AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

COP401

Customizing and scaling your AWS Control Tower environment

Remek Hetman
Principal Cloud Architect
Amazon Web Services

Nivas Durairaj
Senior Control Services Specialist
Amazon Web Services

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Enable
AWS Control Tower

Your organization requirements

- Operations
- ML and analytics
- Application development
- Security tooling
- Cost tracking

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

AWS Control Tower landing zone

Common customizations

The Customizations for AWS Control Tower (CfCT) solution

CfCT best practices and considerations

Multi-organization deployments

End-to-end account vending example

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Before we begin

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Control Tower

The easiest self-service solution to automate the setup of **new AWS multi-account environments**



AWS Managed Services (AMS) version of multi-account environment



Deployment of AWS best-practice blueprints and guardrails



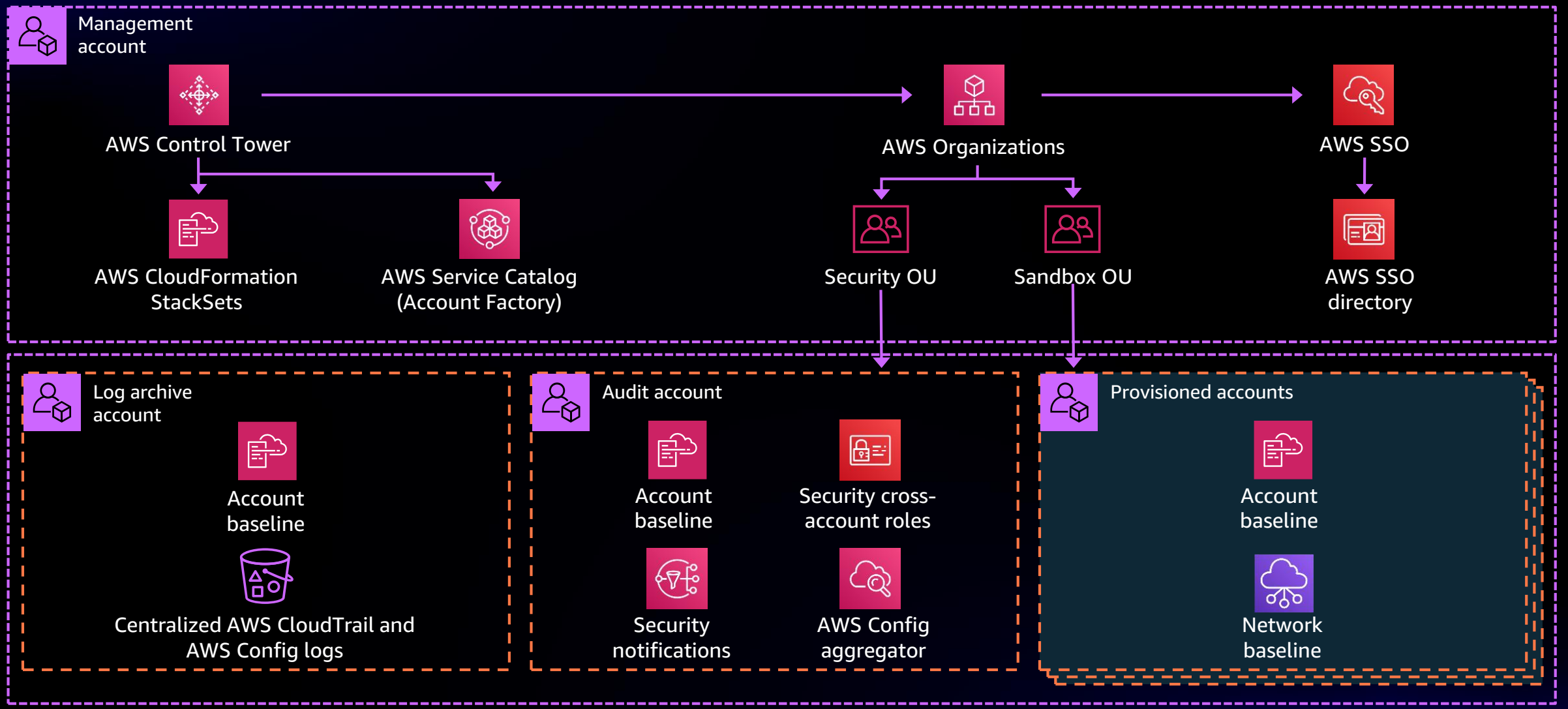
An AWS service, offering automated account creation based on AWS best practices



Dashboard for monitoring compliance status

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Landing zone provisioned by AWS Control Tower



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

With your baseline environment set up, what's next?

