SENTINEL®

Modern Identity Strategies to Securely Manage Your Cloud Infrastructure

SANS Cloud Security Summit

SANS

Michael Soule
@MySnozzberries

X.500

Foundation of Active Directory

Helps define what is a “digital identity”

In some form of use in every business

1930s

1980s

1990s

2000s

Social Security Numbers

Standard for nearly 100 years

$2.3B Identity Theft Services Industry

Very Common Issue

Kerberos

Solves auth to resources

Requires a common Key Dist. Center

Business to business trust is tricky

Modern Auth

Abstraction of auth for use on the web

Simplifies inter-organization trusts

Separation of identity and resources

AWS **Accounts** are Segmentation Boundaries

This includes **Users, Roles, & Policies**

Service Provider (SP) Accepts SAML assertions signed by the **Identity Provider (IdP)**

Policies have a many to many relationship with **Roles** & **Users**

Services can assume **Roles** in **Accounts** as well

AWS Account
Segmented service tenants

IAM Role
Associates a **Policy** with an acting **Principal**

Identity & Access Management (IAM) Policy
Defines specific **Actions** to specific **Resources** with specific **Conditions**

Lambda
Compute platform that executes code on triggers

Role Assumption

Alice's credentials in an **Identity Account** provide access in all accounts

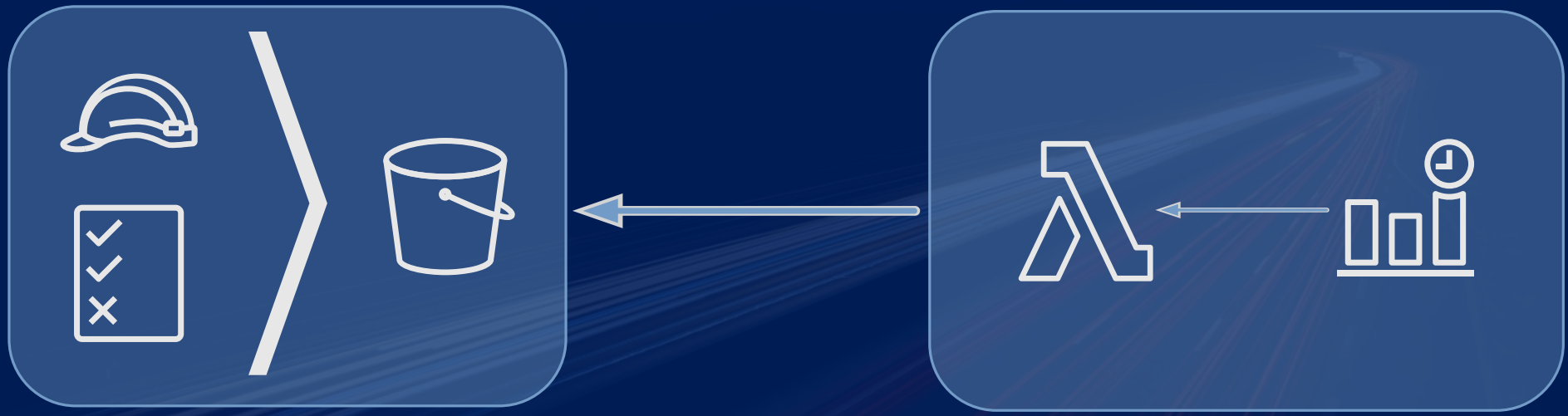
Use SAML

Authentication happens at the **IdP** and the user is assigned a **Role**

Consistent management

across accounts

of **Policies** and **Roles**



Simple Storage Service (S3)
Binary Large OBject (BLOB) storage bucket

CloudWatch Event
Time based event trigger, similar to Cron

Encourages good scripting practices

Experience with current trends

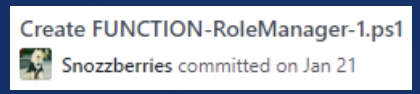
1 Million

Free requests per month per account

Purpose built “utility server”

Direct integration with other services

Demo

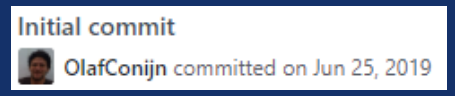


Code: https://bit.ly/2T9DTJK

https://github.com/Snozzberries/AWS-Role-Manager

Blog: https://bit.ly/36cUp1a

https://adamtheautomator.com/aws-lambda-powershell



Organization Formation https://bit.ly/2zEmv9f

https://github.com/OlafConijn/AwsOrganizationFormation

Organization CloudFormation StackSets https://go.aws/2zFDjgf

https://aws.amazon.com/blogs/aws/new-use-aws-cloudformation-stacksets-for-multiple-accounts-in-an-aws-organization/

