Securely Collaborating Across Multiple Cloud Providers

Joshua Krstic

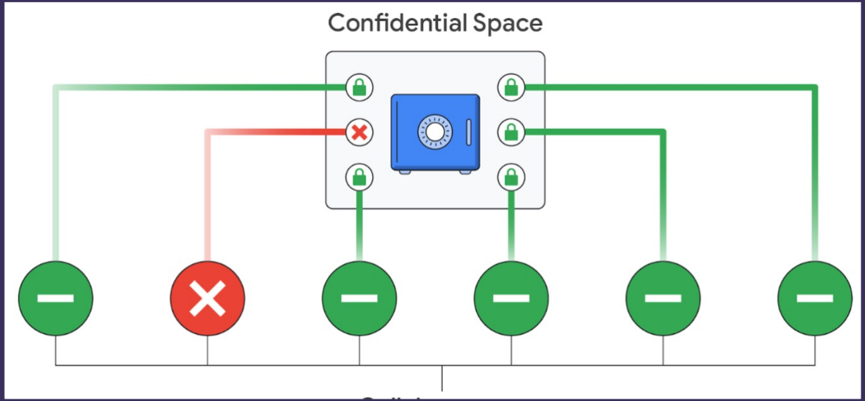
Google Cloud

What is Confidential Space

An introduction to Confidential Space

Confidential Space

- Google Cloud Offering
- Trusted Execution Environment
- Securely process sensitive data
  - ML models
  - PII
  - Health Data



Confidential Space Components

- **Workload**
  - customer authored containerized image
- **Confidential Space Image**
  - Hardened COS-based image
- **Google Attestation Service**
  - an OpenID Connect (OIDC) token provider hosted by Google
- **Protected Resource**
  - decryption key, sensitive data, etc

Demo!

Demo – Meal Corp

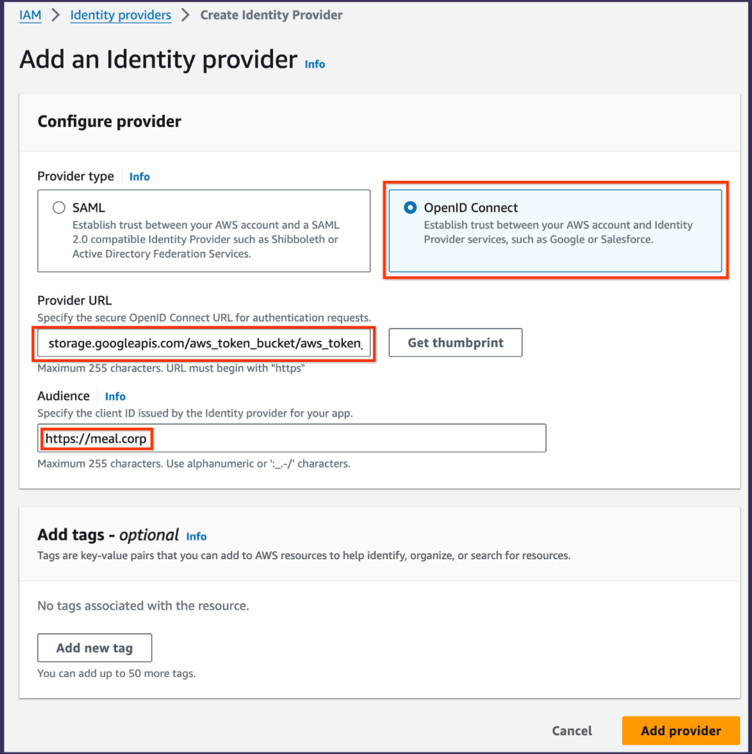
- Meal Corp™ has an application to order meals based on highly sensitive meal preference data

- Corporation Corp™ has employee food preferences

Demo Setup

- Decryption Key in AWS Key Management Service (KMS)
- Policy created to release decryption key
- Sensitive, encrypted data in an S3 bucket
- Run Confidential Space workload

Create an Identity Provider



IAM > Identity providers > Create Identity Provider

Add an Identity provider Info

Configure provider

Provider type Info

○ SAML
Establish trust between your AWS account and a SAML 2.0 compatible Identity Provider such as Shibboleth or Active Directory Federation Services.

● OpenID Connect
Establish trust between your AWS account and Identity Provider services, such as Google or Salesforce.

