COPEBIT

Best Practices for IAM with Amazon Web Services

Marco Kuendig, CTO

19th September 2024

Agenda

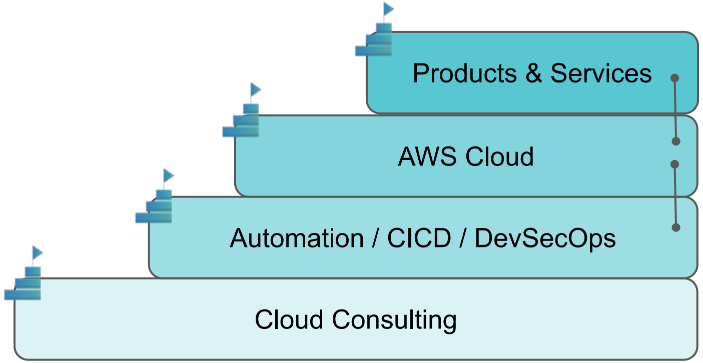
- Brief introduction of copebit
- Global IAM at AWS
    - LandingZone
    - Identities with IAM Identity Center
    - Integration with EntraID or Google Workspace, etc.
    - PermissionSets and Roles
    - Global Policy Enforcement with SCP
    - Temporary elevated access / PIM
- Child Account IAM
    - Automatic Role Assumption
    - Technical Users (Roles)
        - For AWS Services
        - For Kubernetes

Introduction Copebit

Facts & figures

- copebit AG founded 2016
- SG / ZH
- 100+ customers
- 6 partners / 1 premium and 1 offshore
- ~30 employees
- 3 products

Focus on



focuses on

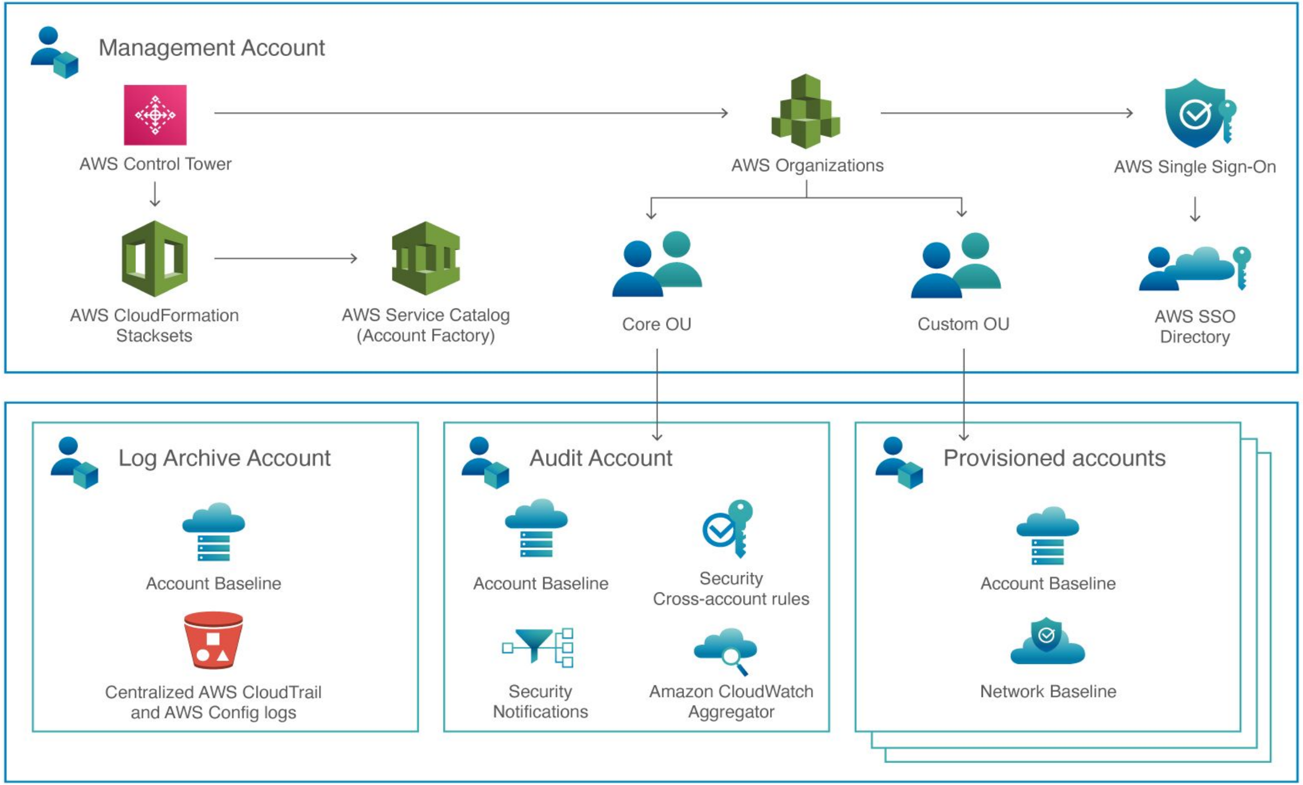
- Products & Services
- Amazon Web Services (AWS)
- Automation (on-premise)
- Cloud Consulting

COPEBIT

Global IAM with AWS

LandingZone

Landing Zone with AWS Control Tower



AWS Control Tower orchestrates AWS IAM Identity Centre centralize identity and access

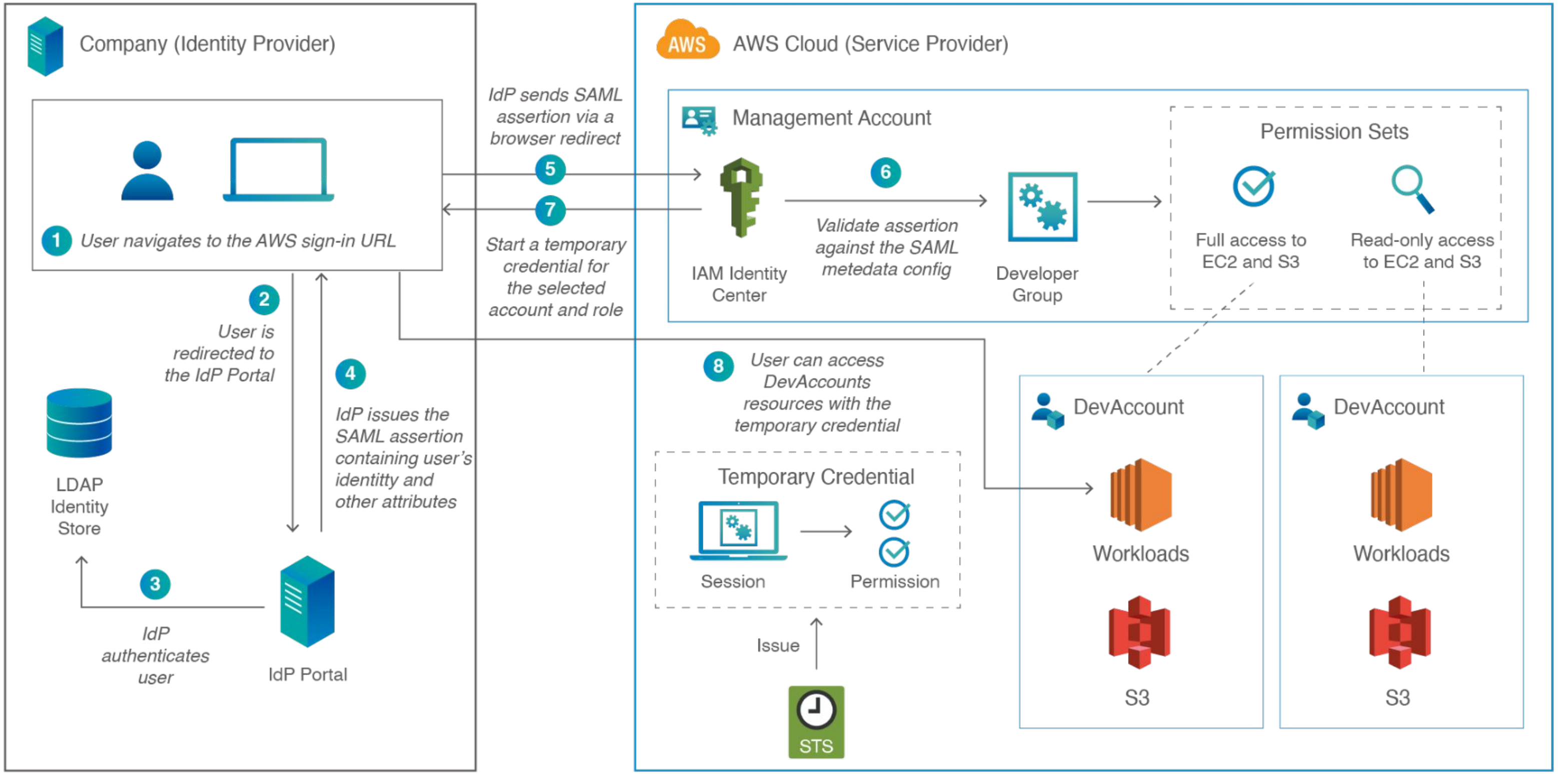
- AWS IAM Identity Center provides default directory for identity
- AWS IAM Identity Center also allows federated access management across all accounts in your organization
- Preconfigured groups (such as AWS Control Tower administrators, auditors and AWS Service Catalog end users)
- Preconfigured permission sets (e.g., admin, read-only, write)
- AWS IAM Identity Center integrates with third-party IDP (Microsoft Azure AD, Ping, Okta)

COPEBIT

Global IAM with AWS

Identity Center and Integration
with external IDP

Federated Login with AWS IAM Identity Center


Company (Identity Provider)
1 User navigates to the AWS sign-in URL
2 User is redirected to the IdP Portal
LDAP Identity Store
3 IdP authenticates user
IdP Portal
4 IdP issues the SAML assertion containing user's identtity and other attributes
IdP sends SAML assertion via a browser redirect
5
7
Start a temporary credential for the selected account and role
AWS
AWS Cloud (Service Provider)
Management Account
IAM Identity Center
6
Validate assertion against the SAML metedata config
Developer Group
Permission Sets
Full access to EC2 and S3
Read-only access to EC2 and S3
8 User can access DevAccounts resources with the temporary credential
Temporary Credential
Session
Permission
Issue
STS
DevAccount
Workloads
S3
DevAccount
Workloads
S3