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Top 5 customization categories



Identity

Identity providers

IAM role and policy

Service control policy



Security and compliance

Security tooling

Encryption



Networking

AWS Transit Gateway

IP allocation

Routing

Security groups



Logging

AWS CloudTrail (data events)

VPC Flow Logs

Firewall logs

Amazon CloudWatch logs



Control

AWS Config rules

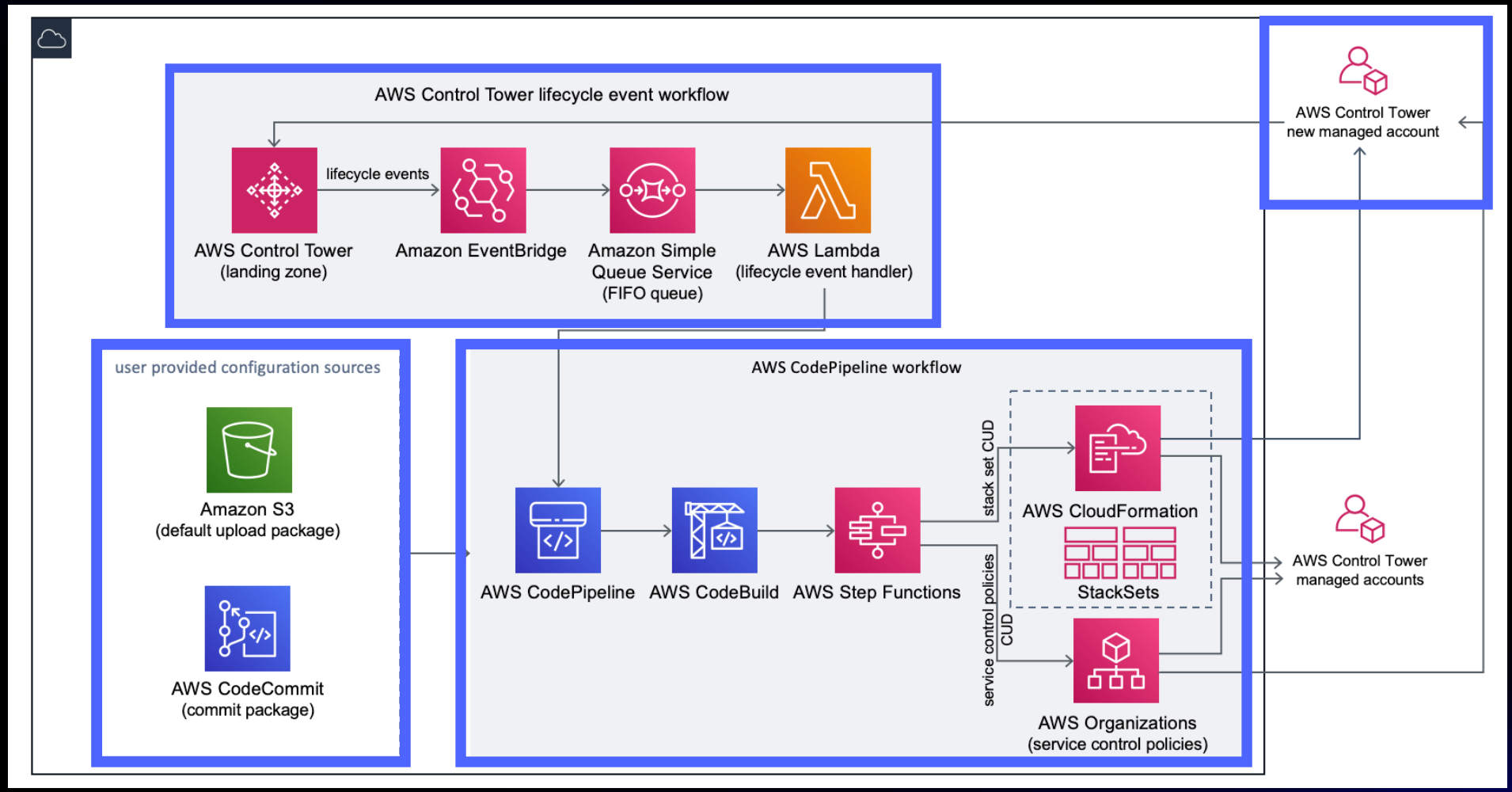
Resource policy (Amazon S3, Amazon SNS, AWS KMS)

