

IAM Roles Beyond EC2 Instances

Security-in-Depth for AWS

Loïc Simon



Who Am I?

- Loïc Simon
- Principal Security Engineer @ NCC Group
- Author of open-source software
 - Scout2
 - Security Auditing Tool for AWS environments
 - Static analysis of AWS resources
 - Security-oriented views of key resources
 - AWS-recipes
 - Repository of various tools and policies



Goal

- Discuss IAM roles, in particular their use to create a new IAM security model for defense-in-depth



Agenda

- Intro to IAM Roles
 - Authentication in AWS
 - What is an IAM role?
 - Applications of IAM roles
- IAM roles for IAM users
 - Workflow
 - Permissions in IAM
 - Least privilege with IAM Roles



Intro to IAM Roles

- Authentication in AWS
- What is an IAM role?
- Applications of IAM roles



Authentication in AWS

- Identity and Access Management (IAM)
 - AWS' "directory" (users and groups)
 - AWS' access controls (done via policies)
 - IAM credentials valid until user deletes/changes them
- Security Token Service (STS)
 - Issues temporary, limited-privilege credentials
 - STS credentials valid between 15 minutes and 36 hours



What is an IAM Role?

- AWS identity with permissions
 - Inline or managed IAM policies
- Not associated with a single user
 - Assumable by various parties
 - Trust relationship (a.k.a AssumeRole policy)
- No long-lived credentials associated with it
 - Short-lived (STS) credentials issued when requested



What is an IAM Role?

- AWS identity with permissions
 - Inline or managed IAM policies

Policy #1

- Not associated with a single user

- Assumable by various parties
 - Trust relationship (a.k.a AssumeRole policy)

Policy #2

- No long-lived credentials associated with it
 - Short-lived (STS) credentials issued when requested



Reminder about IAM policies

- Policy
 - Set of permissions defined as a list of statements
 - JSON
- Statement
 - Rule defined by
 - Effect: Allow or Deny
 - Action
 - Resource: object the action applies to
 - Condition