Supported IDP’s

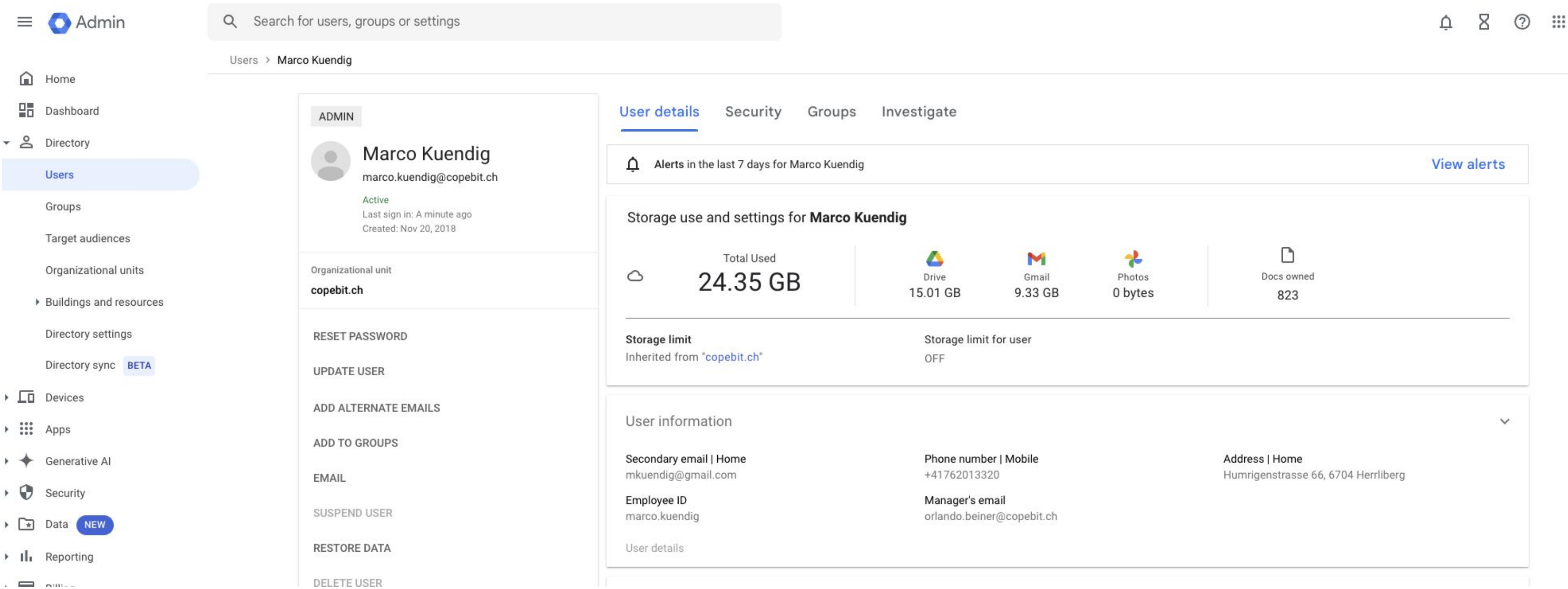
- AWS Identity Center (Built-in User Directory)
  - No external IdP needed, AWS manages the user directory.
- SAML 2.0-based IdPs AWS supports any IdP that is SAML 2.0 compliant:
  - Microsoft EntraID
  - Okta
  - Google Workspace (formerly G Suite)
  - OneLogin
  - Ping Identity
  - ADFS (Active Directory Federation Services)
- OIDC (OpenID Connect) OpenID Connect-based identity providers:
  - Auth0
  - Okta (as an OIDC provider)
  - Google
  - EntraID
  - Active Directory
- AWS supports integration with Microsoft Active Directory, either through:
  - AWS Managed Microsoft AD
  - On-premises Active Directory (connected via AWS Directory Service)

COPEBIT

Global IAM with Identity Center

Short Demo of IDC

User in Google Workspace



Users > Marco Kuendig

ADMIN

Marco Kuendig
marco.kuendig@copebit.ch
Active
Last sign in: A minute ago
Created: Nov 20, 2018

Organizational unit
copebit.ch

Alerts in the last 7 days for Marco Kuendig

Storage use and settings for **Marco Kuendig**

Total Used	Drive	Gmail	Photos	Docs owned
24.35 GB	15.01 GB	9.33 GB	0 bytes	823

Storage limit
Inherited from "copebit.ch"

Storage limit for user
OFF

User information

Secondary email | Home
mkuendig@gmail.com

Phone number | Mobile
+41762013320

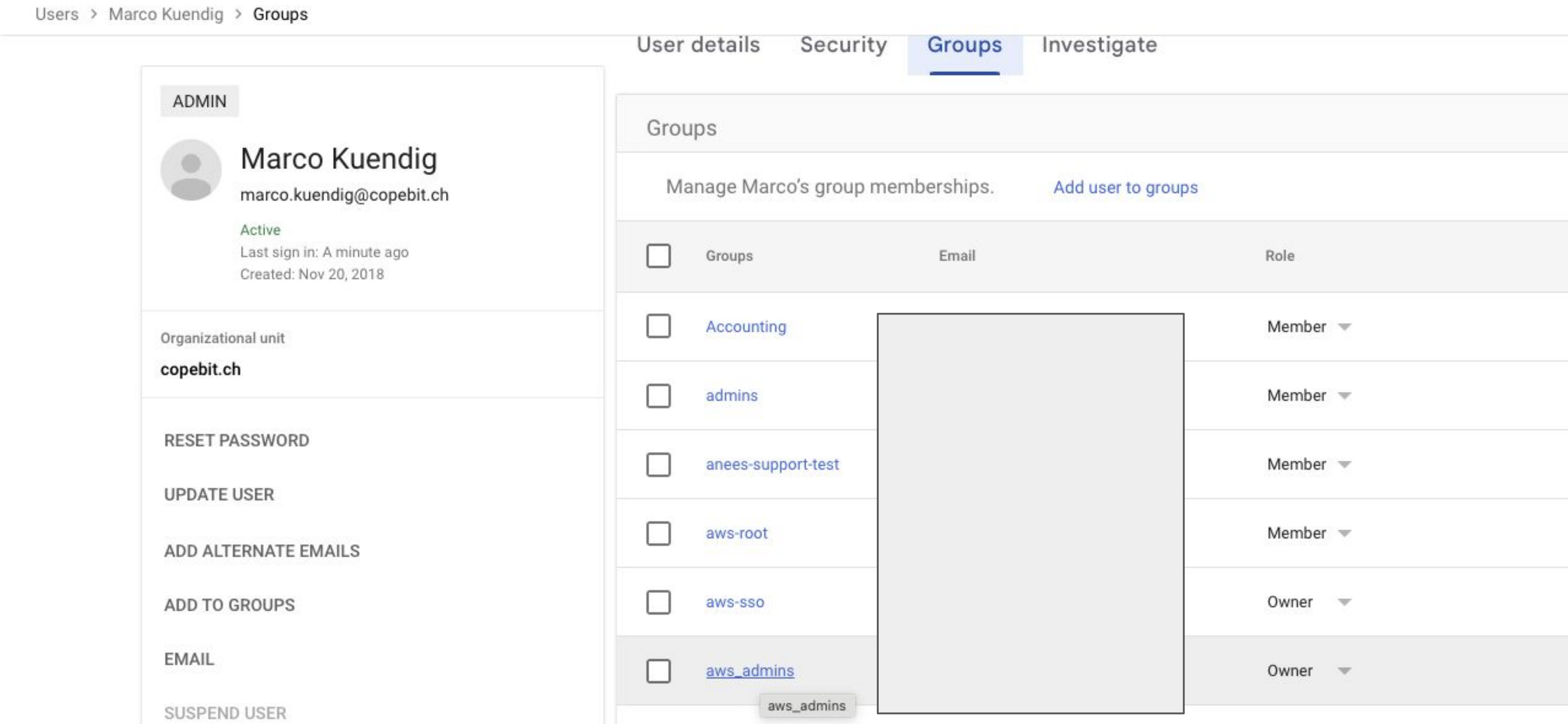
Address | Home
Humrigenstrasse 66, 6704 Herrliberg

Employee ID
marco.kuendig

Manager's email
orlando.beiner@copebit.ch

User details

User in Google Group



Users › Marco Kuendig › Groups

User details | Security | **Groups** | Investigate

ADMIN

Marco Kuendig
marco.kuendig@copebit.ch
Active
Last sign in: A minute ago
Created: Nov 20, 2018

Organizational unit
copebit.ch

RESET PASSWORD
UPDATE USER
ADD ALTERNATE EMAILS
ADD TO GROUPS
EMAIL
SUSPEND USER

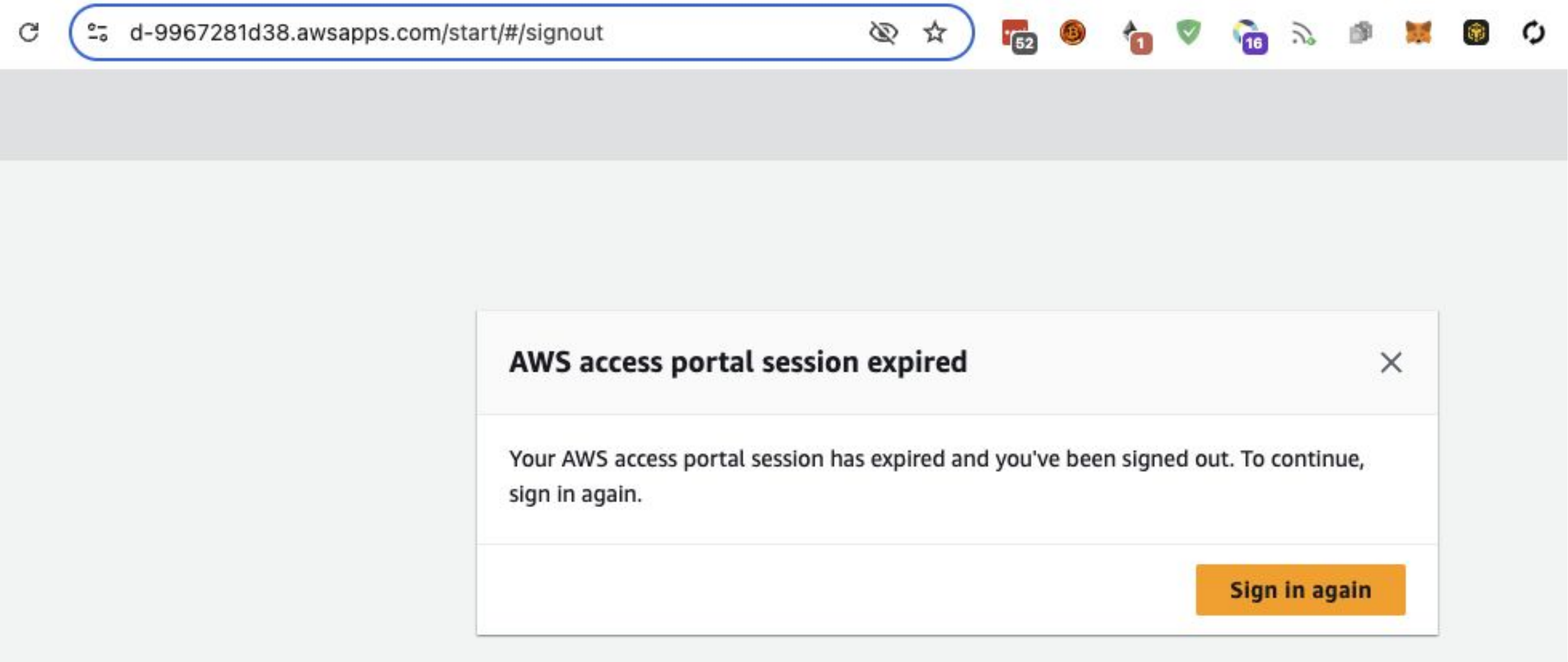
Groups

Manage Marco's group memberships. Add user to groups

□	Groups	Email	Role
□	Accounting	[redacted]	Member
□	admins	[redacted]	Member
□	anees-support-test	[redacted]	Member
□	aws-root	[redacted]	Member
□	aws-sso	[redacted]	Owner
□	aws_admins	[redacted]	Owner