Preconfigured products

aws

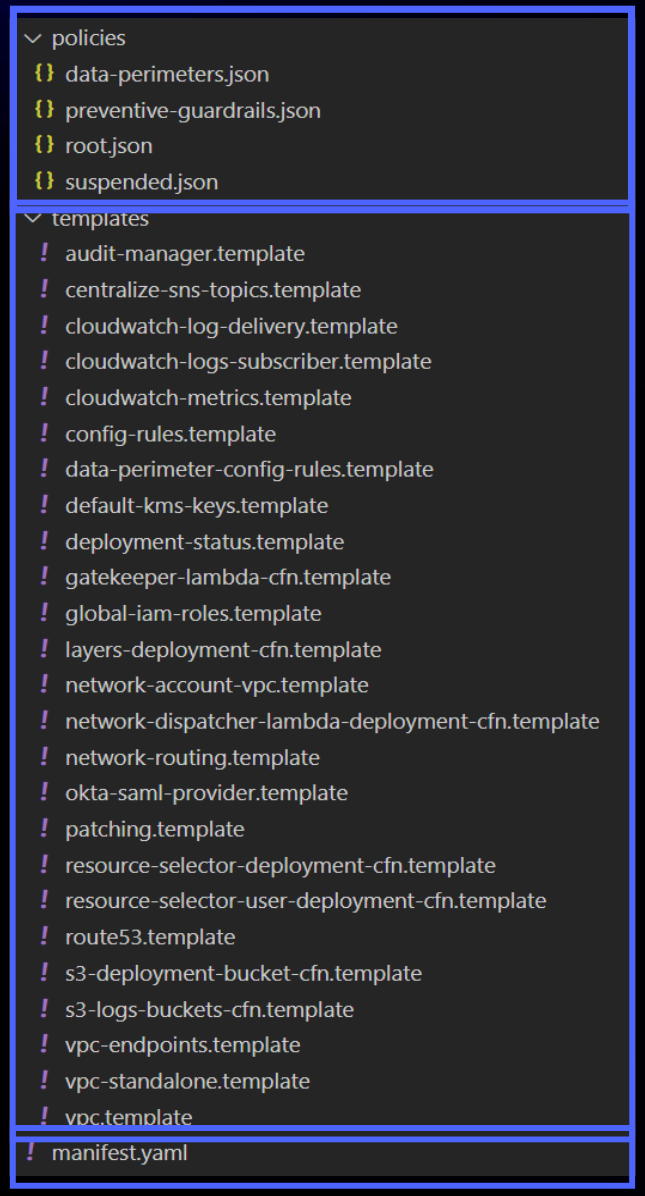
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Customization framework for AWS Control Tower



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Control Tower customization – Example




```
---
region: us-east-1
version: 2021-03-15

resources:
  - name: IDP-Type1
    resource_file: templates/saml-provider.template
    deployment_targets:
      organizational_units:
        - Infra-Prod
      accounts:
        - <account_id>
    deploy_method: (stack_set or scp)
    parameters:
      - parameter_key: Organization
        parameter_value: $[alfred_ssm_/corporate/organization]
    export_outputs:
      - name: /corporate/param_name
        value: $[output_<cf_output_name>]
    regions:
      - us-east-1
```

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CfCT best practices and considerations

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CfCT considerations

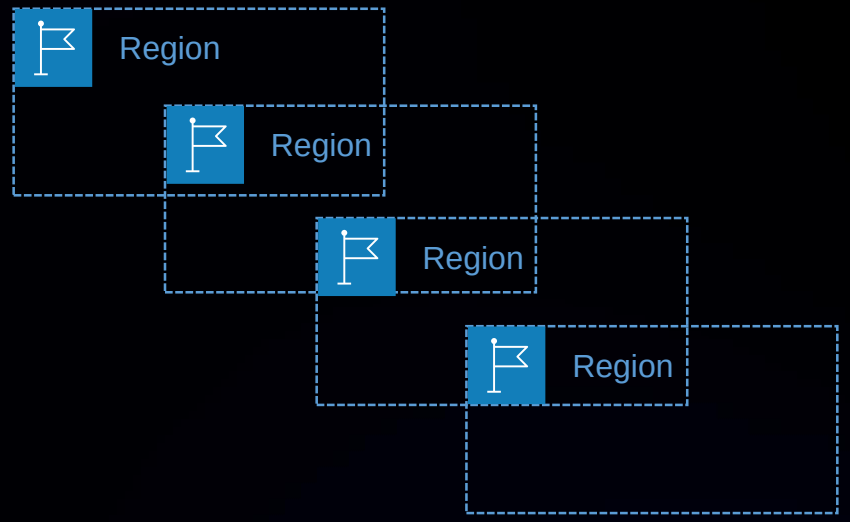
Any resource supported by CloudFormation should be deployed by CfCT



