



# Modern Identity Strategies to Securely Manage Your Cloud Infrastructure

SANS Cloud Security Summit



Michael Soule  
@MySnozzberries

1930s

### Social Security Numbers

Standard for nearly 100 years  
\$2.3B Identity Theft Services Industry  
Very Common Issue

1980s

### X.500

Foundation of Active Directory  
Helps define what is a “digital identity”  
In some form of use in every business

1990s

### Kerberos

Solves auth to resources  
Requires a common Key Dist. Center  
Business to business trust is tricky

2000s

### 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

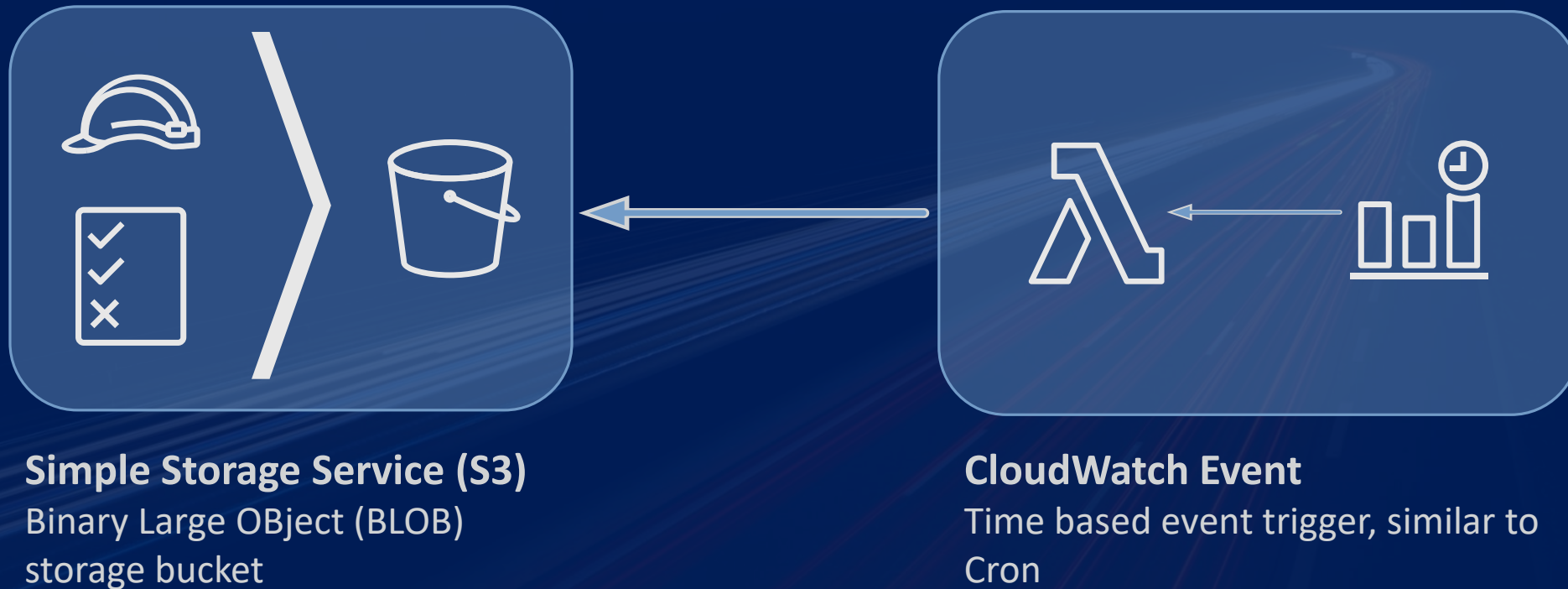
Alice's credentials in an **Identity Account** provide access in all accounts

## Use SAML

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



Consistent management  
across accounts  
of **Policies** and **Roles**



Encourages good  
scripting practices

Experience with  
current trends

**1 Million**

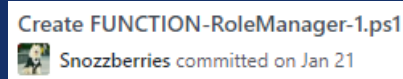
Free requests per  
month per account

Purpose built  
“utility server”

Direct integration  
with other services



# Demo



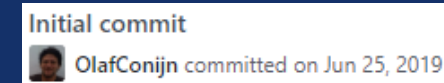
Code: <https://bit.ly/2T9DTJK>

<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>

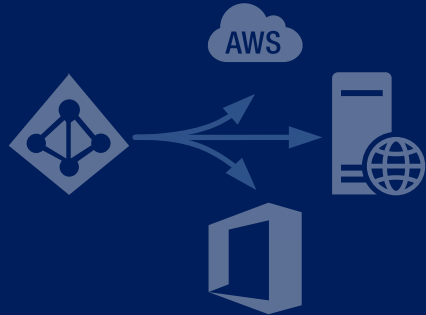
Reach out to me:

Mike Soule - [misoule@sentinel.com](mailto:misoule@sentinel.com) - @MySnozzberries



## Define a federation strategy

- Deploy an Identity Provider (IdP)



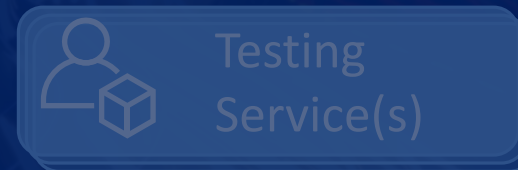
Production  
Service(s)



Audit



Identity



Testing  
Service(s)



Developer(s)

## 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



x100s



x1



x10s



x100s

S3 Management Console

s3.console.aws.amazon.com/s3/buckets/aws-role-manager/699356685230/ROLE-Test/?region=us-east-1&tab=overview#

ServicesResource Groups

Amazon S3 > aws-role-manager > 699356685230 > ROLE-Test

aws-role-manager

Overview

Q Type a prefix and press Enter to search. Press ESC to clear.

UploadCreate folderDownloadActions

US East (N. Virginia)

Viewing 1 to 1

<input type="checkbox"/>	Name	Last modified	Size	Storage class
<input type="checkbox"/>	managed.json	May 9, 2020 1:45:21 PM GMT-0700	80.0 B	Standard

Viewing 1 to 1

S3 Management Console

s3.console.aws.amazon.com/s3/buckets/aws-role-manager/?region=us-east-1&tab=permissions

ServicesResource Groups

Amazon S3 > aws-role-manager

aws-role-manager

OverviewPropertiesPermissionsManagementAccess points

Block public accessAccess Control ListBucket PolicyCORS configuration

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

On

Block public access to buckets and objects granted through new access control lists (ACLs)

On

Block public access to buckets and objects granted through any access control lists (ACLs)

On

Block public access to buckets and objects granted through new public bucket or access point policies

On

Block public and cross-account access to buckets and objects through any public bucket or access point policies

On

Edit

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

S3 Management Console

s3.console.aws.amazon.com/s3/buckets/aws-role-manager/?region=us-east-1&tab=permissions

ServicesResource Groups

Amazon S3 > aws-role-manager

aws-role-manager

OverviewPropertiesPermissionsManagementAccess points

Block public accessAccess Control ListBucket PolicyCORS configuration

Bucket policy editor ARN: arn:aws:s3:::aws-role-manager

Type to add a new policy or edit an existing policy in the text area below.

