
AWS
re:Inforce
JULY 26 – 27, 2022 | BOSTON, MA

GRC374

Automate governance of environments with AWS Control Tower

Ron Melanson
Business Development
AWS

Vishal Sharma
Business Development
AWS

Agenda

- AWS Control Tower deployment/setup
- AWS Control Tower overview
- Hands-on lab: https://controltower.aws-management.tools
- Next steps

AWS Control Tower setup

AWS Control Tower deployment/setup

- AWS account (required): In order to launch AWS Control Tower, create a brand-new AWS account – this will be the AWS Control Tower Management Account
  - Launch Amazon EC2 to test the account – Instructions to launch Amazon EC2
- Launch/setup AWS Control Tower:
  - From the AWS Management Console, launch AWS Control Tower using the AWS account created in step #1
  - The setup of AWS Control Tower requires 2 emails for the audit and logging accounts created by AWS Control Tower
  - Launch/setup AWS Control Tower – Instructions to launch AWS Control Tower
- Credit is provided for the resources created during the lab

Credits

- $25 promotional credit provided for each attendee
- You can apply credit to only one AWS account (payer account)
- You can redeem credit in an existing account or a new AWS account that you created today
- More Information: aws.amazon.com/awscredits

AWS Control Tower overview

AWS Control Tower: A self-service solution to automate the setup of new AWS multi-account environments

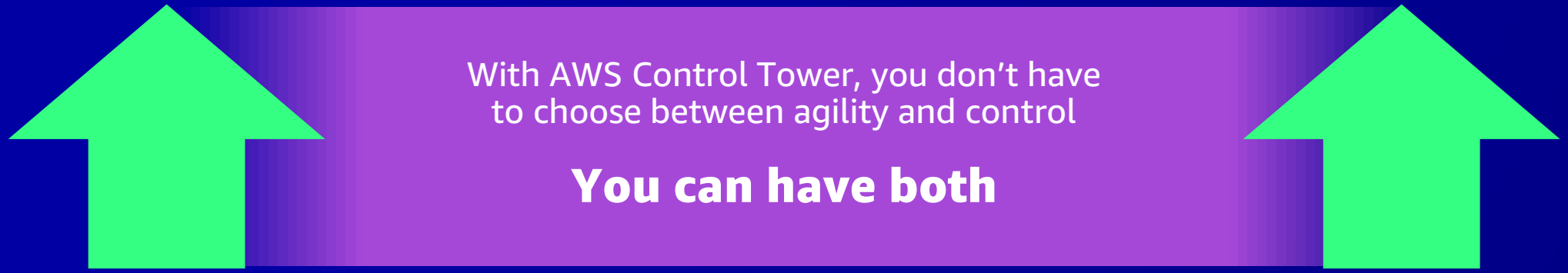
AWS-managed-service version of multi-account environment