Azure AD Integration with AWS for SAML https://bit.ly/2AA9zSd

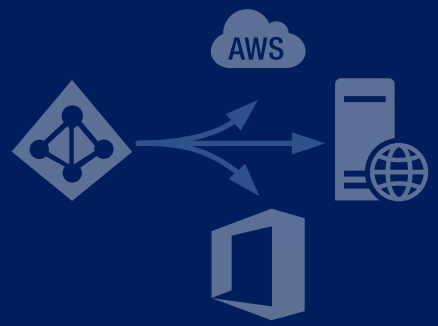
https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/aws-multi-accounts-tutorial

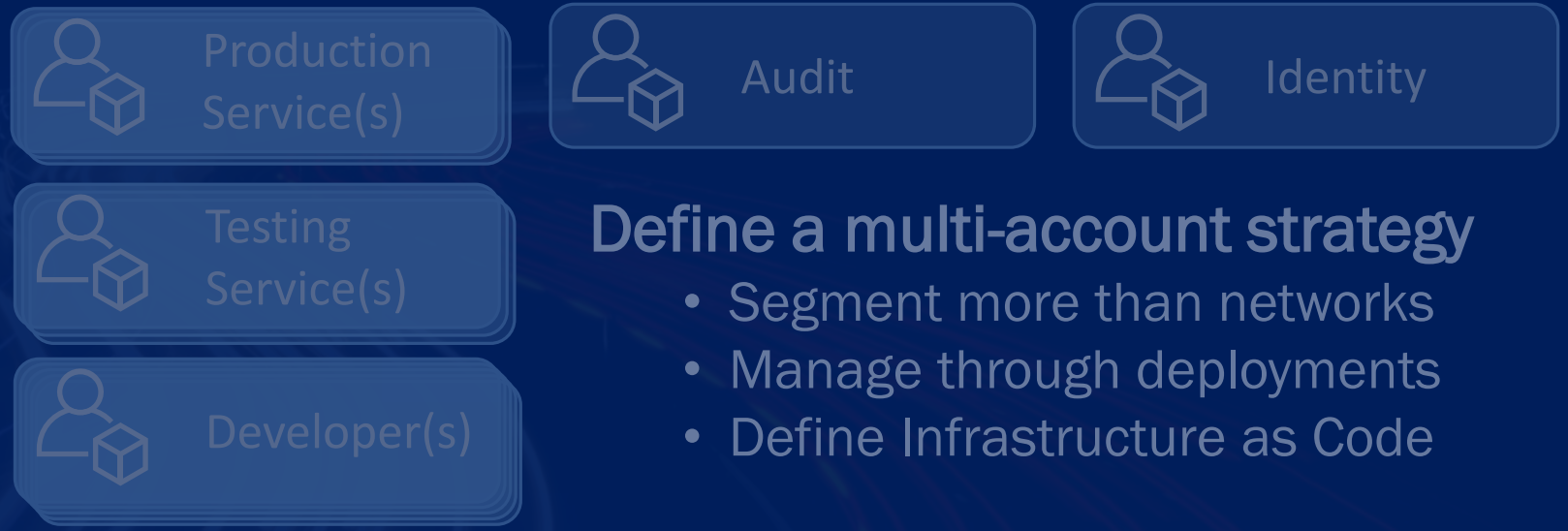
Reach out to me:

Mike Soule - misoule@sentinel.com - @MySnozzberries

Define a federation strategy

- Deploy an Identity Provider (IdP)