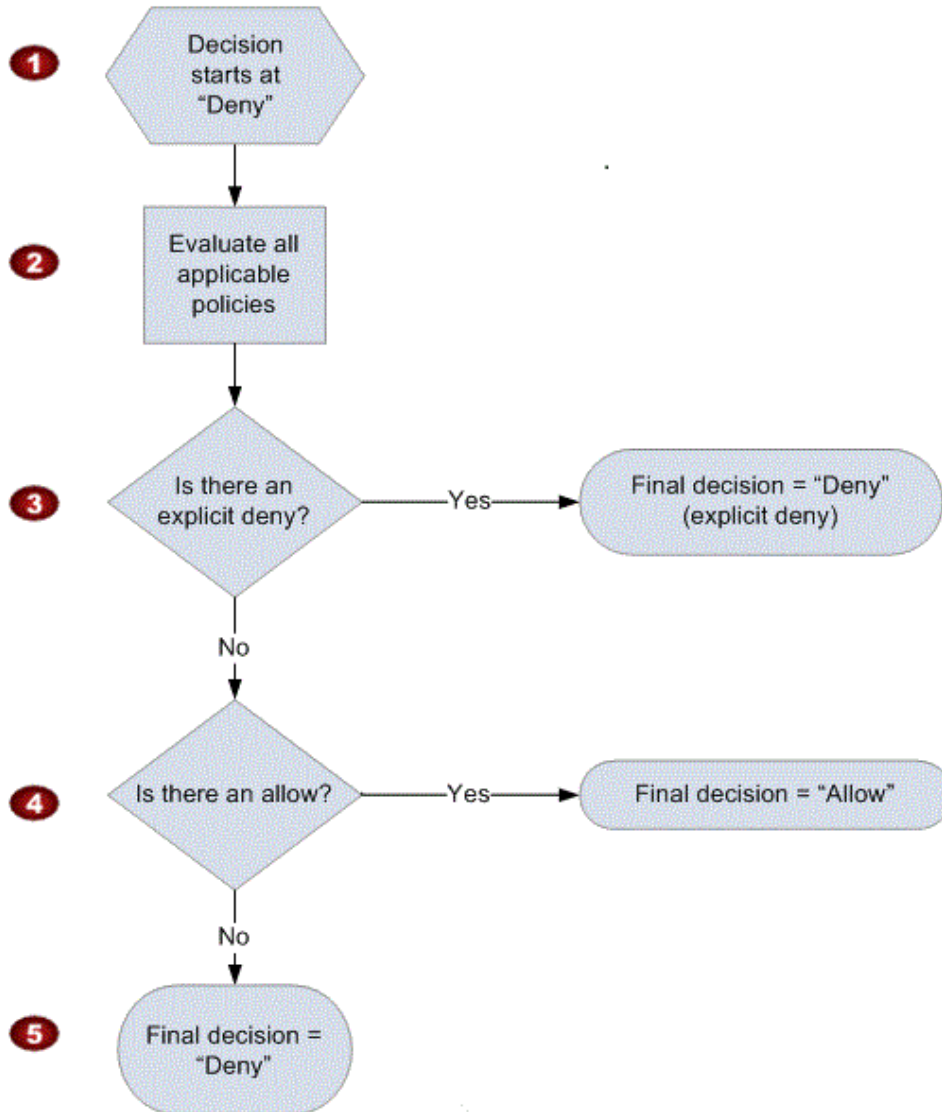


Reminder about IAM policies

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "ec2:*",  
      "Resource": "*"   
    },  
  ]  
}
```



Reminder about IAM policies



Trust Relationship

- Syntax similar to IAM policy's syntax
- Only one AssumeRole policy per IAM role
- Principal must be specified
- Resource is implicit (Role's ARN)
- Action can only be a subset of
 - [AssumeRole](#)
 - [AssumeRoleWithSAML](#)
 - [AssumeRoleWithWebIdentity](#)



What is a Principal?

- The entity who is allowed access to the actions and resources in the statement.



What is a Principal?

- Everyone
 - "*"
 - {"AWS": "*"}



What is a Principal?

- Everyone
 - "*"
 - {"AWS": "*" }
- AWS Account
 - {"AWS": "AWS-account-ID" }
 - {"AWS": "arn:aws:iam::AWS-account-ID:root" }



What is a Principal?

- Everyone
 - "*"
 - {"AWS": "*" }
- AWS Account
 - {"AWS": "AWS-account-ID" }
 - {"AWS": "arn:aws:iam::AWS-account-ID:root" }
- IAM user or role
 - {"AWS": "arn:aws:iam::AWS-account-ID:user/loic" }



What is a Principal?

- Everyone
 - "*"
 - {"AWS": "*" }
- AWS Account
 - {"AWS": "AWS-account-ID" }
 - {"AWS": "arn:aws:iam::AWS-account-ID:root" }
- IAM user or role
 - {"AWS": "arn:aws:iam::AWS-account-ID:user/loic" }
- Identity Provider
 - {"Federated": "arn:aws:iam::AWS-account-ID:saml-provider/SAML" }



What is a Principal?

- Everyone
 - "*"
 - {"AWS": "*" }
- AWS Account
 - {"AWS": "AWS-account-ID" }
 - {"AWS": "arn:aws:iam::AWS-account-ID:root" }
- IAM user or role
 - {"AWS": "arn:aws:iam::AWS-account-ID:user/loic" }
- Identity Provider
 - {"Federated": "arn:aws:iam::AWS-account-ID:saml-provider/SAML" }
- AWS Service
 - {"service": "ec2.amazonaws.com" }



Trust Relationship

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "ec2.amazonaws.com",  
        "AWS": "arn:aws:iam::936728503675:root"  
      },  
      "Action": [  
        "sts:AssumeRole",  
        "sts:AssumeRoleWithSAML",  
        "sts:AssumeRoleWithWebIdentity"  
      ]  
    }  
  ]  
}
```



Trust Relationship vs. IAM Policy

- IAM Policy
 - Defines what actions a role can do
- Trust Relationship
 - Defines who can assume the role
- How does one affect the other?



Trust Relationship vs. IAM Policy

User's IAM permissions Allow AssumeRole	Role's Trust Relationship Allows AssumeRole	User can AssumeRole
No	No	No
Yes	No	No
No	Yes	No
Yes	Yes	Yes



Trust Relationship vs. IAM Policy

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "sts:AssumeRole",  
      "Resource": "*" }  
  ]  
}
```

User's permissions

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "sts:AssumeRole",  
      "Principal": { "Service": "ec2.amazonaws.com" } }  
  ]  
}
```

Role's trust relationship



Trust Relationship vs. IAM Policy

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "sts:AssumeRole",  
      "Resource": "*" }  
  ]  
}
```

User's permissions

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "sts:AssumeRole",  
      "Principal": { "Service": "ec2.amazonaws.com" } }  
  ]  
}
```

Role's trust relationship

User cannot assume role



Trust Relationship vs. IAM Policy

- IAM Users
 - Require two authorizations
 - IAM Permissions
 - Role's Trust Relationship
- Other Principals
 - Only limited by Role's Trust Relationship



Applications of IAM Roles

- Amazon application or service (EC2, Lambda, EMR, ..)
 - No need to share and maintain long-term credentials
- Cross-account access
 - No need to maintain a user base for vendors/partners
- Users (IAM, SAML)
 - Federated Users (SAML)
 - IAM Users



Example: IAM role with EC2 instance

- Pass an IAM role to EC2 instance at creation time
- Manual inspection
 - SSH/RDP into the EC2 instance
 - Browse to instance's metadata URL
<http://169.254.169.254/latest/meta-data/iam/security-credentials>
 - If you wait long enough, AWS will rotate the credentials
- Application
 - Use an AWS-SDK and instantiate an API client



Example: IAM Role For Federated Users

- Create an Identity Provider in AWS
 - Upload metadata document
- Configure IdP with Role's ARN
- IdP sends signed SAML assertion
- AWS returns STS credentials



