amazon web services | Professional Services

AWS Organizations and IAM Policy Management

… is crucial to running a Secure Cloud Environment

Marcus Fritsche

18.05.2017

amazon web services

In the beginning…

You

Today

Your Cloud Team

Cross Account Resource Access

Jump Account

Cross Account Trusts

Dev Account

Data Science Account

Prod Account

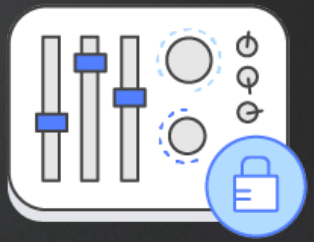
Security Account

amazon web services

What do YOU want to do?

Use **AWS account boundaries** for isolation.

Centrally manage policies across many accounts.

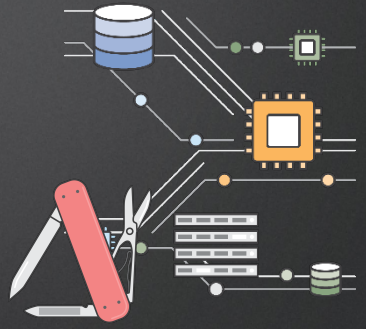


Delegate permissions, but maintain guardrails.

See combined view of all charges.

What challenges are customers facing?

Creating a new AWS account involves many manual processes.



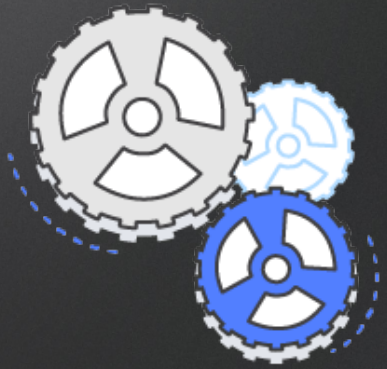
Managing IAM policies across many AWS accounts requires custom automation and scripting.

Delegating local administration is an all or nothing proposition.

Introducing AWS Organizations

… a new policy-based management capability for multiple AWS accounts.

