

AWS re:INVENT

GPSTEC310

IAM Best Practices and Becoming an IAM Ninja

Scott Ward – Solutions Architect
Pat McDowell – Solutions Architect

AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Identity & Access Management is the foundation that all AWS services require to function and perform any action. Mastering IAM is the skill set you need in your arsenal so that you can provide best-in-breed services through your application or services to your customers. This session shows you best practices for IAM, the latest service additions, and advanced automation techniques to become a certified IAM ninja.

"I have been to IAM presentations before and I have seen the best practices. I get all that you have told me. What else can you tell me? I want to be dazzled."

How can I improve via Automation or Machine Learning?"



AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



AWS re:INVENT

GPSTEC310

Extending AWS Identity and Access
Management through Automation
and Machine Learning

Scott Ward – Solutions Architect
Pat McDowell – Solutions Architect

New

AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Cross Account Roles

This can for SaaS operators that requires access into their customer AWS accounts, customers can use this partner solution to do things like monitoring



*Customer: "I would like to use your
service to monitor my account."*

Cross Account Roles

Scenario 1 – Access Keys

Partner: “Sure, just send me your access keys...”



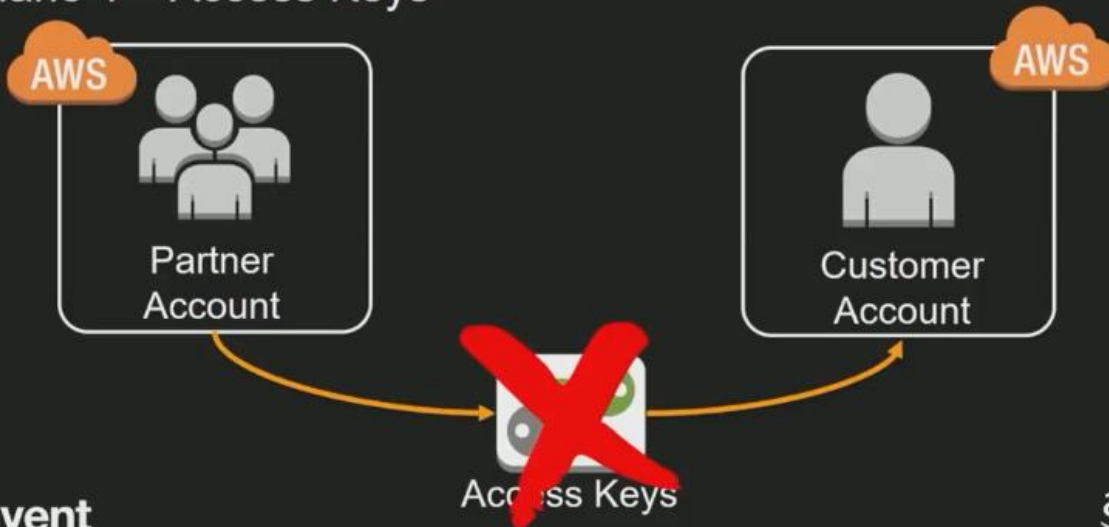
AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Cross Account Roles

Scenario 1 – Access Keys



AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Cross Account Roles

Scenario 2 – Manual Cross Account Role

Partner: “Sure, just follow this guide to create a cross account role. Create a policy, then create a role with our account number and this unique external id, then give us the ARN of your role.”



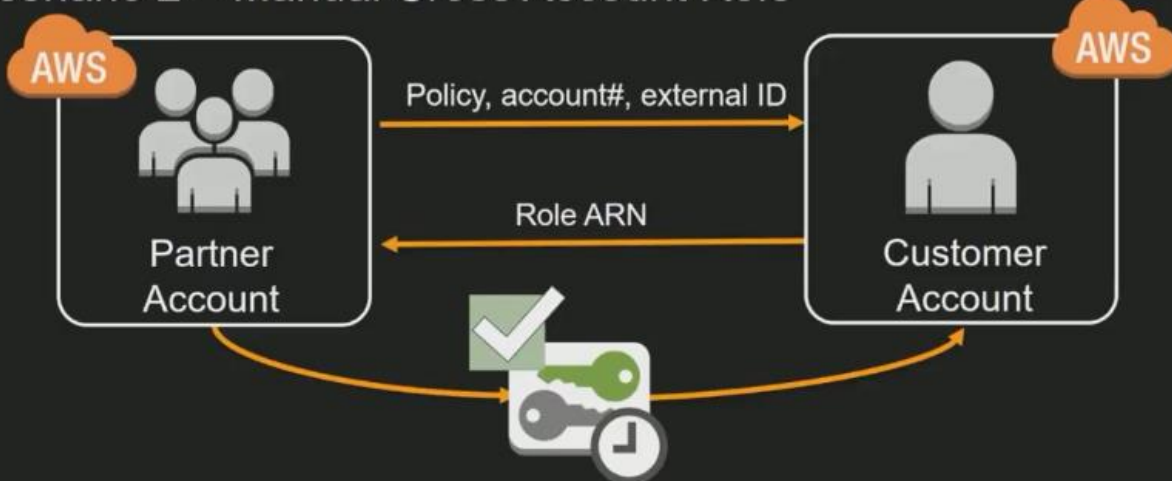
AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Cross Account Roles