Example: IAM Role For Federated Users

- Pros
 - Single user database (rely on LDAP/AD groups)
 - On/off boarding, group changes automatically reflected
 - No long-lived creds in AWS (use those in LDAP/AD)
- Cons
 - Trust domain crossing (corp/IT vs. prod)
 - No MFA (rely on Identity Provider)
 - Harder to work with CLI (need to build custom tools)



Applications of IAM Roles

- Amazon application or service (EC2, Lambda, EMR, ..)
 - No need to share and maintain long-term credentials
- Cross-account access
 - No need to maintain a user base for vendors/partners
- Users (IAM, SAML)
 - Federated Users (SAML)
 - IAM Users

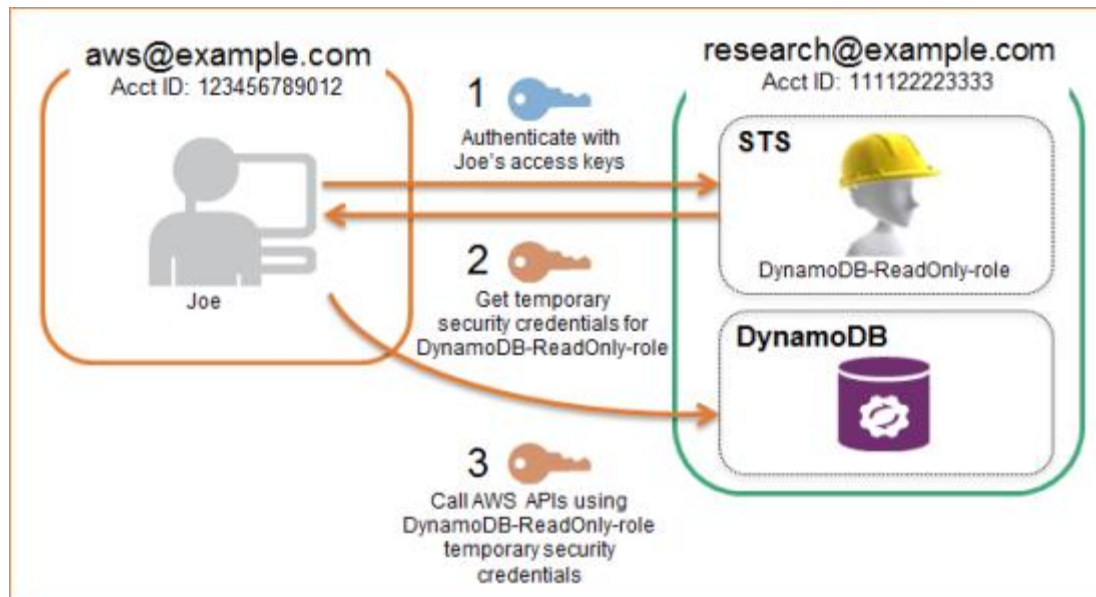


IAM Roles for IAM Users

- Workflow
- Traditional authorization scheme in IAM
- Least-Privileges with IAM Roles



Workflow



Traditional Authorization Scheme

- IAM users
 - Have no inline / managed policies
 - Inherit permissions from group memberships
- IAM groups
 - Have managed policies
 - Have no inline policies



Traditional Authorization Scheme

The screenshot displays the AWS IAM console interface. The top navigation bar includes 'AWS', 'Services', and 'Edit'. The user profile 'Isimon @ Isec-pso' and regional settings 'Global' and 'Support' are visible. The left sidebar contains navigation options: Dashboard, Search IAM, Details, Groups, Users (highlighted), Roles, Policies, Identity Providers, Account Settings, Credential Report, and Encryption Keys. The main content area shows the path 'IAM > Users > TestUser1' and a 'Summary' section with the following details:

- User ARN:** arn:aws:iam::936728503675:user/TestUser1
- Has Password:** No
- Groups (for this user):** 3
- Path:** /
- Creation Time:** 2016-09-21 17:40 EDT

Below the summary, there are tabs for 'Groups', 'Permissions', 'Security Credentials', and 'Access Advisor'. The 'Groups' tab is active, showing a message: 'This view shows all groups the User belongs to: 3 Groups'. A blue button 'Add User to Groups' is present. A table lists the groups:

Group	Actions
GroupA	
GroupB	
GroupC	

A red arrow points from a red-bordered box containing the text 'Member of 3 groups' to the group list table.

At the bottom of the console, there are links for 'Feedback', 'English', and a footer with copyright information: '© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.' along with 'Privacy Policy' and 'Terms of Use'.