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CfCT considerations

Parallel vs. sequential





© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CfCT considerations

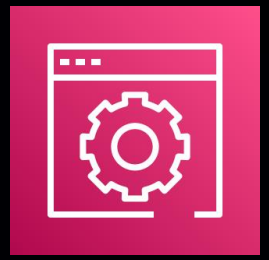
Fault tolerance – performance vs. consistency



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CfCT considerations

Proactively manage service quotas



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CfCT considerations

Global resources

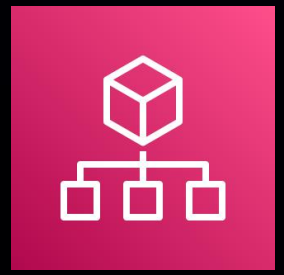
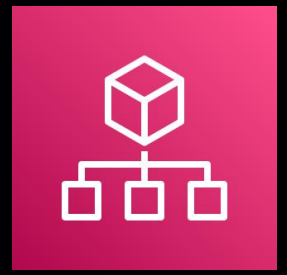
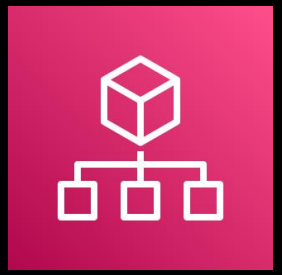




© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

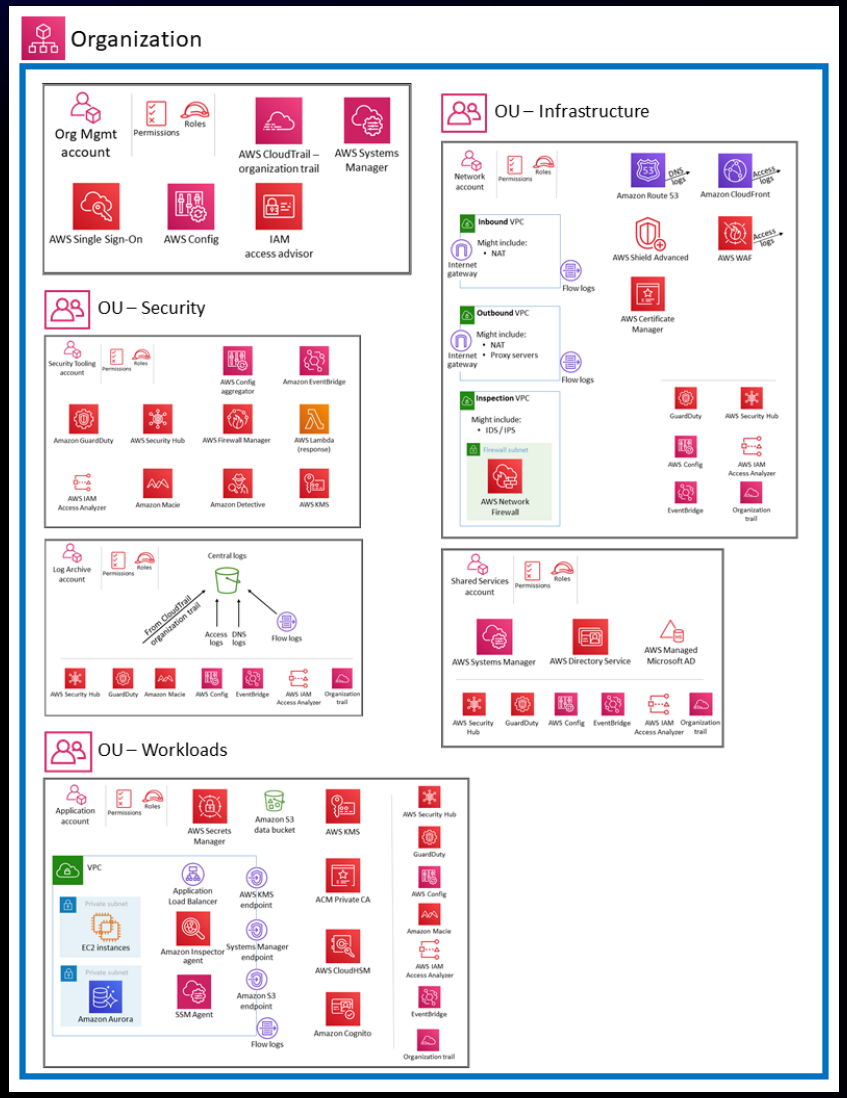
CfCT considerations

Using multiple organizations

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Security Reference Architecture