Scenario 2 – Manual Cross Account Role



AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Temporary Access Keys



An external ID is a long secret value that the partner also needs to provide along with the ARN of the role. The partner now has the ability to make API calls within our account. But there is still a lot of steps in this approach

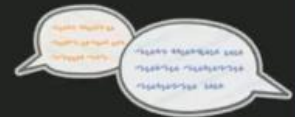
Cross Account Roles

"My customers don't like the number of steps to setup a cross account role... or they don't understand why they are doing the steps..."

Cross Account Roles

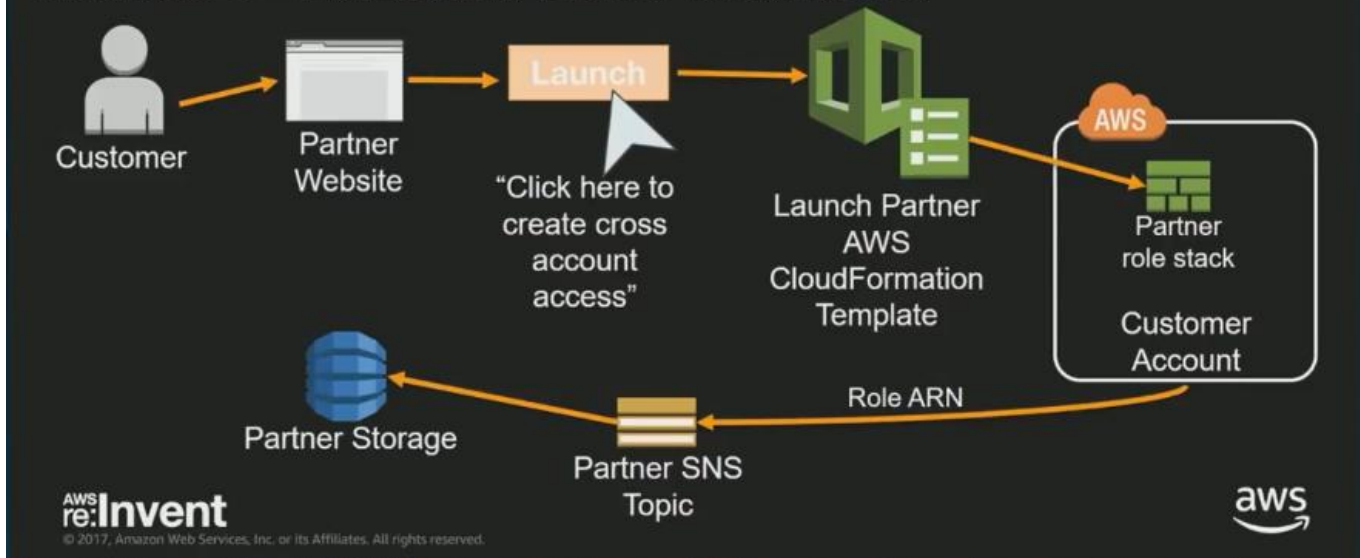
Scenario 3 – Automated Cross Account Role