Traditional Authorization Scheme

The screenshot shows the AWS IAM console interface. The breadcrumb navigation is IAM > Users > TestUser1. The 'Summary' section displays the following details:

- User ARN: arn:aws:iam::936728503675:user/TestUser1
- Has Password: No
- Groups (for this user): 3
- Path: /
- Creation Time: 2016-09-21 17:40 EDT

The 'Permissions' tab is selected, showing a 'Managed Policies' section with the message: 'There are no managed policies attached to this user.' Below this is an 'Attach Policy' button. The 'Group Policies' section contains a table of policies attached to groups that this user is in:

Policy Name	Group Name	Actions
IAMFullAccess	GroupA	Show Policy
AmazonEC2ReadOnlyAccess	GroupB	Show Policy
AmazonS3ReadOnlyAccess	GroupC	Show Policy

The 'Inline Policies' section below shows: 'There are no inline policies to show. To create one, [click here](#).'

A red box highlights the 'List of policies' text, and a red arrow points from this box to the 'IAMFullAccess' policy in the table.



Traditional Authorization Scheme

The screenshot shows the AWS IAM console interface. The breadcrumb navigation is IAM > Users > TestUser1. The 'Summary' tab is active, displaying user details: User ARN (arn.aws.iam.:936728503675:user/TestUser1), Has Password (No), Groups (for this user) (3), Path (/), and Creation Time (2016-09-21 17:40 EDT). Below this, the 'Permissions' tab is selected, showing 'Managed Policies' and 'Group Policies'. A 'Show Policy' dialog box is open, displaying the following JSON:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:*",
      "Resource": "*"
    }
  ]
}
```

A red arrow points from the 'Show Policy' dialog box to the 'Show Policy' button in the 'Group Policies' table below. The table has the following data:

Policy Name	Group Name	Actions
IAMFullAccess	GroupA	Show Policy
AmazonEC2ReadOnlyAccess	GroupB	Show Policy
AmazonS3ReadOnlyAccess	GroupC	Show Policy



Traditional Authorization Scheme

- GroupA
 - User and permissions management
- GroupB
 - Audit of EC2 usage and security groups
- GroupC
 - Read access to S3 buckets



Traditional Authorization Scheme

- GroupA
 - User and permissions management
 - ~ once a week
- GroupB
 - Audit of EC2 usage and security groups
 - ~ once a month
- GroupC
 - Read access to S3 buckets
 - ~ Every day



Traditional Authorization Scheme

At any time

User can do

User needs to do

IAMFullAccess

And

Or

AmazonEC2ReadOnlyAccess

And

Or

AmazonS3ReadOnlyAccess



Least-Privileges with IAM Roles

At any time

User can do

User needs to do

IAMFullAccess

Or

Or

AmazonEC2ReadOnlyAccess

Or

Or

AmazonS3ReadOnlyAccess

- Proposal: use IAM roles



Least-Privileges with IAM Roles

- Create one role corresponding to each group
 - Apply similar permissions
 - Allow same AWS account ID to AssumeRole
- Modify each group's permissions
 - Allow to AssumeRole the corresponding role



Least-Privileges with IAM Roles

The screenshot displays the AWS IAM console interface. The breadcrumb navigation at the top shows 'IAM > Roles > TestRoleIAMFullAccess', with the role name highlighted by a red box. The main content area shows the role's details, including its ARN, path, and creation time. A 'Show Policy' dialog box is overlaid in the center, displaying the following JSON policy document:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:*",
      "Resource": "*"
    }
  ]
}
```

The dialog box also features a 'Cancel' button at the bottom right. In the background, the 'Permissions' tab is active, showing a list of managed policies, with 'IAMFullAccess' highlighted. A red circular graphic is partially visible in the bottom right corner of the image.

Least-Privileges with IAM Roles

Dashboard

Search IAM

Details

Groups

Users

Roles

Policies

Identity Providers

Account Settings

Credential Report

Encryption Keys

AWS Services Edit

simon @ isec-psy Global Support

IAM > Roles > TestRoleIAMFullAccess

Summary

Role ARN arn:aws:iam::936728503675:role/TestRoleIAMFullAccess

Instance Profile ARN(s)

Path /

Creation Time 2016-09-21 17:52 EDT

Give this link to users who can switch roles in the console <https://signin.aws.amazon.com/switchrole?account=isec-psy&roleName=TestRoleIAMFullAccess> [Copy Link](#)

Permissions Trust Relationships Access Advisor Revoke Sessions

You can view the trusted entities that can assume the role and the access conditions for the role. [Show policy document](#)

[Edit Trust Relationship](#)

Trusted Entities

The following trusted entities can assume this role.

Trusted Entities

The account 936728503675

Conditions

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

There are no conditions associated with this role.



Least-Privileges with IAM Roles

Edit Trust Relationship

Edit Trust Relationship

You can customize trust relationships by editing the following access control policy document.