The block public access settings turned on for this bucket prevent granting public access.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": [
8           "arn:aws:iam::644971651154:role/ROLE-OrgAdministrator",
9           "arn:aws:iam::644971651154:role/ROLE-RoleManager",
10          "arn:aws:iam::699356685230:role/ROLE-RoleManager"
11        ]
12      },
13      "Action": "s3:*",
14      "Resource": [
15        "arn:aws:s3:::aws-role-manager",
16        "arn:aws:s3:::aws-role-manager/*"
17      ]
18    }
19  ]
20 }
```

SENTINEL

16

Identity and Access Management (IAM)

Dashboard

Access management

- Groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
  - Archive rules
  - Analyzers
  - Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Search IAM

AWS account ID: 644971651154

Create role

Delete role

ROLE-Test

Showing 0 results

Role name	Trusted entities	Last activity
No results		

Identity and Access Management (IAM)

Dashboard

Access management

- Groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
  - Archive rules
  - Analyzers
  - Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Search IAM

AWS account ID: 644971651154

Roles > ROLE-RoleManager

Summary

Delete role

Role ARN

Role description

Instance Profile ARNs

Path

Creation time

Last activity

Maximum CLI/API session duration

Permissions

Trust relationships

Tags

Access Advisor

Revoke sessions

Permissions policies (3 policies applied)

Attach policies

Add inline policy

Policy name	Policy type	
AmazonS3ReadOnlyAccess	AWS managed policy	
AWSLambdaBasicExecutionRole	AWS managed policy	
POLICY-ROLE-RoleManager	Inline policy	

Permissions boundary (not set)

Feedback

English (US)

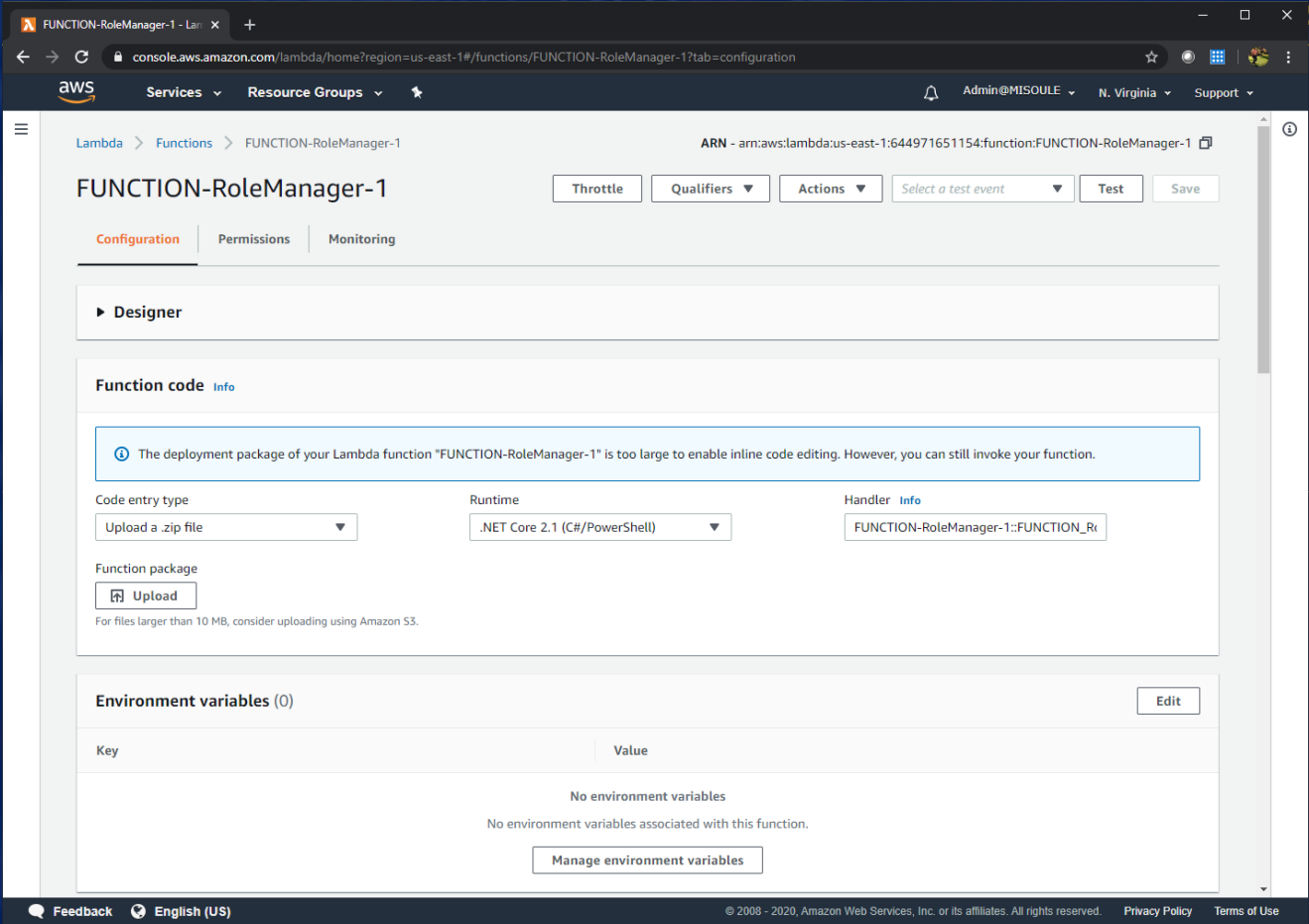
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use





```
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
```

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

Identity and Access Management (IAM)

Dashboard

Access management

Groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analizers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Search IAM

AWS account ID: 644971651154

Roles > ROLE-Test

Summary

Role ARN

Role description

Instance Profile ARNs

Path

Creation time

Last activity

Maximum CLI/API session duration

Give this link to users who can switch roles in the console

Permissions

Trust relationships

Tags

Access Advisor

Revoke sessions

You can view the trusted entities that can assume the role and the access conditions for the role.

Edit trust relationship

Trusted entities

The following trusted entities can assume this role.

The account 699356685230

Conditions

The following conditions define how and when trusted entities can assume the role.

There are no conditions associated with this role.

Identity and Access Management (IAM)

Dashboard

Access management

Groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analizers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Search IAM

AWS account ID: 644971651154

Roles > ROLE-Test

Summary

Role ARN

Role description

Instance Profile ARNs

Path

Creation time

Last activity

Maximum CLI/API session duration

Give this link to users who can switch roles in the console

Permissions

Trust relationships

Tags

Access Advisor

Revoke sessions

Permissions policies (1 policy applied)

Attach policies

Add inline policy

Policy name

Policy type

AdministratorAccess

AWS managed policy

Permissions boundary (not set)

