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

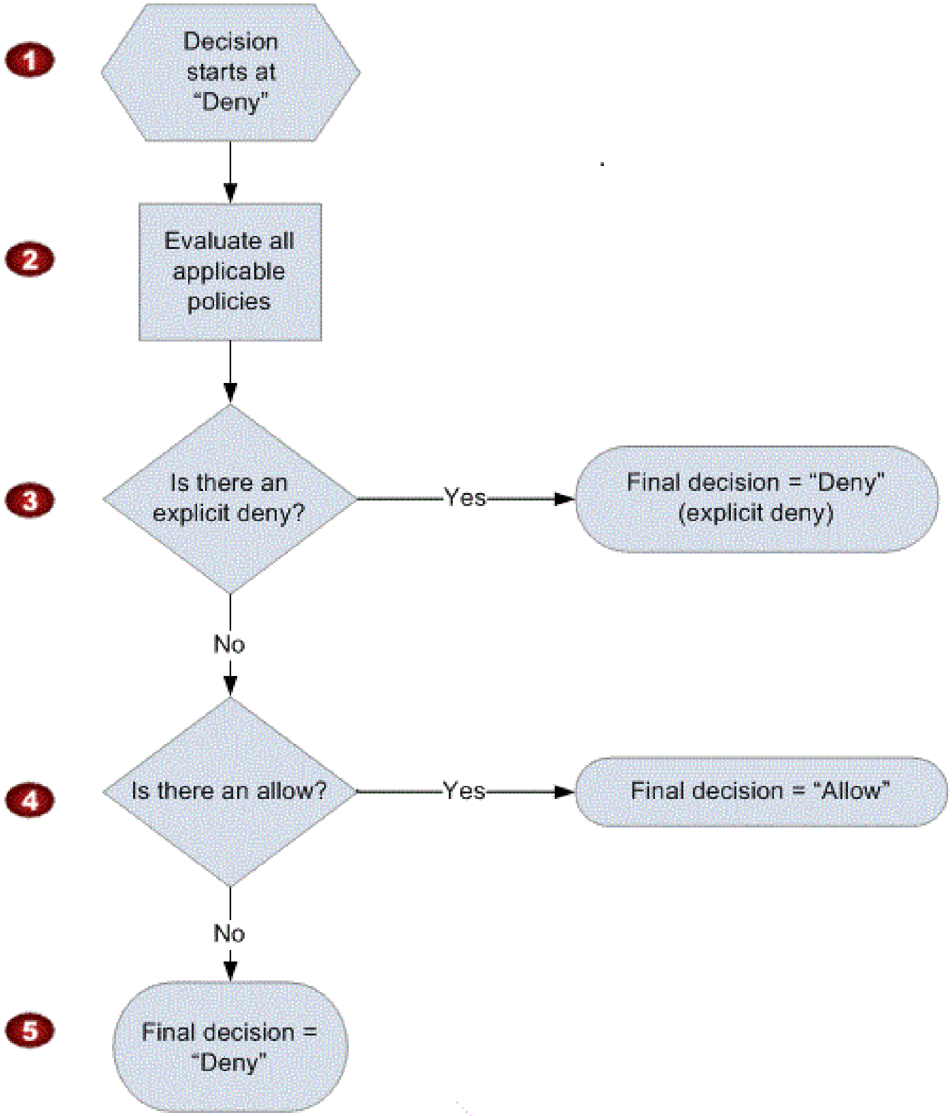
- Policy
  - Set of permissions defined as a list of statements
  - JSON

- 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


1
Decision starts at "Deny"
2
Evaluate all applicable policies
3
Is there an explicit deny?
Yes
Final decision = "Deny" (explicit deny)
No
4
Is there an allow?
Yes
Final decision = "Allow"
No
5
Final decision = "Deny"

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)

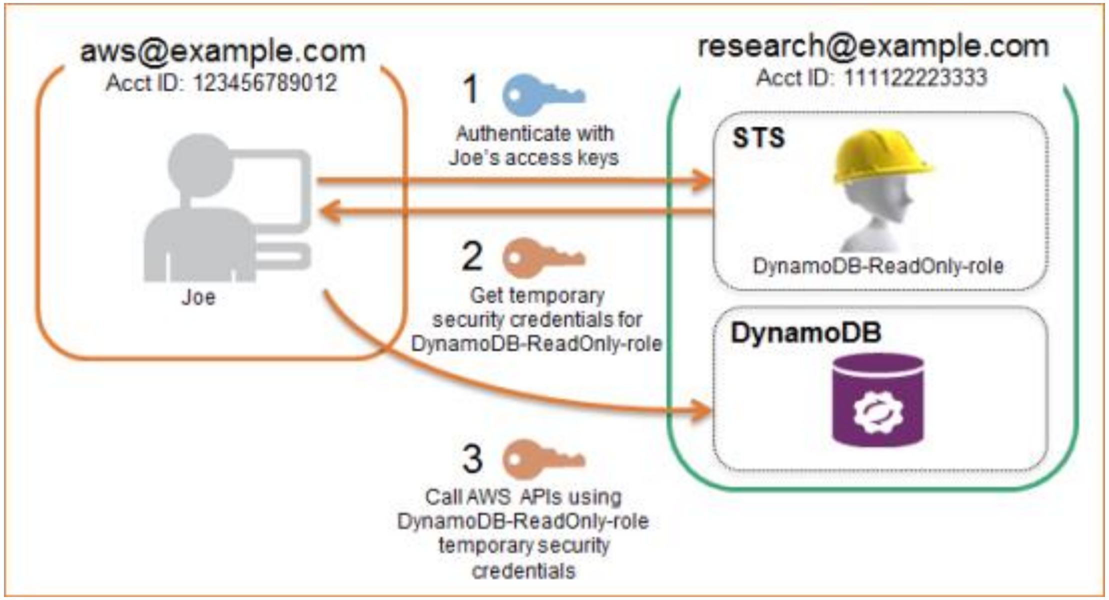
Applications of IAM Roles

- 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

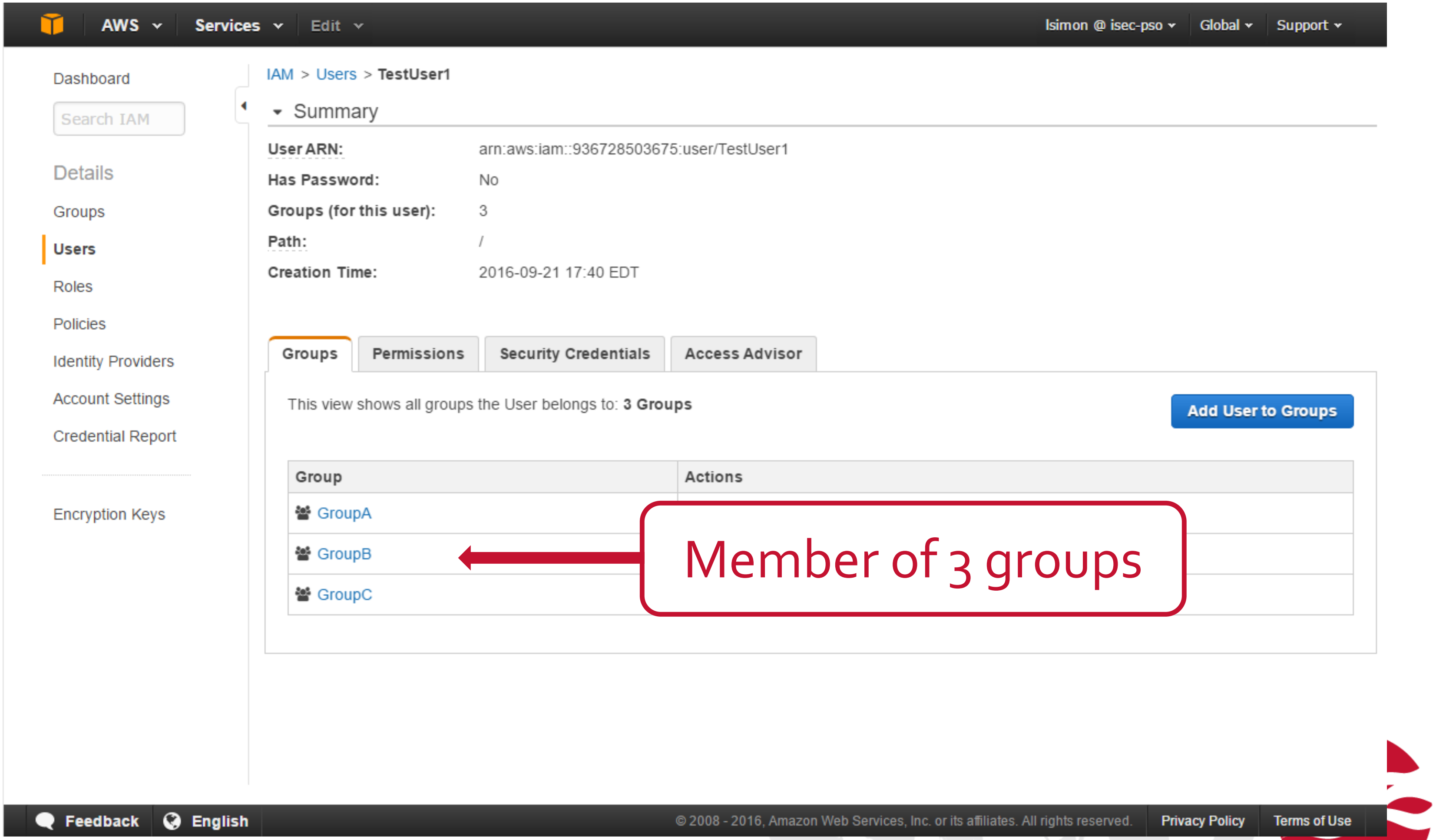

aws@example.com
Acct ID: 123456789012
Joe
1
Authenticate with Joe's access keys
2
Get temporary security credentials for DynamoDB-ReadOnly-role
3
Call AWS APIs using DynamoDB-ReadOnly-role temporary security credentials
research@example.com
Acct ID: 111122223333
STS
DynamoDB-ReadOnly-role
DynamoDB