aws_admins

Login to IDC Landingpage

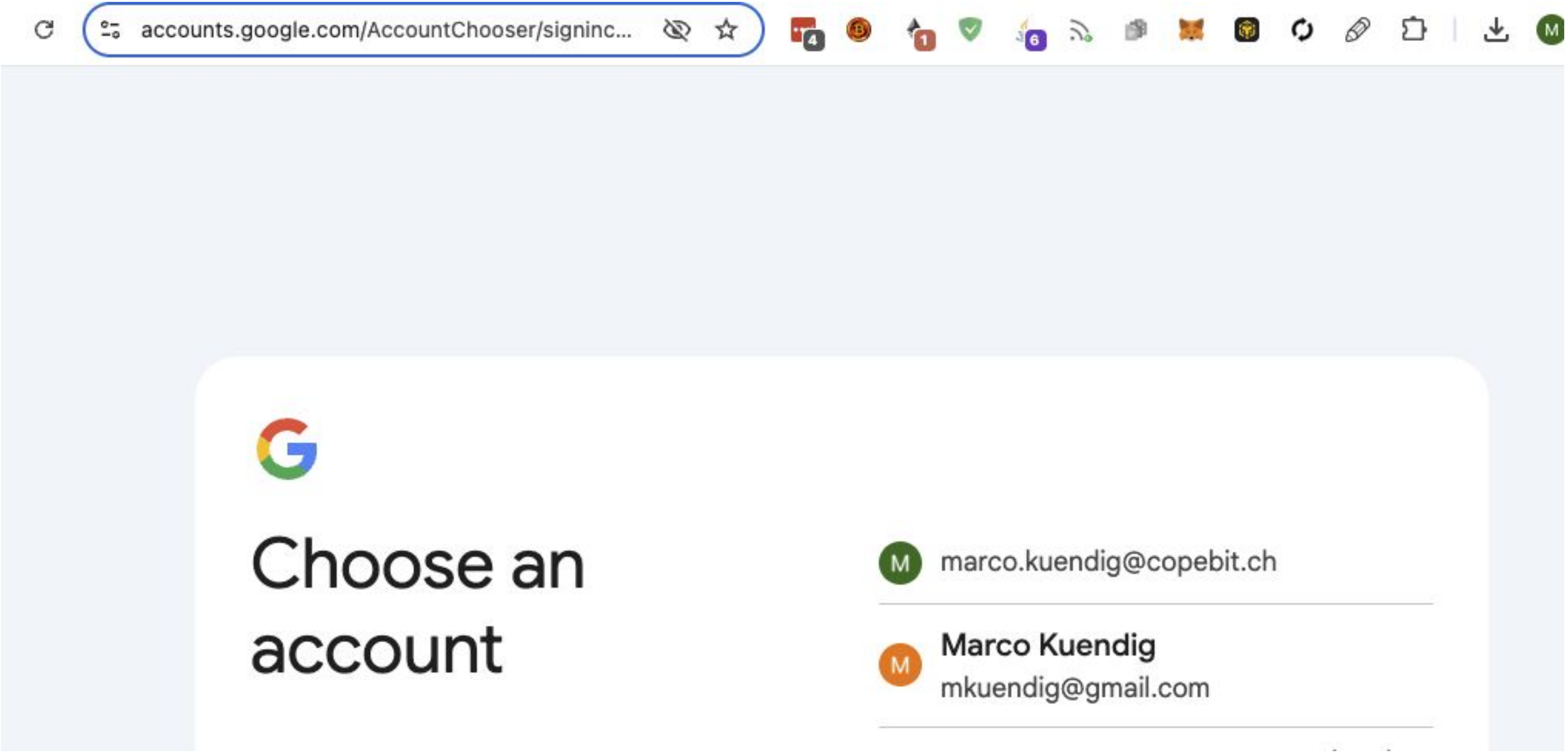


d-9967281d38.awsapps.com/start/#/signout

AWS access portal session expired

Your AWS access portal session has expired and you've been signed out. To continue, sign in again.

Redirect to IDP (Google)



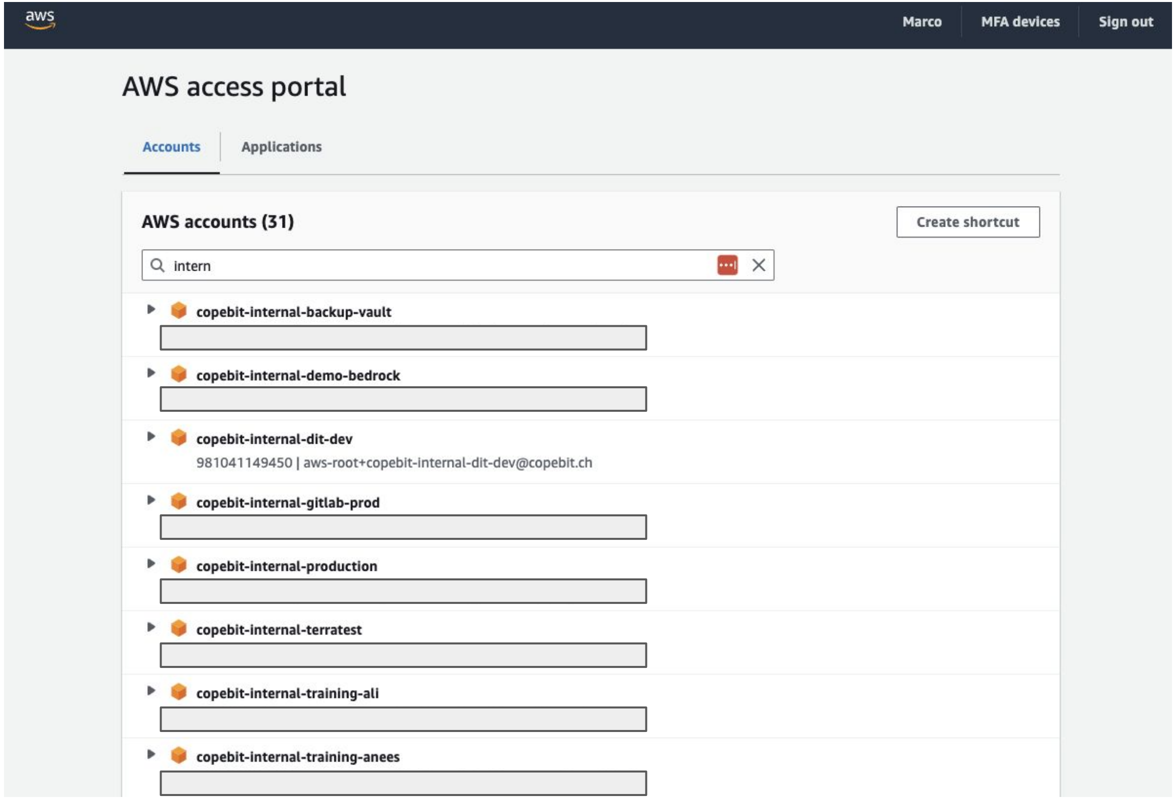
accounts.google.com/AccountChooser/signinc...

Choose an account

marco.kuendig@copebit.ch

Marco Kuendig
mkuendig@gmail.com

Access to AWS granted



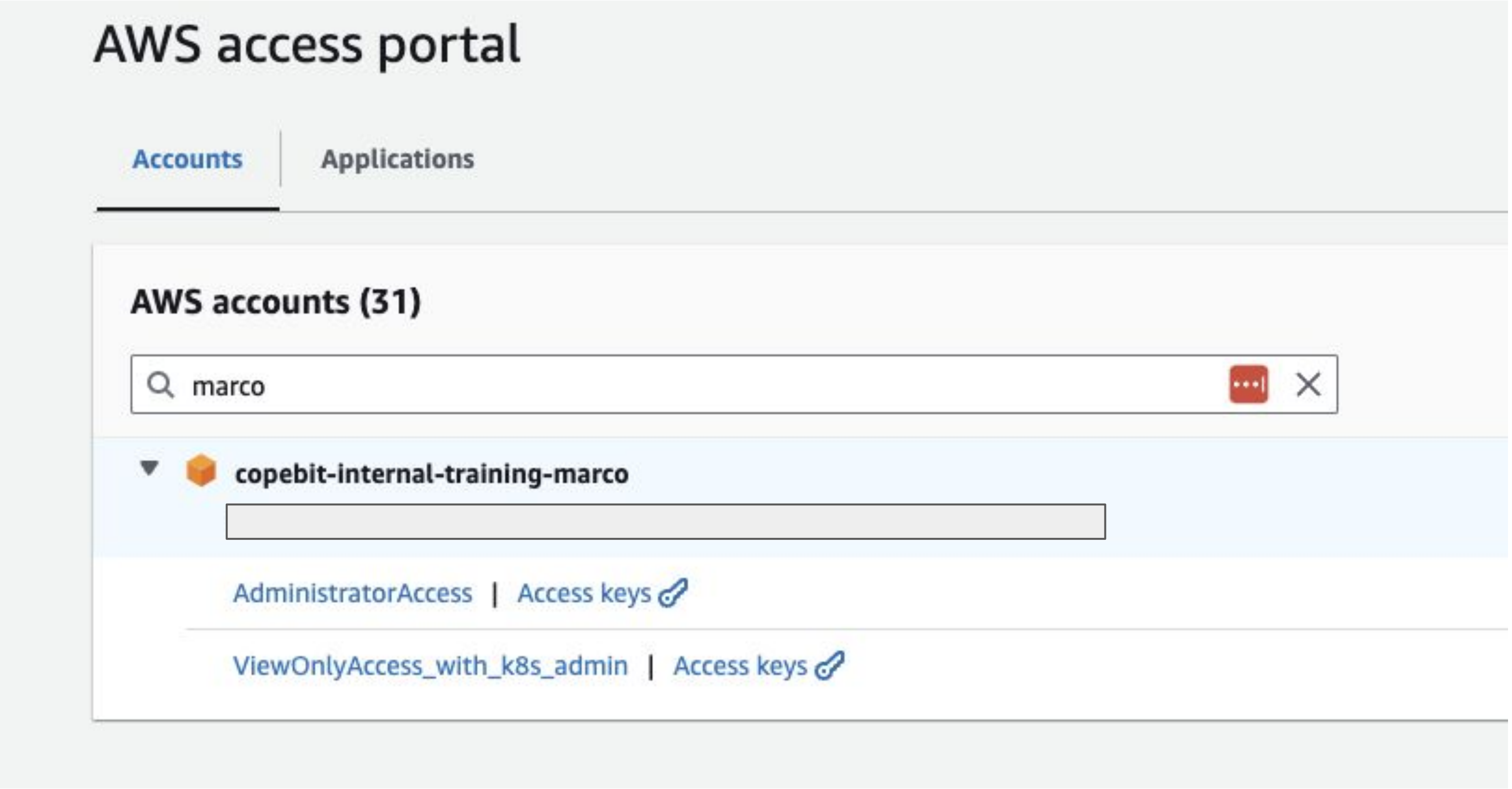
AWS access portal

AWS accounts (31)

intern

- copebit-internal-backup-vault
  [redacted]
- copebit-internal-demo-bedrock
  [redacted]
- copebit-internal-dit-dev
  981041149450 | aws-root+copebit-internal-dit-dev@copebit.ch
- copebit-internal-gitlab-prod
  [redacted]
- copebit-internal-production
  [redacted]
- copebit-internal-terratest
  [redacted]
- copebit-internal-training-ali
  [redacted]
- copebit-internal-training-anees
  [redacted]

