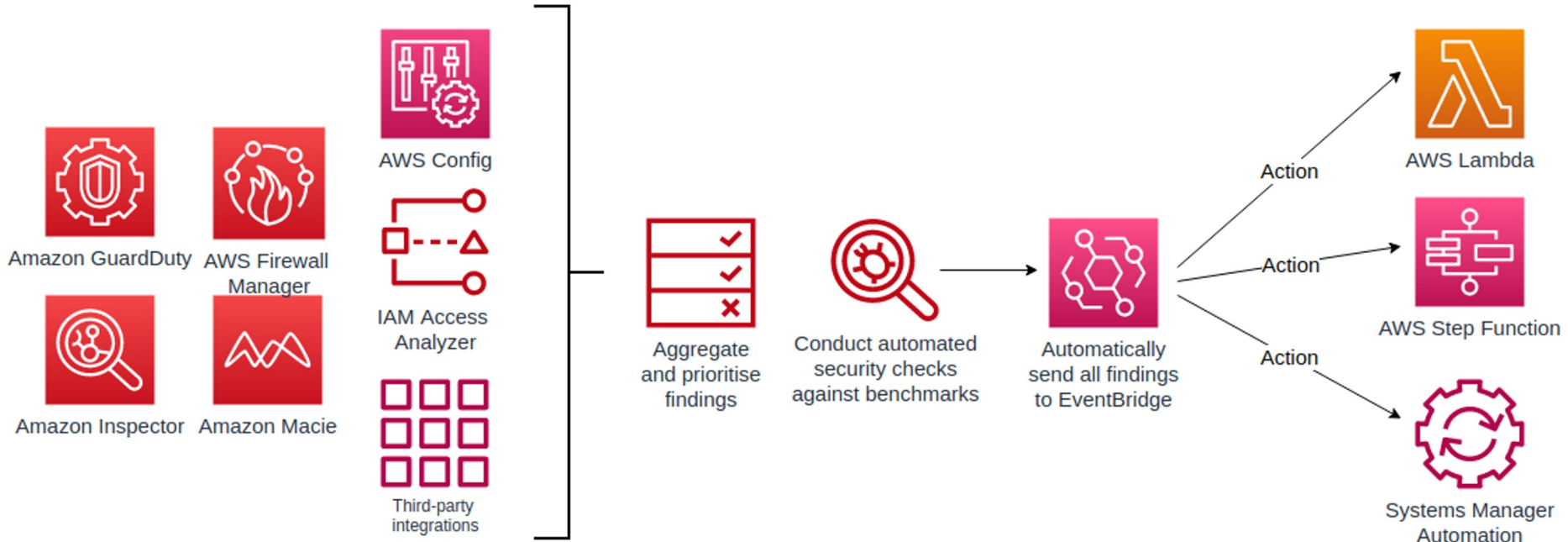
Find organizational units < 1 >

Name	Parent organizational unit	State	Compliance
Custom	Root	Registered	Compliant
Core	Root	Registered	Compliant
Sandboxes	Root	Registered	Compliant
Root	-	Registered	Compliant

[View all organizational units](#)

AWS Security Hub

Security posture management service that performs security best practice **checks**, aggregates **alerts**, and enables **automated remediation**.



Continuous monitoring of security best practices



Security Hub > Summary

Summary

Insights

	Results
1. AWS resources with the most findings	43
2. S3 buckets with public write or read permissions	0
3. AMIs that are generating the most findings	0
4. EC2 instances involved in known Tactics, Techniques, and Procedures (TTPs)	0
5. AWS principals with suspicious access key activity	0

Latest findings from AWS integrations

- Amazon GuardDuty** 3 months ago
[Open the GuardDuty console](#) [See findings](#)
- Amazon Inspector** No findings
[Open the Inspector console](#)
- Amazon Macie** No findings
[Open the Macie console](#)
- AWS IAM Access Analyzer** No findings
[Open the IAM Access Analyzer console](#)
- AWS Systems Manager Patch Manager** No findings
[Open the Systems Manager Patch Manager console](#)
- AWS Firewall Manager** No findings
[Open the Firewall Manager console](#)