Policy Document

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "AWS": "arn:aws:iam::936728503675:root"  
8       },  
9       "Action": "sts:AssumeRole"  
10    }  
11  ]  
12 }
```

Cancel Update Trust Policy



Least-Privileges with IAM Roles

The screenshot shows the AWS IAM console interface. At the top, there is a navigation bar with 'AWS', 'Services', and 'Edit' menus. On the right, it shows the user 'Isimon @ isec-pso', the region 'Global', and a 'Support' link. A left-hand navigation pane lists various IAM components: Dashboard, Search IAM, Details, Groups (highlighted), Users, Roles, Policies, Identity Providers, Account Settings, Credential Report, and Encryption Keys. The main content area shows the breadcrumb 'IAM > Groups > GroupAA', with 'Groups' and 'GroupAA' highlighted in a red box. Below the breadcrumb is a 'Summary' section with the following details: Group ARN: am:aws:iam::936728503675:group/GroupAA, Users (in this group): 1, Path: /, and Creation Time: 2016-09-21 18:01 EDT. There are three tabs: 'Users', 'Permissions' (selected), and 'Access Advisor'. The 'Permissions' tab displays 'Managed Policies' with a message: 'The following managed policies are attached to this group. You can attach up to 10 managed policies.' Below this is an 'Attach Policy' button and a table of attached policies. The table has two columns: 'Policy Name' and 'Actions'. One policy is listed: 'TestPolicyIAMFullAccess' with actions 'Show Policy', 'Detach Policy', and 'Simulate Policy'. At the bottom, there is a section for 'Inline Policies' which is currently collapsed.

Dashboard

Search IAM

Details

Groups

Users

Roles

Policies

Identity Providers

Account Settings

Credential Report

Encryption Keys

IAM > Groups > GroupAA

Summary

Group ARN: am:aws:iam::936728503675:group/GroupAA

Users (in this group): 1

Path: /

Creation Time: 2016-09-21 18:01 EDT

Users Permissions Access Advisor

Managed Policies

The following managed policies are attached to this group. You can attach up to 10 managed policies.

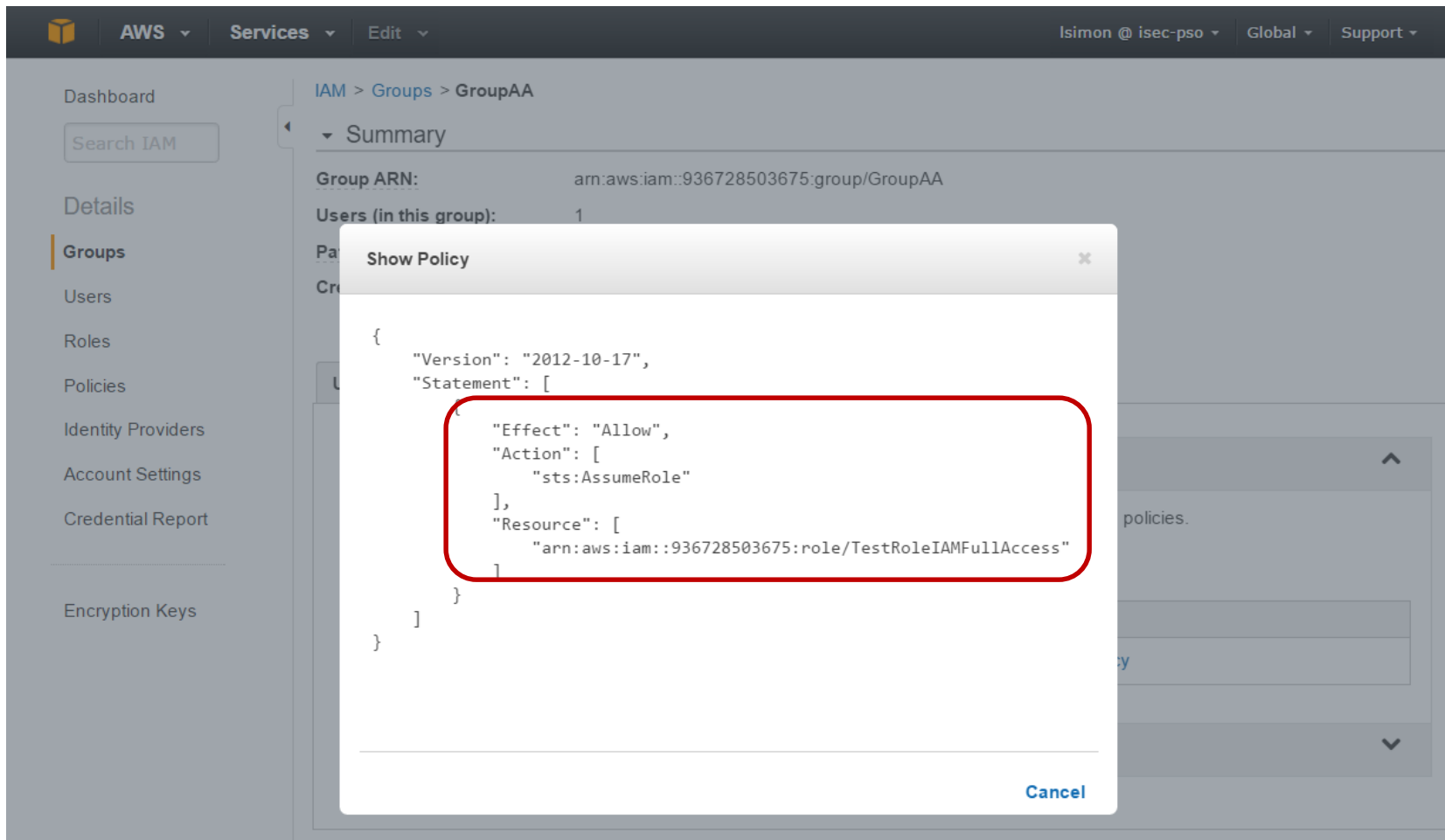
Attach Policy

Policy Name	Actions
TestPolicyIAMFullAccess	Show Policy Detach Policy Simulate Policy

Inline Policies



Least-Privileges with IAM Roles



The screenshot displays the AWS IAM console interface. The main content area shows the 'Summary' for an IAM Group named 'GroupAA'. The 'Group ARN' is 'arn:aws:iam::936728503675:group/GroupAA' and there is '1 User (in this group)'. A 'Show Policy' dialog box is open, displaying a JSON policy document. A red rounded rectangle highlights the following section of the policy:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "sts:AssumeRole"  
      ],  
      "Resource": [  
        "arn:aws:iam::936728503675:role/TestRoleIAMFullAccess"  
      ]  
    }  
  ]  
}
```