Choose Permission or CLI Access Keys



AWS access portal

Accounts | Applications

AWS accounts (31)

marco

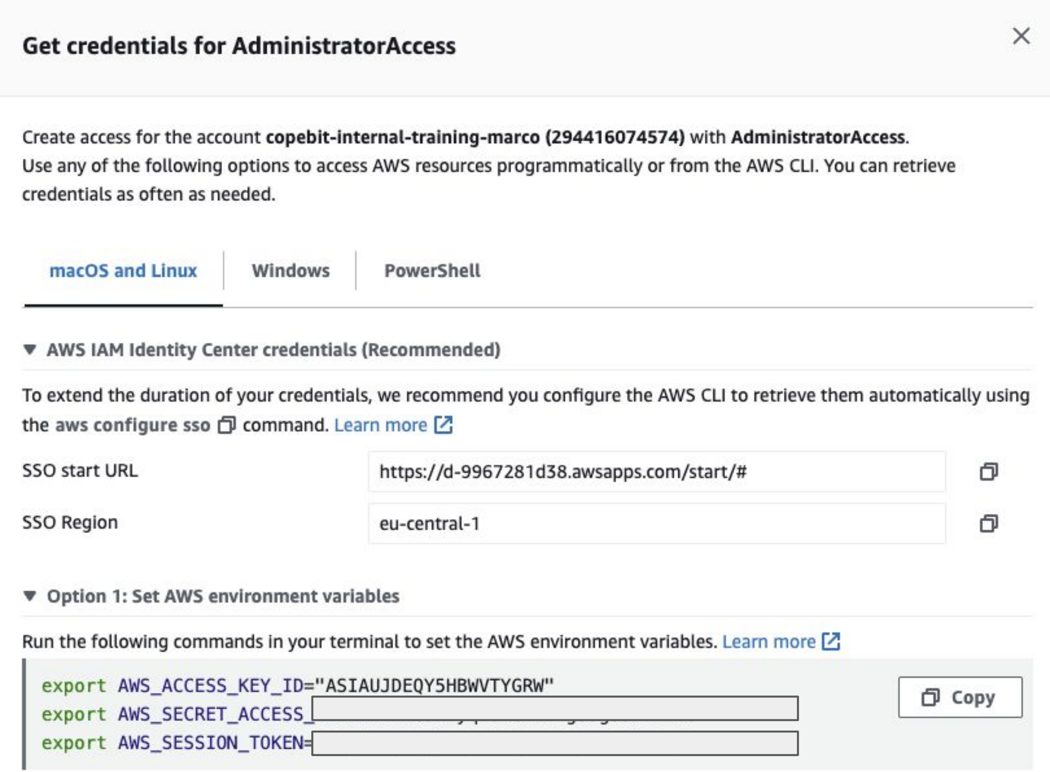
▼ **copebit-internal-training-marco**

[redacted]

AdministratorAccess | Access keys

ViewOnlyAccess_with_k8s_admin | Access keys

No long-running access keys anymore



Get credentials for AdministratorAccess

Create access for the account **copebit-internal-training-marco (294416074574)** with **AdministratorAccess**.
Use any of the following options to access AWS resources programmatically or from the AWS CLI. You can retrieve credentials as often as needed.

▼ **AWS IAM Identity Center credentials (Recommended)**

To extend the duration of your credentials, we recommend you configure the AWS CLI to retrieve them automatically using the **aws configure sso** command. Learn more

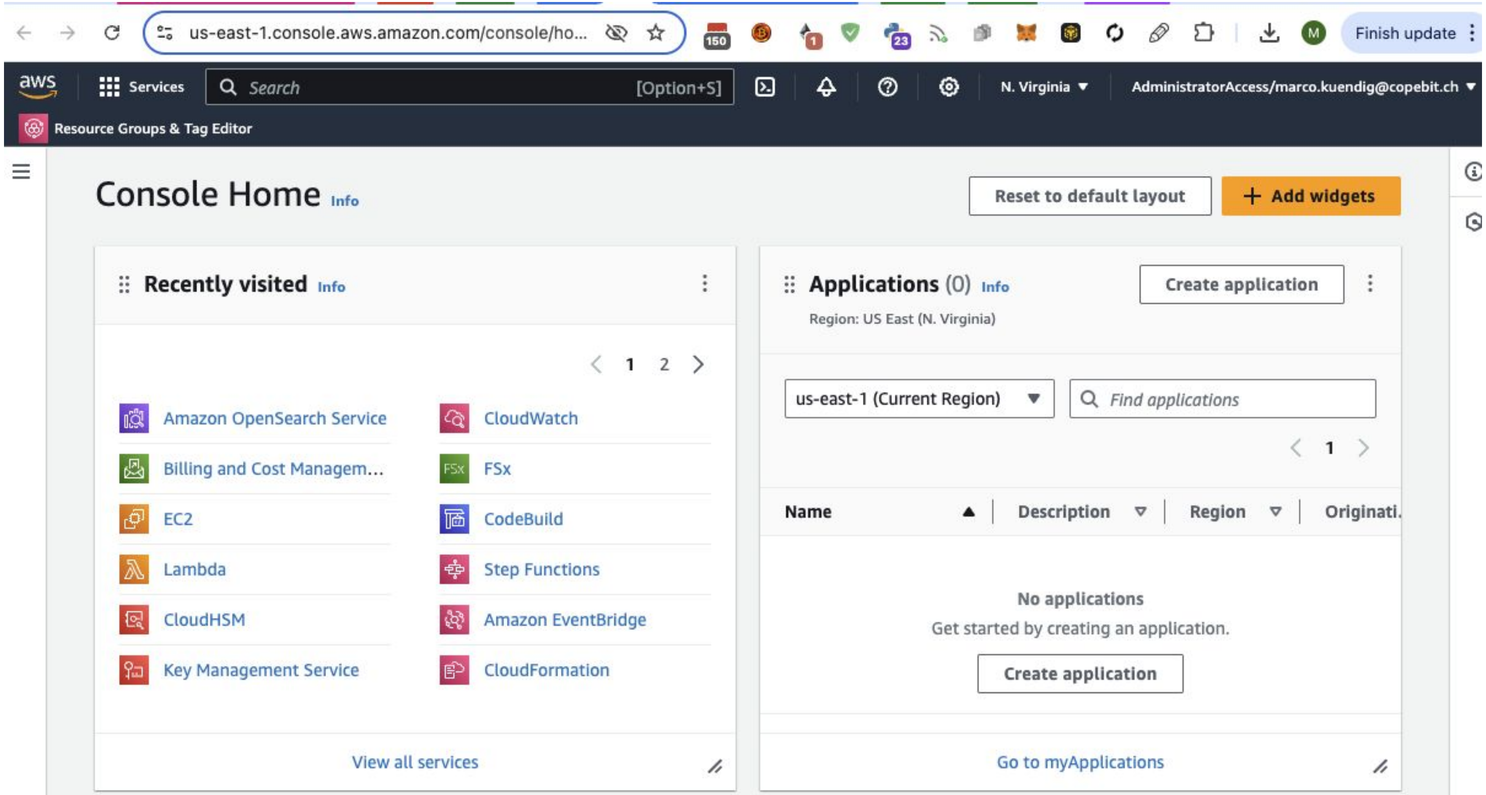
SSO start URL	https://d-9967281d38.awsapps.com/start/#
SSO Region	eu-central-1

▼ **Option 1: Set AWS environment variables**

Run the following commands in your terminal to set the AWS environment variables. Learn more

```
export AWS_ACCESS_KEY_ID="ASIAUJDEQY5HBWVTYGRW"
export AWS_SECRET_ACCESS_[redacted]
export AWS_SESSION_TOKEN=[redacted]
```

Access to AWS Account with right permissions



us-east-1.console.aws.amazon.com/console/ho...

AdministratorAccess/marco.kuendig@copebit.ch

Console Home

Recently visited

1 2

- Amazon OpenSearch Service
- Billing and Cost Managem...
- EC2
- Lambda
- CloudHSM
- Key Management Service
- CloudWatch
- FSx
- CodeBuild
- Step Functions
- Amazon EventBridge
- CloudFormation

View all services

Applications (0)

Region: US East (N. Virginia)

us-east-1 (Current Region)

Find applications

1

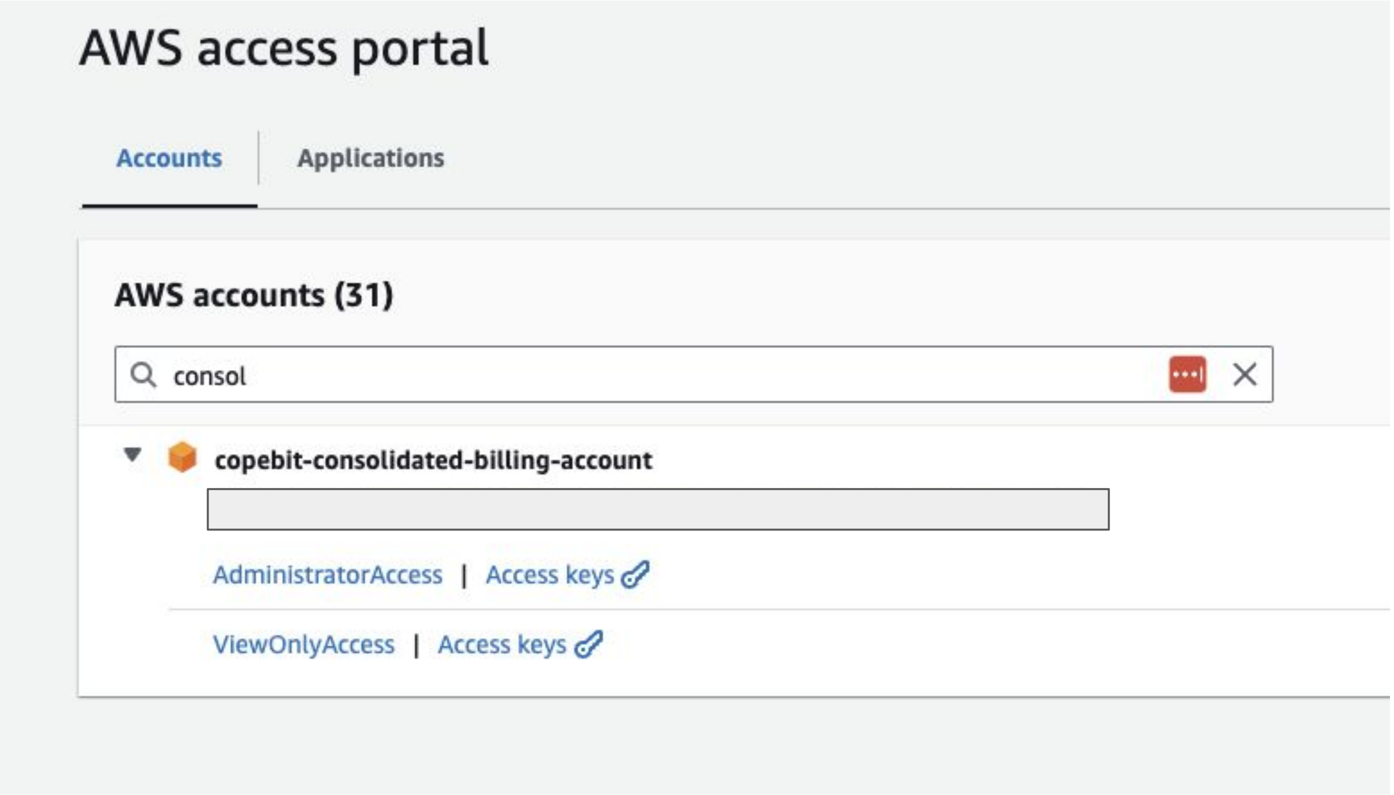
Name	Description	Region	Originati.

