

SUMMARY:

This Lab covers fundamental IAM functions, AWS Orgs, SCP's, and Cloud Trail logging

Contents

1. Simple Identity Permissions in AWS	1
2. Groups in IAM	3
3. AWS Organization Creation:	5
4. Create Service Control Policy for the ORG.....	8
5. Cloud Trail – implementing and ORG trail	10

1. Simple Identity Permissions in AWS

CFN Template to use for default user with password change policy:

```
AWSTemplateFormatVersion: "2010-09-09"
Description: >
  This template implements an IAM user 'Sally'
  An S3 bucket for cat pictues
  An S3 bucket for dog pictures
  An S3 bucket for other animals
  And permissions appropriate for Sally.
Parameters:
  sallypassword:
    NoEcho: true
    Description: IAM User Sallys Password
    Type: String
Resources:
  catpics:
    Type: AWS::S3::Bucket
  animalpics:
    Type: AWS::S3::Bucket
  sally:
    Type: AWS::IAM::User
    Properties:
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/IAMUserChangePassword
      LoginProfile:
        Password: !Ref sallypassword
        PasswordResetRequired: "true"
  policy:
    Type: AWS::IAM::ManagedPolicy
    Properties:
      Description: Allow access to all S3 buckets, except catpics
      ManagedPolicyName: AllowAllS3ExceptCats
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Action: 's3:*
```

```

Resource: '*'
- Effect: Deny
Action: 's3:*'
Resource: [ !GetAtt catpics.Arn, !Join ['', [!GetAtt catpics.Arn, '/*']] ]

```

Outputs:

```

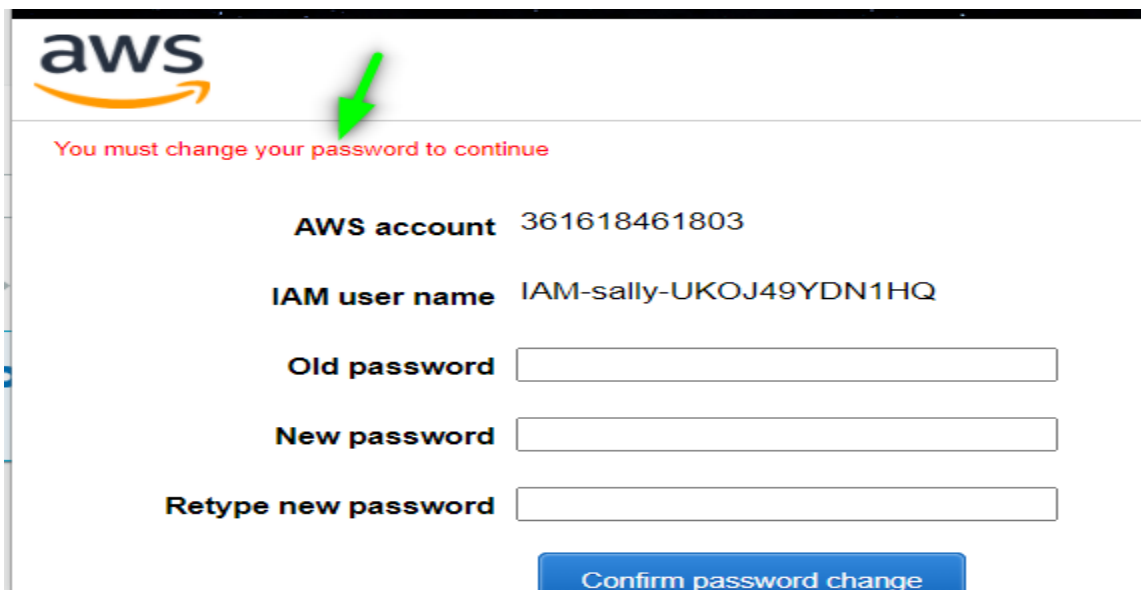
catpicsbucketname:
  Description: Bucketname for catpictures (the best animal!)
  Value: !Ref catpics
animalpicsbucketname:
  Description: Bucketname for animalpics (the almost best animals!)
  Value: !Ref animalpics
sallyusername:
  Description: IAM Username for Sally
  Value: !Ref sally