Security tooling

- Amazon GuardDuty
- Amazon Macie
- AWS Security Hub
- And more

Check out: https://a.co/75iVViP

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Account Factory for Terraform (AFT)

- Terraform-based account provisioning pipeline
- Feature support
  - AWS Enterprise Support enrollment
  - Amazon GuardDuty
  - AWS CloudTrail data events for Amazon S3 and AWS Lambda
  - Default VPC deletion
- Bring your own TF customizations

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Managing multiple organizations with CfCT

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multi-organization management

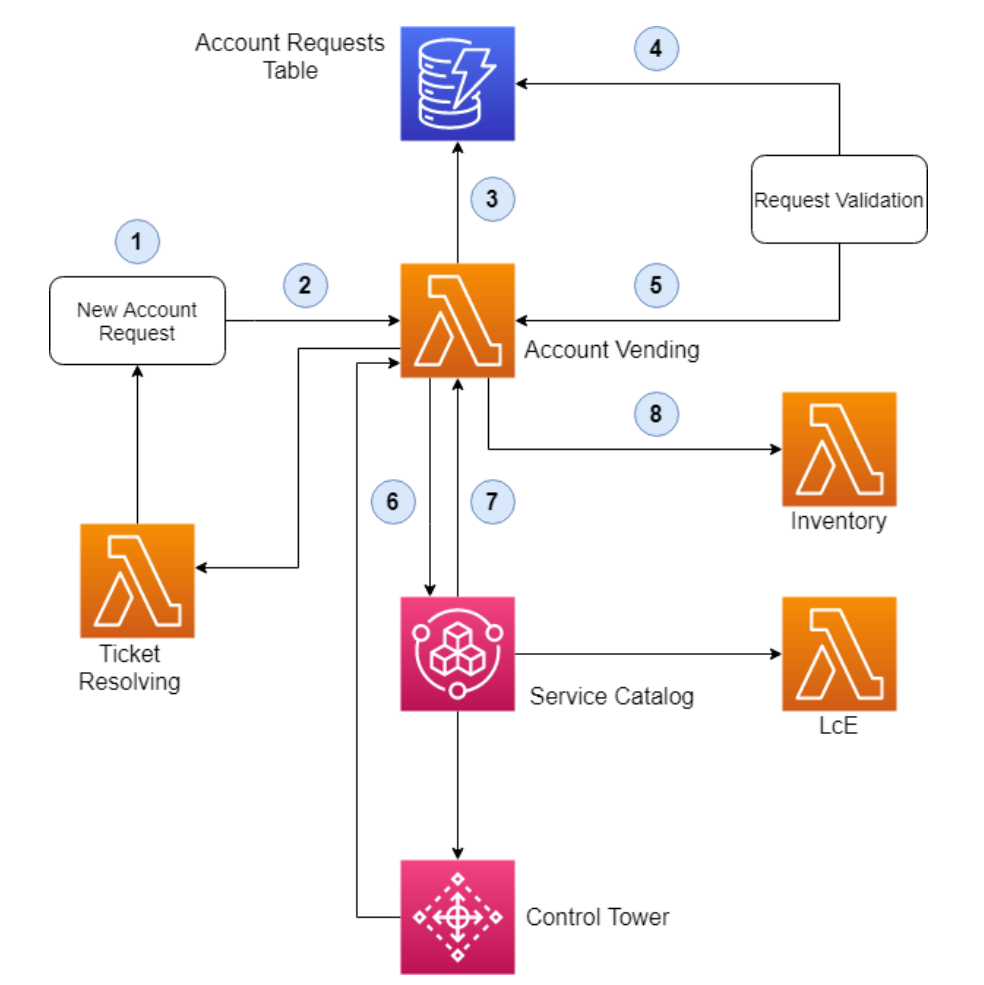
- Development vs. production organizations
- Challenges
  - Environment properties
  - Automation
- Single manifest pattern