No applications

Get started by creating an application.

Go to myApplications

Switch Account



AWS access portal

AWS accounts (31)

consol

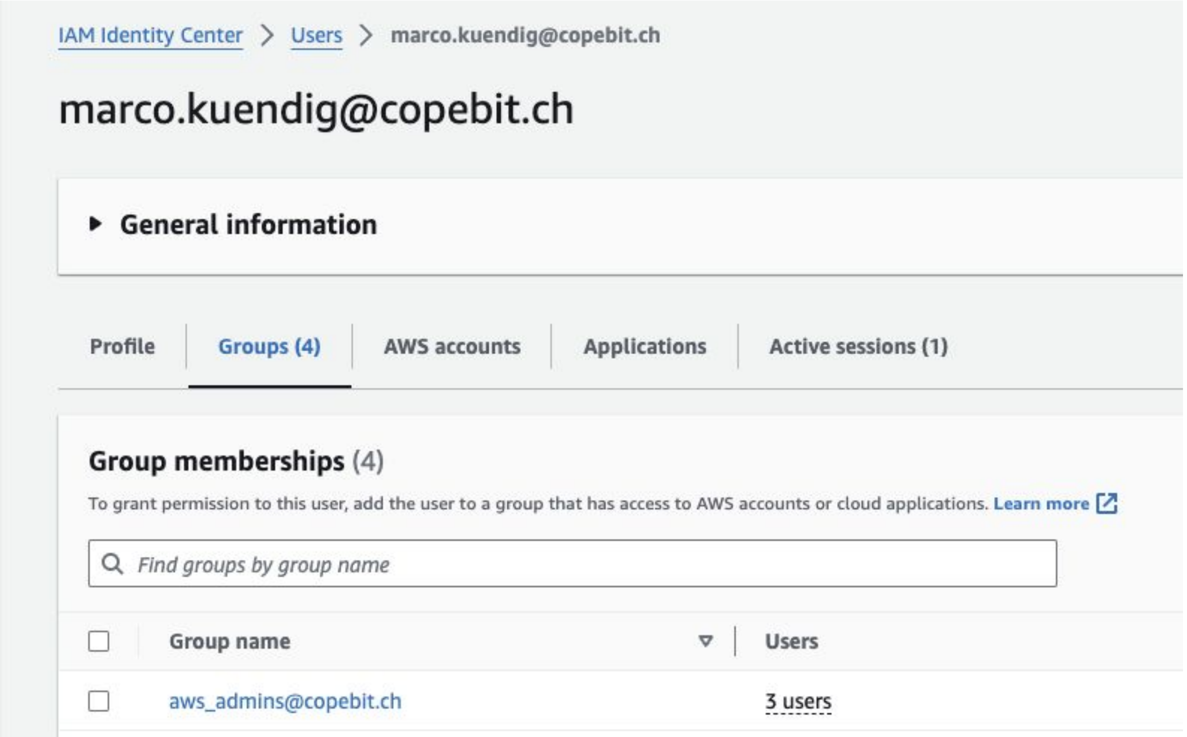
copebit-consolidated-billing-account

[redacted]

AdministratorAccess | Access keys

ViewOnlyAccess | Access keys

IDC quick view, users/groups synced with SCIM in a lambda



IAM Identity Center > Users > marco.kuendig@copebit.ch

marco.kuendig@copebit.ch

▸ General information

Group memberships (4)

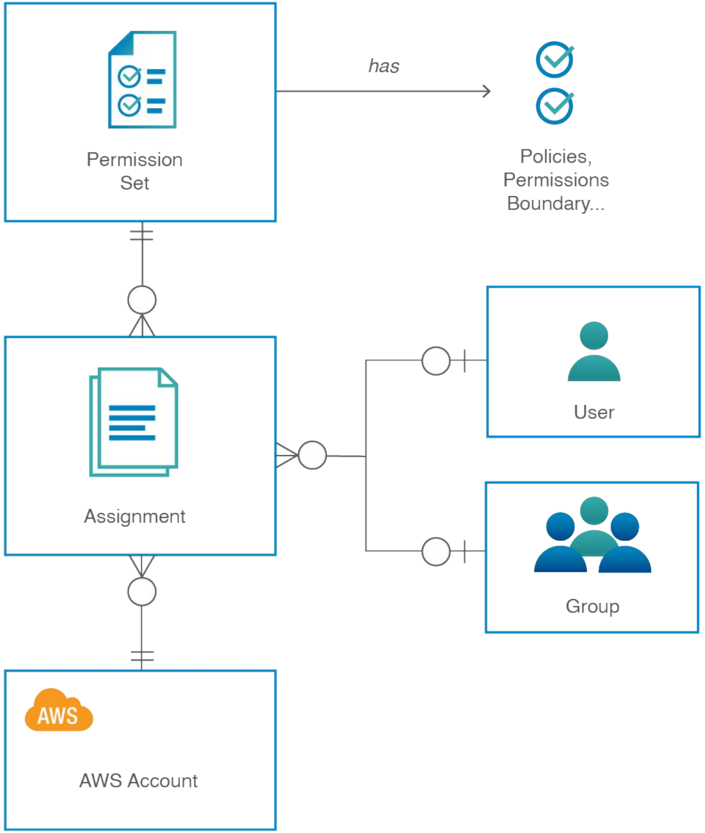
To grant permission to this user, add the user to a group that has access to AWS accounts or cloud applications. Learn more

□	Group name	Users
□	aws_admins@copebit.ch	3 users

Global IAM with AWS

Permission sets and Roles

IDC PermissionSet and IAM-Roles



COPEBIT

Global IAM with IAM

Global Policy Enforcement with SCP

Policy Enforcement with SCP

Enables you to control which AWS service APIs are accessible

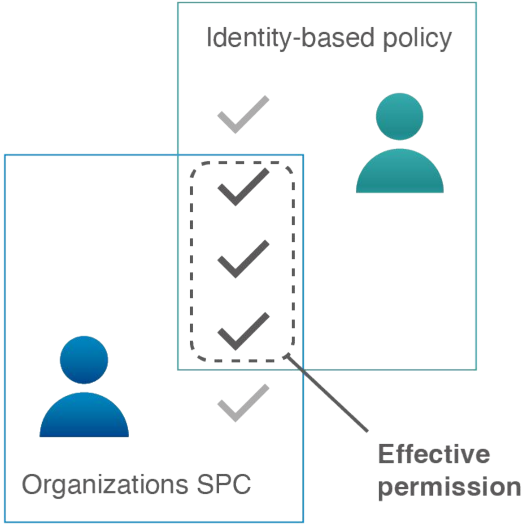
- Define the list of APIs that are allowed — **allow list**
- Define the list of APIs that must be blocked — **deny list**

SCPs are:

- Invisible to all users in the child account, **including root user**
- Applied to all users in the child account, **including root user**
- Do not apply to the management account

Permission:

- intersection between the SCP and IAM permissions
- IAM policy simulator is SCP aware



Disable Service APIs you Won’t be Using

```
{
    "Version": “2012-10-17”,
    "Statement": [
    {
        "Effect": "Deny",
        "Action": "<Insert unwanted service prefix here>:*",
        "Resource": "*"
    }
   ]
}
```

`NotAction` (Optional) List the AWS actions exempt from the SCP. Used in place of the Action element.

`Resource` List the AWS resources the SCP applies to.

`Condition` (Optional) Specify conditions for when the statement is in effect.