The dialog box also includes a 'Cancel' button at the bottom right.

Least-Privileges with IAM Roles

- GroupAA
 - User and permissions management
- GroupBB
 - Audit of EC2 usage and security groups
- GroupCC
 - Audit of S3 usage and bucket access controls



Least-Privileges with IAM Roles

- GroupAA
 - **AssumeRole** User and permissions management
- GroupBB
 - **AssumeRole** Audit of EC2 usage and security groups
- GroupCC
 - **AssumeRole** Audit of S3 usage and bucket access controls



Least-Privileges with IAM Roles

The screenshot shows the AWS IAM console interface. The top navigation bar includes 'AWS', 'Services', and 'Edit'. The user profile 'Isimon @ isec-pso' and regional settings 'Global' and 'Support' are visible. The left sidebar contains navigation options: Dashboard, Search IAM, Details, Groups, Users (highlighted), Roles, Policies, Identity Providers, Account Settings, Credential Report, and Encryption Keys. The main content area is titled 'IAM > Users > TestUser2' and shows a 'Summary' section with the following details:

- User ARN:** arn:aws:iam::936728503675:user/TestUser2
- Has Password:** No
- Groups (for this user):** 3
- Path:** /
- Creation Time:** 2016-07-05 21:16 EDT

Below the summary, there are tabs for 'Groups', 'Permissions', 'Security Credentials', and 'Access Advisor'. The 'Groups' tab is active, showing a message: 'This view shows all groups the User belongs to: 3 Groups'. A blue button labeled 'Add User to Groups' is present. A table lists the groups:

Group	Actions
GroupAA	
GroupBB	
GroupCC	

A red callout box with the text 'Member of 3 groups' and a red arrow points to the 'GroupBB' row in the table.



Least-Privileges with IAM Roles

IAM > Users > TestUser2

Summary

User ARN: arn:aws:iam::936728503675:user/TestUser2
Has Password: No
Groups (for this user): 3
Path: /
Creation Time: 2016-07-05 21:16 EDT

Groups | **Permissions** | Security Credentials | Access Advisor

Managed Policies

There are no managed policies attached to this user.

[Attach Policy](#)

Group Policies

This view shows policies that are attached to groups that this user is in.

Policy Name	Group Name	Actions
TestPolicyIAMFullAccess	GroupAA	Show Policy
TestPolicyAmazonEC2ReadOnlyAccess	GroupBB	Show Policy
TestPolicyAmazonS3ReadOnlyAccess	GroupCC	Show Policy

Inline Policies



Least-Privileges with IAM Roles

The screenshot shows the AWS IAM console interface. The main content area displays the 'Summary' for a user named 'TestUser2'. A 'Show Policy' dialog box is open, showing the following JSON policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": [
        "arn:aws:iam::936728503675:role/TestRoleIAMFullAccess"
      ]
    }
  ]
}
```

A red box highlights the 'Action' and 'Resource' fields in the policy statement. A red arrow points from this box to the 'Show Policy' button in the table below.

Policy	Actions
TestP	Show Policy
TestP	Show Policy
TestPolicyAmazonS3ReadOnlyAccess	Show Policy



Least-Privileges with IAM Roles

At any time

User can do

User needs to do

AssumeRole IAMFullAccess

And

Or

AssumeRole AmazonEC2ReadOnlyAccess

And

Or

AssumeRole AmazonS3ReadOnlyAccess



Least-Privileges with IAM Roles

- Security through obscurity
 - Attacker needs to know the role's ARN
- Increased robustness
 - Extra step lowers risks of unintended API access
- How to achieve least privilege?



Least-Privileges with IAM Roles

- Security through obscurity
 - Attacker needs to know the role's ARN
- Increased robustness
 - Extra step lowers risks of unintended API access
- How to achieve least privilege?
 - Add MFA requirements



Least-Privileges with IAM Roles

- MFA Conditions in AWS policies
 - MFA used at authentication time
 - Always required
 - Age of authentication
 - Varies for each role



Least-Privileges with IAM Roles

- GroupAA
 - **AssumeRole** User and permissions management
 - MFA within last minute
- GroupBB
 - **AssumeRole** Audit of EC2 usage and security groups
 - MFA within last minute
- GroupCC
 - **AssumeRole** Audit of S3 usage and bucket access controls
 - MFA within last minute



Least-Privileges with IAM Roles

Edit Trust Relationship

You can customize trust relationships by editing the following access control policy document.

Policy Document

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": "arn:aws:iam::936728503675:root"
8       },
9       "Action": "sts:AssumeRole",
10      "Condition": {
11        "Bool": {
12          "aws:MultiFactorAuthPresent": "true"
13        },
14        "NumericLessThan": {
15          "aws:MultiFactorAuthAge": "60"
16        }
17      }
18    }
19  ]
20 }
```

