superluminar

Deploying a Production-Ready AWS Cloud Setup

@s0enke

@superluminario

About me (Sönke Ruempler)

- Co-Founder of superluminar.io
- AWS since 2009
- AWS DevOps Pro / Solutions Architect Pro Certified
- AWS Partner Network Ambassador
- Founder of Serverless Hamburg Meetup
- Co-Orga of ServerlessDays Hamburg
- Sporadic blogger (https://ruempler.eu)
- Wardley Mapper

About superluminar

Mission: “With us to the core”

We help our clients to focus on their business core and competitive advantage by leveraging Public Cloud providers.

To achieve this:

- Strategic Consulting (e.g. Wardley Mapping)
- AWS Cloud Setups Workshops
- Serverless Workshops and Development
- Coaching / Training-on-the-Job

Partnerships:

- AWS Advanced Partner
- Serverless.com Dev Partner

superluminar

We are hiring cloud consultants!

https://superluminar.io/jobs

superluminar

Who of you operates a Multi-Account AWS Setup?

How many AWS Accounts?

< 5?

< 10?

< 50?

> 50?

superluminar

superluminar

Why should you have multiple AWS Accounts?

superluminar

Blast radius reduction

superluminar

Hard limits per AWS Account

superluminar

AWS Per-Account Service and API limits

superluminar

Security / Environment separation

superluminar

Making implicit resource sharing harder by design

superluminar

Ownership and billing

superluminar

Cloud Setups with AWS

superluminar

Questions from new and existing AWS users

- What are AWS Best Practices?
- How do I secure my workloads?
- How can I give teams maximum autonomy (without compromising security or consistency)?
- Which basic design should I use in AWS?
- How do I manage users and access rights?
- How does AWS Multi-Account work?

superluminar

Before AWS Landing Zone

Problems, Problems

- Often not-codified clicked AWS Account structure
- Tribal knowledge
- Security issues
- No easy on or offboarding
- Difficult AWS Account creation leads to big messy AWS Accounts
- Best practises evolve over time, how does your custom built setup?

superluminar

AWS Landing Zone

superluminar

Who knows it?

superluminar

Who is using it?

superluminar

A configured, secure, scalable, multi-account AWS environment based on AWS best practices

superluminar

What do you get?

Account Management

- Framework for creating and baselining a multi-account environment
- 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 security baselines

Security

- Multiple accounts enable separation of duties
- Initial account security and AWS Config rules baseline

superluminar

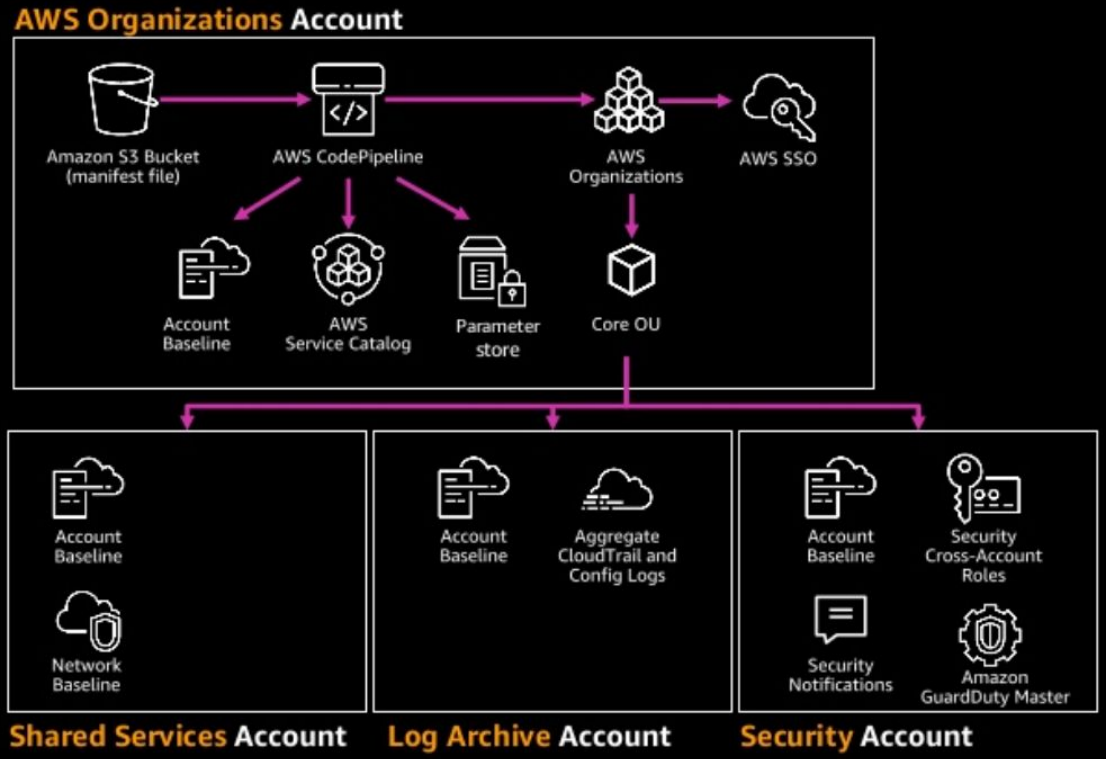
Many years
of accumulated
best practises.