COPEBIT

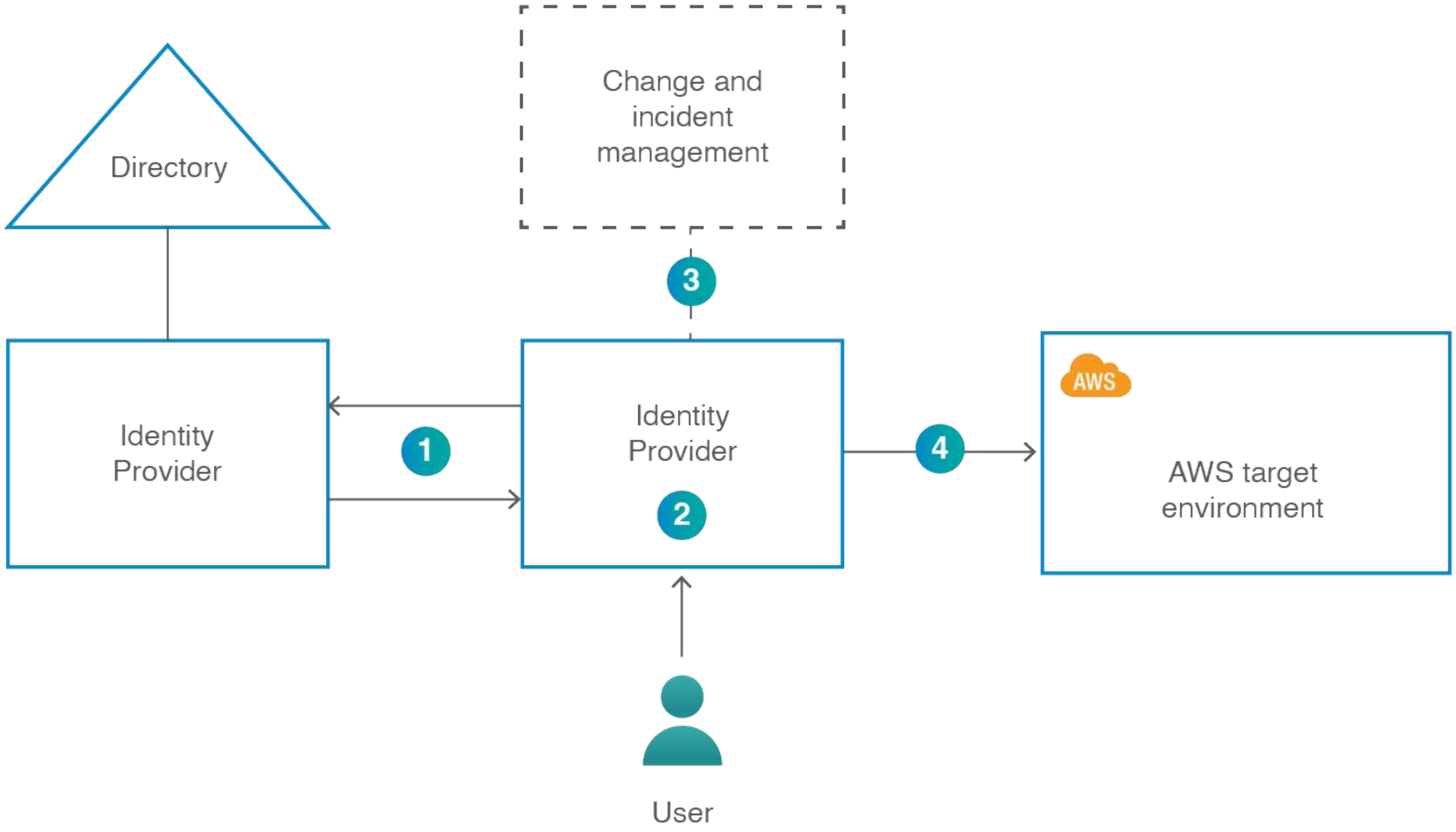
Global IAM with IAM

Temporary elevated access / PIM

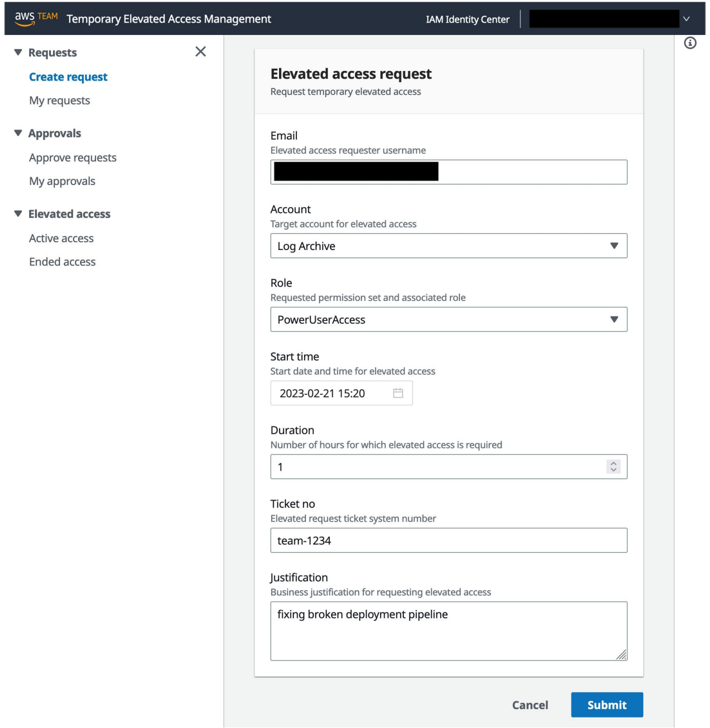
Options

- Use Azure PIM if you already have it (just changes group assignment)
- Use AWS TEAM
- ITSense CoreOne Identity Platform

AWS TEAM Workflow



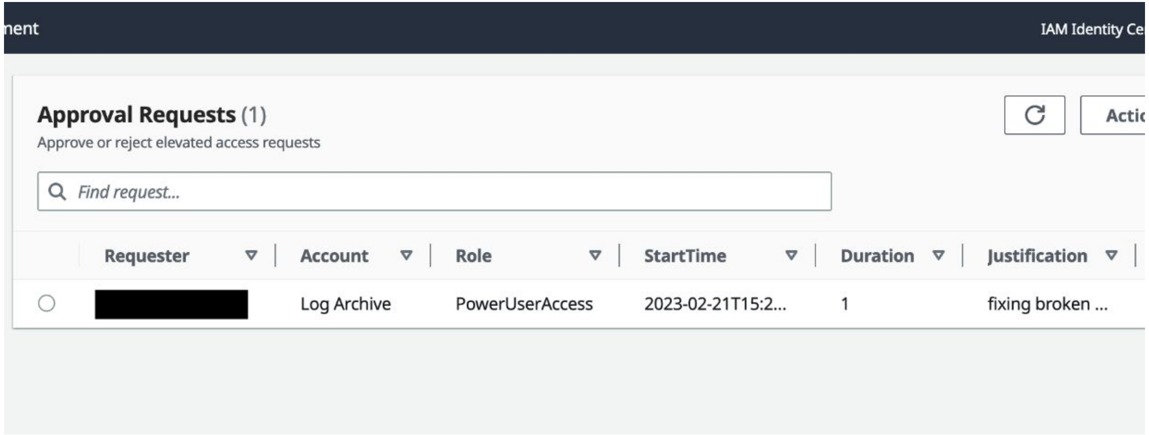
AWS TEAM Requests



Elevated access request

Request temporary elevated access

Email Elevated access requester username	[redacted]
Account Target account for elevated access	Log Archive
Role Requested permission set and associated role	PowerUserAccess
Start time Start date and time for elevated access	2023-02-21 15:20
Duration Number of hours for which elevated access is required	1
Ticket no Elevated request ticket system number	team-1234
Justification Business justification for requesting elevated access	fixing broken deployment pipeline

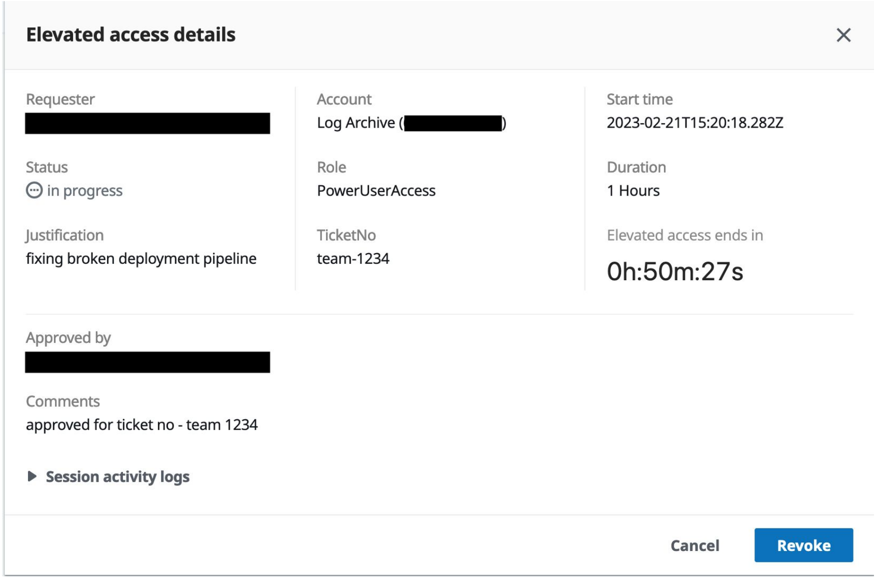


Approval Requests (1)

Approve or reject elevated access requests

	Requester	Account	Role	StartTime	Duration	Justification
○	[redacted]	Log Archive	PowerUserAccess	2023-02-21T15:2...	1	fixing broken ...

AWS TEAM Approved



Elevated access details

Requester
[redacted]

Account
Log Archive ([redacted])

Start time
2023-02-21T15:20:18.282Z

Status
in progress

Role
PowerUserAccess

Duration
1 Hours

Justification
fixing broken deployment pipeline

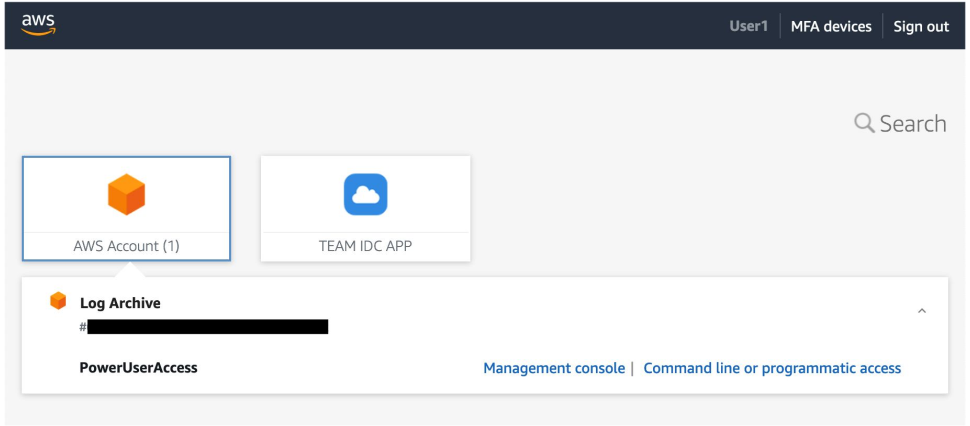
TicketNo
team-1234

Elevated access ends in
0h:50m:27s

Approved by
[redacted]

Comments
approved for ticket no - team 1234

▶ Session activity logs



Log Archive
#[redacted]

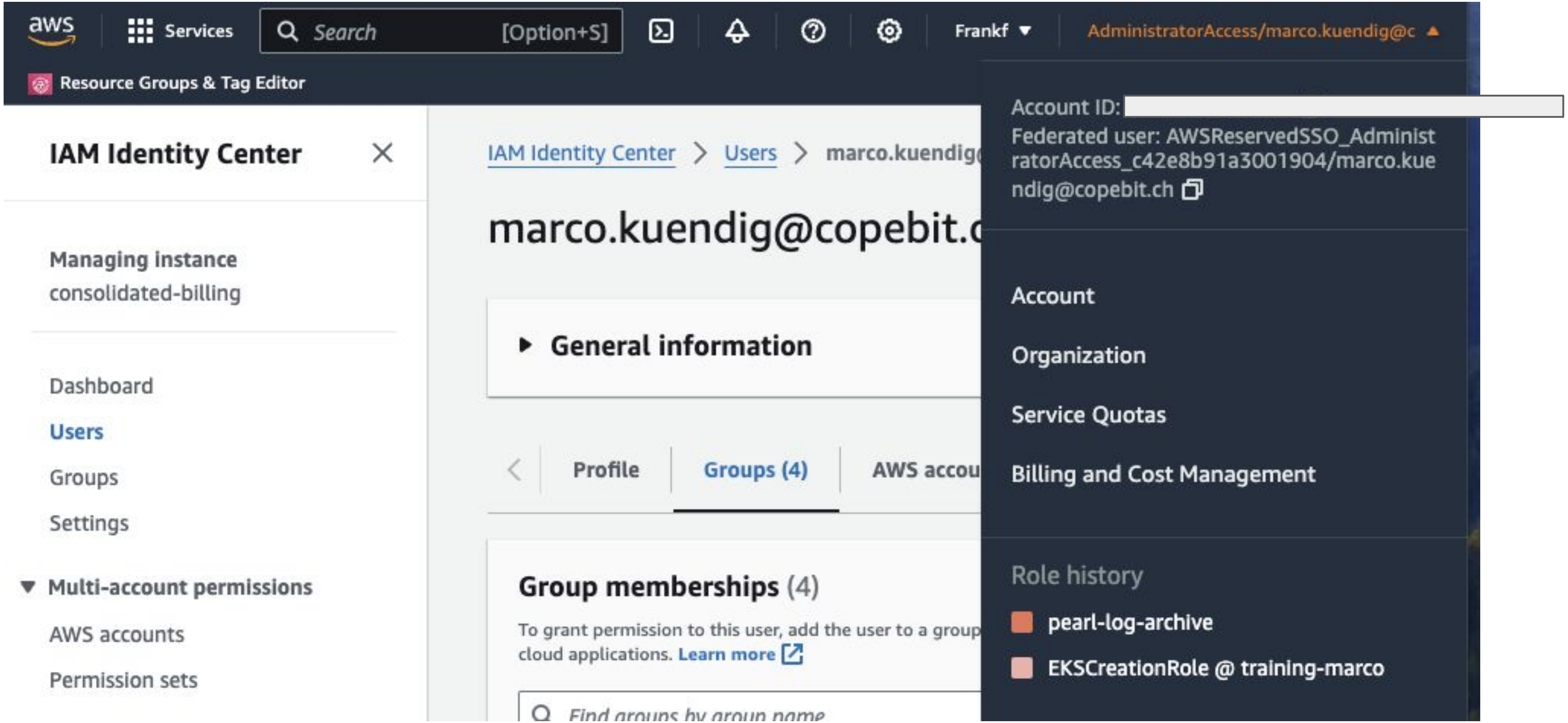
PowerUserAccess   Management console | Command line or programmatic access