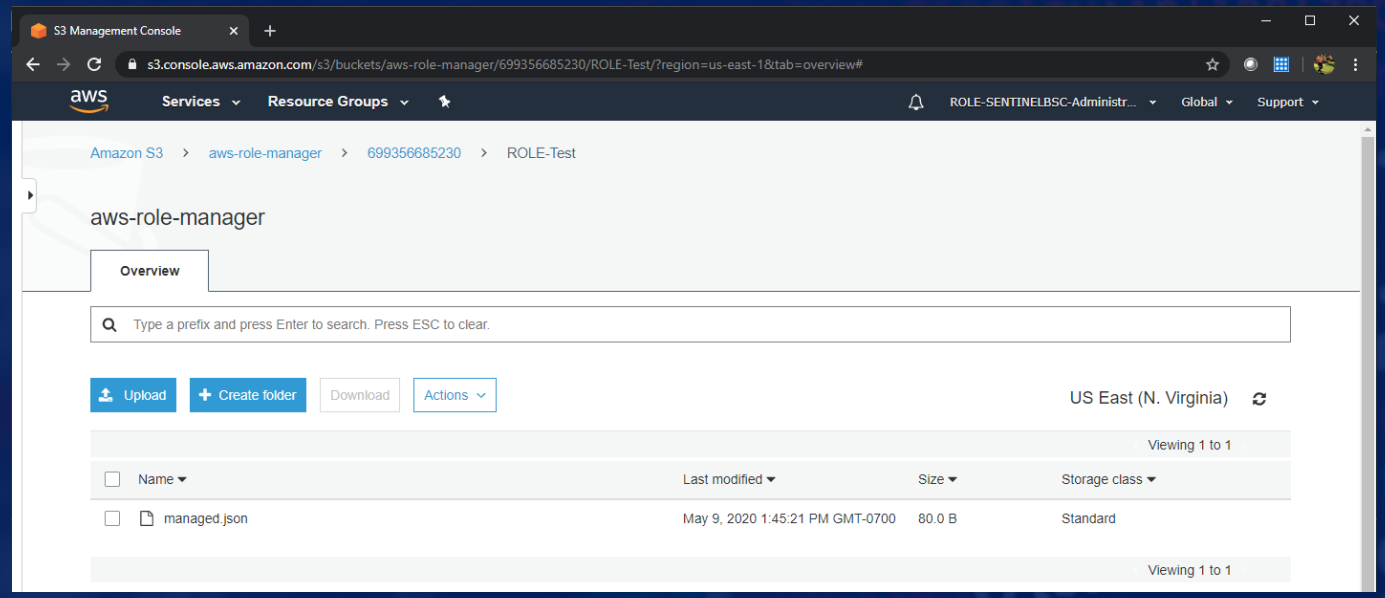
Define a multi-account strategy

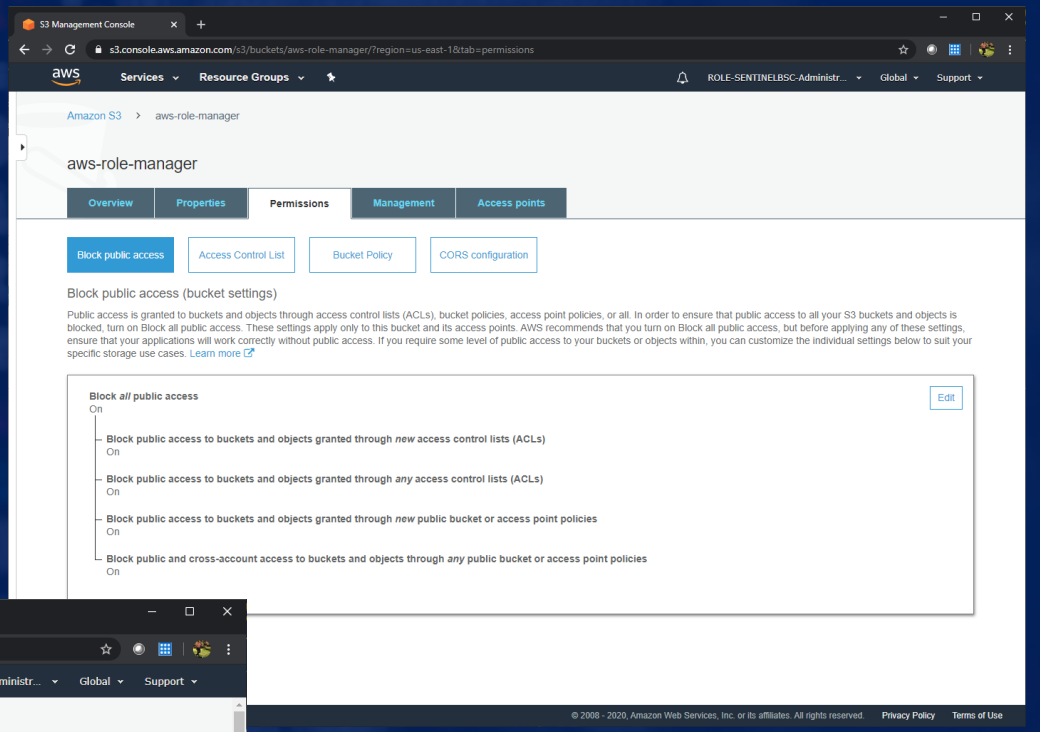
- Segment more than networks
- Manage through deployments
- Define Infrastructure as Code