Security standards

72% Security score

Standard	Passed	Failed	Score
CIS AWS Foundations Benchmark v1.2.0	16	27	37%
AWS Foundational Security Best Practices v1.0.0	84	12	88%
PCI DSS v3.2.1			Enable

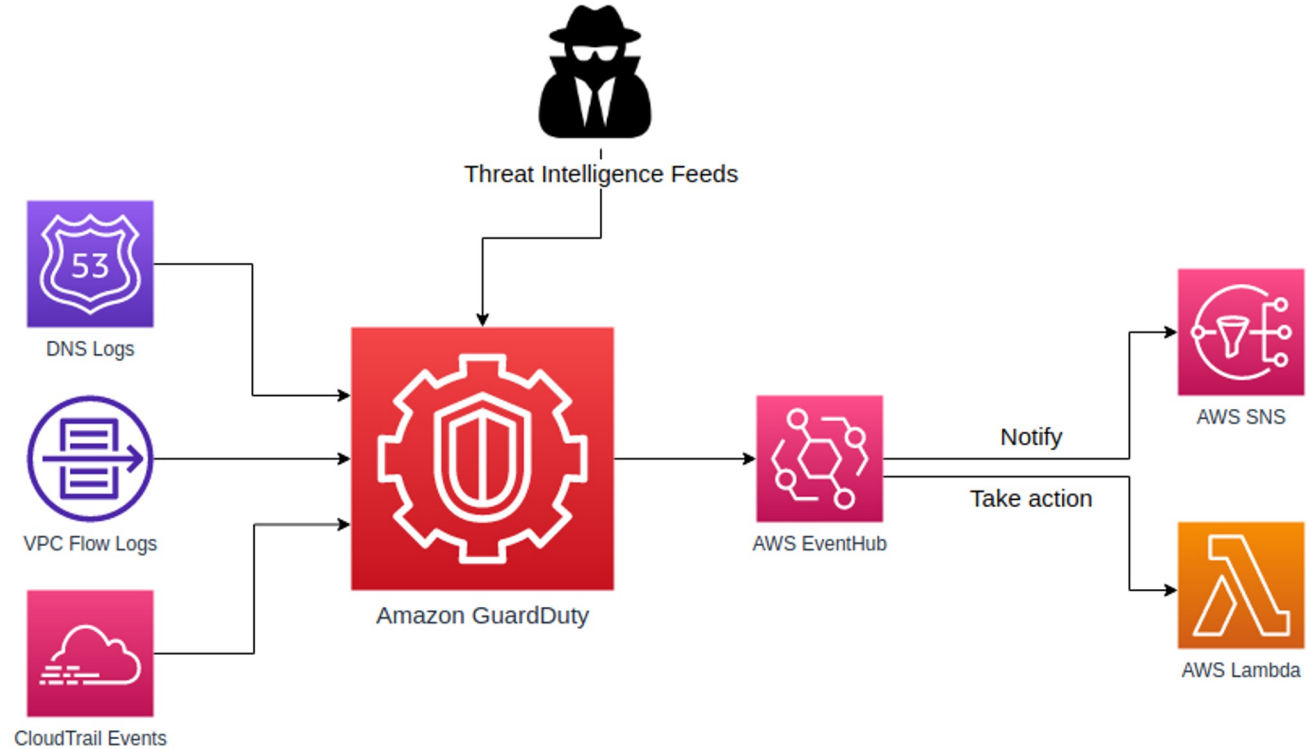
[View all standards](#)

Resources with the most failed security checks

Resource	Failed checks
AWS::Account:3 [redacted]	29
AWS::Account:4 [redacted]	29
AWS::Account:6 [redacted]	29
AWS::Account:8 [redacted]	29
AWS::Account:8 [redacted]	29