Deployment of AWS best-practice blueprints and guardrails

Automated account creation based on AWS best practices

Dashboard for monitoring compliance status

Business agility and governance control



Governance

Security

Compliance

Operations

Spend management

Agility

Self-service access

Experiment fast

Respond quickly to change

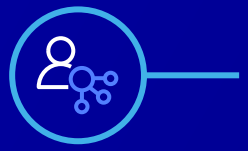
AWS Control Tower benefits

Automated landing zone with best practice blueprints

AWS best-practice guardrails for policy management

Account factory for account provisioning

Dashboard for visibility and actions



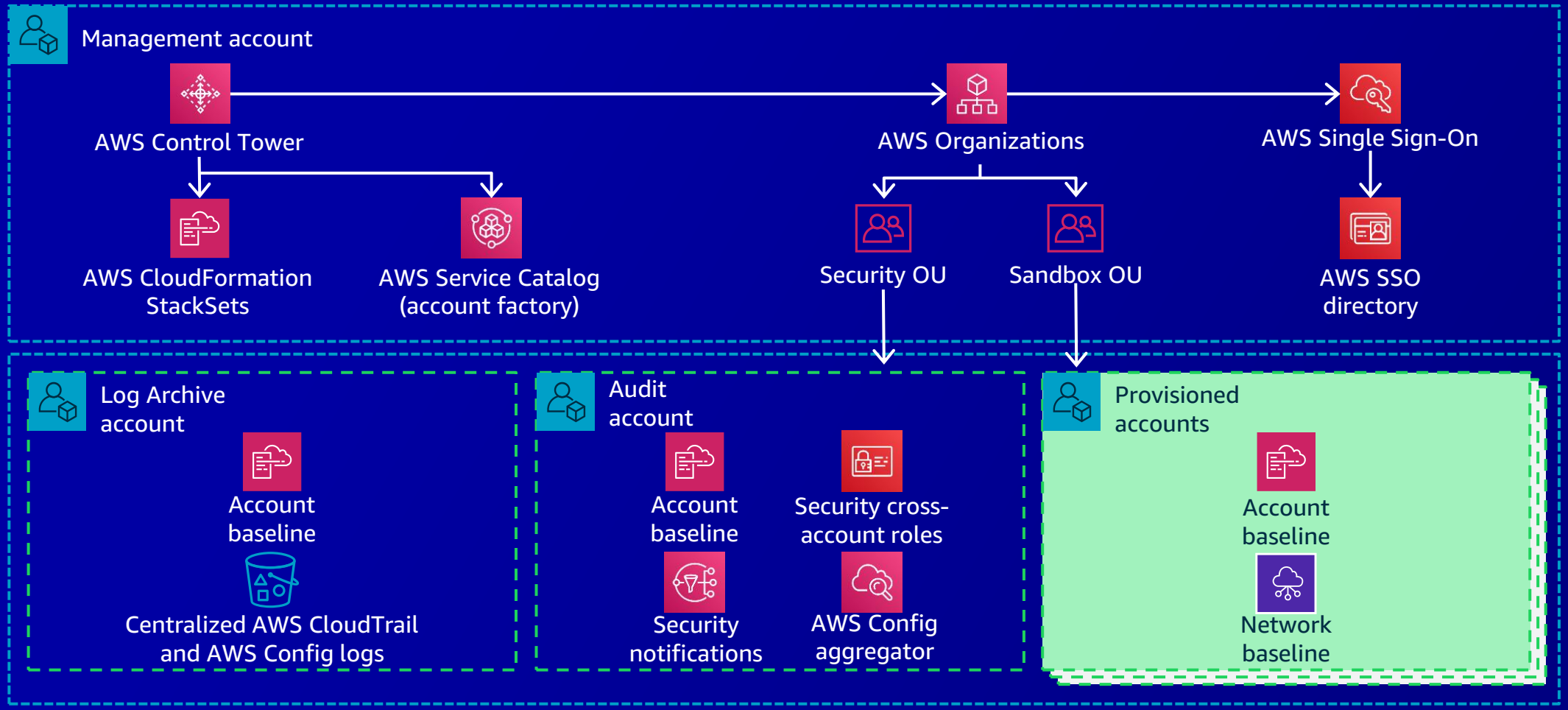
Built-in identity and access management (IAM)

Preconfigured log archive and audit access to accounts

Built-in monitoring and notifications

Extensible with third-party ISV solutions available through AWS Marketplace

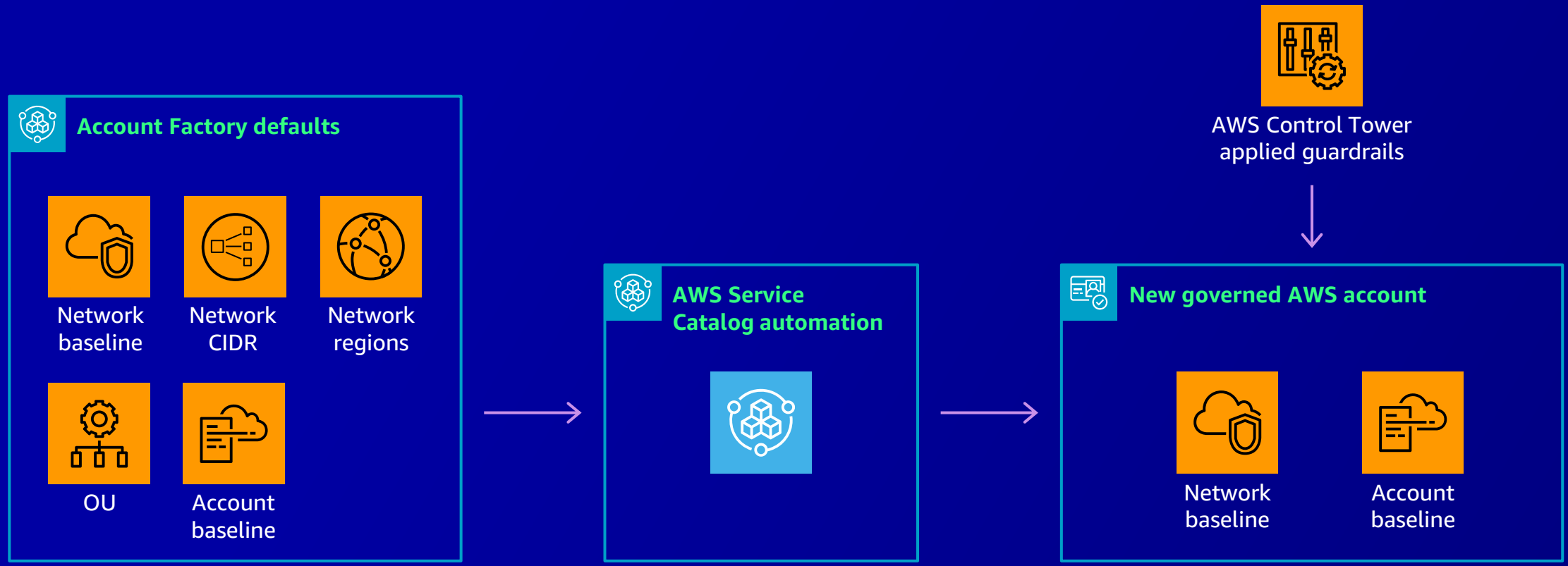
AWS Control Tower landing zone foundation