Control AWS service use across accounts



Automate AWS account creation

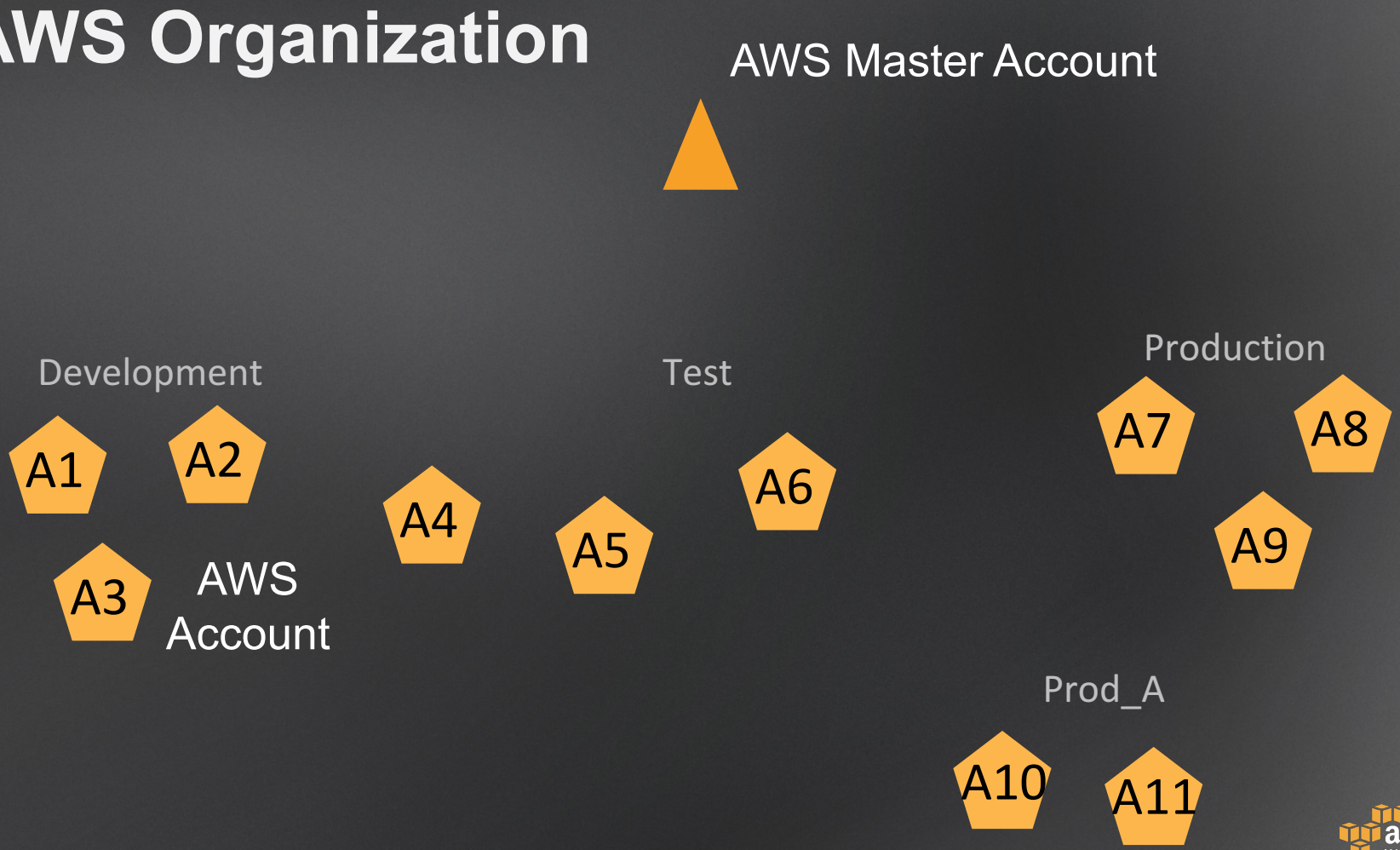
Consolidate billing

AWS Organization

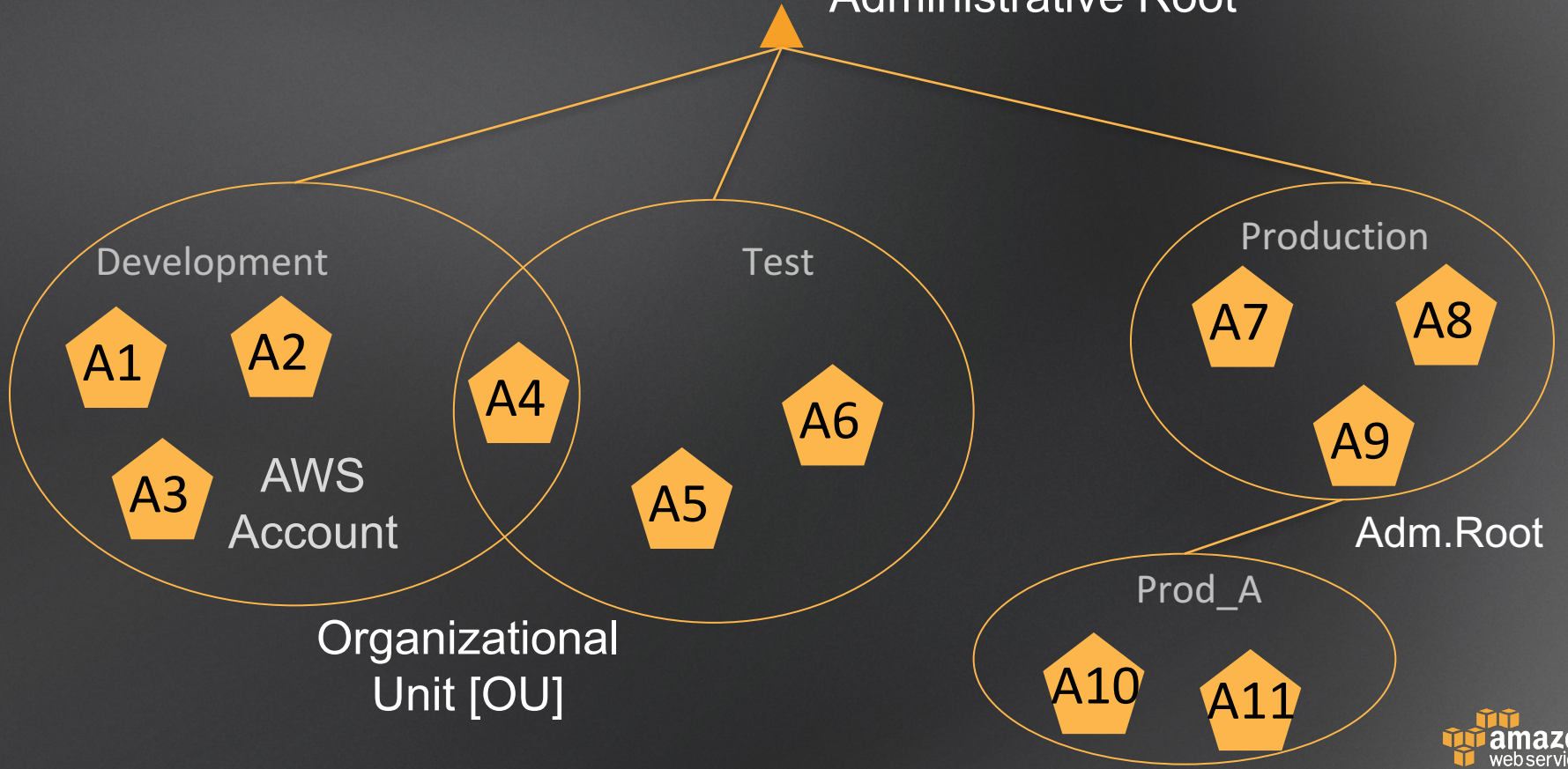
AWS Master Account

=> the Structure

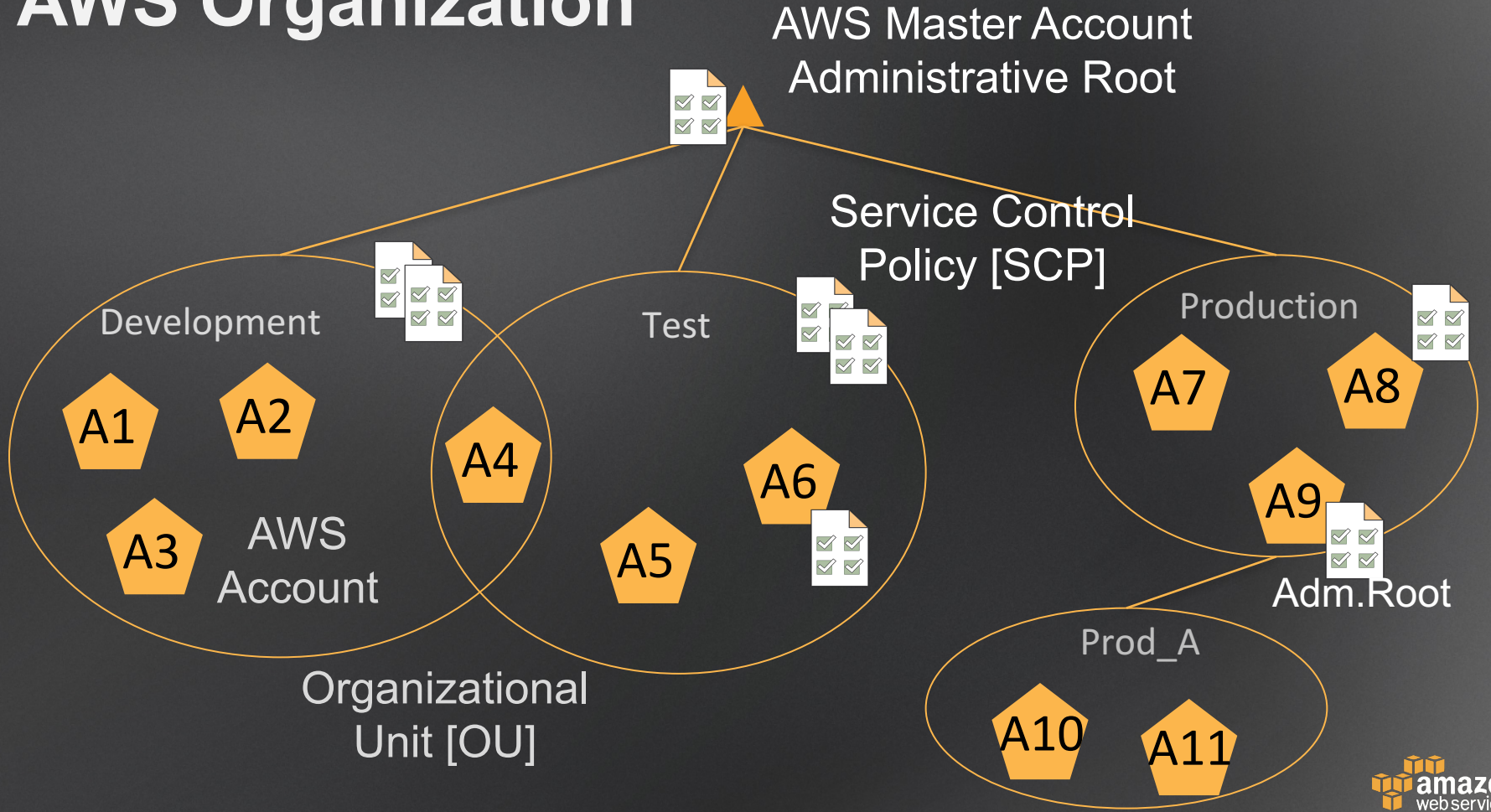
AWS Organization



AWS Organization



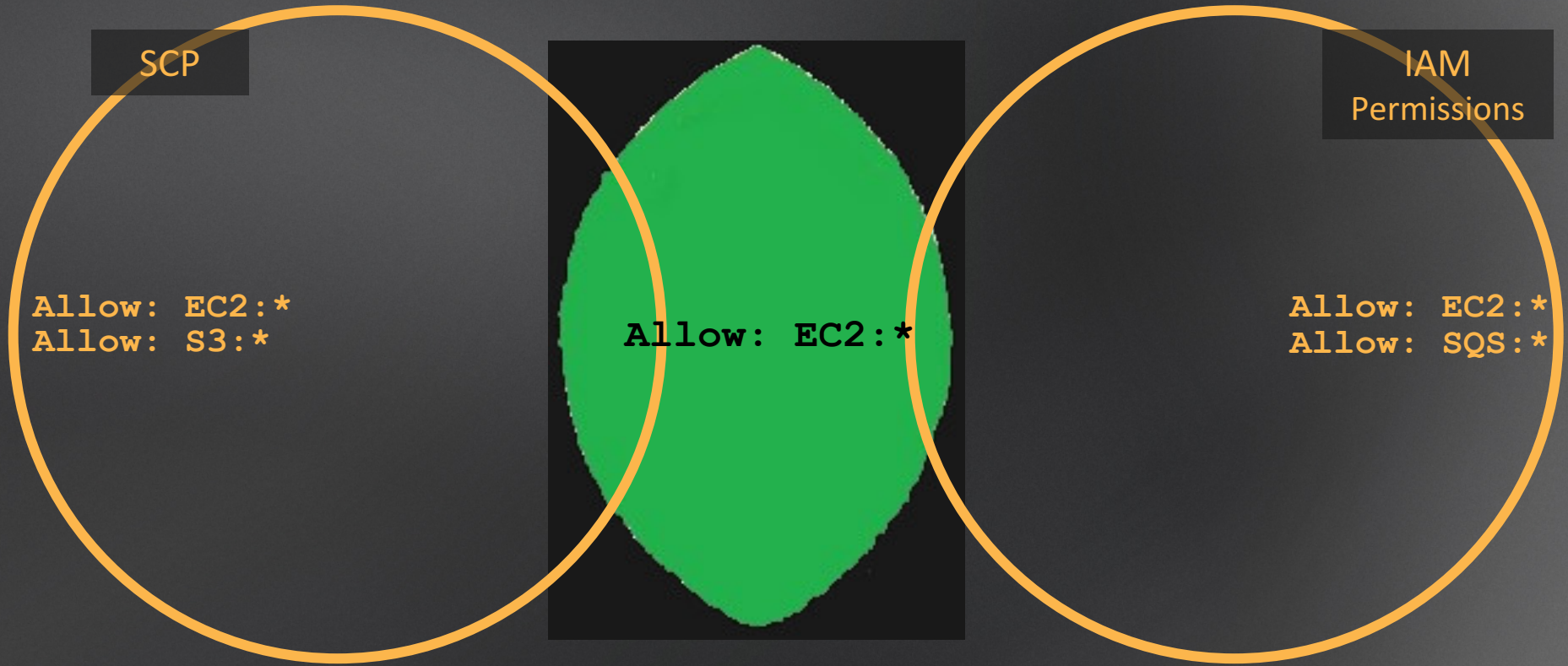
AWS Organization



AWS Organizations & AWS IAM-Policies

- Create groups of AWS accounts with AWS Organizations
- Use Organizations to attach SCPs to those groups to centrally control AWS service use.
- **SCP**olicies start from “all is ALLOWED”
  IAM-Policies start from “all is DENIED”
- Entities in the AWS accounts can only use the AWS services allowed by both the SCP and the IAM policies

SCPs are necessary but not sufficient



Blacklisting example

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

Whitelisting example

```
{