MFA used



Least-Privileges with IAM Roles

Edit Trust Relationship

You can customize trust relationships by editing the following access control policy document.

Policy Document

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "AWS": "arn:aws:iam::936728503675:root"  
8       },  
9       "Action": "sts:AssumeRole",  
10      "Condition": {  
11        "Bool": {  
12          "aws:MultiFactorAuthPresent": "true"  
13        },  
14        "NumericLessThan": {  
15          "aws:MultiFactorAuthAge": "60"  
16        }  
17      }  
18    }  
19  ]  
20 }
```

Within the last minute



Least-Privileges with IAM Roles

Dashboard AWS Services Edit Isimon @ isec-pso Global Support

Dashboard
Search IAM
Details
Groups
Users
Roles
Policies
Identity Providers
Account Settings
Credential Report
Encryption Keys

IAM > Roles > TestRoleIAMFullAccess

Summary

Role ARN arn:aws:iam::936728503675:role/TestRoleIAMFullAccess

Instance Profile ARN(s)

Path /

Creation Time 2016-09-21 17:52 EDT

Give this link to users who can switch roles in the console <https://signin.aws.amazon.com/switchrole?account=isec-pso&roleName=TestRoleIAMFullAccess> [Copy Link](#)

Permissions Trust Relationships Access Advisor Revoke Sessions

You can view the trusted entities that can assume the role and the access conditions for the role. [Show policy document](#)

[Edit Trust Relationship](#)

Trusted Entities

The following trusted entities can assume this role.

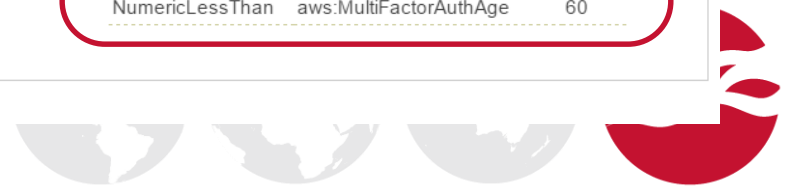
Trusted Entities

The account 936728503675

Conditions

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

Condition	Key	Value
Bool	aws:MultiFactorAuthPresent	true
NumericLessThan	aws:MultiFactorAuthAge	60



Least-Privileges with IAM Roles

At any time

User can do

User needs to do

AssumeRole IAMFullAccess

Or

Or

AssumeRole AmazonEC2ReadOnlyAccess

Or

Or

AssumeRole AmazonS3ReadOnlyAccess



Least-Privileges with IAM Roles

- Security through MFA
- Compromise is limited to scope of current session
 - Attacker less likely to gain IAM/EC2 admin privileges
 - Attacker less likely to maintain API access



Usage in Web Console

The screenshot shows the AWS IAM console interface. The breadcrumb navigation is IAM > Roles > TestRoleAmazonEC2ReadOnlyAccess. The 'Trust Relationships' tab is selected, showing a table of trusted entities and conditions. A user menu is open over the 'IAM User' field, listing options like 'IAM User: Isimon', 'Account: isec-pso', 'My Account', 'Billing & Cost Management', 'Security Credentials', 'Switch Role', and 'Sign Out'.

Role ARN `arn:aws:iam::936728503675:role/TestRoleAmazonEC2ReadOnlyAccess`

Instance Profile ARN(s) /

Path /

Creation Time 2016-09-21 17:53 EDT

Give this link to users who can switch roles in the console <https://signin.aws.amazon.com/switchrole?account=isec-pso&roleName=TestRoleAmazonEC2ReadOnlyAccess>

Permissions **Trust Relationships** **Access Advisor** **Revoke Sessions**

You can view the trusted entities that can assume the role and the access conditions for the role. [Show policy document](#)

[Edit Trust Relationship](#)

Trusted Entities

The following trusted entities can assume this role.

Trusted Entities
The account 936728503675

Conditions

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

Condition	Key	Value
Bool	aws:MultiFactorAuthPresent	true
NumericLessThan	aws:MultiFactorAuthAge	3600



Usage in Web Console



Switch Role

Allows management of resources across AWS accounts using a single user ID and password. You can switch roles after an AWS administrator has configured a role and given you the account and role details. [Learn more.](#)

Account* ⓘ

Role* ⓘ

Display Name ⓘ

Color ■ a ■ a ■ a ■ a ■ a ■ a

*Required

Cancel

Switch Role

English ▼



Usage in Web Console

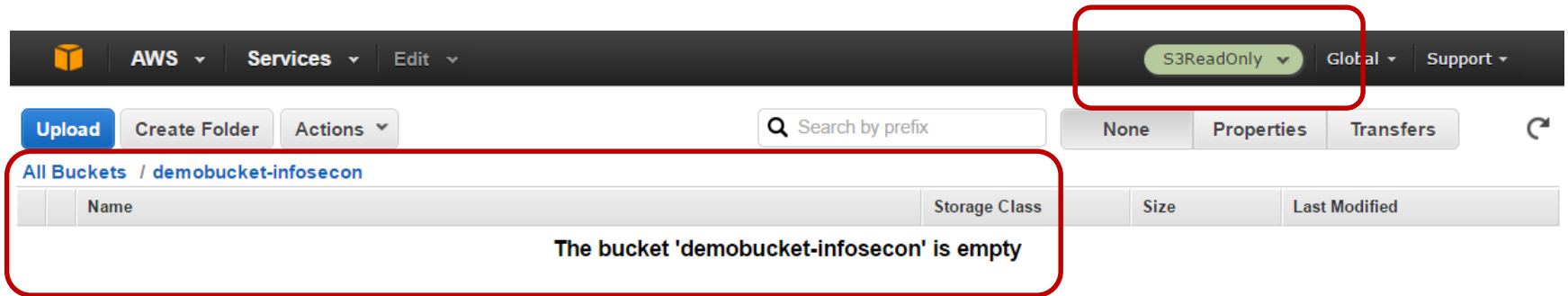
The screenshot shows the AWS IAM console interface. The top navigation bar includes 'AWS', 'Services', 'Edit', 'S3ReadOnly', 'Global', and 'Support'. The left sidebar lists navigation options: Dashboard, Search IAM, Details, Groups, Users, Roles (highlighted), Policies, Identity Providers, Account Settings, Credential Report, and Encryption Keys. The main content area shows a table with columns 'Role Name' and 'Creation Time'. Below the table, an error message is displayed:

We encountered the following errors while processing your request:

- ✘ User: arn:aws:sts::936728503675:assumed-role/TestRoleAmazonS3ReadOnlyAccess/simon is not authorized to perform: iam:ListRoles on resource: arn:aws:iam::936728503675:role/



Usage in Web Console



The screenshot shows the AWS S3 console interface. At the top, there is a navigation bar with 'AWS', 'Services', and 'Edit' menus. A red box highlights the 'S3ReadOnly' dropdown menu. Below the navigation bar, there are buttons for 'Upload', 'Create Folder', and 'Actions', along with a search box labeled 'Search by prefix'. The main content area shows the bucket 'demobucket-infosecon' is empty. A red box highlights the message 'The bucket 'demobucket-infosecon' is empty'. The interface also includes tabs for 'None', 'Properties', and 'Transfers', and a refresh button.

All Buckets / demobucket-infosecon

Name	Storage Class	Size	Last Modified
The bucket 'demobucket-infosecon' is empty			



Usage in CLI