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



IAM > Users > TestUser1

Summary

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

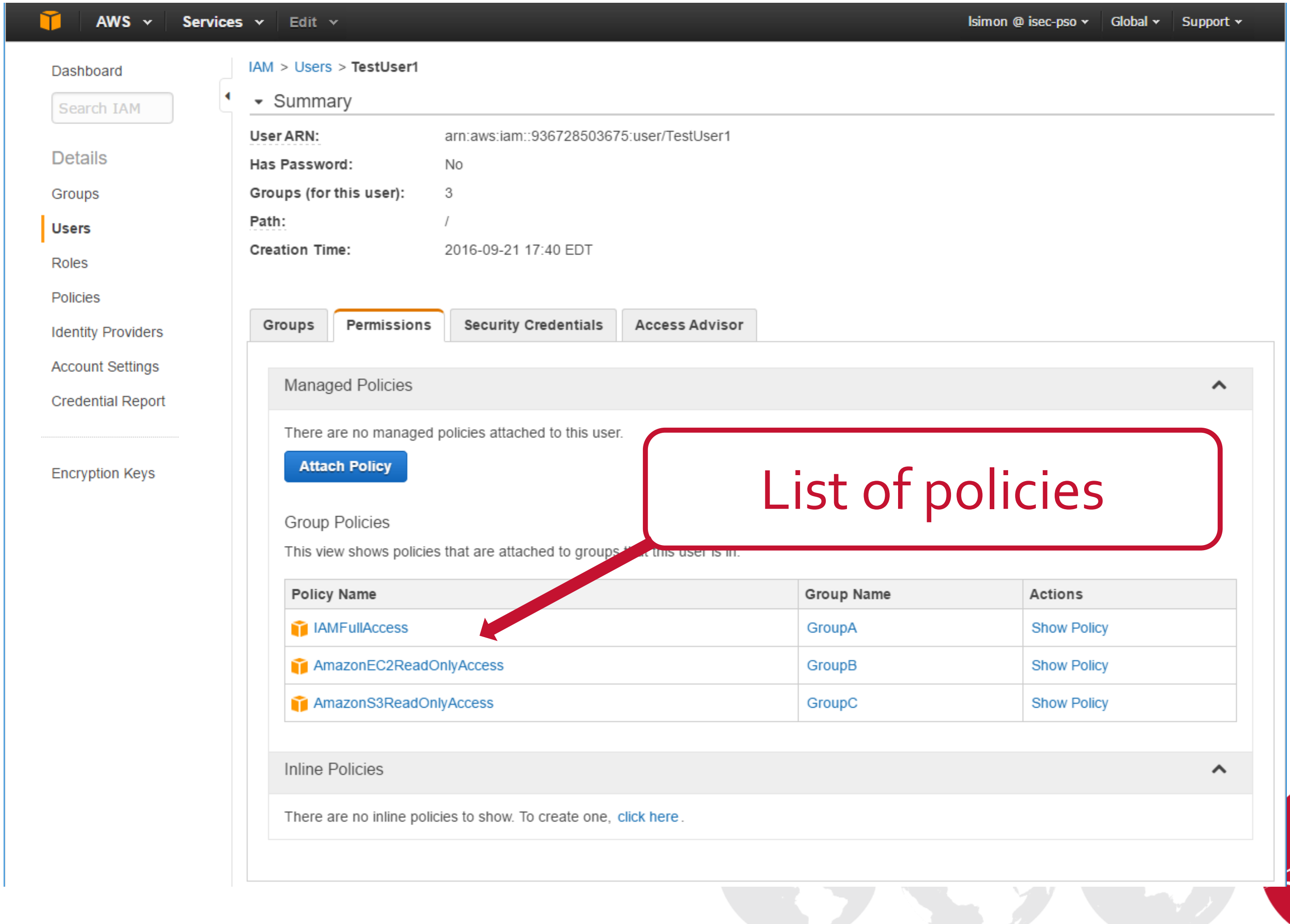
This view shows all groups the User belongs to: **3 Groups**

Group	Actions
GroupA	
GroupB	
GroupC	

Member of 3 groups

© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Traditional Authorization Scheme



IAM > Users > TestUser1

Summary

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

Managed Policies

There are no managed policies attached to this user.

Group Policies

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

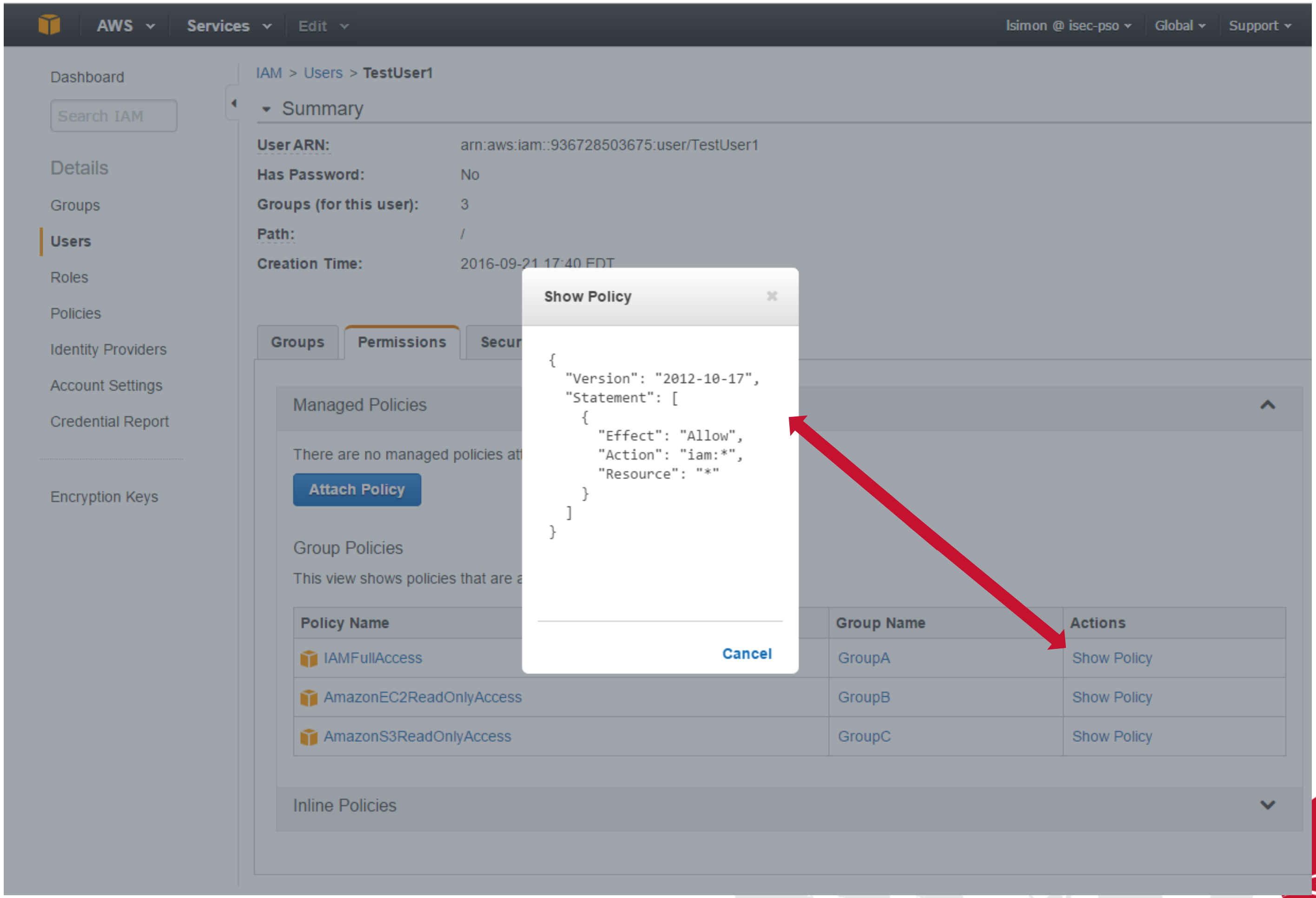
Policy Name	Group Name	Actions
IAMFullAccess	GroupA	Show Policy
AmazonEC2ReadOnlyAccess	GroupB	Show Policy
AmazonS3ReadOnlyAccess	GroupC	Show Policy

Inline Policies

There are no inline policies to show. To create one, click here.

List of policies

Traditional Authorization Scheme



IAM > Users > TestUser1

Summary

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

Show Policy

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

Managed Policies

There are no managed policies at

Group Policies

This view shows policies that are a

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

Inline Policies

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	

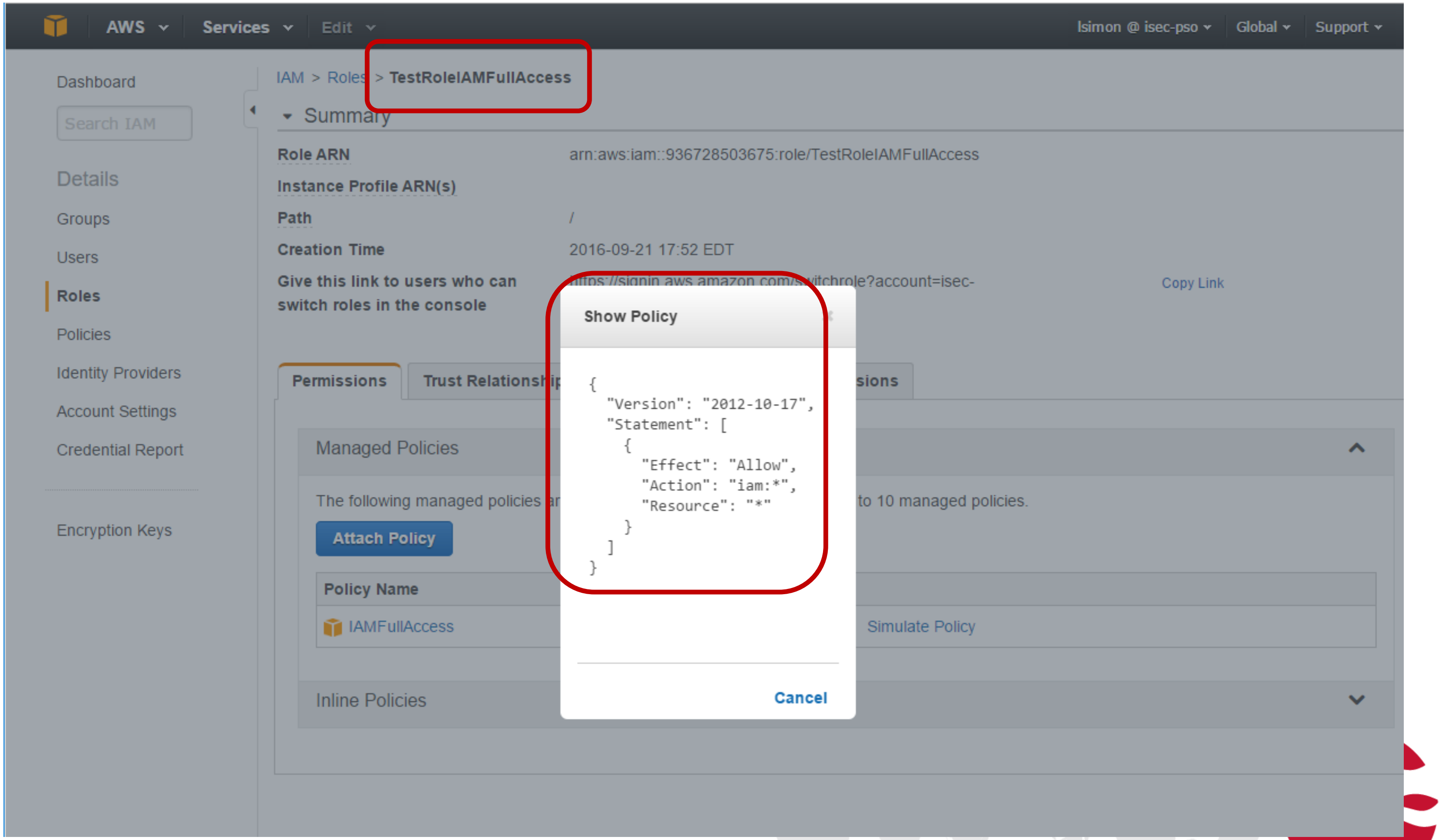
- Proposal: use IAM roles

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



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

Instance Profile ARN(s)