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multi-organization manifest file overview

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

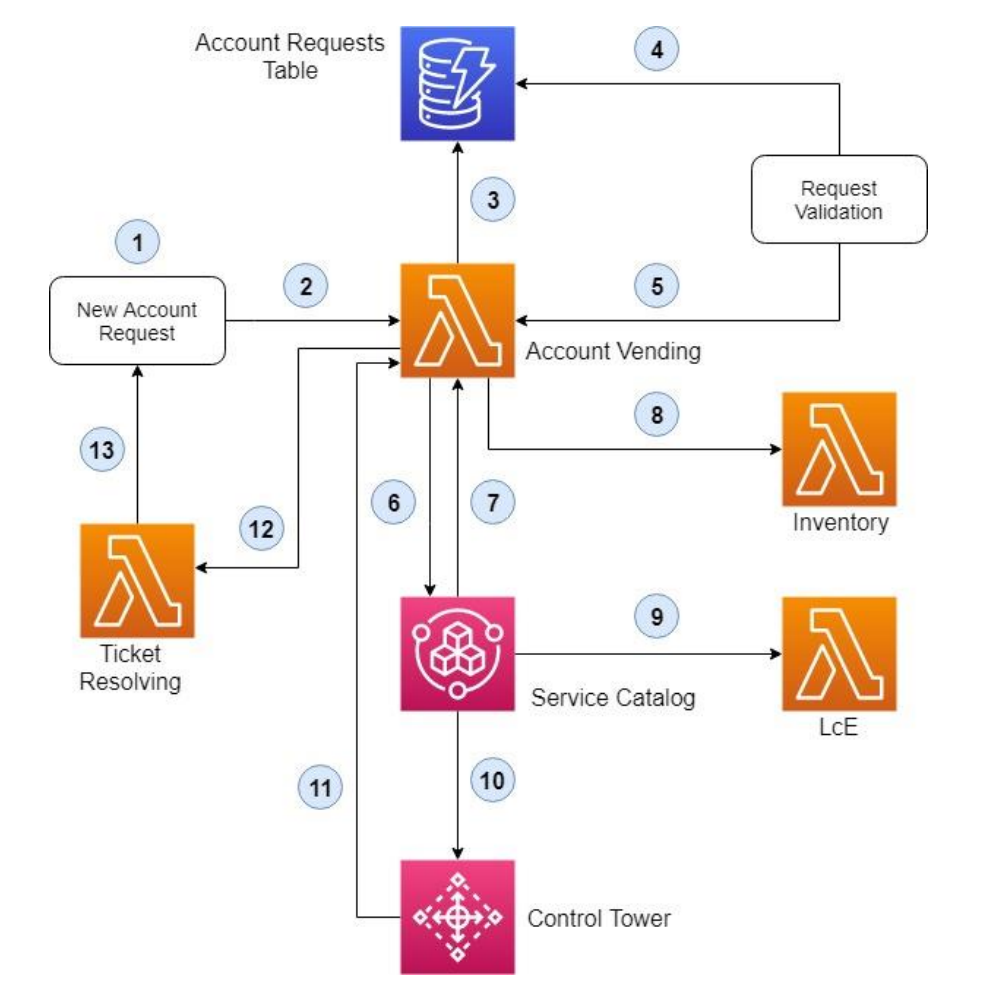
End-to-end account vending solution example



1. User requests a new account using a ticketing system
2. Ticketing system calls account vending Lambda function
3. Lambda records request details in an Amazon DynamoDB table
4. Request validation (optional)
5. After validation, calls account vending function to proceed with account vending
6. Lambda calls AWS Service Catalog to create a new account
7. Monitor progress using AWS Step Functions
8. After account is successfully created, Lambda inventory functions registers a new account

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

End-to-end account vending solution example



9. Creation of new account triggers lifecycle event Lambda function to
   - Add account to Active Directory and grant user(s) permission
   - Create alias for the new account
   - Grant new account permission to call network dispatcher
   - Grant new account permission for CloudWatch log destination
   - Update Amazon S3 account public access
   - Other as needed
10. Triggers AWS Control Tower customization to deploy necessary infrastructure and resources in the new account
11. When all resources are deployed, AWS Control Tower customization calls account vending function to update status
12. When all steps succeed, vending function calls ticketing system
13. Lambda resolves ticket and notifies user that requested account is ready for use

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Remek Hetman
rhetman@amazon.com

Nivas Durairaj
nivasd@amazon.com

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.