Partner: *"Sure, tell us your account number and we will get you setup."*



Cross Account Roles

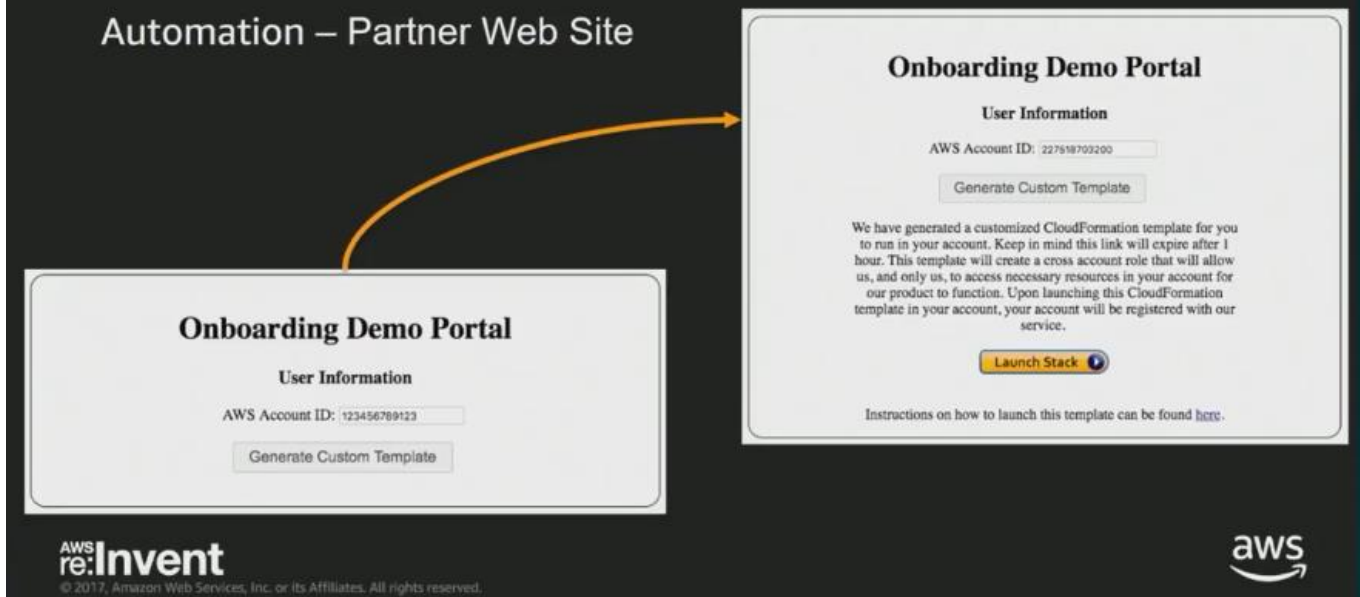
Scenario 3 – Automated Cross Account Role



The Partner stack will create the role, define the policy, pass in the value of the account number and the external ID of the account number needed to create that role. All within the partner's account and will also send back that role to the customer account without them having to copy and paste into the partner portal. The partner can now consume that and put it into their storage.