Path: /

Creation Time: 2016-09-21 17:52 EDT

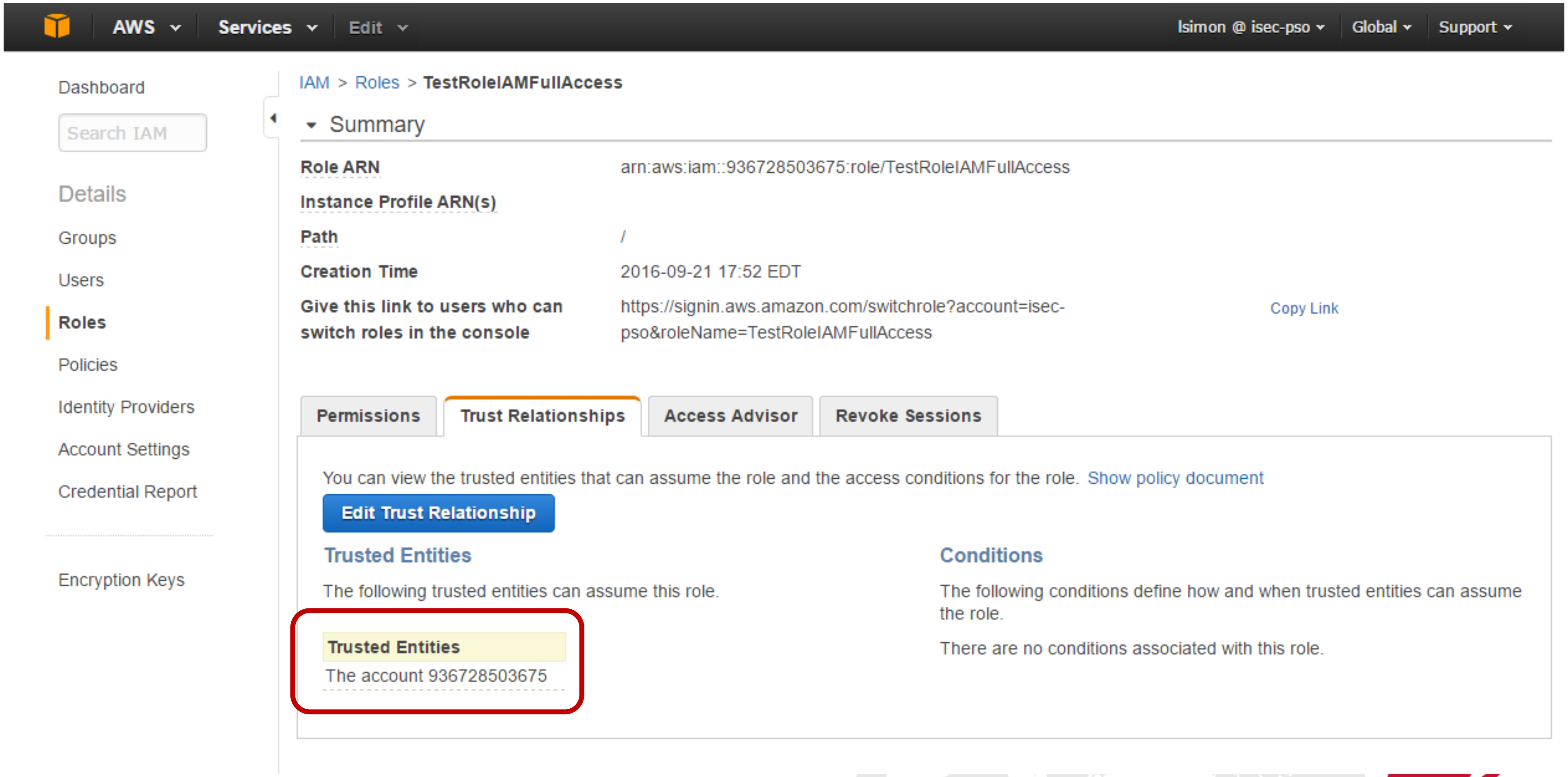
Give this link to users who can switch roles in the console: https://signin.aws.amazon.com/switchrole?account=isec-

The following managed policies ar… to 10 managed policies.

IAMFullAccess

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

Least-Privileges with IAM Roles



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

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

Trusted Entities

The following trusted entities can assume this role.

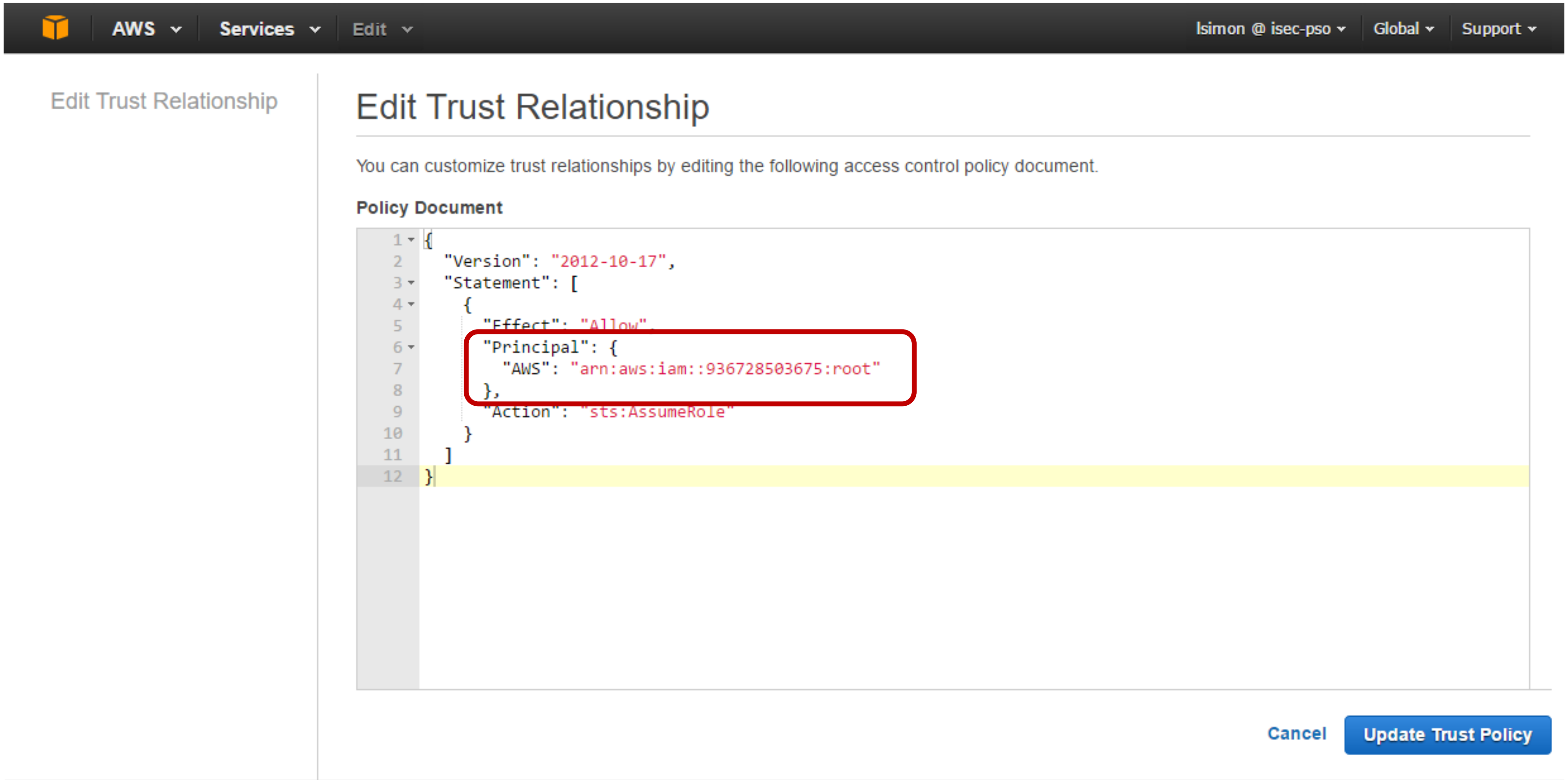
Trusted Entities
The account 936728503675

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

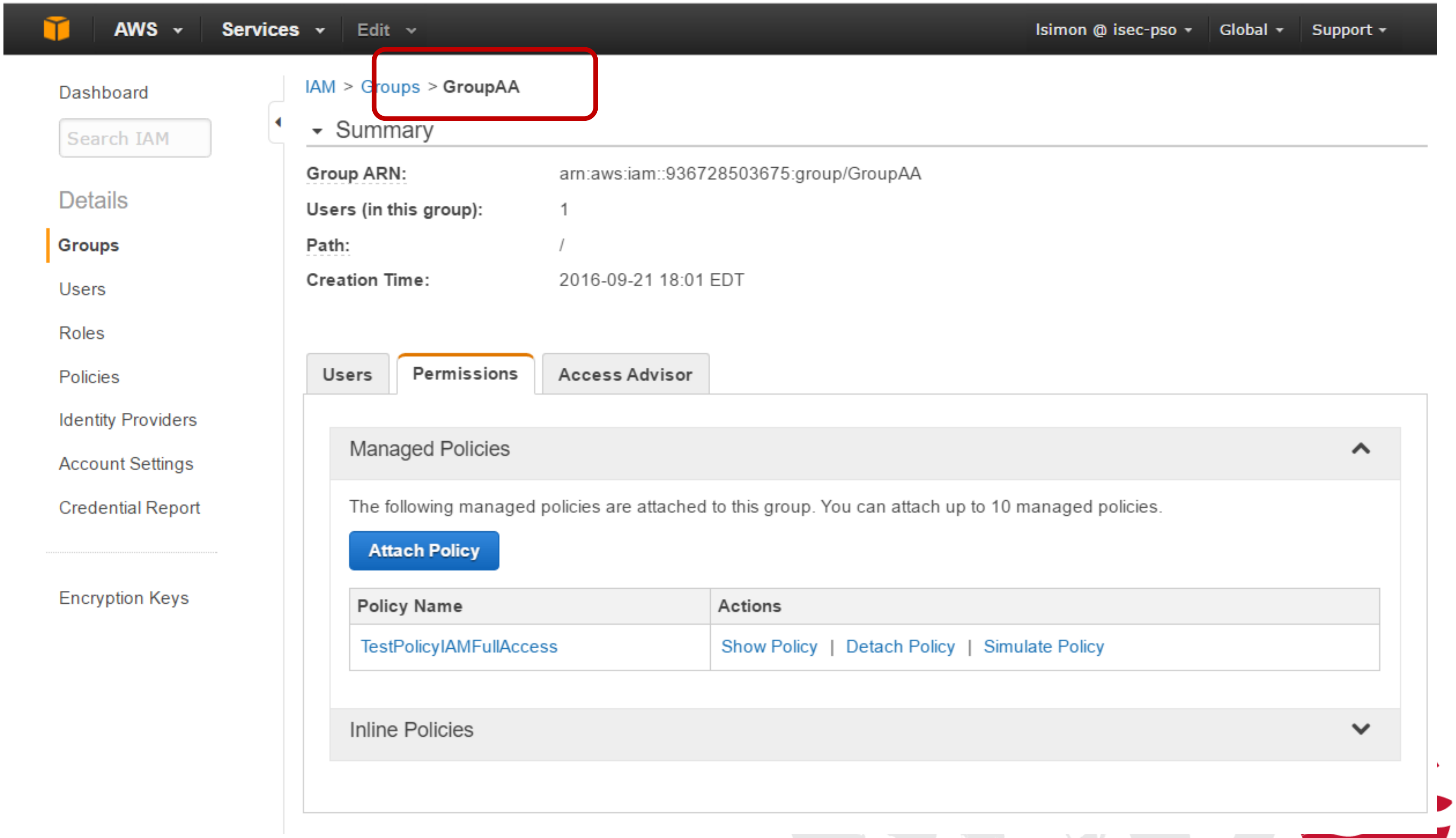
You can customize trust relationships by editing the following access control policy document.