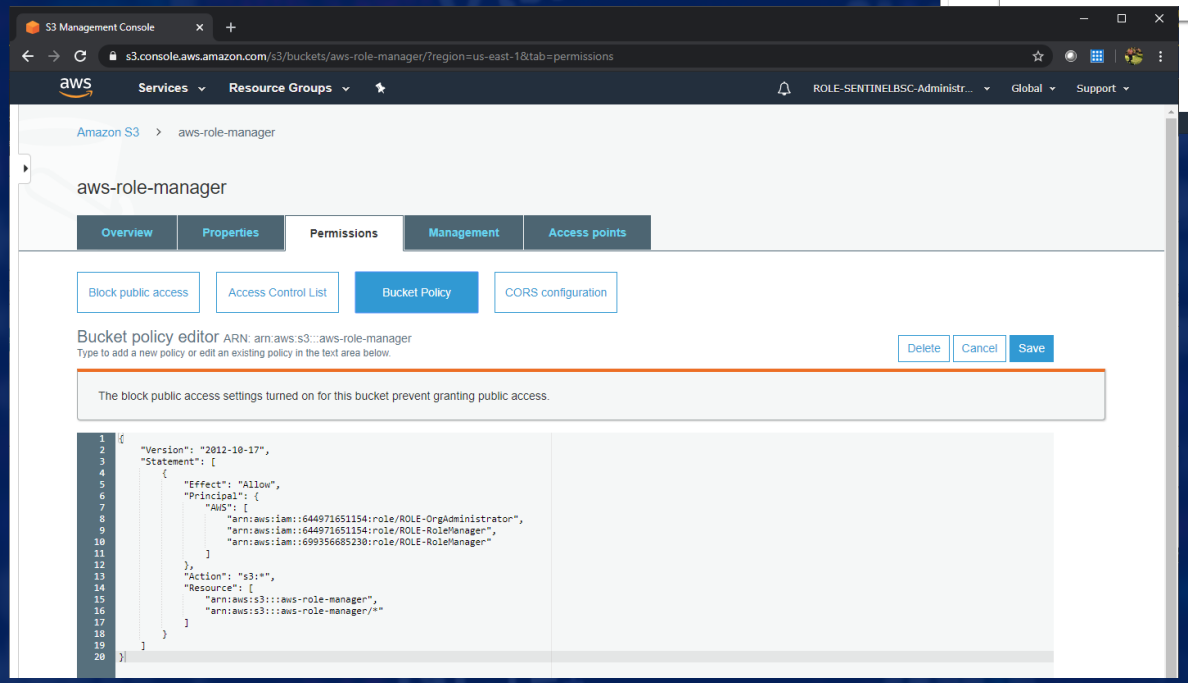
Use specific permissions

- Use single purpose policies
- Add to preventative maintenance

Code Demo – S3 Config

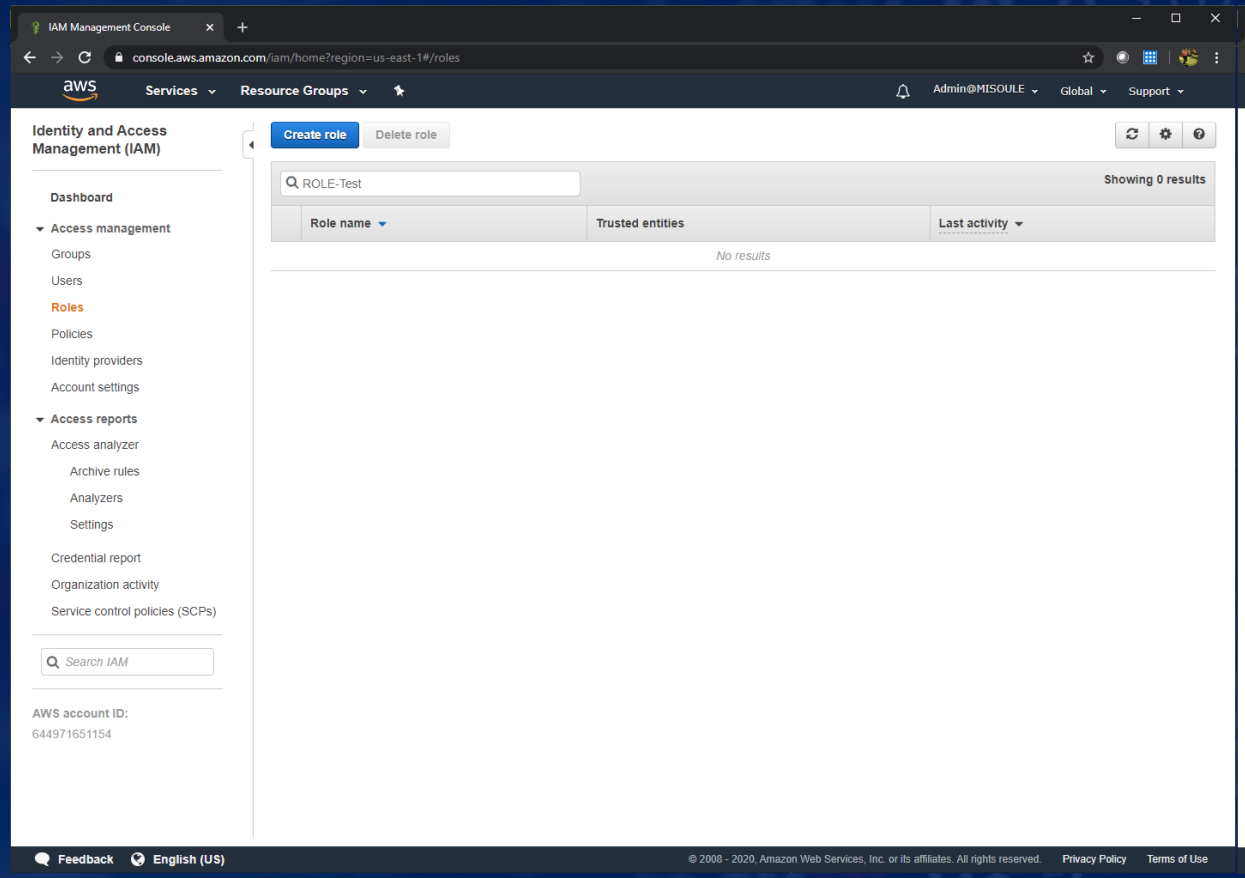


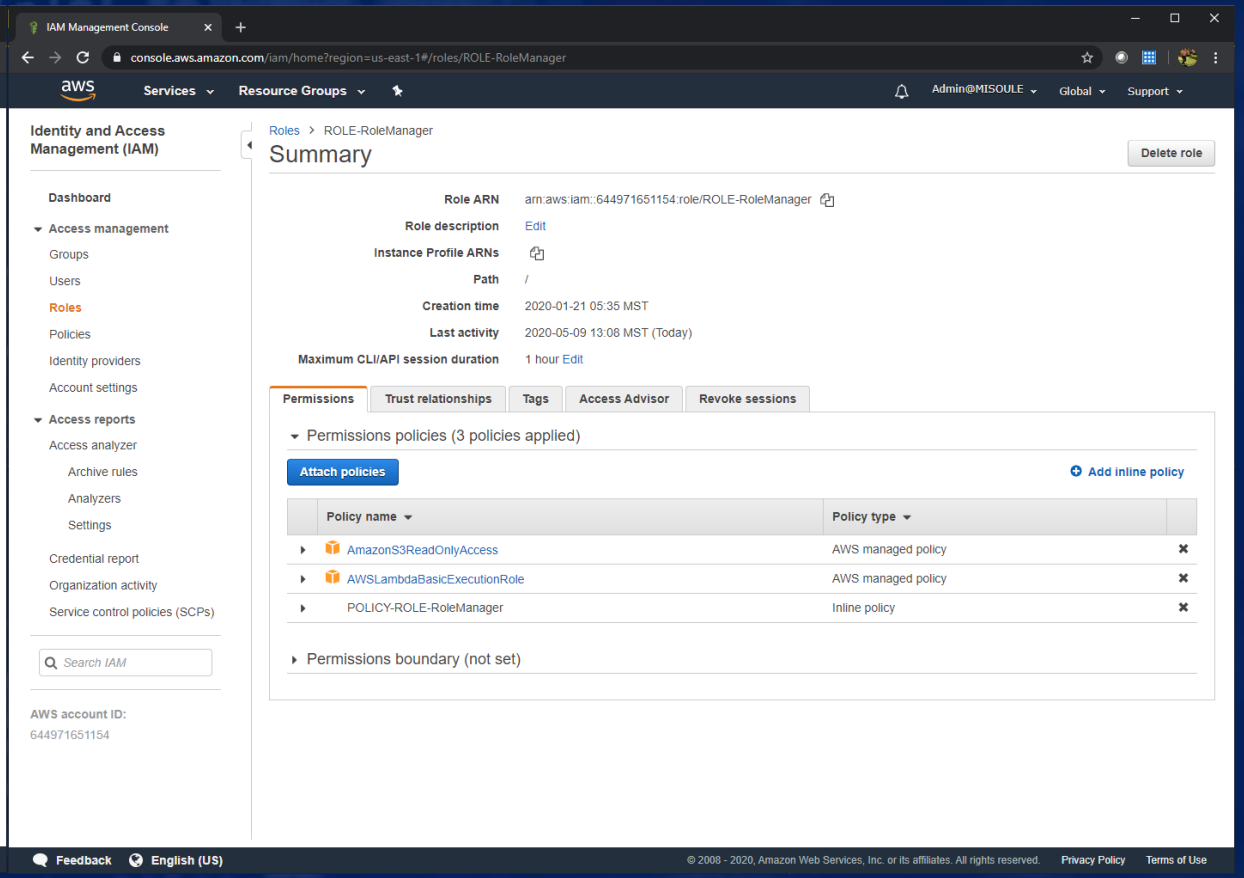


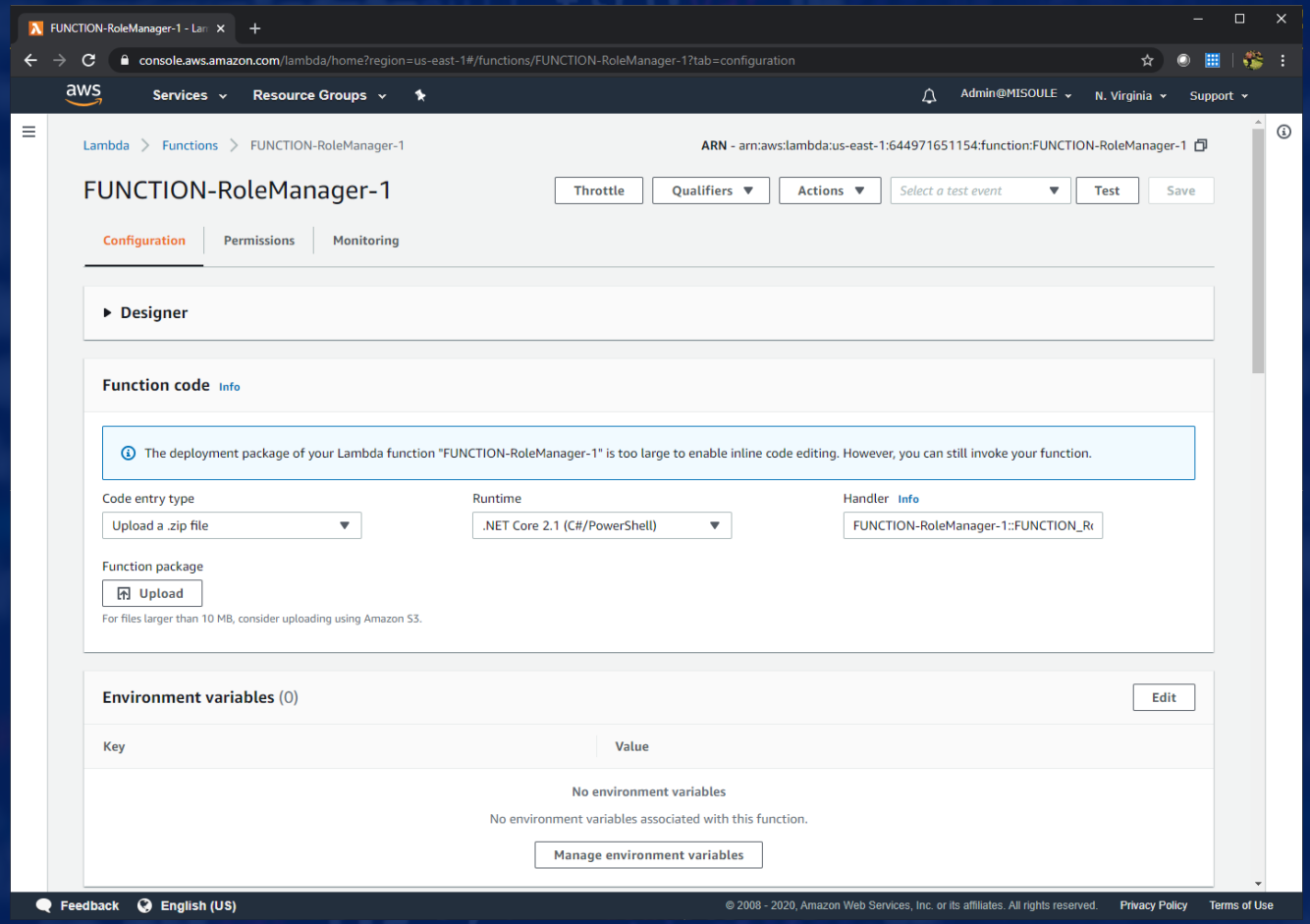


SENTINEL®

Code Demo – IAM Config






FUNCTION-RoleManager-1 - Lar