Amazon GuardDuty

Continuous
security
monitoring
and
intelligent
threat
detection



Continuous threat detection



GuardDuty > Findings Showing 25 of 25 3 20 2

Findings Info

Info Saved rules No saved rules

Current

<input type="checkbox"/>	Finding type	Resource	La...	Account ID	Count
<input type="checkbox"/>	Policy:IAMUser/RootCre...	Root: AS[REDACTED]	22 days ...	[REDACTED]	115
<input type="checkbox"/>	△ Impact:IAMUser/Anomal...	AWSReservedSSO_AWSAdministrator#	a month...	[REDACTED]	1
<input type="checkbox"/>	△ Impact:IAMUser/Anomal...	AWSReservedSSO_AWSAdministrator#	a month...	[REDACTED]	1
<input type="checkbox"/>	○ Discovery:IAMUser/Ano...	OliverGehrmannBillingAdmin: AS[REDACTED]	a month...	[REDACTED]	1
<input type="checkbox"/>	□ Persistence:IAMUser/Ano...	AWSReservedSSO_AWSAdministrator#	a month...	[REDACTED]	1
<input type="checkbox"/>	○ Discovery:IAMUser/Ano...	AWSReservedSSO_AWSAdministrator#	a month...	[REDACTED]	1
<input type="checkbox"/>	□ Recon:IAMUser/TorIPCaller	AWSReservedSSO_AWSAdministrator#	3 month...	[REDACTED]	11
<input type="checkbox"/>	□ UnauthorizedAccess:IAM...	AWSReservedSSO_AWSAdministrator#	3 month...	[REDACTED]	15
<input type="checkbox"/>	□ UnauthorizedAccess:IAM...	AWSReservedSSO_AWSAdministrator#	3 month...	[REDACTED]	4
<input type="checkbox"/>	□ Recon:IAMUser/TorIPCaller	AWSReservedSSO_AWSAdministrator#	3 month...	[REDACTED]	5
<input type="checkbox"/>	□ UnauthorizedAccess:IAM...	AWSReservedSSO_AWSAdministrator#	3 month...	[REDACTED]	5
<input type="checkbox"/>	□ Recon:IAMUser/TorIPCaller	AWSReservedSSO_AWSAdministrator#	3 month...	[REDACTED]	28

Impact:IAMUser/AnomalousBehavior

Finding ID: 88bd12640e0ee1a471ddf8ae97fe2ade

High APIs commonly used in Impact tactics were invoked by user AssumedRole : AWSReservedSSO_AWSAdministratorAccess_[REDACTED] under anomalous circumstances. Such activity is not typically seen from this user. [Info](#)

[Investigate with Detective](#)

Overview	
Severity	HIGH <input type="button" value="Info"/>
Region	eu-central-1
Count	1
Account ID	[REDACTED] <input type="button" value="Info"/>
Resource ID	[REDACTED] <input type="button" value="Info"/>
Created at	06-19-2021 16:58:52 (a month ago)
Updated at	06-19-2021 16:58:52 (a month ago)