Policy Document

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::936728503675:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Least-Privileges with IAM Roles

nccgroup
freedom from doubt



IAM > Groups > GroupAA

Summary

Group ARN:	arn:aws:iam::936728503675:group/GroupAA
Users (in this group):	1
Path:	/
Creation Time:	2016-09-21 18:01 EDT

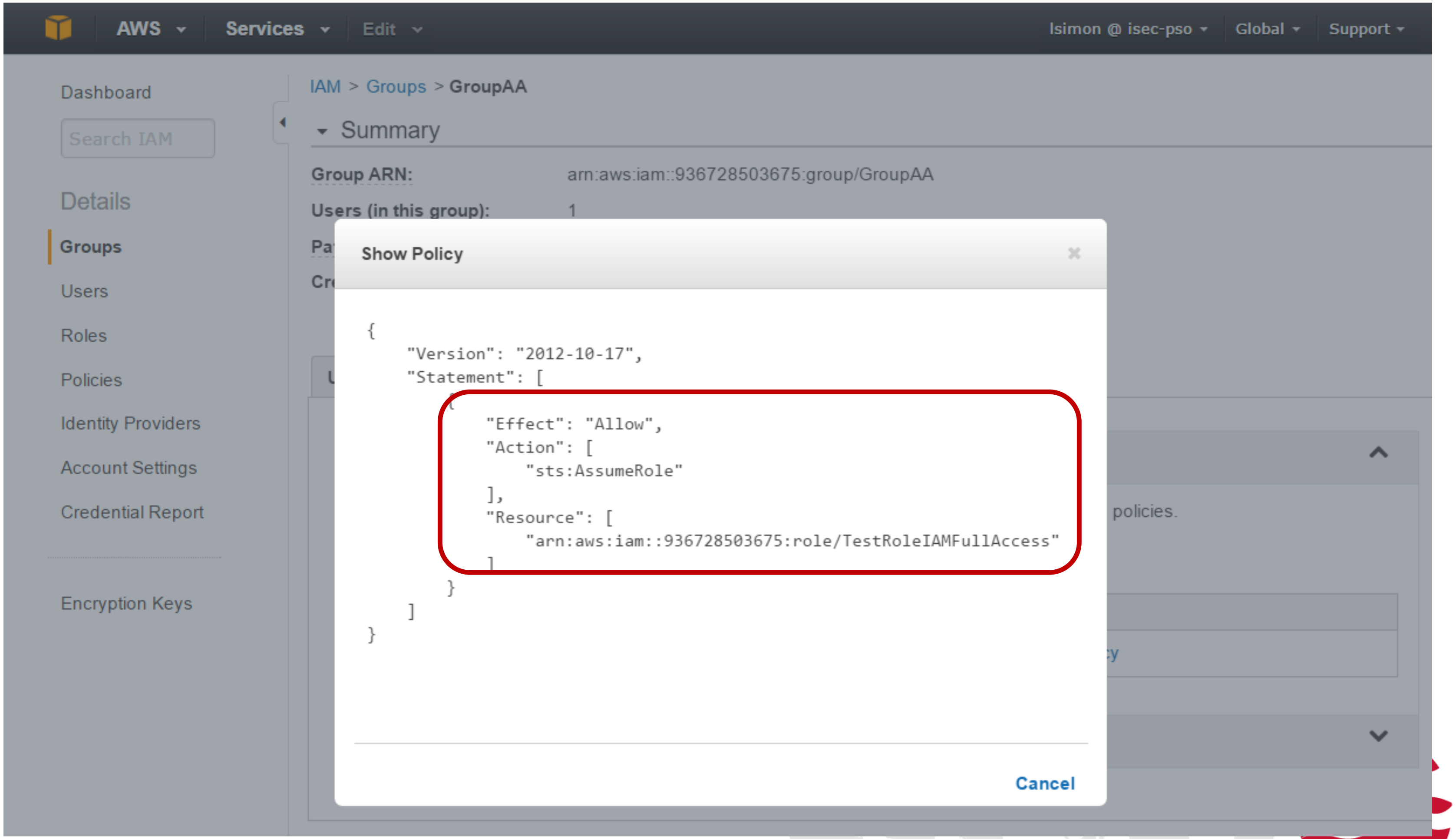
Managed Policies

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

Policy Name	Actions
TestPolicyIAMFullAccess	Show Policy | Detach Policy | Simulate Policy

Inline Policies

Least-Privileges with IAM Roles



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

Users (in this group): 1

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

Least-Privileges with IAM Roles

- GroupAA
  - User and permissions management

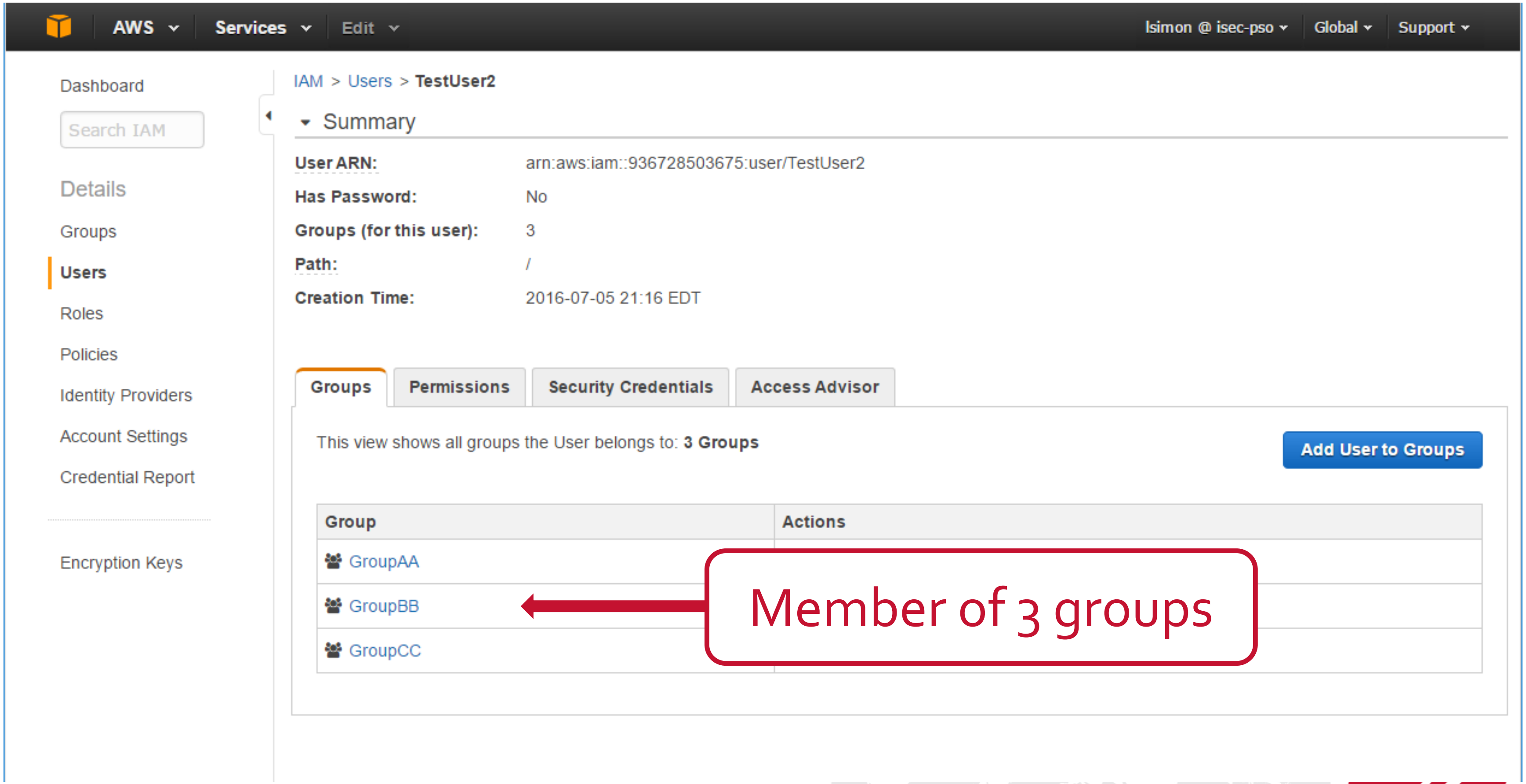
- GroupBB
  - Audit of EC2 usage and security groups

- 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



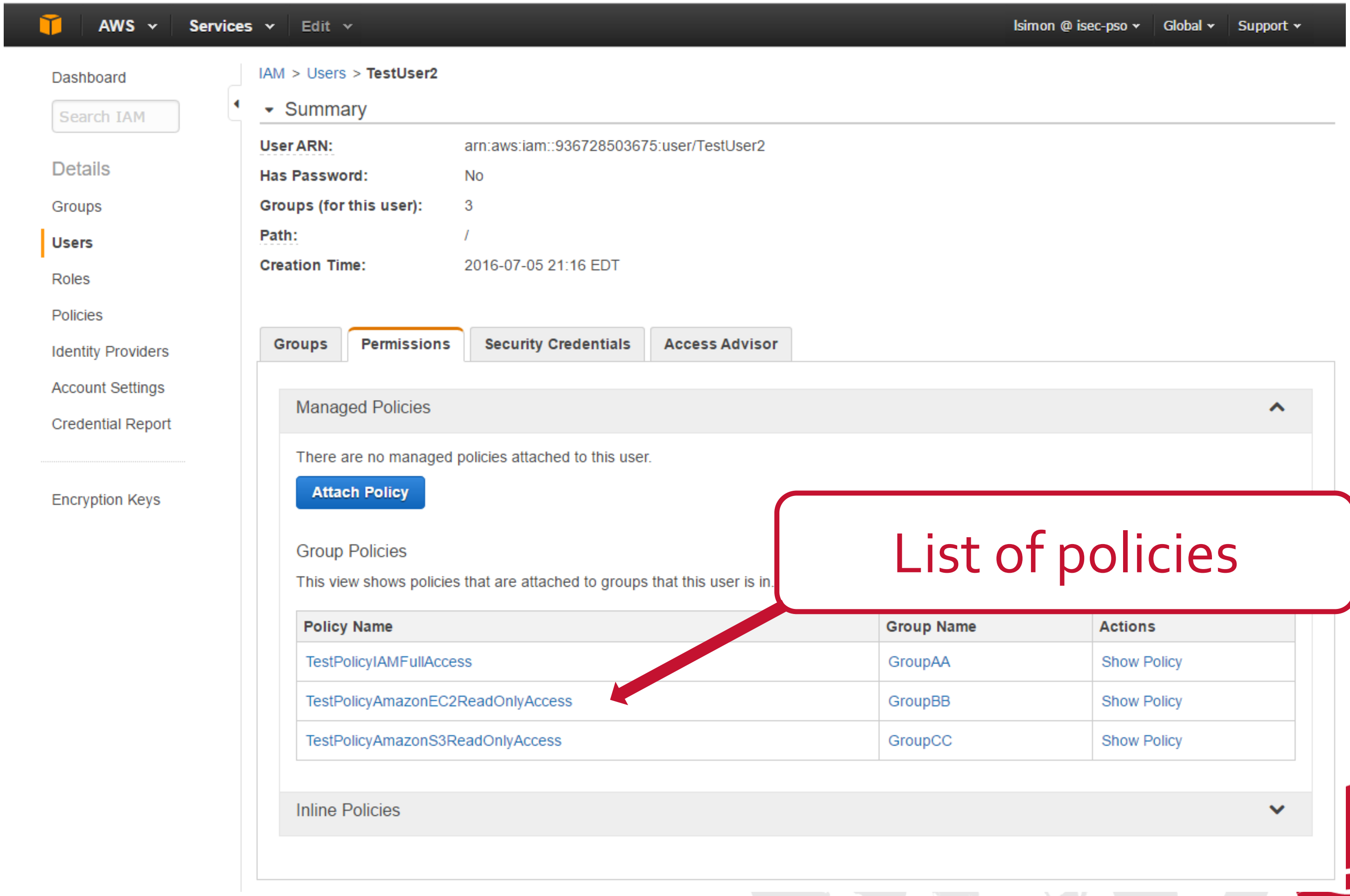
User ARN:	arn:aws:iam::936728503675:user/TestUser2
Has Password:	No
Groups (for this user):	3
Path:	/
Creation Time:	2016-07-05 21:16 EDT

This view shows all groups the User belongs to: **3 Groups**

Group	Actions
GroupAA	
GroupBB	
GroupCC	

Member of 3 groups

Least-Privileges with IAM Roles



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

Managed Policies

There are no managed policies attached to this user.