Cross Account Roles

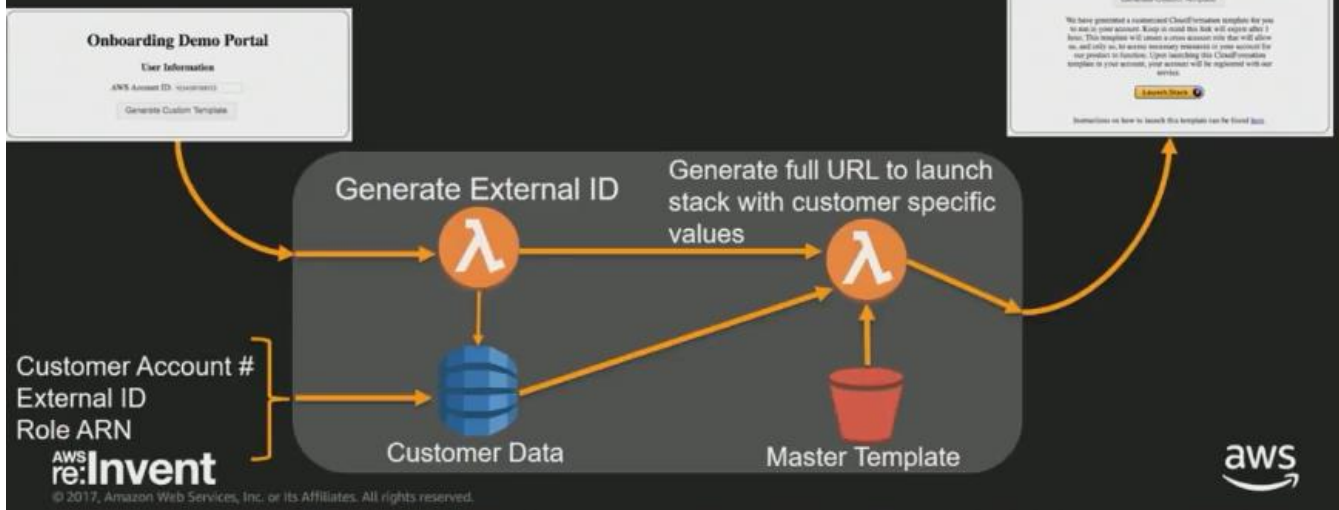
Automation – Partner Web Site



The customer comes to the partner portal and sees this form, puts in their AWS account number to generate a custom template. Then they will get routed to the next screen where they can click on a button to launch the stack generated for them as a CF template with all the right information.

Cross Account Roles

Automation – Partner Web Site



This workflow shows how this was done.

Cross Account Roles

Automation – The AWS CloudFormation Template

Create stack

Template

Template URL

https://n0-v8-ws01-2.amazonaws.com/doc/stacked-yml

Description

This template creates a Cross-Account-Role that will grant ExampleCorp permissions to your account

Details

Stack name

CrossAccountRoleSetup

Parameters

Cross-Account Role Configuration, "Do Not Modify"

AWS Account ID to Grant Permission

123456789012


Account ID to Grant Account Role

ExternalID

abcd1234

External ID for Cross Account Role

Capabilities

 The following resource(s) require capabilities: [AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. [Learn more](#)

☐ I acknowledge that AWS CloudFormation might create IAM resources

Cancel

Create

This is where the URL will lead the customer to, this is the review screen of launching a CF stack.

Cross Account Roles

Automation – The AWS CloudFormation Template

```
https://console.aws.amazon.com/cloudformation/home?region=us-east-1#/stacks/create/review?
templateURL=https://s3-us-west2.amazonaws.com/isco/wizard.yml&
stackName=CrossAccountRoleSetup&
param_TrustedAccount=123456789012&
param_ExternalId=abcd1234
```

We are directing that the user be taken to the **review** screen of the CF template creation process

Cross Account Roles

Automation – Getting Data Back from the Customer

Use an AWS CloudFormation custom resource to “phone home” with the final ARN

```
PhoneHomeCustomResource:
  Properties:
    ServiceToken: arn:aws:sns:us-west-2:111111111112:ARNSnsTopic
    RoleArn: !GetAtt CrossAccountRole.Arn
    AccountID: !Ref AWS::AccountId
  Type: Custom::PhoneHomeCustomResource
  Version: '1.0'
```