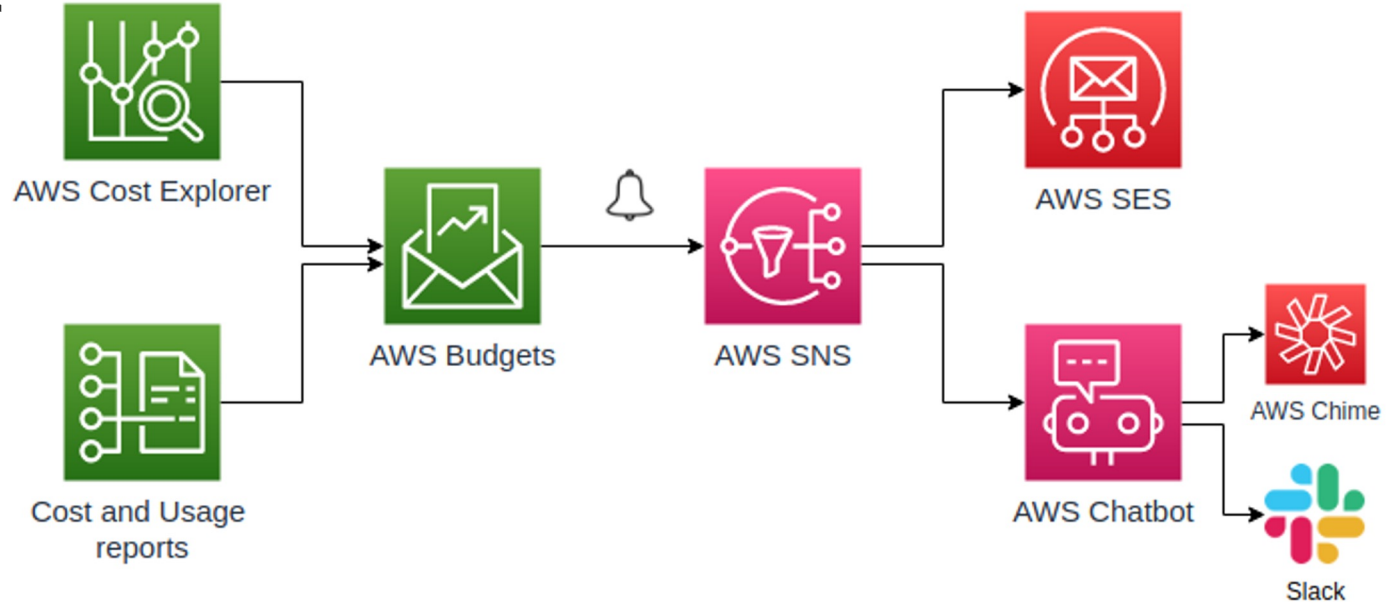
Anomalous APIs (6) **Usual APIs**

Successfully called

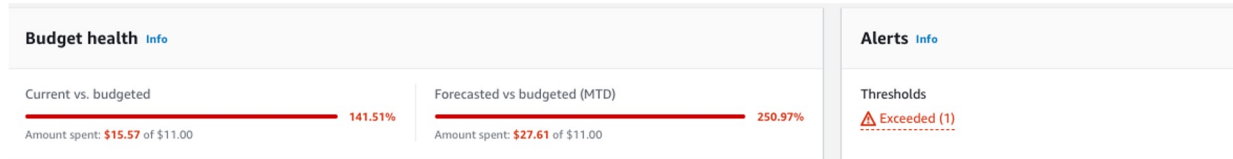
S3	PutBucketPolicy
	GetBucketVersioning
	ListAccessPoints
SignIn	ConsoleLogin

AWS Budgets

Keep your spending in check with **custom budget threshold and auto alert notification.**

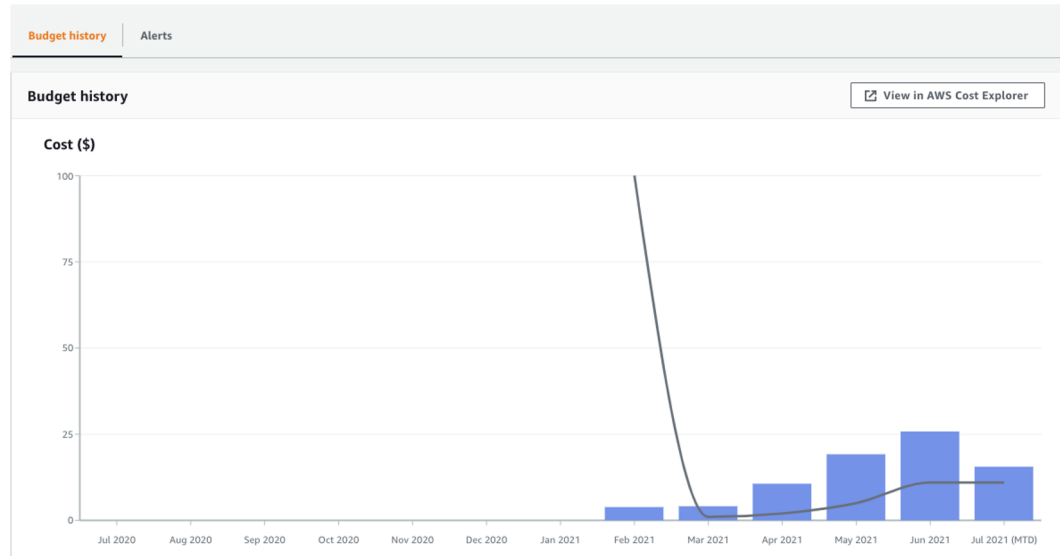


Automated Billing and Budget Setup



Get alerted when overall
AWS spend reaches
defined thresholds

- **100\$ / month**
- rolling update over
the last 3 months



Quick-start dashboard

superwerker

🏠 630007732912.a4662202-595c-46a8-87be-22c29f9d33ad.net

✅ DNS configuration is set up correctly.