Group Policies

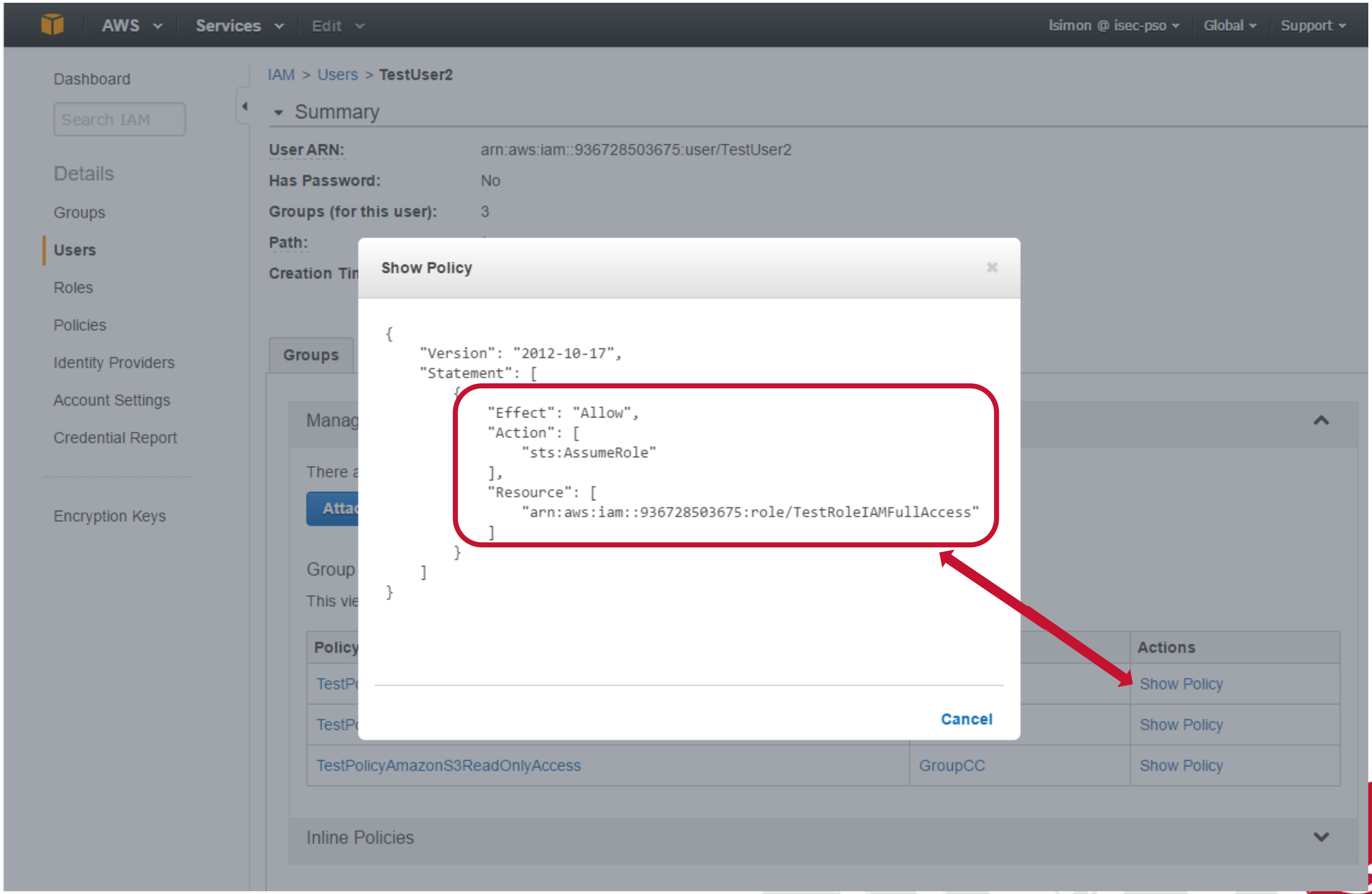
This view shows policies that are attached to groups that this user is in.

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

Inline Policies

List of policies

Least-Privileges with IAM Roles



IAM > Users > TestUser2

User ARN: arn:aws:iam::936728503675:user/TestUser2

Has Password: No

Groups (for this user): 3

Path:

Creation Tim

Show Policy

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

Policy		Actions
TestP		Show Policy
TestP		Show Policy
TestPolicyAmazonS3ReadOnlyAccess	GroupCC	Show Policy

Least-Privileges with IAM Roles

<table>
<tr><th colspan="2">At any time</th></tr>
<tr><th>User can do</th><th>User needs to do</th></tr>
<tr><td colspan="2">AssumeRole IAMFullAccess</td></tr>
<tr><td>And</td><td>Or</td></tr>
<tr><td colspan="2">AssumeRole AmazonEC2ReadOnlyAccess</td></tr>
<tr><td>And</td><td>Or</td></tr>
<tr><td colspan="2">AssumeRole AmazonS3ReadOnlyAccess</td></tr>
</table>

Least-Privileges with IAM Roles

- Security trough 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 trough 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

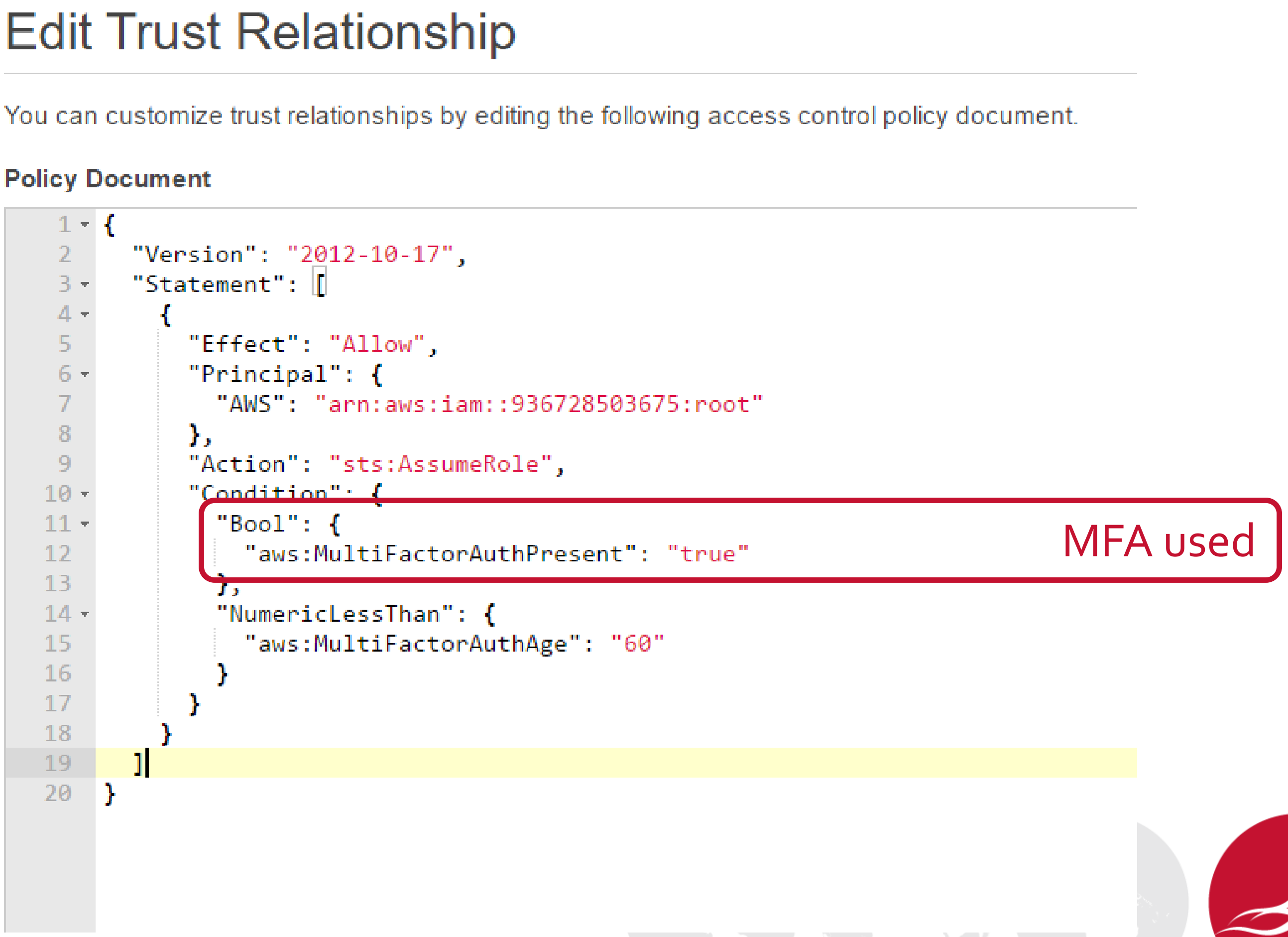
- MFA Conditions in AWS policies
  - MFA used at authentication time
    - Always required
  - Age of authentication
    - Varies for each role