```

CFN Resources completed:

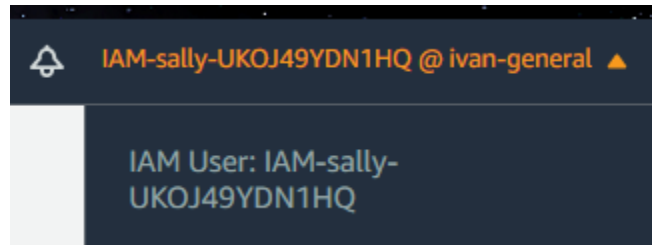
animalpics	←	iam-animalpics-tmy8z0gp5ut0	AWS::S3::Bucket	✓ CREATE_COMPLETE	-
catpics	←	iam-catpics-1553i1oem4ibo	AWS::S3::Bucket	✓ CREATE_COMPLETE	-
policy	←	arn:aws:iam::361618461803:policy/AllowAllS3ExceptCats	AWS::IAM::ManagedPolicy	✓ CREATE_COMPLETE	-
sally	←	IAM-sally-UKOJ49YDN1HQ	AWS::IAM::User	✓ CREATE_COMPLETE	-

Confirm and Login as Sally user:



The screenshot shows the AWS 'Change Password' interface. At the top is the AWS logo. Below it, a red message states: 'You must change your password to continue'. A green arrow points to this message. The page displays the following information:

- AWS account:** 361618461803
- IAM user name:** IAM-sally-UKOJ49YDN1HQ
- Old password:** [input field]
- New password:** [input field]
- Retype new password:** [input field]
- Confirm password change:** [blue button]



CFN to add to sally user – as an in-line policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

Add a managed policy to Sally user:

	Policy name ▼	Type	Used as
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	AWS managed	None
<input checked="" type="checkbox"/>	AllowAllS3ExceptCats	Customer managed	None
<input type="checkbox"/>	AmazonAPIGatewayAdministrator	AWS managed	None
<input type="checkbox"/>	AmazonAPIGatewayInvokeFullAccess	AWS managed	None
<input type="checkbox"/>	AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	None
<input type="checkbox"/>	AmazonAppFlowFullAccess	AWS managed	None

Cancel Next: Review

2. Groups in IAM

Create “developers” group > remove sally managed permissions, and switch over to group:

Add users to developers

Other users in this account (Selected 1/2) [Info](#)

Search

	User name	Groups	Last activity	Creation time
<input checked="" type="checkbox"/>	IAM-sally-UKOJ49YDN1HQ	0	2 hours ago	2 hours ago
<input type="checkbox"/>	iamadmin	0	2 hours ago	Yesterday

Cancel Add users

User group name developers	Creation time July 12, 2021, 20:48 (UTC-05:00)	ARN arn:aws:iam::361618461803:group/developers
-------------------------------	---	---

Users **Permissions** Access advisor

Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter

	Policy Name	Type	Attached entities
<input type="checkbox"/>	AllowAllS3ExceptCats	Customer managed	1

Clean up account when finished, delete CFN IAM stack:

IAM Delete Update Stack actions Create stack

Stack info Events Resources Outputs Parameters Template Change sets

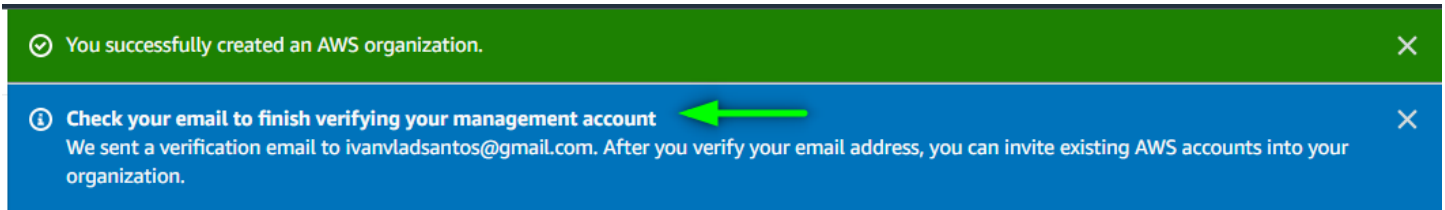
Overview

Stack ID arn:aws:cloudformation:us-east-1:361618461803:stack/IAM/73194f60-e366-11eb-8474-124aa02dc2ed	Description This template implements an IAM user 'Sally' An S3 bucket for cat pictures An S3 bucket for dog pictures An S3 bucket for other animals And permissions appropriate for Sally.
Status DELETED_COMPLETE	Status reason -

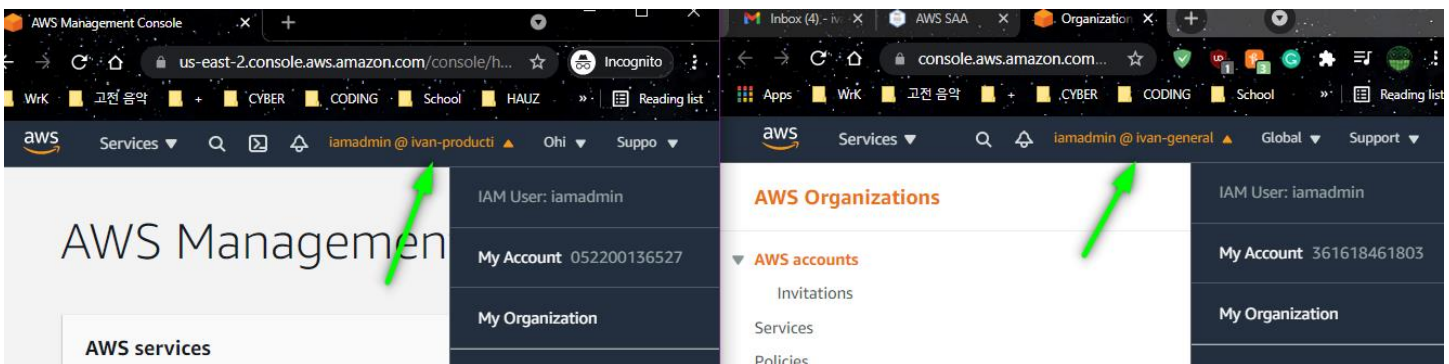
3. AWS Organization Creation:

- The GENERAL account will become the MASTER account for the organisation
- We will invite the PRODUCTION account as a MEMBER account and create the DEVELOPMENT account as a MEMBER account.
- Finally - we will create an OrganizationAccountAccessRole in the production account, and use this role to switch between accounts.