Next steps - finish setup

SSO Setup

- Check your e-mail inbox for "Invitation to join AWS Single Sign-On" and follow the setups to accept the invitation. After finishing, log in into AWS via the AWS SSO portal.
- [Configure AWS SSO with identity providers](#), e.g. [Azure AD](#), [Google Workspace](#), [Okta](#), [OneLogin](#), to login to AWS with your existing login mechanisms.

Organizations Setup

- Set up recommended organizational units via [Control Tower](#) according to the [Organizing Your AWS Environment Using Multiple Accounts whitepaper](#)
 - Create a `Workloads_Prod` organizational unit for production workloads
 - Create a `Workloads_Test` organizational unit for test/dev workloads

What now? Standard operating procedures

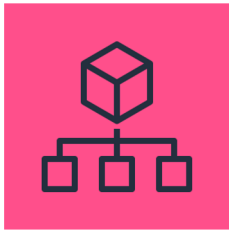
- Create AWS accounts for each of your workloads via the [Control Tower Account Factory](#) (for "Account email" use `root+<random_suffix>@630007732912.a4662202-595c-46a8-87be-22c29f9d33ad.net`.)
- Check [OpsCenter for incoming events and messages](#)
- Check [AWS Security Hub](#) for security best practise violations (login to Audit Account via AWS SSO portal first)
- Check [Amazon GuardDuty](#) for threats against your AWS accounts (login to Audit Account via AWS SSO portal first)
- Exclude resources from being backed-up by changing the `superwerker:backup` tag to `none`.

Help and more information

- [superwerker on GitHub](#)
- [Architecture Decision Records](#)
- [#superwerker](#) Slack channel in [og-aws](#)
- [Mailing list](#)

Updated at 2021-03-30 19:39:50.683659 (use browser reload to refresh)

Secure Root Mail Handling



AWS accounts need **unique email addresses**. Access to these email accounts has to be secured properly since they provide full access to the AWS accounts.

superwerker sets up a secure mail (sub-)domain in the DNS namespace of the AWS user

Takes care of generating email addresses for new AWS accounts

- E.g. **root+22c29f9d33ad@aws.<yourcompany>.com**

Consolidates all mail traffic / notifications to SSM OpsCenter

superworker is available as AWS Quickstart & OSS  **kreuzwerker**

For updates, please look at the homepage, the Quickstart home and subscribe to our mailing list or join the Slack channel.

- www.superworker.cloud
- aws.amazon.com/quickstart/architecture/superworker
- github.com/superworker/superworker
- Slack: og-aws [#superworker](#) ([invite](#))

free and open-source jumpstart for AWS

superwerker is a free and open-source solution that allows you to quickly set up a secure AWS Cloud environment for your business without investment in extensive research or consultancy fees. It is built by AWS Advanced Partners [kreuzwerker](#) and [superluminar](#) who have decades of experience setting up and automating AWS Cloud environments.

SET IT UP YOURSELF



GUIDED INSTALLATION

See a full overview of all features [here](#)



GitHub

Key takeaways

- AWS gives you maximum flexibility, however setting up the foundation correctly is crucial 
- AWS has a lot of services, you simply need to know that they exist and then **how to use** them, and **how to connect them** together
- We recommend to start your journey with an AWS Partner 





Thank you!
Questions?

manuel.vogel@kreuzwerker.de

Please take a
moment and rate
your experience -
>



Thank you for attending our Startup Day!



kreuzwerker GmbH
Ritterstr. 12
10969 Berlin
aws@kreuzwerker.de

www.kreuzwerker.de
Fon +49 30 609 838 80
Fax +49 30 609 838 899