Least-Privileges with IAM Roles

nccgroup
freedom from doubt

- 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

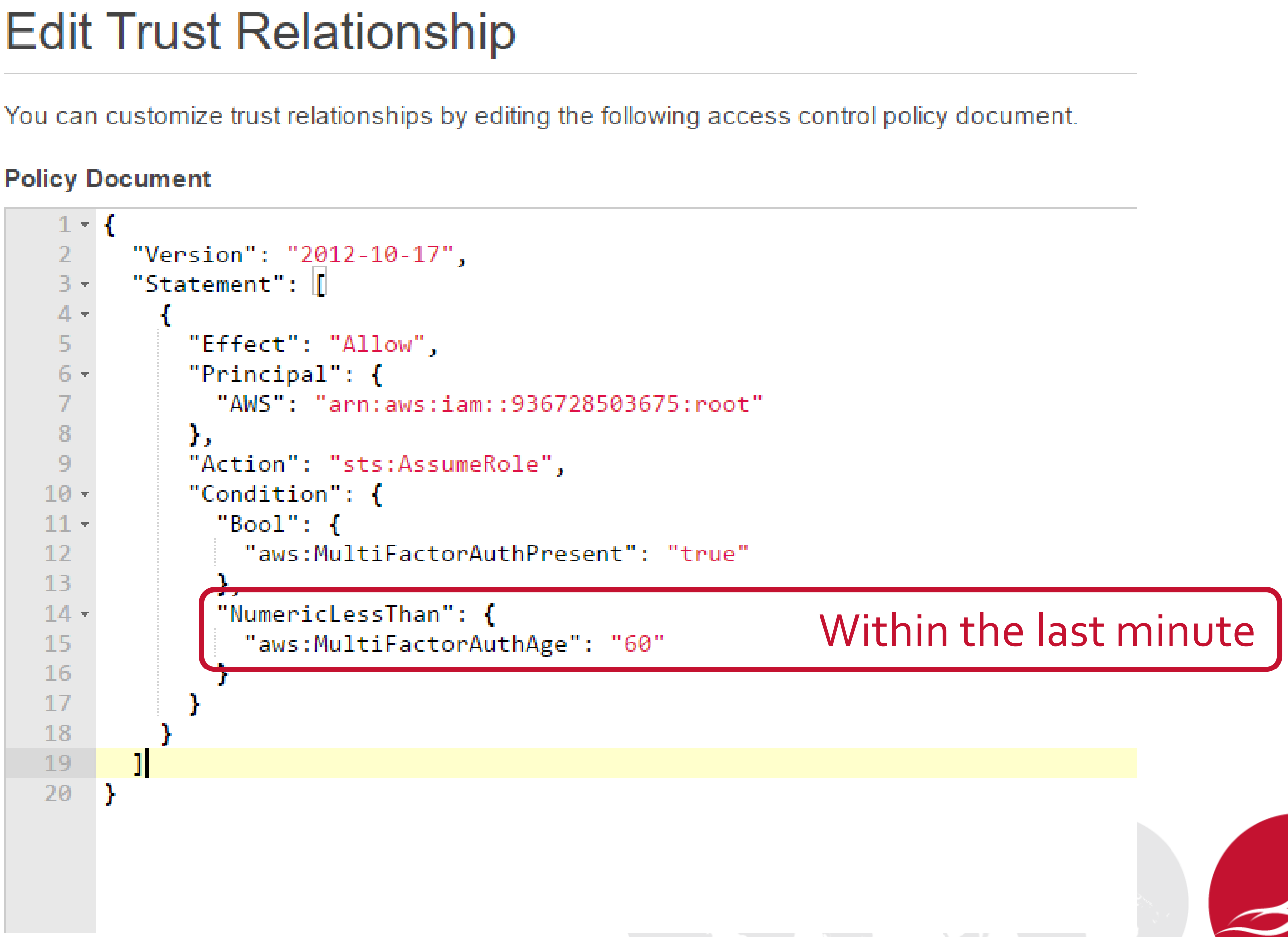
You can customize trust relationships by editing the following access control policy document.

Policy Document

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::936728503675:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "Bool": {
          "aws:MultiFactorAuthPresent": "true"
        },
        "NumericLessThan": {
          "aws:MultiFactorAuthAge": "60"
        }
      }
    }
  ]
}
```

MFA used

Least-Privileges with IAM Roles



Edit Trust Relationship

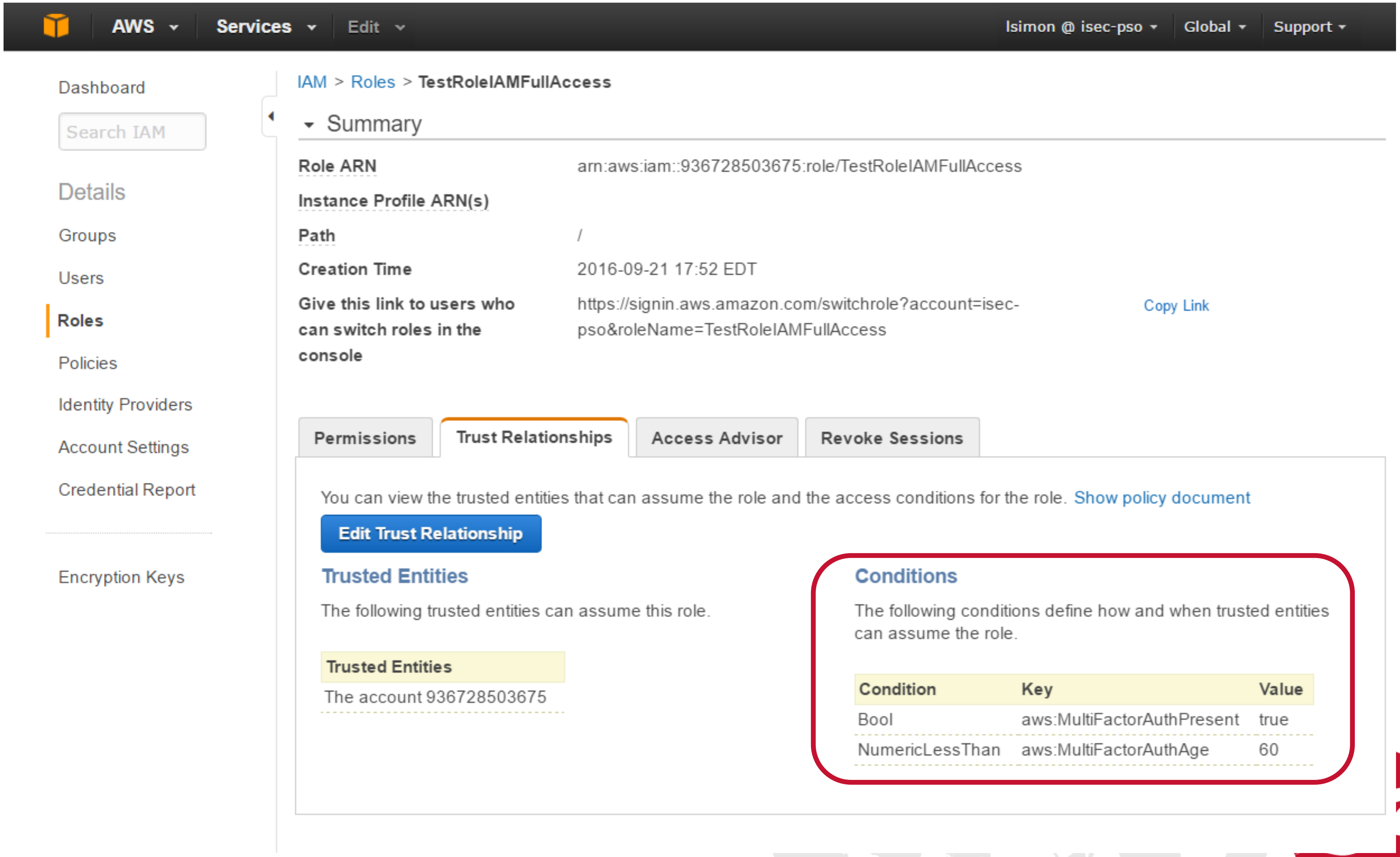
You can customize trust relationships by editing the following access control policy document.

Policy Document

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::936728503675:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "Bool": {
          "aws:MultiFactorAuthPresent": "true"
        },
        "NumericLessThan": {
          "aws:MultiFactorAuthAge": "60"
        }
      }
    }
  ]
}
```

Within the last minute

Least-Privileges with IAM Roles



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

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

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

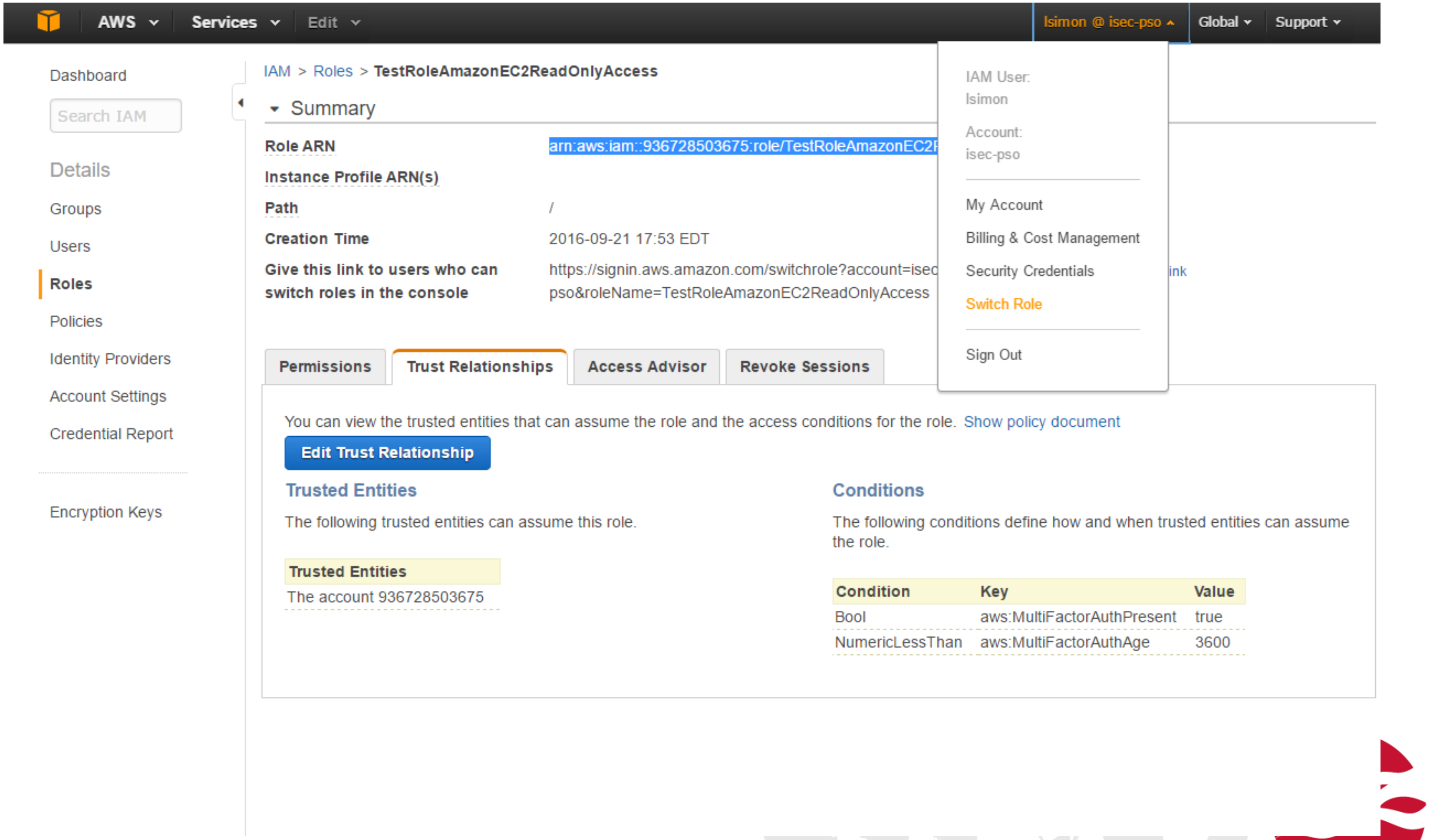
<table>
<tr><th colspan="2">At any time</th></tr>
<tr><td>User can do</td><td>User needs to do</td></tr>
<tr><td colspan="2">AssumeRole IAMFullAccess</td></tr>
<tr><td>Or</td><td>Or</td></tr>
<tr><td colspan="2">AssumeRole AmazonEC2ReadOnlyAccess</td></tr>
<tr><td>Or</td><td>Or</td></tr>
<tr><td colspan="2">AssumeRole AmazonS3ReadOnlyAccess</td></tr>
</table>

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



IAM > Roles > TestRoleAmazonEC2ReadOnlyAccess

Summary

Role ARN: arn:aws:iam::936728503675:role/TestRoleAmazonEC2F

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

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

Trusted Entities

The following trusted entities can assume this role.