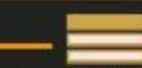


Role ARN



AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



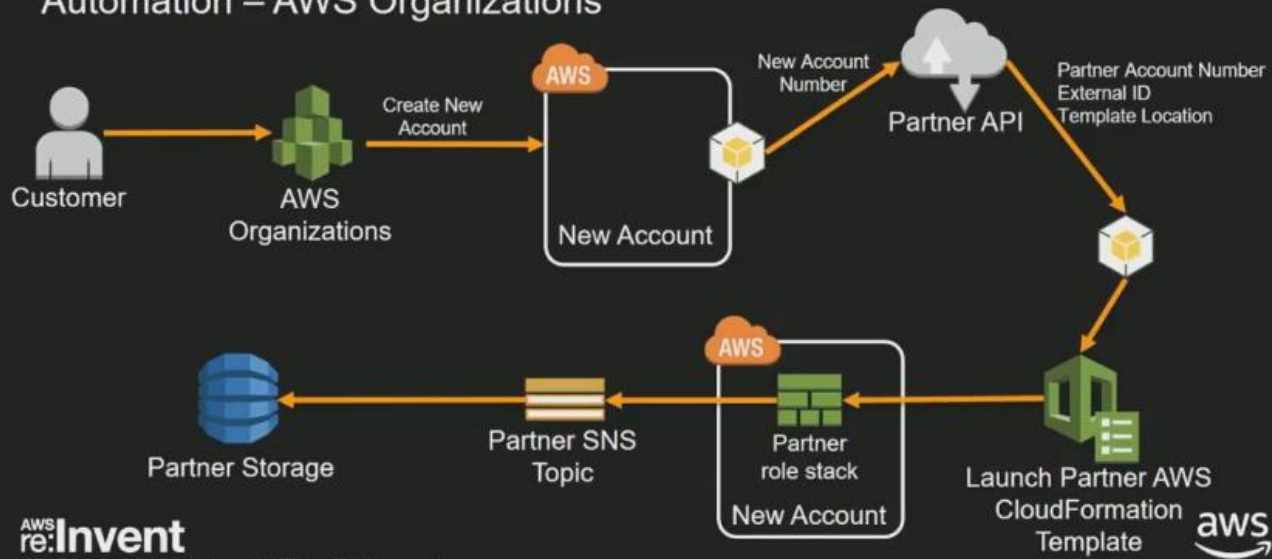
Partner SNS Topic

aws

We then get the stack ARN information back from the user by defining a custom resource defined by a SNS topic.

Cross Account Roles

Automation – AWS Organizations



This is for customers having multiple accounts strategy like for Dev, Test, Prod

Cross Account Roles

Automating the Creation of Cross Account Roles

Why should I take this approach?

- Less steps for the customer to understand.
- Enables customer and partner to easily be at the right security configuration.
- Ensures consistency across all the partners customers.
- Enables automation for setup of many accounts.

AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

When Should I Create an IAM User?

When should I create an IAM user?

- Need programmatic access from a resource that is not housed in AWS.
- Individual user needs access and you are not linked into an identity provider yet.
- You want to enforce MFA on specific API calls.
- You want to enable longer lived sessions at the command line level (get-federated-token).
- Break Glass.

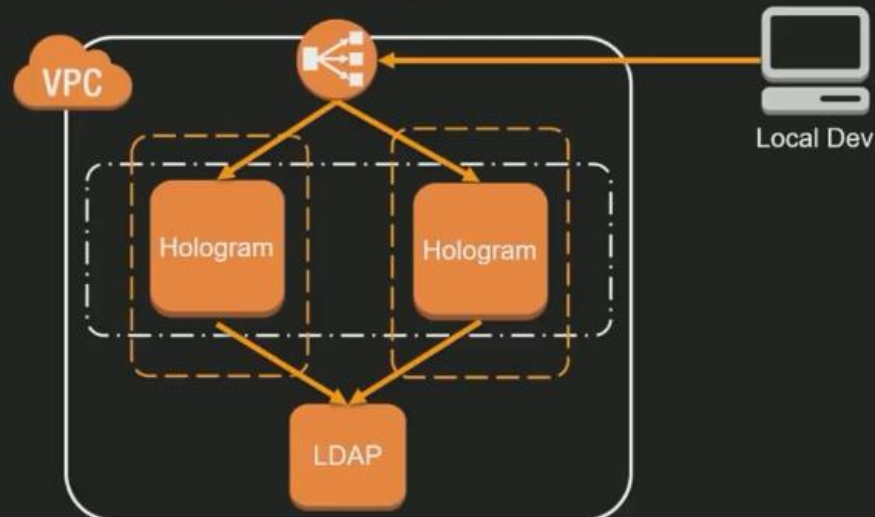
AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Federation and the Command Line

<https://github.com/AdRoll/hologram>



AWS
re:Invent

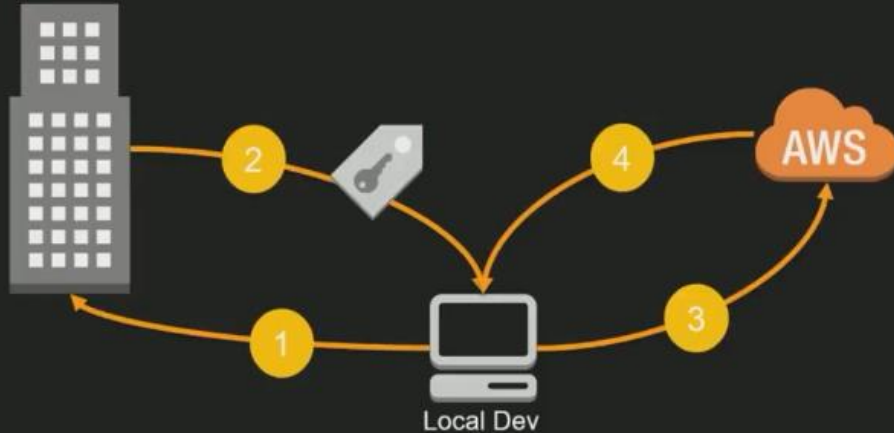
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Federation and the Command Line

<https://github.com/rapid7/awsaml>

Identity Provider



AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Local Dev

aws

Amazon Macie



Amazon Macie – Not just for S3!