superluminar

Short into:
How does it work?

superluminar

AWS Landing Zone structure - basic



Organizations Account

- Account Provisioning
- Account Access (SSO)

Shared Services Account

- Active Directory
- Log Analytics

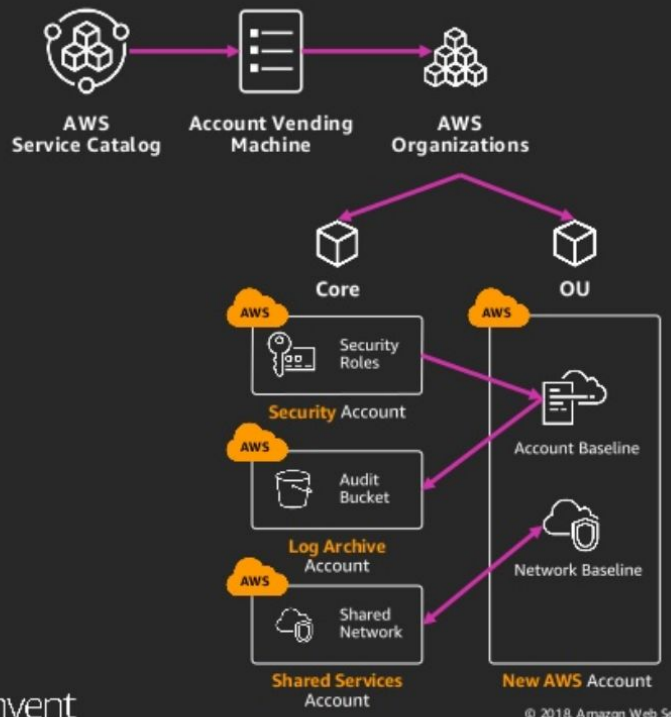
Log Archive

- Security Logs

Security Account

- Audit / Break-glass

Account Vending Machine



Account Vending Machine (AWS Service Catalog)

- Account creation UI
- Account baseline versioning
- Launch constraints

Creates/updates AWS account

Apply account baseline stack sets

Create network baseline

Apply account security control policy

Advantages: Why AWS Landing Zone?

- **Actively developed and maintained by AWS**
- **No additional third party consultant/solution lock-in**
- Codified Best practises
- Forwards compatible to coming AWS Control Tower Product
- Quick Start: Solution is ready in < 1 hour
- Fully codified and Infrastructure as Code
- Basic extendable framework
- Easy new AWS account creation

Gotchas / Caveats

- Steep learning curve because many AWS Services are involved (Service Catalog, Step Functions, CloudFormation, CodePipeline, …)
- Can be complicated to debug / understand if something does not work
- The proposed AWS SSO Service still lacks basic things like API access and Multi Factor Auth
- No concept yet of protecting resources created by Landing Zone in Subaccounts (might be solved with SCPs)

superluminar

Frequently Asked Questions.

How do I try it out / install it?

Quickstart via CloudFormation “initiation” template.

Read our blog post :) ->
https://medium.com/@superluminar/tested-for-you-multi-account-setups-with-aws-landing-zone-b934154cfc78

What about existing setups?

It’s possible to install Landing Zone to existing setups.

Even if not officially supported.

Landing Zone is relativity unintrusive.

Can be adopted in rolling manner on an account-by-account basis.

Need help? Ask us :)

How do Updates work?

Usually a update of the CloudFormation Initiation template.

superluminar

Use Case / Demo Time

Demos

- Create a new AWS Account
- Rollout Service Control Policy: Restrict to EU regions
- SAML SSO Login: Deploying a new Baseline Resource

References

- https://ruempler.eu/2017/07/09/advantages-aws-multi-account-architecture/
- https://medium.com/@superluminar/tested-for-you-multi-account-setups-with-aws-landing-zone-b934154cfc78
- https://www.slideshare.net/AmazonWebServices/setting-up-a-landing-zone
- https://www.slideshare.net/AmazonWebServices/aws-landing-zone-deep-dive-ent350r2-aws-reinvent-2018
- AWS re:Invent 2018: Architecting Security & Governance across your AWS Landing Zone (SEC303-R1)

superluminar

Thanks.

Questions?

Feedback?

Use cases?