```
loic@wh  
File Edit View Search Terminal Help  
loic@whichaway:~$  
loic@whichaway:~$ aws --profile testrole iam list-users --max-items 1  
{  
  "NextToken": "[REDACTED]i0iAxfQ==",  
  "Users": [  
    {  
      "UserName": "[REDACTED]",  
      "PasswordLastUsed": "2016-01-14T17:03:42Z",  
      "CreateDate": "2016-01-08T19:25:54Z",  
      "UserId": "[REDACTED]",  
      "Path": "/",  
      "Arn": "arn:aws:iam::936728503675:user/[REDACTED]"  
    }  
  ]  
}  
loic@whichaway:~$
```



Takeaways

- IAM roles
 - Defined by two policies
 - IAM permissions policy
 - Trust relationship (a.k.a AssumeRole policy)
 - Allow implementation of least privilege for IAM users
 - Allow implementation of finer-grained access controls
 - Can be used when working with the CLI / 3rd party tools



Takeaways

- Security-in-depths and least privilege
 - Group allows AssumeRole
 - Role's policy defines roles' privileges
 - AssumeRole policy defines trusted entities
 - AssumeRole requires MFA within N hours or minutes



Thank You, Questions?

- Loïc Simon
 - Loic.Simon@nccgroup.trust
- Tools on GitHub
 - <https://github.com/nccgroup/AWS-recipes>
 - <https://github.com/nccgroup/Scout2>
- Slides
 - <https://lo1cd3v.github.io/slides>