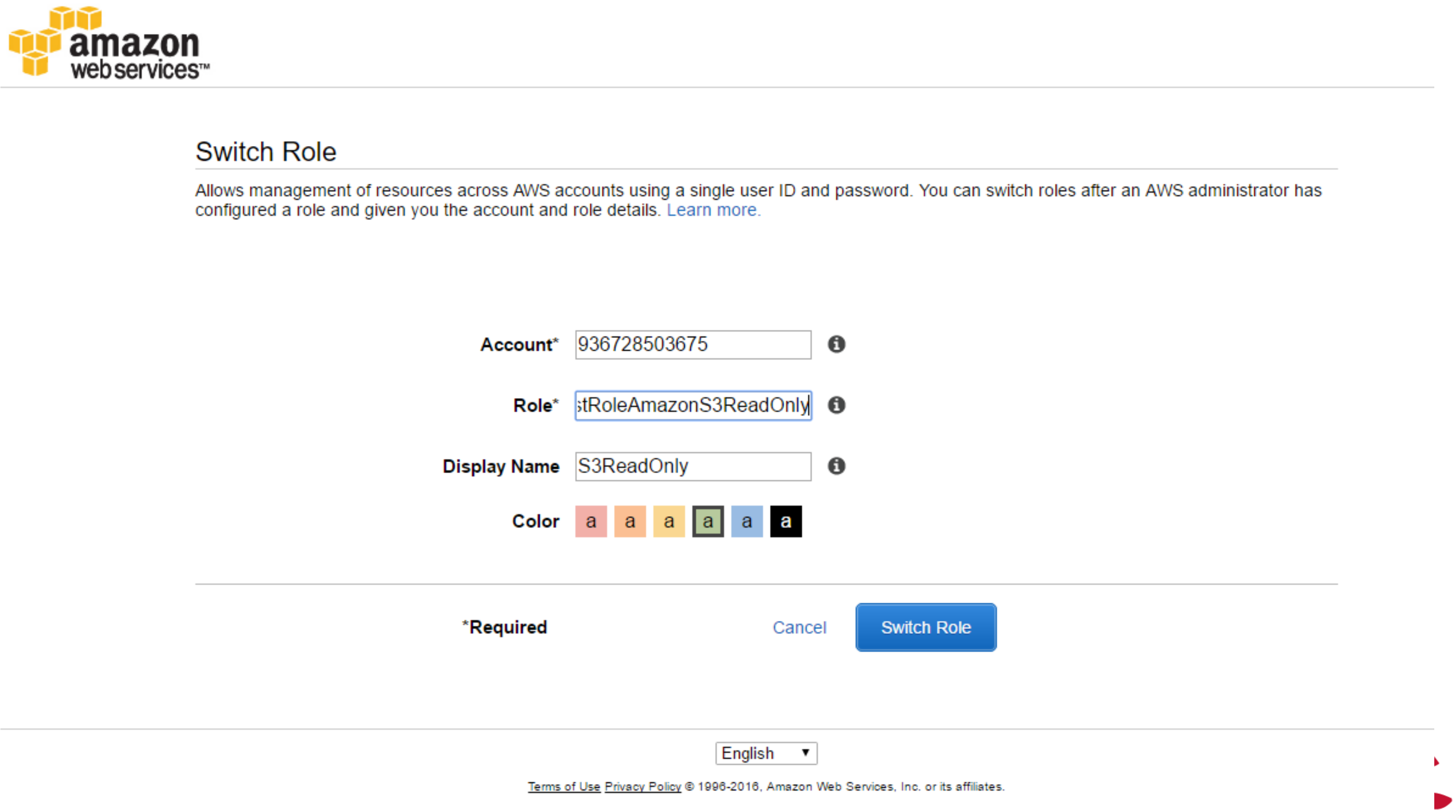
Trusted Entities
The account 936728503675

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*	936728503675
Role*	:tRoleAmazonS3ReadOnly
Display Name	S3ReadOnly
Color	a a a a a a

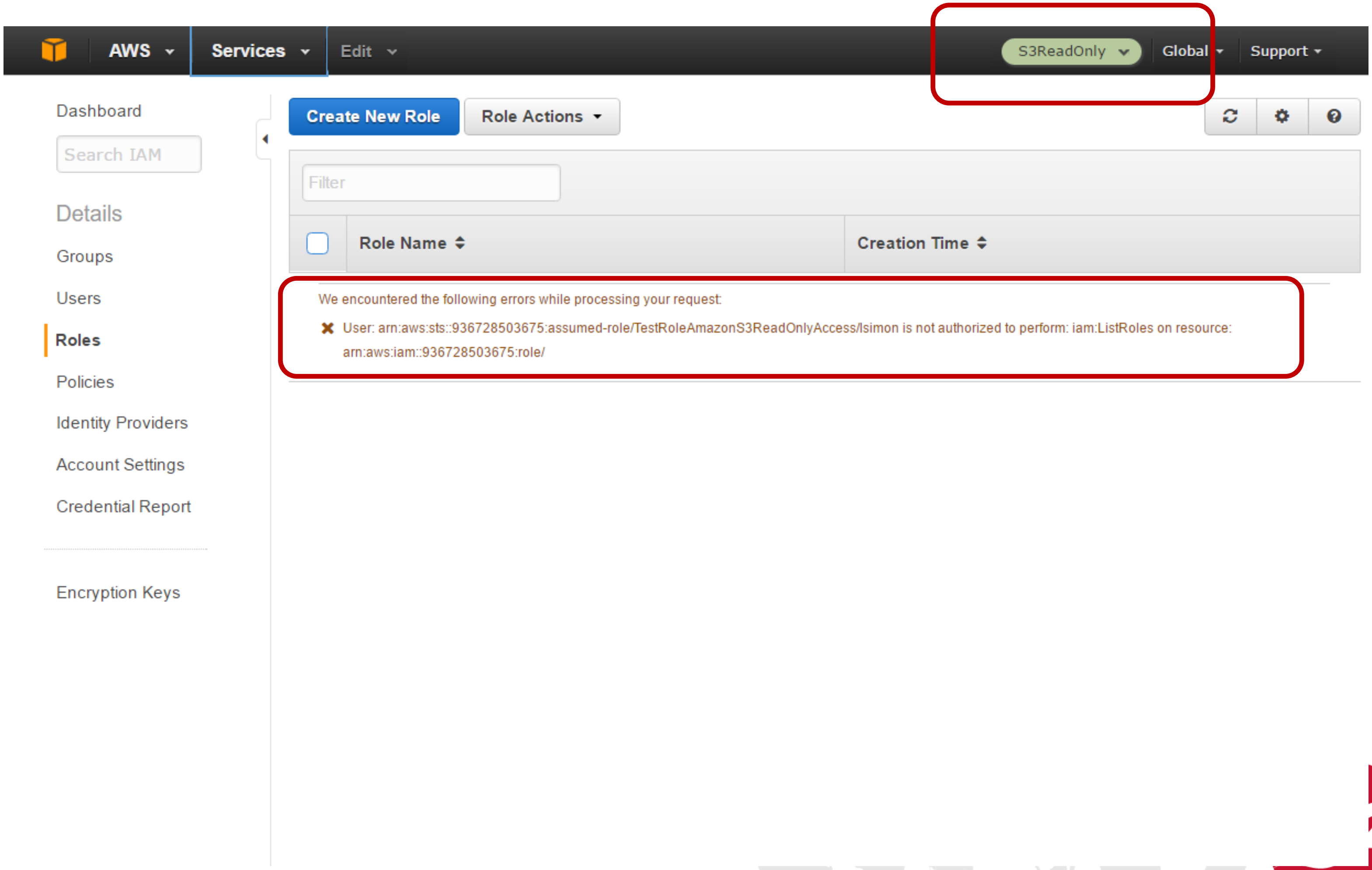
*Required

Cancel Switch Role

English ▼

Terms of Use Privacy Policy © 1996-2016, Amazon Web Services, Inc. or its affiliates.

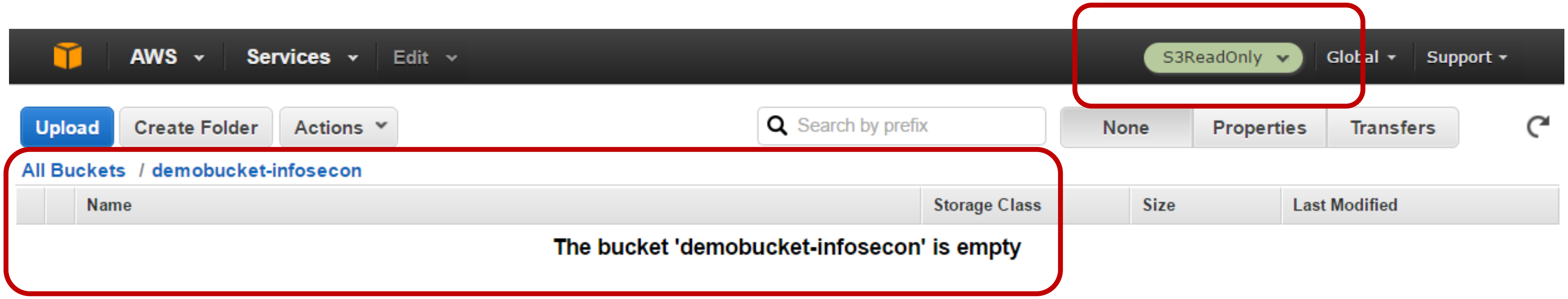
Usage in Web Console



We encountered the following errors while processing your request:

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

Usage in Web Console

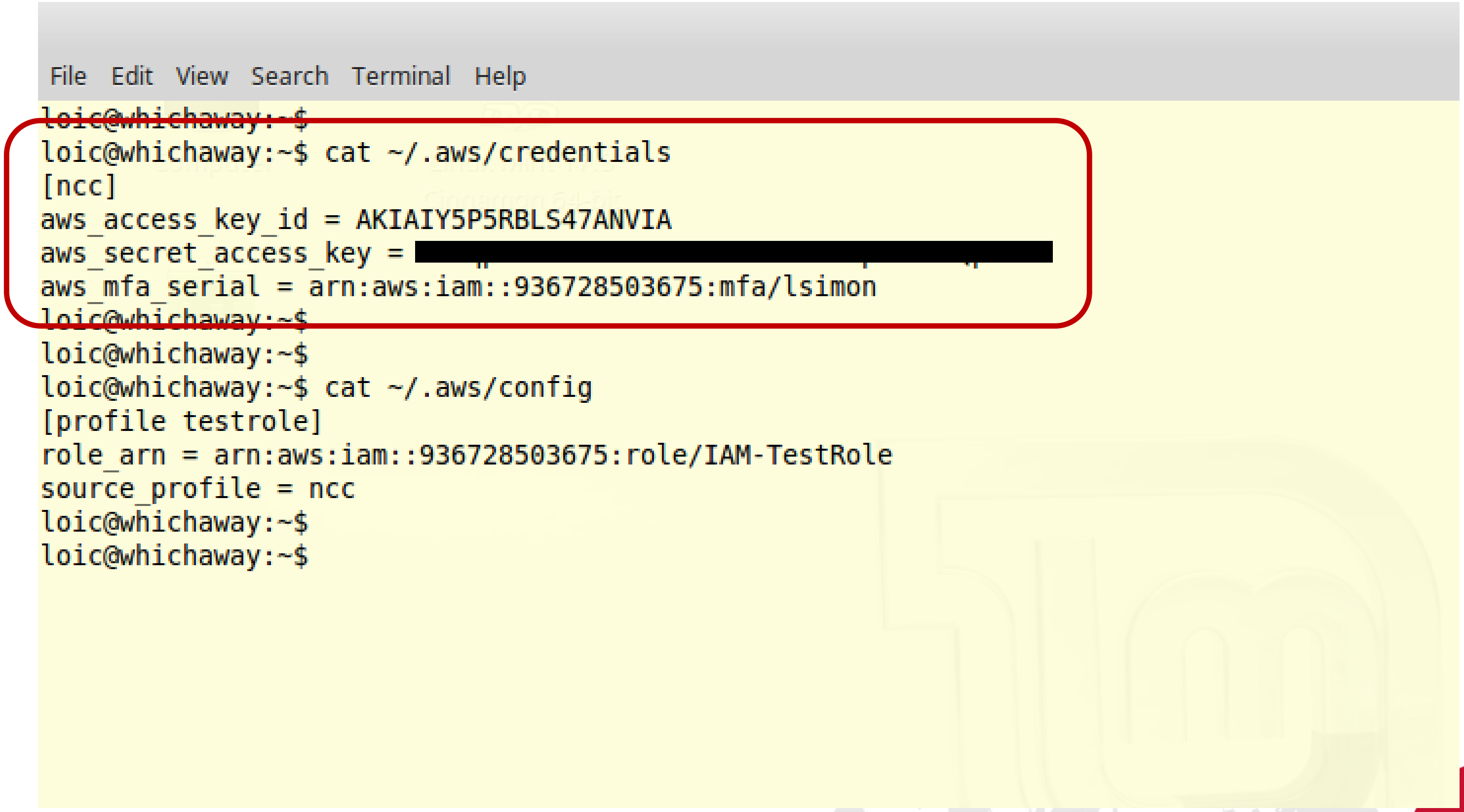


All Buckets / demobucket-infosecon

Name	Storage Class	Size	Last Modified

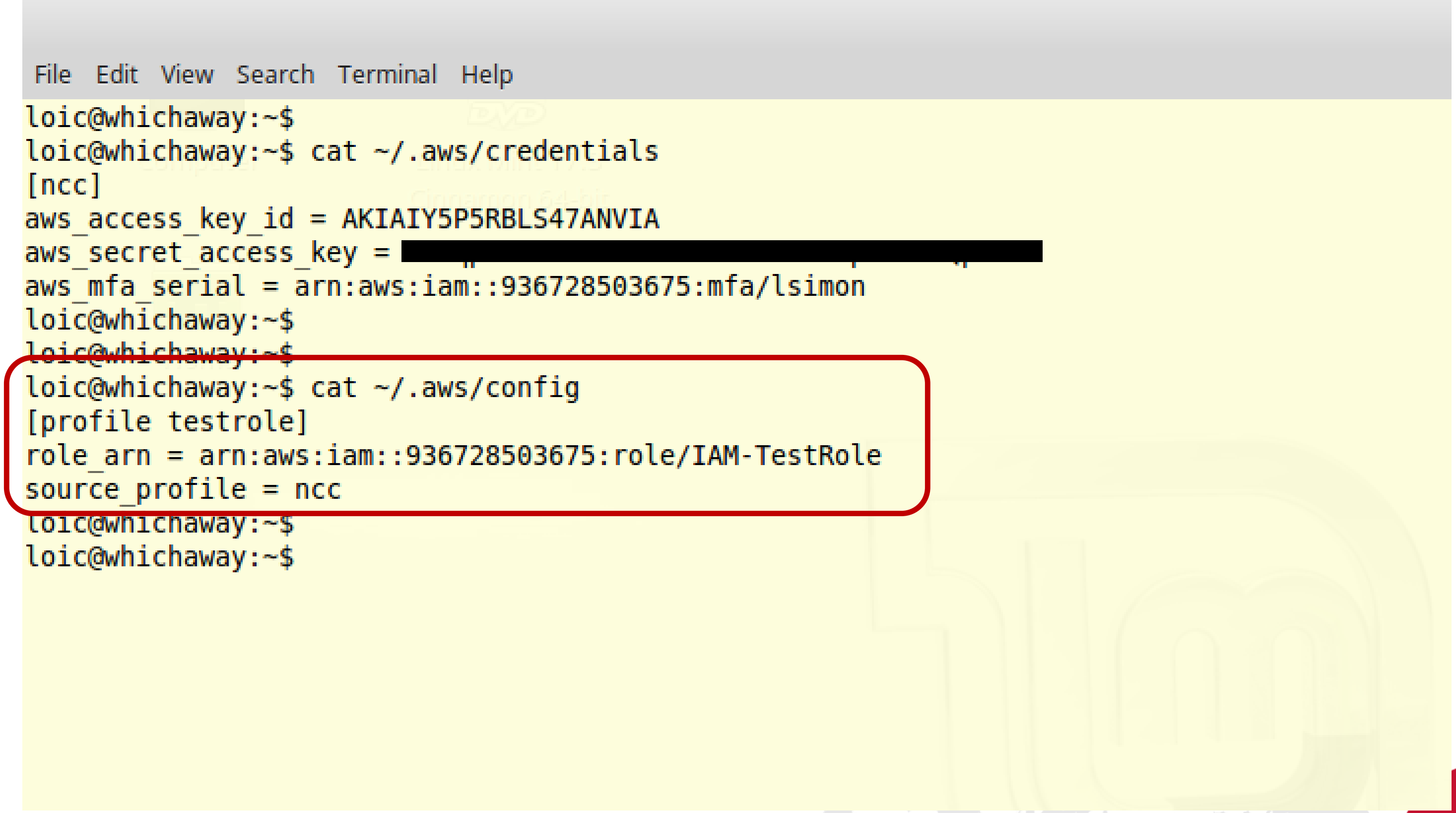
The bucket 'demobucket-infosecon' is empty

Usage in CLI



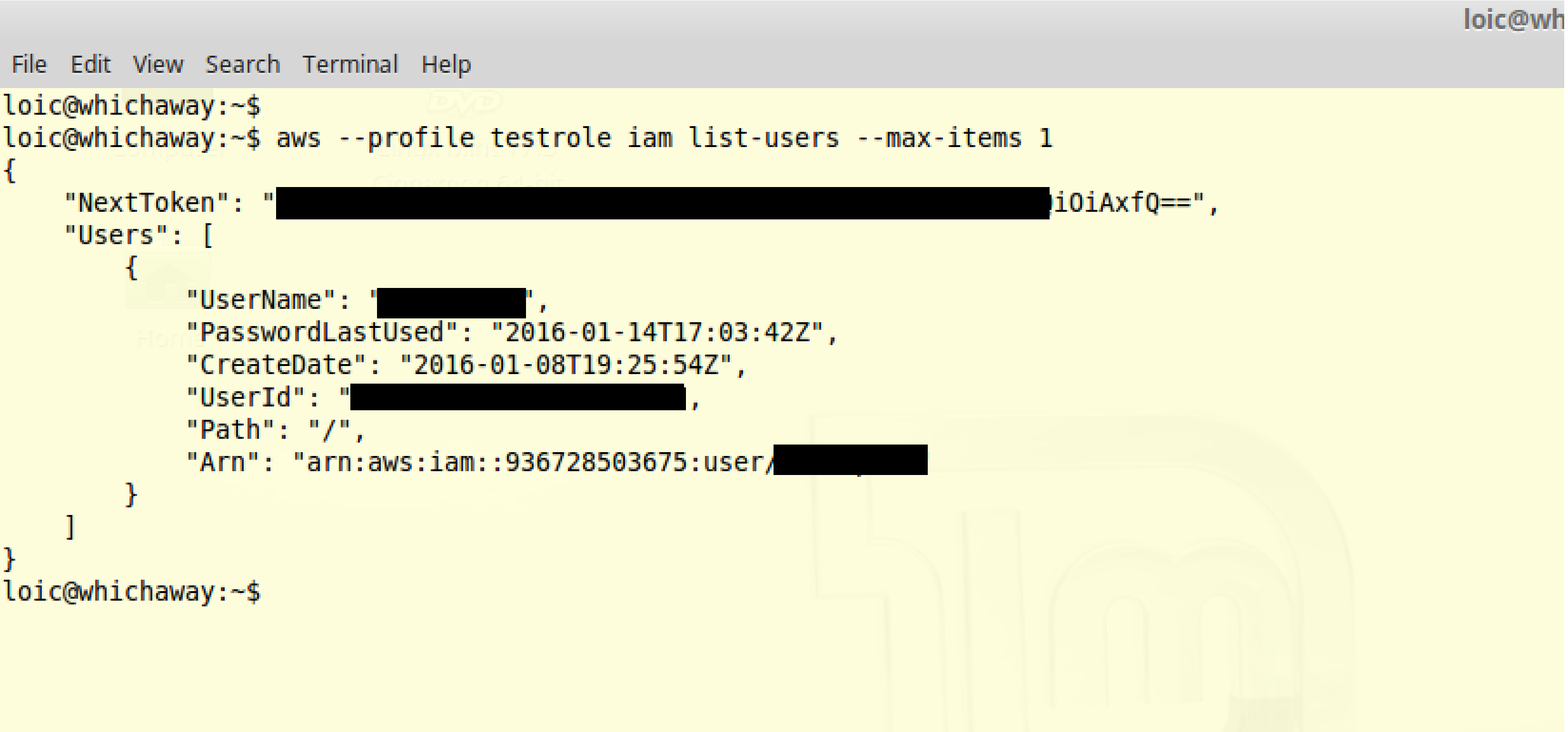
```
loic@whichaway:~$
loic@whichaway:~$ cat ~/.aws/credentials
[ncc]
aws_access_key_id = AKIAIY5P5RBLS47ANVIA
aws_secret_access_key = [redacted]
aws_mfa_serial = arn:aws:iam::936728503675:mfa/lsimon
loic@whichaway:~$
loic@whichaway:~$
loic@whichaway:~$ cat ~/.aws/config
[profile testrole]
role_arn = arn:aws:iam::936728503675:role/IAM-TestRole
source_profile = ncc
loic@whichaway:~$
loic@whichaway:~$
```

Usage in CLI



```
loic@whichaway:~$
loic@whichaway:~$ cat ~/.aws/credentials
[ncc]
aws_access_key_id = AKIAIY5P5RBLS47ANVIA
aws_secret_access_key = [redacted]
aws_mfa_serial = arn:aws:iam::936728503675:mfa/lsimon
loic@whichaway:~$
loic@whichaway:~$
loic@whichaway:~$ cat ~/.aws/config
[profile testrole]
role_arn = arn:aws:iam::936728503675:role/IAM-TestRole
source_profile = ncc
loic@whichaway:~$
loic@whichaway:~$
```

Usage in CLI



```
loic@whichaway:~$
loic@whichaway:~$ aws --profile testrole iam list-users --max-items 1
{
    "NextToken": "[redacted]iOiAxfQ==",
    "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