AWS Control Tower orchestrates AWS Single Sign-On to centralize identity and access

- AWS SSO provides default directory for identity
- AWS SSO also allows federated access management across all accounts in your organization
- Preconfigured groups (such as AWS Control Tower administrators, auditors and AWS Service Catalog end users)
- Preconfigured permission sets (such as admin, read-only, write)
- AWS SSO integrates with third-party IDP (Microsoft Azure AD, Ping, Okta)

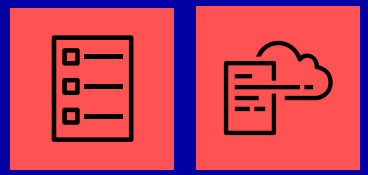
Provisioning with AWS Service Catalog: AWS Control Tower Account Factory



Customizations for AWS Control Tower

- CI/CD pipeline to extend Account Factory
- Keeps resources in sync via CloudFormation StackSets
- Account creation and customization of new or existing accounts
- Customization to meet your procedures

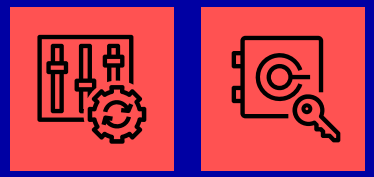
Terraform pipeline to provision and customize accounts in AWS Control Tower



- AWS Control Tower Account Factory for Terraform (AFT)
- AWS Control Tower governance benefits with Terraform-based account provisioning pipeline
- Supports Terraform Cloud, Terraform Enterprise, and Terraform Open Source
- Account creation and customization of new or existing accounts
- Customization to meet your procedures

Two types of guardrails: Preventive and detective

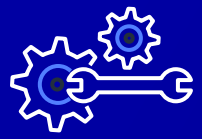
Simplify data residency controls with AWS Control Tower



- Limit customer data within geographic locations
- Reduce complexity
- Keep your customer data compliant
- Use purpose-built guardrails
- Set up in minutes

Enhance the AWS Control Tower experience

Scale with superior visibility and control



Automate operations with integrated security services

Cloud operations

Enforce guardrails for centralized security

Global security and compliance controls

Security operations

Centralized security and network operations

Network operations

Extend AWS Control Tower with AWS Organizations

Centrally provision resources in a multi-account environment

- AWS CloudFormation
- AWS Systems Manager
- AWS Service Catalog

Share resources and control access to accounts, regions, and services

- AWS Personal Health Dashboard
- AWS Resource Access Manager
- AWS Backup and backup policies
- Tag policies

Optimize costs and identify cost-saving measures

- AWS Trusted Advisor
- AWS Compute Optimizer
- AWS Cost Explorer
- AWS License Manager
- Amazon S3 Storage Lens

Seamlessly integrate with AWS security services

- AWS Audit Manager
- Amazon GuardDuty
- Amazon Cloud Directory
- AWS Firewall Manager
- Amazon Macie
- AWS Security Hub
- AWS IAM Access Analyzer
- AI/ML Policies

https://docs.aws.amazon.com/organizations/

Pricing and availability

Generally available in
- Americas (Canada, N. Virginia, Ohio, Oregon, Brazil)
- APAC (Australia, Singapore, India, Japan, Korea)
- EU (Ireland, Germany, England, Sweden, France)

No additional charge for using AWS Control Tower

Pay only for underlying AWS services (such as AWS Config rules or AWS CloudTrail) that are activated

Hands-on lab

Lab steps

1. Deploy AWS Control Tower in your account (https://controltower.aws-management.tools/core/overview/)
2. Create a new organizational unit (OU) (https://controltower.aws-management.tools/core/accountfactory/)
3. Apply elective guardrail to the OU (https://controltower.aws-management.tools/core/accountfactory/)
4. Create a new AWS account in the OU (https://controltower.aws-management.tools/core/accountfactory/)
5. Test the applied guardrail (https://controltower.aws-management.tools/core/accountfactory/)
6. Tasks in AWS Control Tower (https://controltower.aws-management.tools/core/cttasks/)
7. AWS data residency guardrails (https://controltower.aws-management.tools/security/restrict_regions/)
8. Cleanup resources

Next step

More resources

- Getting started
- AWS Control Tower workshops
- Attend an AWS Control Tower activation day held regionally/time-zone based – Contact your account team
- AWS Well-Architected Management and Governance Lens
- AWS Management and Governance blog
- AWS Management and Governance YouTube channel

AWS Control Tower getting started

AWS Management and Governance blog

AWS Well-Architected Management and Governance Lens

Thank you!