COPEBIT

Child Account IAM

Automatic Role Assumption

Automatic Role Assumption

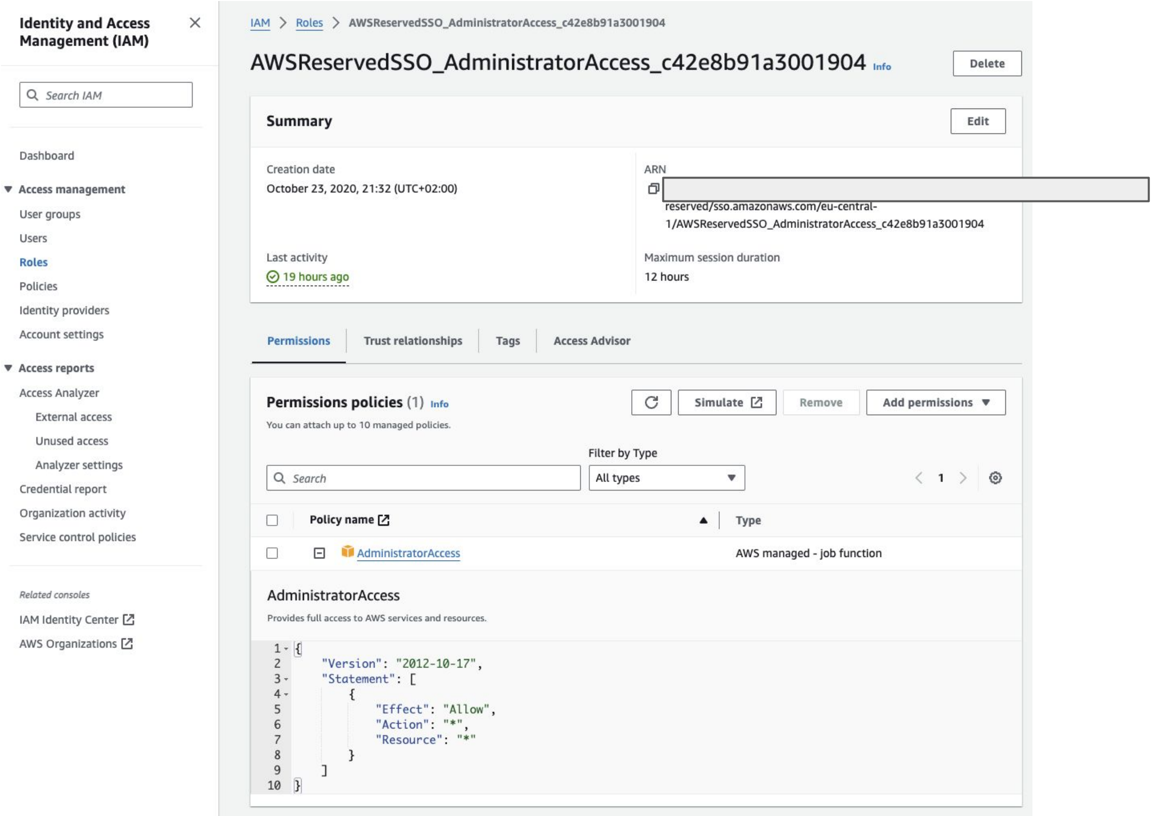


aws
Services
Search [Option+S]
Frankf
AdministratorAccess/marco.kuendig@c
Resource Groups & Tag Editor

Account ID: [redacted]
Federated user: AWSReservedSSO_AdministratorAccess_c42e8b91a3001904/marco.kuendig@copebit.ch

To grant permission to this user, add the user to a group cloud applications. Learn more

Link to local AWS IAM in AWS Account



AWSReservedSSO_AdministratorAccess_c42e8b91a3001904 Info

Summary

Creation date
October 23, 2020, 21:32 (UTC+02:00)

ARN
[redacted]
reserved/sso.amazonaws.com/eu-central-1/AWSReservedSSO_AdministratorAccess_c42e8b91a3001904

Last activity
19 hours ago

Maximum session duration
12 hours

Permissions policies (1) Info

You can attach up to 10 managed policies.

□	Policy name	Type
□	AdministratorAccess	AWS managed - job function

AdministratorAccess

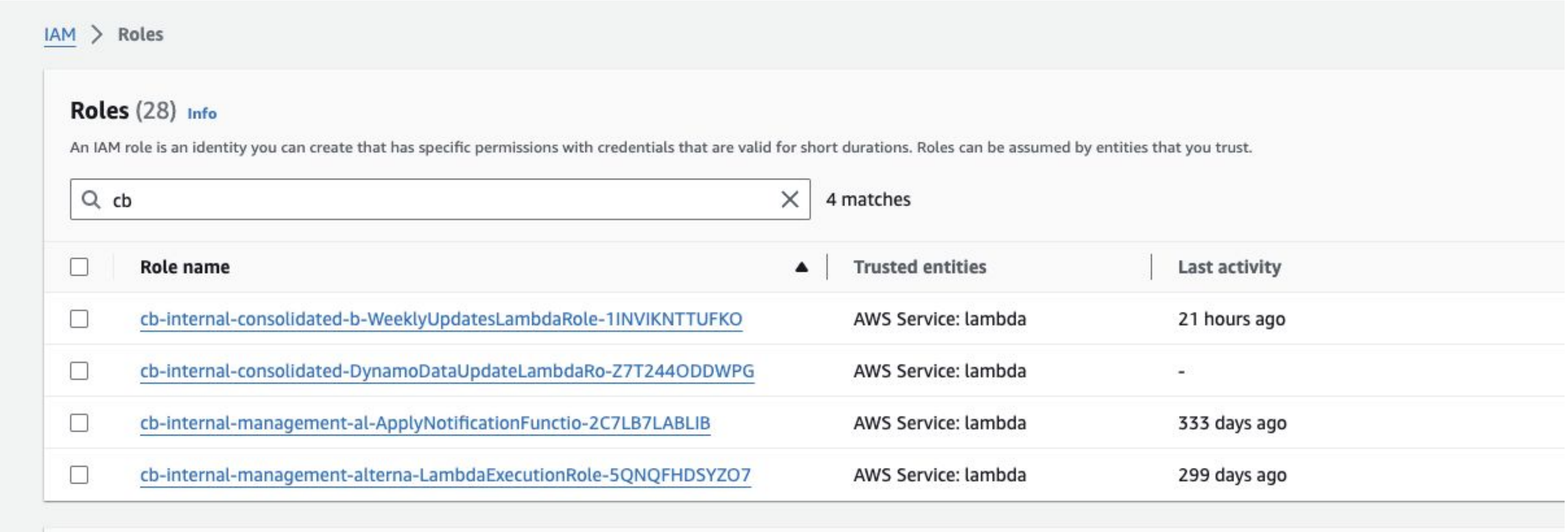
Provides full access to AWS services and resources.

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

Child Account IAM

Technical Users / AWS Services Roles

AWS IAM Roles



IAM > Roles

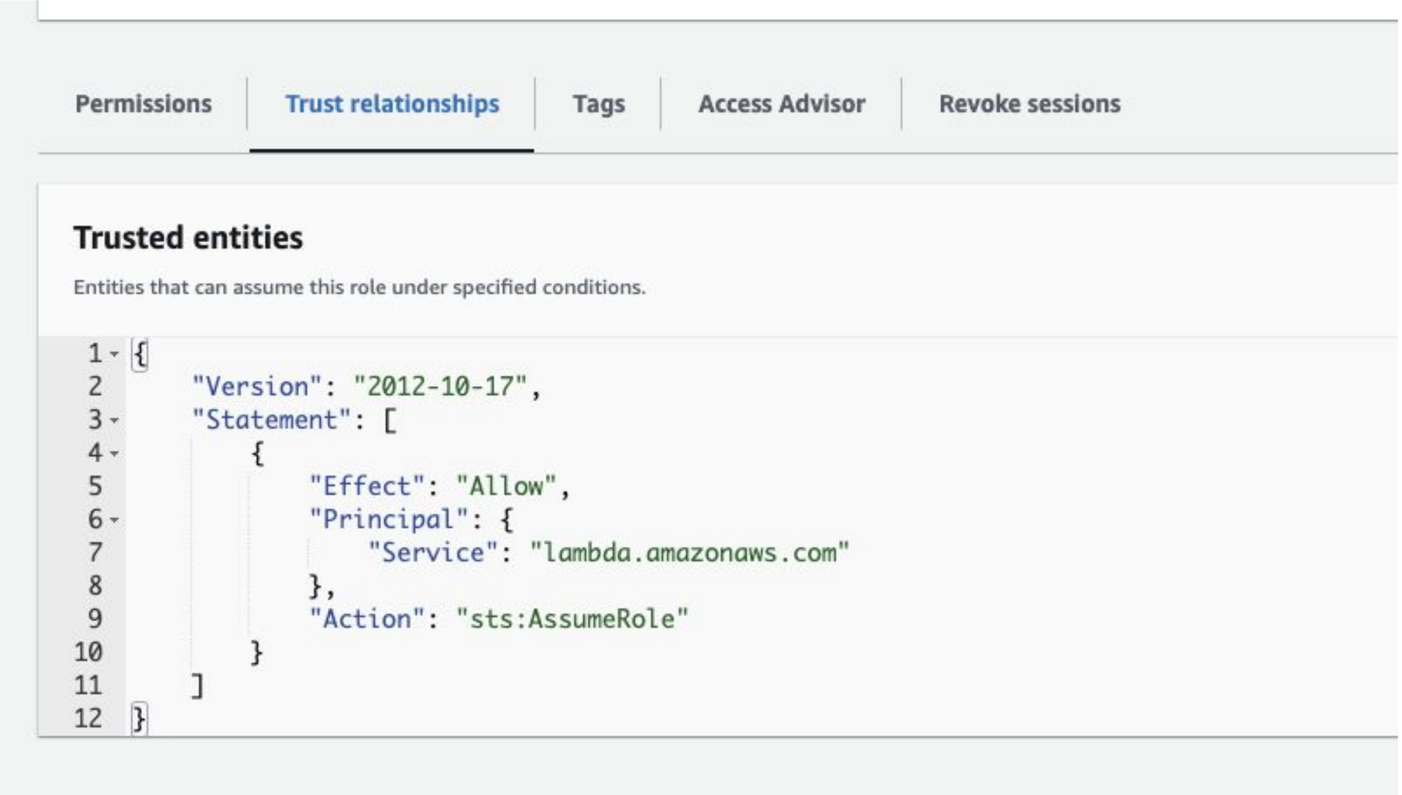
Roles (28) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

cb ✕ 4 matches

□	Role name ▲	Trusted entities	Last activity
□	cb-internal-consolidated-b-WeeklyUpdatesLambdaRole-1INVIKNTTUFKO	AWS Service: lambda	21 hours ago
□	cb-internal-consolidated-DynamoDataUpdateLambdaRo-Z7T244ODDWPG	AWS Service: lambda	-
□	cb-internal-management-al-ApplyNotificationFunctio-2C7LB7LABLIB	AWS Service: lambda	333 days ago
□	cb-internal-management-alterna-LambdaExecutionRole-5QNQFHDSYZO7	AWS Service: lambda	299 days ago