console.aws.amazon.com/lambda/home?region=us-east-1#/functions/FUNCTION-RoleManager-1?tab=configuration
aws
Services
Resource Groups
Admin@MISOULE
N. Virginia
Support
Lambda
Functions
FUNCTION-RoleManager-1
ARN - arn:aws:lambda:us-east-1:644971651154:function:FUNCTION-RoleManager-1
FUNCTION-RoleManager-1
Throttle
Qualifiers
Actions
Select a test event
Test
Save
Configuration
Permissions
Monitoring
Designer
Function code Info
The deployment package of your Lambda function "FUNCTION-RoleManager-1" is too large to enable inline code editing. However, you can still invoke your function.
Code entry type
Upload a .zip file
Runtime
.NET Core 2.1 (C#/PowerShell)
Handler Info
FUNCTION-RoleManager-1::FUNCTION_R
Function package
Upload
For files larger than 10 MB, consider uploading using Amazon S3.
Environment variables (0)
Edit
Key
Value
No environment variables
No environment variables associated with this function.
Manage environment variables
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

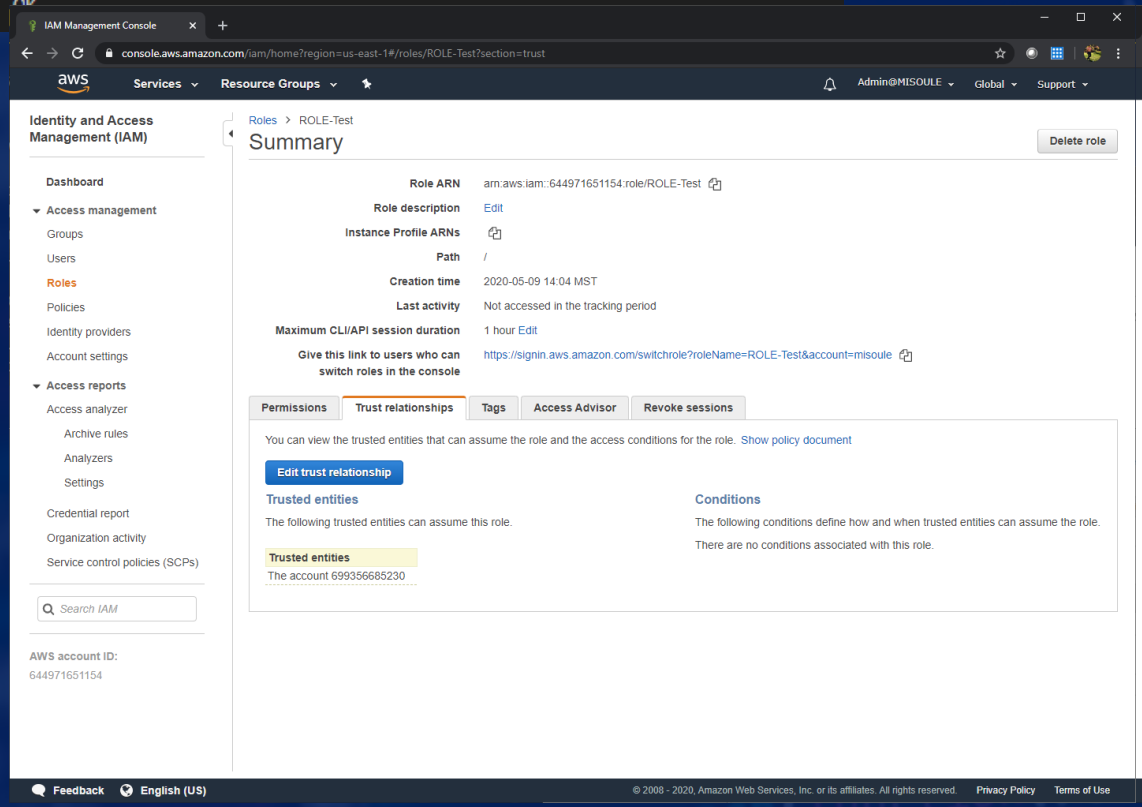
Code Demo – Show me the money!