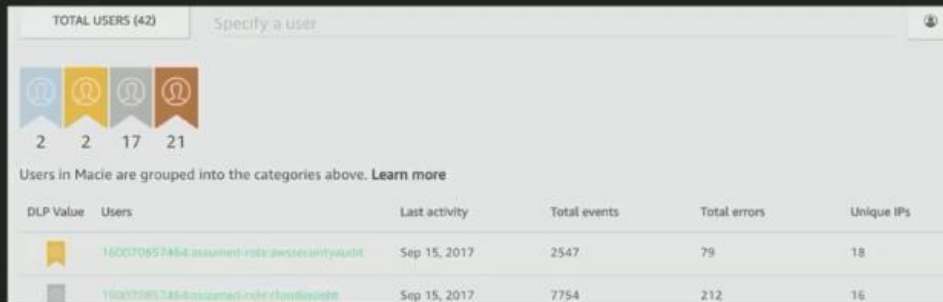
- User Behavior Analytics (UBA) applied to IAM User Activity
- Applies AI to understand historical data access patterns and automatically assesses activity of users, applications and service accounts.



Amazon Macie

Privileged User Identification and Tracking

- Helps classify privileged users into Platinum, Gold, Silver, Bronze
- See total number of user sessions, see whose assuming roles, etc.
- Find the needle in the haystack, see what API calls are never used

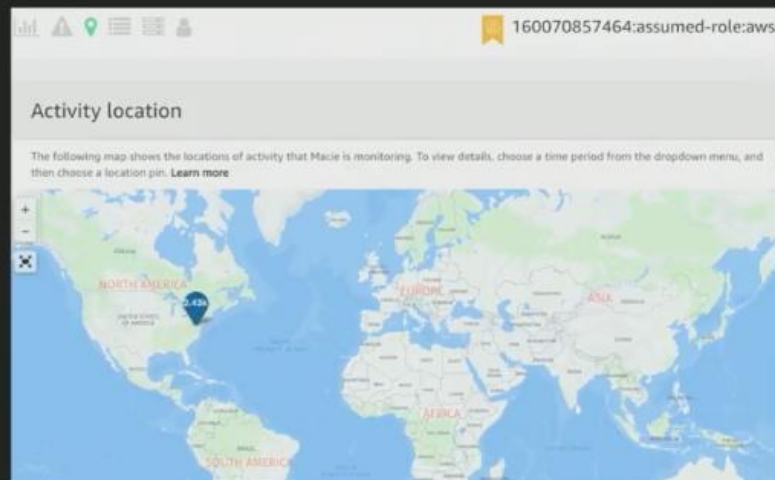


AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Visualize Access Globally



AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



User Investigation and Incident Response

- Harness Macie 'Research' feature to Investigate IAM Anomalies
- Macie assigns a risk level between 1 - 10 for each event
- Alert through Amazon CloudWatch Events
 - Respond with AWS Lambda



AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Least Privilege Made Easy

- Eliminate principals who may not need access
- Reduce access sprawl and debt
- Fine-tune policies to their absolute minimum
- Use in conjunction with Access Advisor



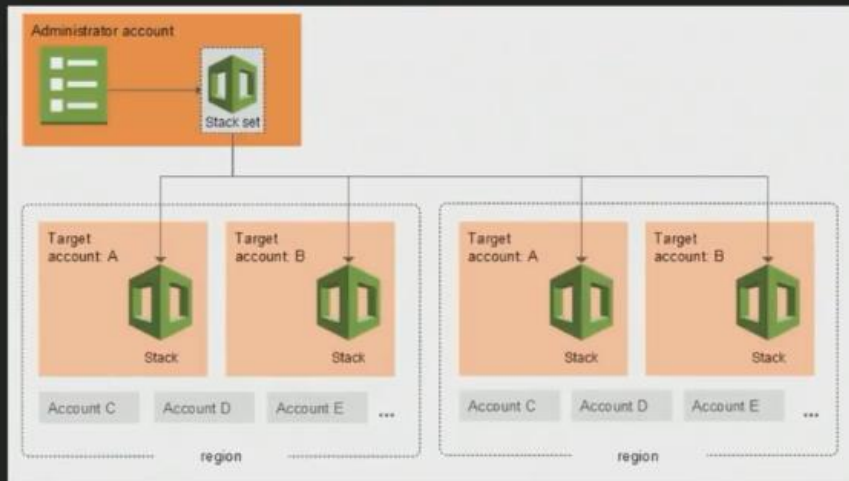
AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Scaling IAM Management