 "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances",
         "ec2:DescribeInstances",
         "ec2:DescribeImages",
         "ec2:DescribeKeyPairs",
         "ec2:DescribeVpcs",
         "ec2:DescribeSubnets",
         "ec2:DescribeSecurityGroups“,
          "s3:*"
      ],
      "Resource": "*"
    }
 ]
}
```

Key Features

- Policy framework for multiple AWS accounts.
- Group-based account management.
- Account creation and management APIs.
- Consolidated billing for all AWS accounts in your organization.
- Enable Consolidated Billing Only or All Features.

- Available at no additional charge.
- Global service, accessed via endpoint in N. Virginia region.

Best practices – AWS Organizations

- Secure new accounts
- Monitor activity in the master account
- No resources in master account
- Principal of “Least privilege”
- Use OUs to assign controls
- Test controls
- Assigned controls not at root of organization
- Avoid “whitelisting” and “blacklisting”

Root - Account

The organization master root account
is **all powerful!**

=> The root account needs protecting, especially
the organizational master root account.

Now - get started!

- Your account segmentation strategy is ..
- Your type of organization is ..
- Organize your AWS accounts according to it
- Test & begin to apply SCPs / IAM Policies slowly
- Iterate on SCPs and IAM Policies, ..
- Use our scripts!

Questions?

Backup Slides

https://code.amazon.com/packages/Organizations-demos/trees/mainline

NAME	SIZE	MODE	AGE
automated-account-creation/	-	-	14 days ago
automated-account-linking/	-	-	5 days ago
central-group-policies/	-	-	14 days ago
blacklist-live-services.scp	148	rw- r-- r--	about 1 month ago
central_group_policies.py	6,155	rwx r-x r-x	14 days ago
CentralGroupPolicies.mp4	13,181,534	rw- r-- r--	14 days ago
CentralGroupPolicies.pptx	2,370,685	rw- r-- r--	about 1 month ago
clidemo.py	1,235	rw- r-- r--	14 days ago
org_prune.py	535	rwx r-x r-x	14 days ago
org_tree.py	360	rwx r-x r-x	14 days ago
orgutils.py	5,855	rw- r-- r--	14 days ago
README.md	5,314	rw- r-- r--	14 days ago
whitelist-approved-services.scp	742	rw- r-- r--	14 days ago
corporate-compliance/	-	-	about 2 months ago
create-account-cli/	-	-	5 days ago

Organizations Demos

Creating an Org from CLI

aws organizations create-organization --feature-set ALL

RETURNS

{ "organization": { "availablePolicyTypes": [{ "status": "ENABLED", "type": "service_control_policy" }], "masterAccountId": "000000000001", "masterAccountArn": "arn:aws:organizations::000000000001:account/o-1234567890/000000000001", "mode": "FULL_CONTROL", "masterAccountEmail": "master.account@example.corp", "id": "o-1234567890", "arn": "arn:aws:organizations::000000000001:organization/o-1234567890" } }

Modify Org to Full Control

aws organizations enable-all-features