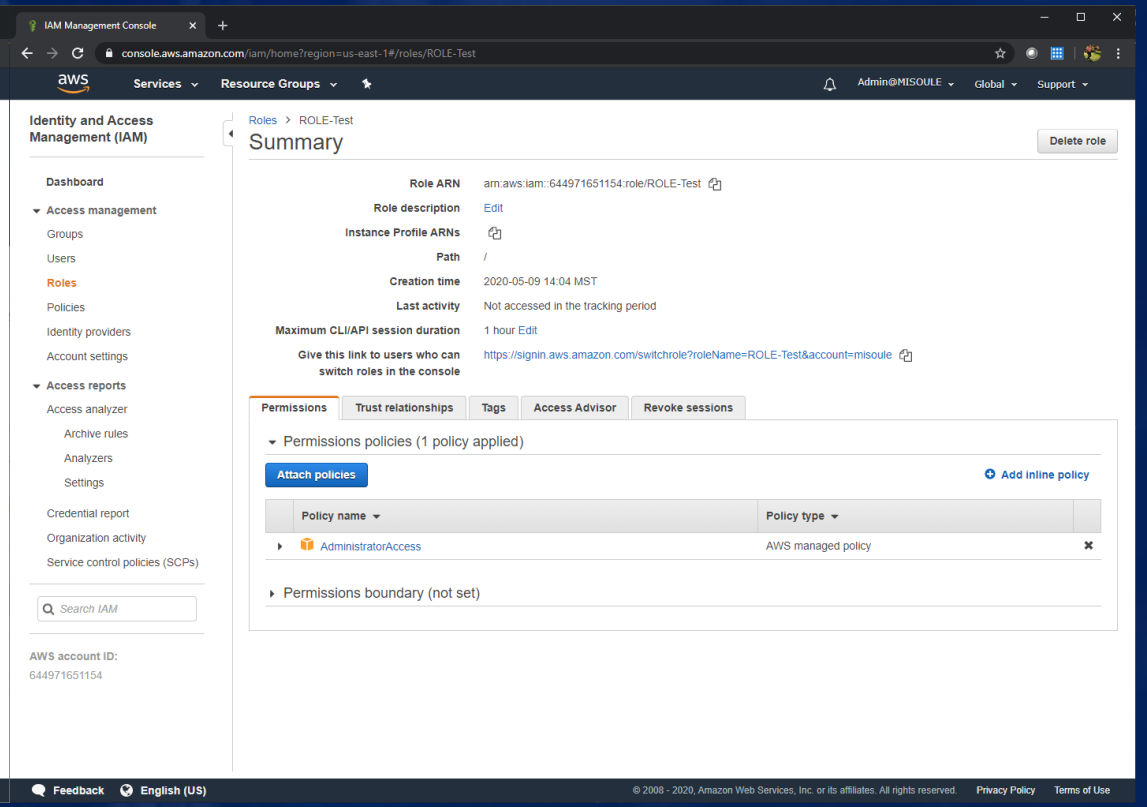

```
PS C:\Users\Mike.SOULE> Get-Date;Invoke-LMFunction -FunctionName FUNCTION-RoleManager-1


Saturday, May 9, 2020 14:04:59

LoggedAt          : 5/9/2020 14:05:00
ExecutedVersion   : $LATEST
FunctionError     : Unhandled
LogResult         :
Payload           : System.IO.MemoryStream
StatusCode        : 200
ResponseMetadata  : Amazon.Runtime.ResponseMetadata
ContentLength     : 2788
HttpStatusCode    : OK
```

S3 Management Console — https://aws-role-manager.s3.us-e

aws-role-manager.s3.us-east-1.amazonaws.com/699356685230/ROLE-Test/managed.json?r

```
{
    "arn": [
        "arn:aws:iam::aws:policy/AdministratorAccess"
    ]
}
```





Code Demo – It worked!