AWS IAM Roles, Trust relationships

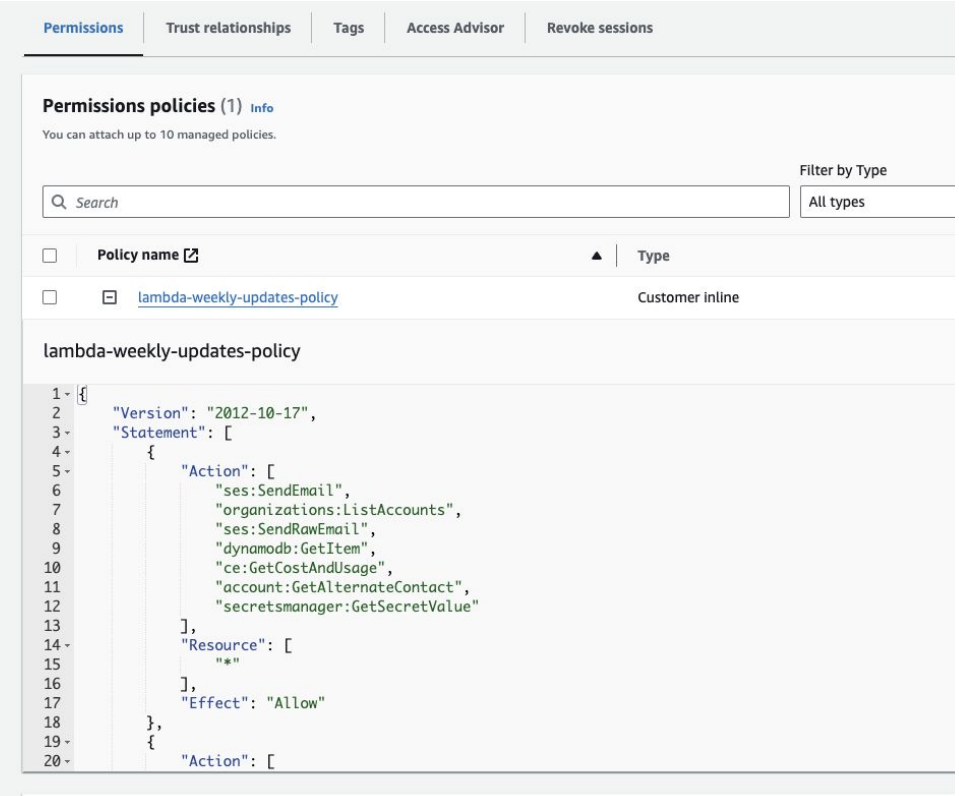


Trusted entities

Entities that can assume this role under specified conditions.

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

AWS IAM Roles, Permissions with policies (POLP)



Permissions policies (1) Info

You can attach up to 10 managed policies.

Filter by Type

Search

All types

□	Policy name	Type
□	⊟ lambda-weekly-updates-policy	Customer inline

lambda-weekly-updates-policy

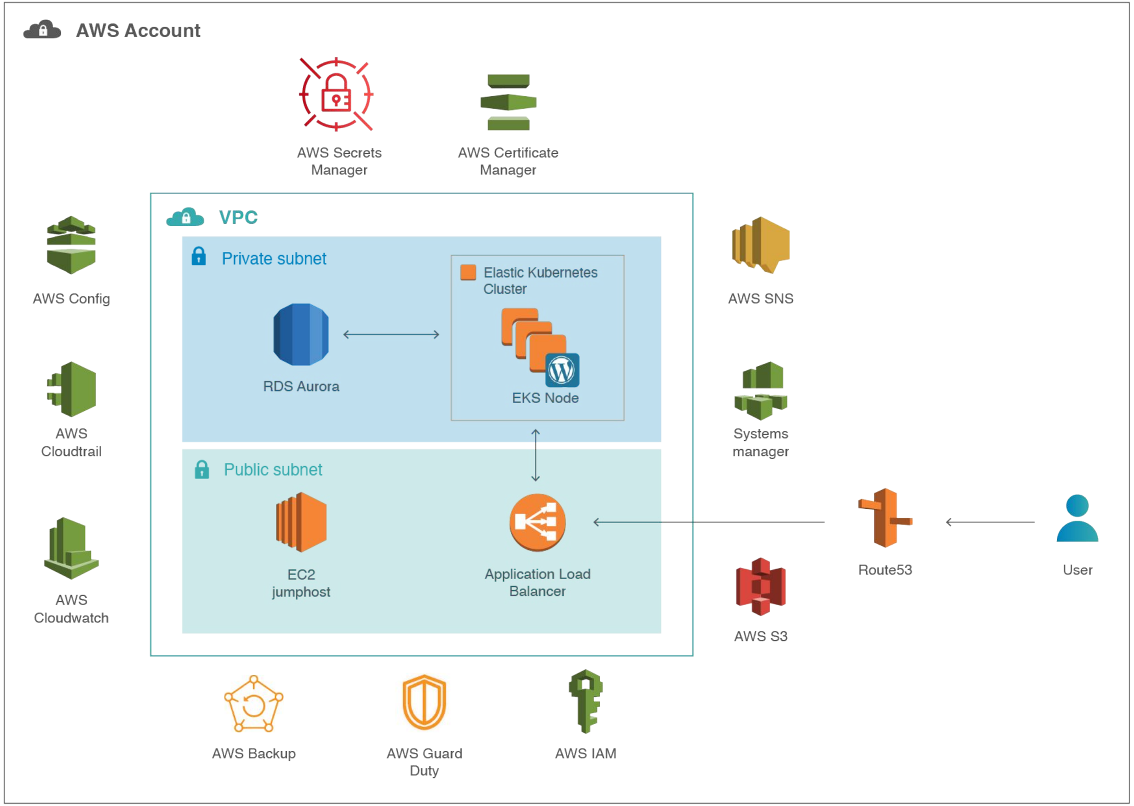
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ses:SendEmail",
                "organizations:ListAccounts",
                "ses:SendRawEmail",
                "dynamodb:GetItem",
                "ce:GetCostAndUsage",
                "account:GetAlternateContact",
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
```

COPEBIT

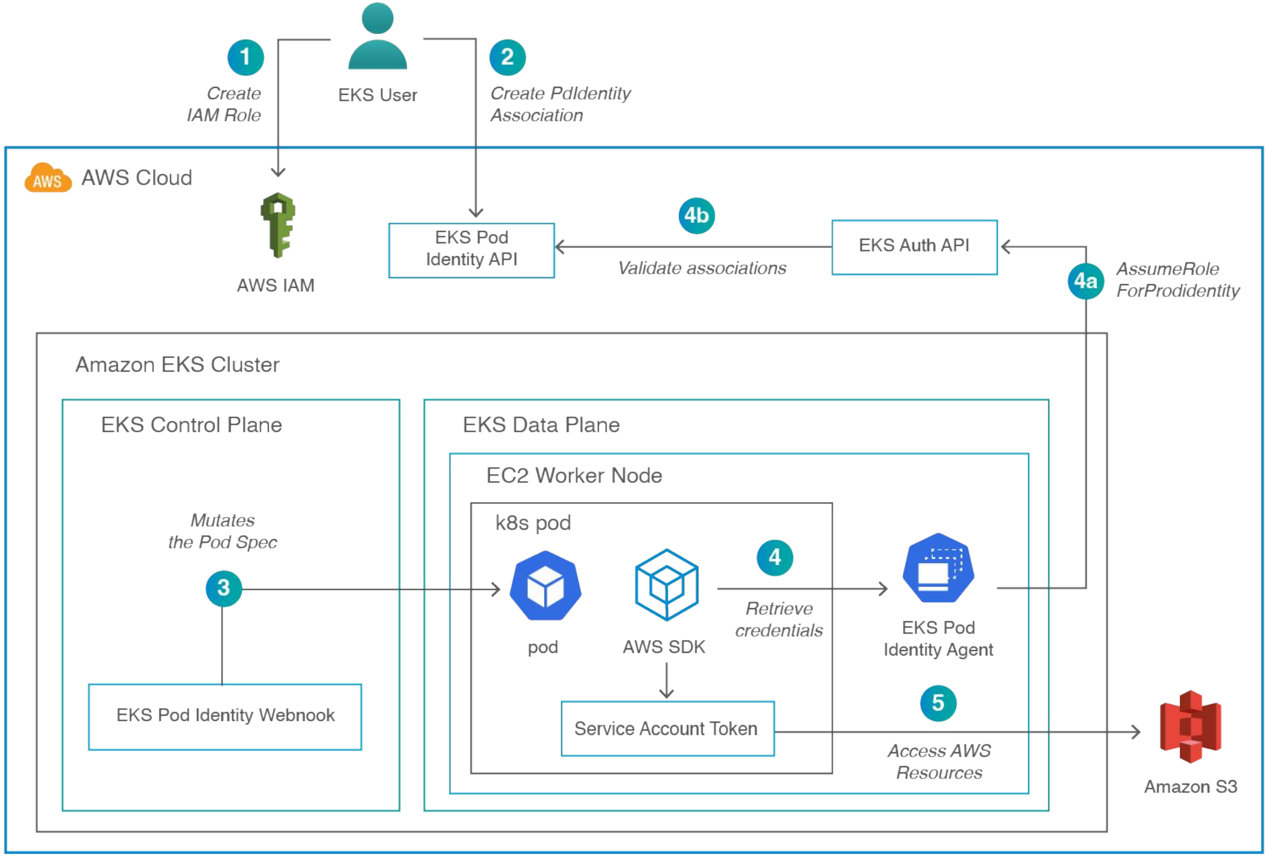
Child Account IAM

Roles for EKS

Sample Containerized Application with Access to AWS Services



AWS IAM Roles for Kubernetes Pods / Containers With Pod Identities



Customer Reference

AR Informatik AG - Success Story

«Together with copebit, we were able to develop, build and commission the ARI Government VPDC (Virtual Private Data Center) within a short period of time. This was done based on AWS' Well-Architected Framework, best practices and additional security services. We were able to increase our AWS expertise immensely and can now ideally implement running and further applications on this very good basis. As a result, we are now able to provide our customers and partners with hybrid services that meet the highest requirements. With copebit, we have gained a qualified and valuable partner who will continue to provide us with advice and support after the go-live.»

Marcel Zoller, Bereichsleiter Infrastructure
AR Informatik AG (ARI)

AWS
Basis VPDC "Virtual Private Data Center"

Mgmt Account
Mgmt & Billing & AD Integration

LogArchive & Security Account
Governance & Security Tooling

Network Account
3rd Party FW Integration / Zone-Concept

HSM & Backup Account
Key- & Backup Management

Workload Accounts
Mehrere Workload Accounts

ARI
Appenzell Ausserrhoden
Informatik

COPEBIT

Thank you!

Contact us: info@copebit.ch