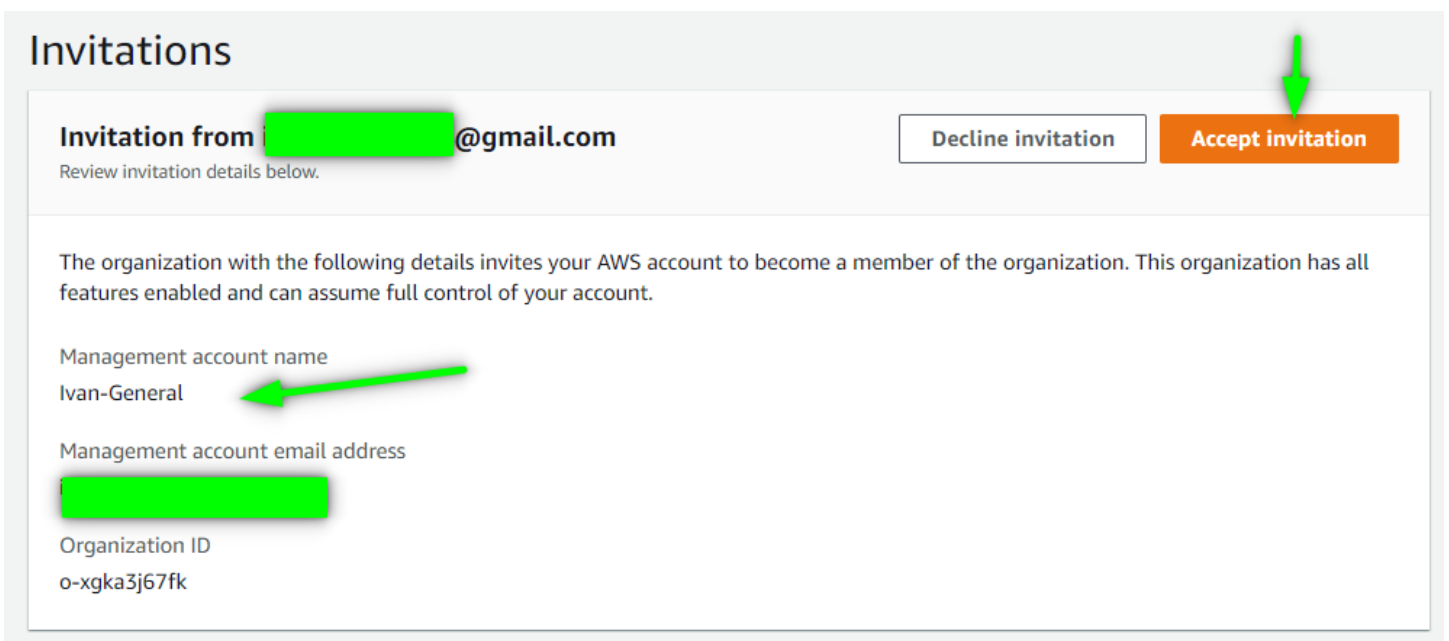
Create main Organization from General account:






Add Production account to new ORG:



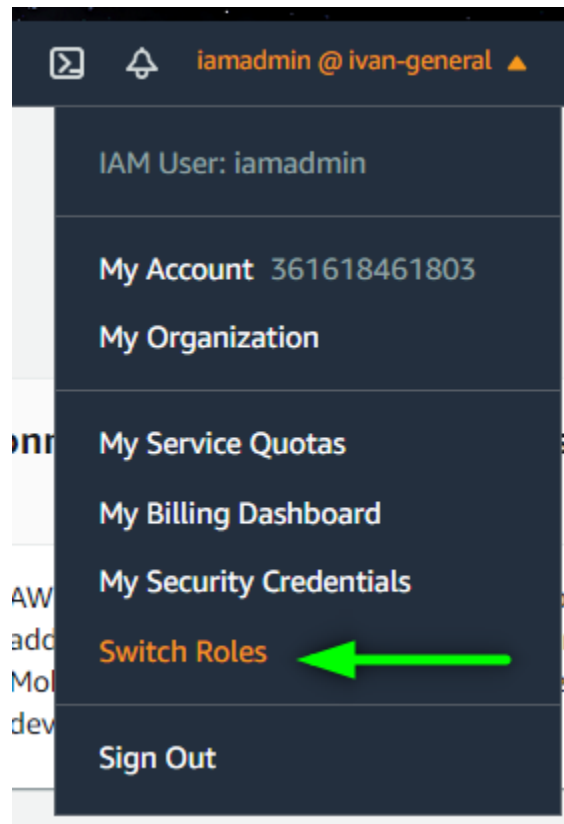
Be sure to accept invite, via email on Production account:



Prod account added:

Organizational structure		Account created/joined date
▼ <input type="checkbox"/>  Root r-6mog		
<input type="checkbox"/>  Ivan-General management account 361618461803 [REDACTED]		2021/07/12
<input type="checkbox"/>  Ivan-Production 052200136527 [REDACTED]		2021/07/12
<input checked="" type="checkbox"/> OrganizationAccountAccessRole Account: 361618461803		

Add the newly added production account to Switch Roles on General acc Console:



Switch Role

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

Account*

052200136527

Role*

OrganizationAccountAcces

Display Name

PROD

Color

a

a

a

a

a

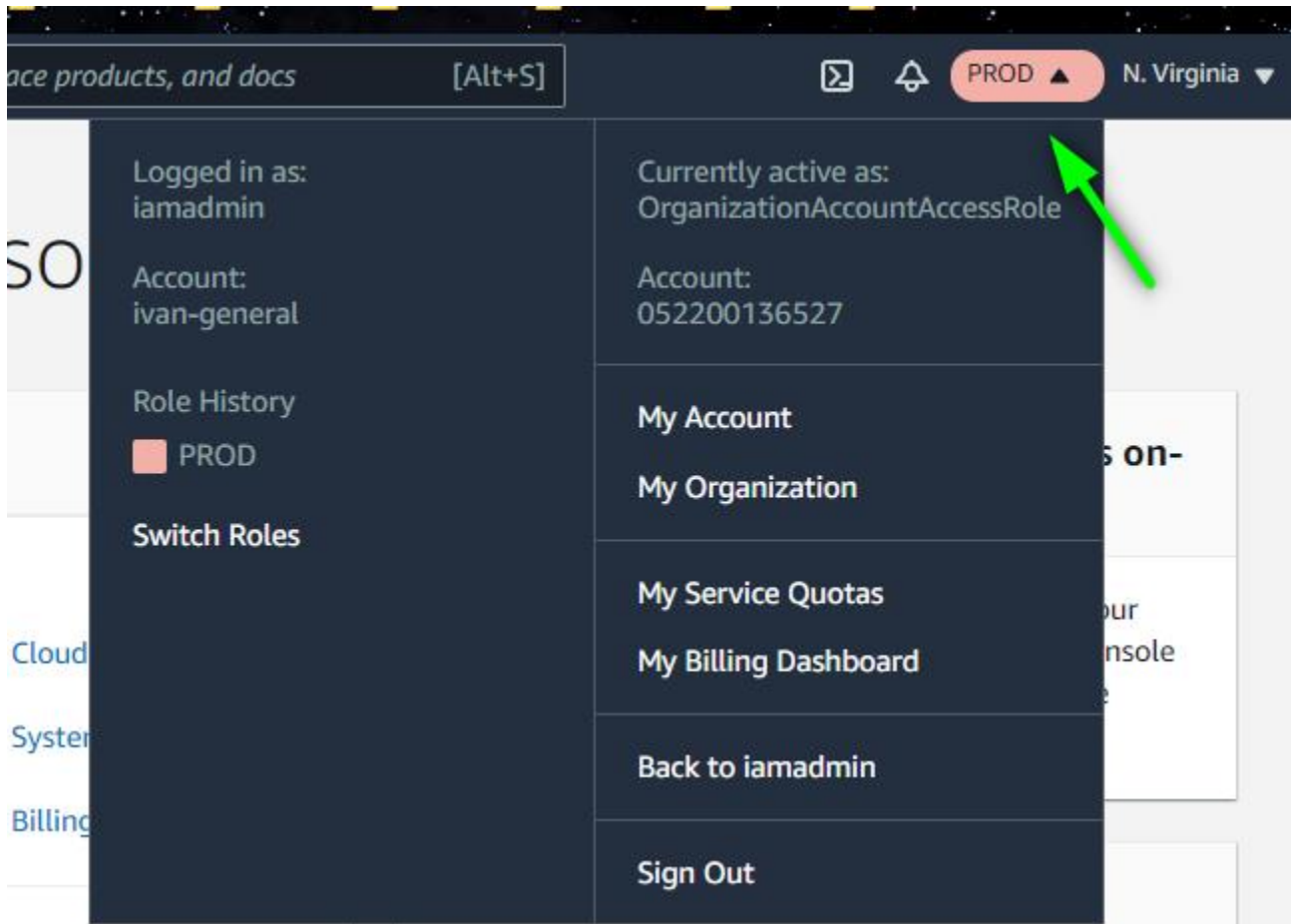
a

*Required

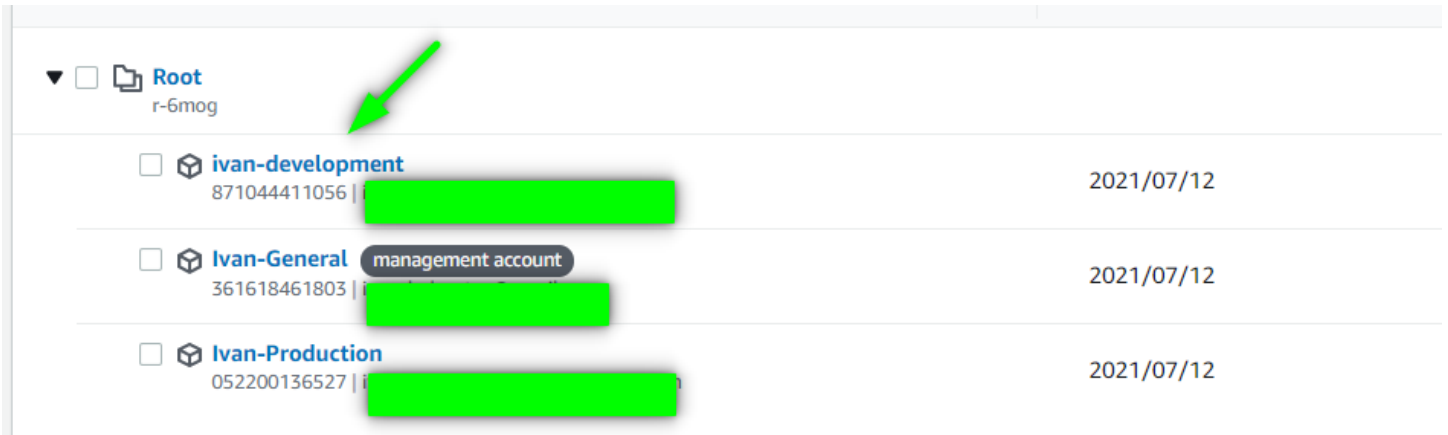
Cancel

Switch Role

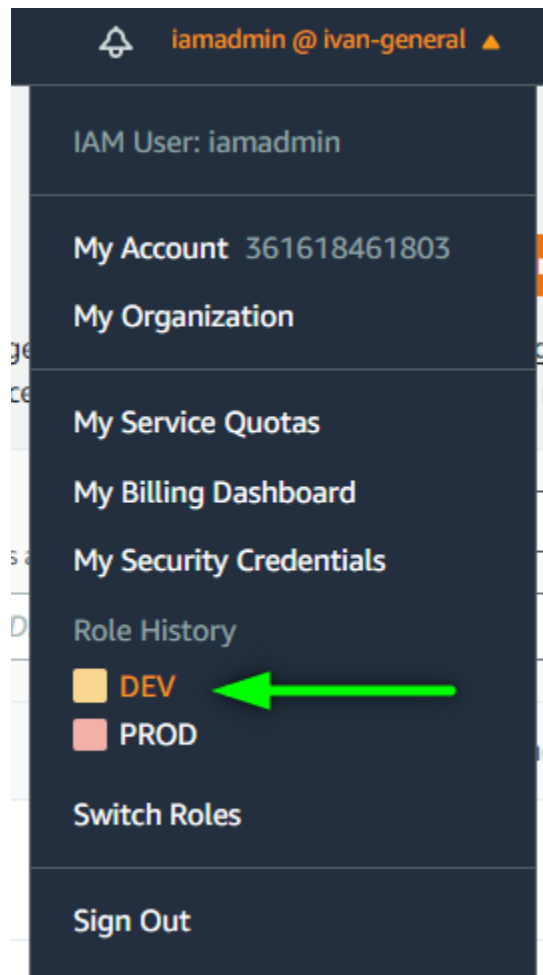
Can now seamlessly switch account from General account:



Create Development account in Organization, and add to switch role to have 3 total accounts in the ORG:



▼	<input type="checkbox"/>		Root	r-6mog	
	<input type="checkbox"/>		Ivan-development	871044411056 [REDACTED]	2021/07/12
	<input type="checkbox"/>		Ivan-General	361618461803 [REDACTED] management account	2021/07/12
	<input type="checkbox"/>		Ivan-Production	052200136527 [REDACTED]	2021/07/12



4. Create Service Control Policy for the ORG

Create OU structure for accounts in ORG:

Organizational structure	Account created/joined date
<div>▼ <input type="checkbox"/> Root r-6mog</div>	
<div> ▼ <input type="checkbox"/> DEV ou-6mog-n0b6f6oc <div> <input type="checkbox"/> ivan-development 871044411056 </div> </div>	2021/07/12
<div> ▼ <input type="checkbox"/> PROD ou-6mog-xb88w8ns <div> <input type="checkbox"/> Ivan-Production 052200136527 </div> </div>	2021/07/12
<div> <input type="checkbox"/> Ivan-General management account 361618461803 </div>	2021/07/12

Enable SCP in AWS ORG:

Service control policies


Service control policies (SCPs) enable central administration over the permissions available within the accounts in your organization. This helps ensure that your accounts stay within your organization's access control guidelines. [Learn more](#)

Enable service control policies

JSON for Policy (denies access to S3):

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```


SCP is created:

Available policies				Actions ▼	Create policy
<input type="checkbox"/>	Name ▲	Kind	Description		
<input type="checkbox"/>	Allow All Except S3 	Customer managed policy	-		
<input type="checkbox"/>	FullAWSAccess	AWS managed policy	Allows access to every operation		

Assign to PROD account, and test with S3:



You don't have permissions to list buckets

After you or your AWS administrator have updated your permissions to allow the s3:ListAllMyBuckets action, refresh this page. Learn more about [Identity and access management in Amazon S3](#) 


SCP kicks in and denies access ^

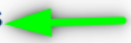
5. Cloud Trail – implementing and ORG trail

- In this [DEMO] lesson we will implement a Organizational CloudTrail for the Animals4life organisation.
- This CloudTrail will be configured for all regions and set to log global services events.
- We will set the trail to log to an S3 bucket and then enhance it to inject data into CloudWatch Logs.
- CloudTrail Pricing : <https://aws.amazon.com/cloudtrail/pricing/>
- CloudWatch Logs Pricing : <https://aws.amazon.com/cloudwatch/pricing/>

Feel free to disable the trail after completion if you are concerned about small S3 costs ... (there is a \$0.01 per 2000 requests and cloudtrail can be pretty noisy)

Setup cloudwatch logs:

General details 		
Trail name Animals4lifeORG	Trail log location cloudtrail-animals4life-ivan19283791826192837/AWSLogs/o-xgka3j67fk/361618461803	Log file validation Disabled
Multi-region trail Yes	Log file SSE-KMS encryption Not enabled	SNS notification delivery Disabled
Apply trail to my organization Enabled for all accounts		

CloudWatch Logs 	
Log group aws-cloudtrail-logs-361618461803-cde4e7f7	IAM Role CloudTrailRoleForCloudWatchLogs_Animals4life

Create Trail:

Trails Refresh Delete Create trail Settings									
	Name ▲	Home region ▼	Multi-region trail ▼	Insights ▼	Organization trail ▼	S3 bucket ▼	Log file prefix ▼	CloudWatch Logs log group ▼	Status ▼
<input type="radio"/>	Animals4life ORG	US East (N. Virginia)	Yes	Disabled	Yes	cloudtrail-animals4life-ivan19283791826192837		arn:aws:logs:us-east-1:361618461803:log-group:aws-cloudtrail-logs-361618461803-cde4e7f7:*	Logging

Can locate Trail log in S3 bucket:

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

1

<div><div></div></div>	Name	Type	Last modified	Size	Storage class
<div><div></div></div>	<div><div></div> 361618461803_CloudTrail_us-east-1_20210713T0445Z_HZFJKmh50Z5Cjtaq.json.gz</div>	gz	July 12, 2021, 23:50:03 (UTC-05:00)	1.1 KB	Standard

Log in JSON:

JSONRaw DataHeaders

SaveCopyCollapse AllExpand AllFilter JSON

▼ Records:

▼ 0:

eventVersion:"1.05"

▼ userIdentity:

type:"IAMUser"

principalId:"AIDAX5K53LLHXAEDUWFRW"

arn:"arn:aws:iam::544047061711:user/iamadmin"

accountId:"544047061711"

accessKeyId:"ASIA5K53LLHYM3F7KVZ"

userName:"iamadmin"

▼ sessionContext:

sessionIssuer: {}

webIdFederationData: {}

▼ attributes:

mfaAuthenticated:"true"

creationDate:"2020-08-19T20:56:50Z"

eventTime:"2020-08-19T22:25:05Z"

eventSource:"health.amazonaws.com"

eventName:"DescribeEventAggregates"

awsRegion:"us-east-1"

sourceIPAddress:"119.18.34.73"

userAgent:"console.amazonaws.com"

▼ requestParameters:

aggregateField:"eventTypeCategory"

▼ filter:

▼ eventStatusCodes:

0:"open"

1:"upcoming"

▼ startTimes:

▼ 0:

from:"Aug 12, 2020 10:25:04 PM"

responseElements:null

requestID:"d17f8424-7db5-4f1c-ab27-b21e376b9192"

eventID:"af127628-86ed-4ddf-afad-13d8ead90c97"

eventType:"AwsApiCall"

recipientAccountId:"544047061711"

Logging also being done in CloudWatch Logs:

CloudWatch X

- Dashboards
- Alarms
- Logs
- Metrics
- Events
- ServiceLens
- Container Insights
- Lambda Insights
- Synthetics
- Contributor Insights
- Settings

Log streams | Metric filters | Subscription filters | Contributor Insights | Tags

Log streams (2) [Refresh] [Delete] [Create log stream] [Search all]

Filter log streams or try prefix search

<input type="checkbox"/>	Log stream	Last event time
<input type="checkbox"/>	o-xgka3j67fk_361618461803_CloudTrail_us-east-1	2021-07-12 23:49:59 (UTC-05:00)
<input type="checkbox"/>	361618461803_CloudTrail_us-east-1	-

Policy for Trail:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailCreateLogStream2014110",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:us-east-1:361618461803:log-group:aws-cloudtrail-logs-361618461803-cde4e7f7:log-stream:361618461803_CloudTrail_us-east-1*",
        "arn:aws:logs:us-east-1:361618461803:log-group:aws-cloudtrail-logs-361618461803-cde4e7f7:log-stream:o-xgka3j67fk_*"
      ]
    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
```

```
"arn:aws:logs:us-east-1:361618461803:log-group:aws-cloudtrail-logs-361618461803-cde4e7f7:log-stream:361618461803_CloudTrail_us-east-1*",  
  "arn:aws:logs:us-east-1:361618461803:log-group:aws-cloudtrail-logs-361618461803-cde4e7f7:log-stream:o-xgka3j67fk_**"  
]  
}  
]  
}
```