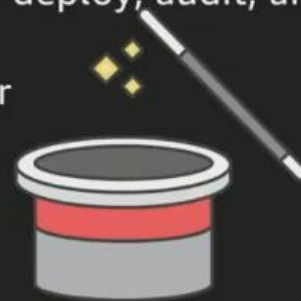
StackSets – Multi-Account AWS CloudFormation



You can now have 1 stack that you can deploy into all your regions and accounts or your entire AWS organization.

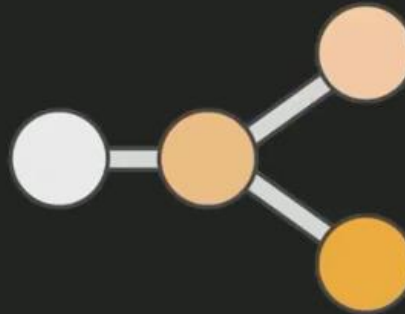
Multiply all the things!

- Create a central IAM Policy CFN – One Stack to Rule them All!
- Multi-Account and Multi-Region via a single click
- ... or Can deploy across your entire AWS Organization
- Removes the friction of IAM management across N-accounts
- Integrate into your CI/CD process to quickly deploy, audit, and collaborate
 - Maintain full process in AWS CodeStar



1 Deploy, Many Updates

- Central Identity Accounts were always a best practice....but operationally challenging
- Scaling IAM Roles/Policies across N-Accounts is now approachable
- Keep Control Central



AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Easily Scale Central Identity Accounts



AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Central Identity Deployment with AWS CloudFormation StackSets

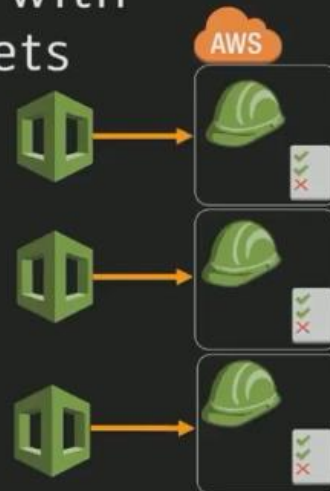


AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

Central Identity Deployment with AWS CloudFormation StackSets



AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

We can replace this as below with a single shareable stackset

Central Identity Deployment with AWS CloudFormation StackSets

StackSet



AWS



Identity Account

AWS



AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

Config Rules for Easy Compliance

Stop bad IAM hygiene before it's problematic

AWS Config – Building your own IAM CMDB

- Maintain historical context and audit of all IAM changes, creates, deletes
- Tracks actual policy and relationship changes
- Auto-Remediate with Config rules and Lambda



Configuration Details

AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

Config Rules - Maintain IAM Governance



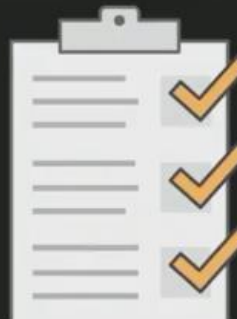
AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Config Rules – DevSecOps for IAM

- Use Lambda to create responses to alerts via Config Rules
 - Hook into HR Systems like Workday or corp directories
 - Suspend principals who violate rules
 - Create Guard Rails that align to corporate governance
- Rules are Evaluated constantly to give a binary compliant or non-compliant state



AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



What's New in IAM?

Roughly the last six months

IAM, What's New?

- Additional IAM Policy resource summaries
- IAM Support for Auto-Scaling actions
- Manage RDS MySQL and Aurora access using IAM
- Service Linked Roles
- IAM Policy Summaries

AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



CLICK TO ADD TEXT

AWS
re:Invent

THANK YOU!

CLICK TO ADD TEXT



AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