Provider URL
Specify the secure OpenID Connect URL for authentication requests.
storage.googleapis.com/aws_token_bucket/aws_token
Maximum 255 characters. URL must begin with "https"

Audience Info
Specify the client ID issued by the Identity provider for your app.
https://meal.corp
Maximum 255 characters. Use alphanumeric or ':_.-/' characters.

Add tags - *optional* Info

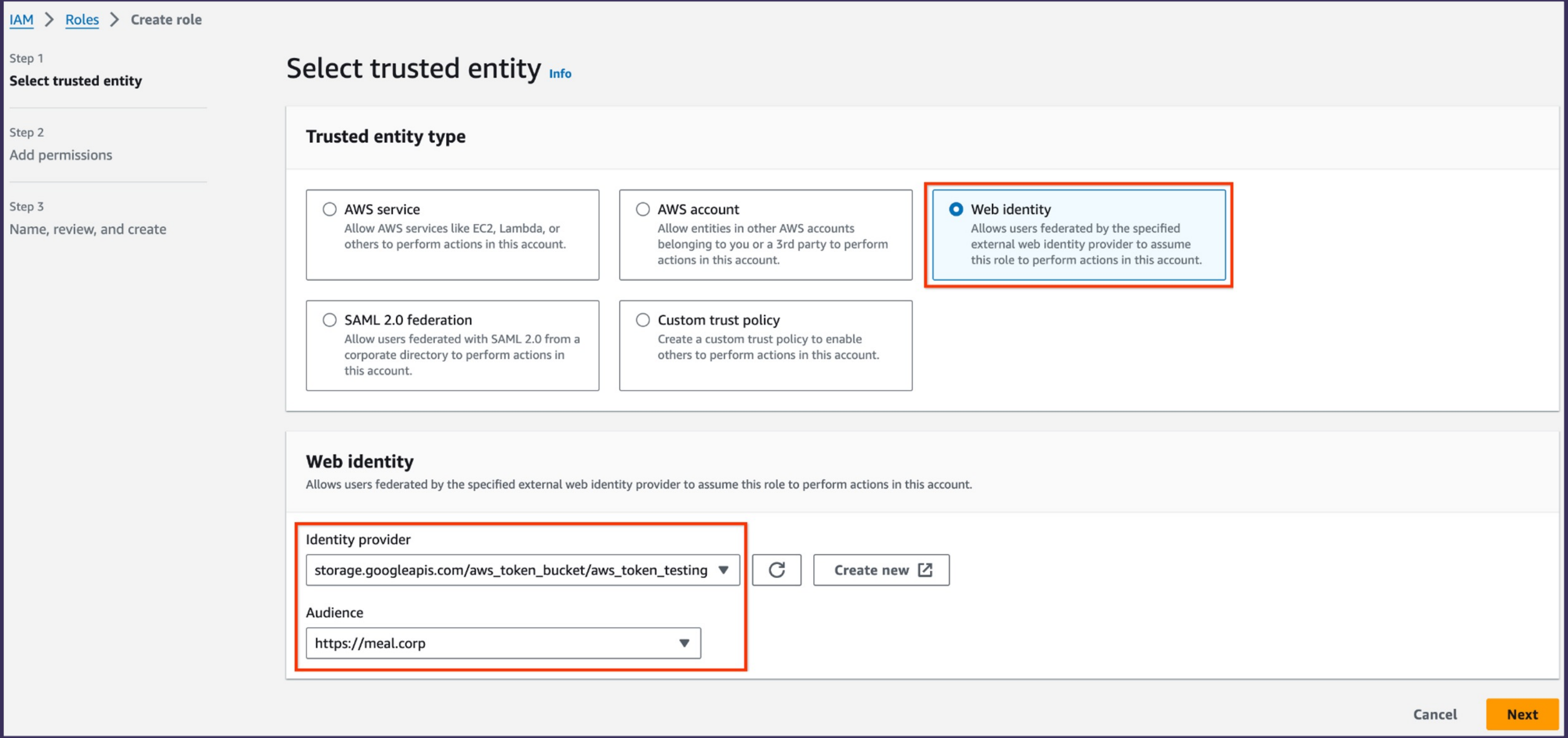
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

You can add up to 50 more tags.

https://confidentialcomputing.googleapis.com/

Create a Role



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

○ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

● Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

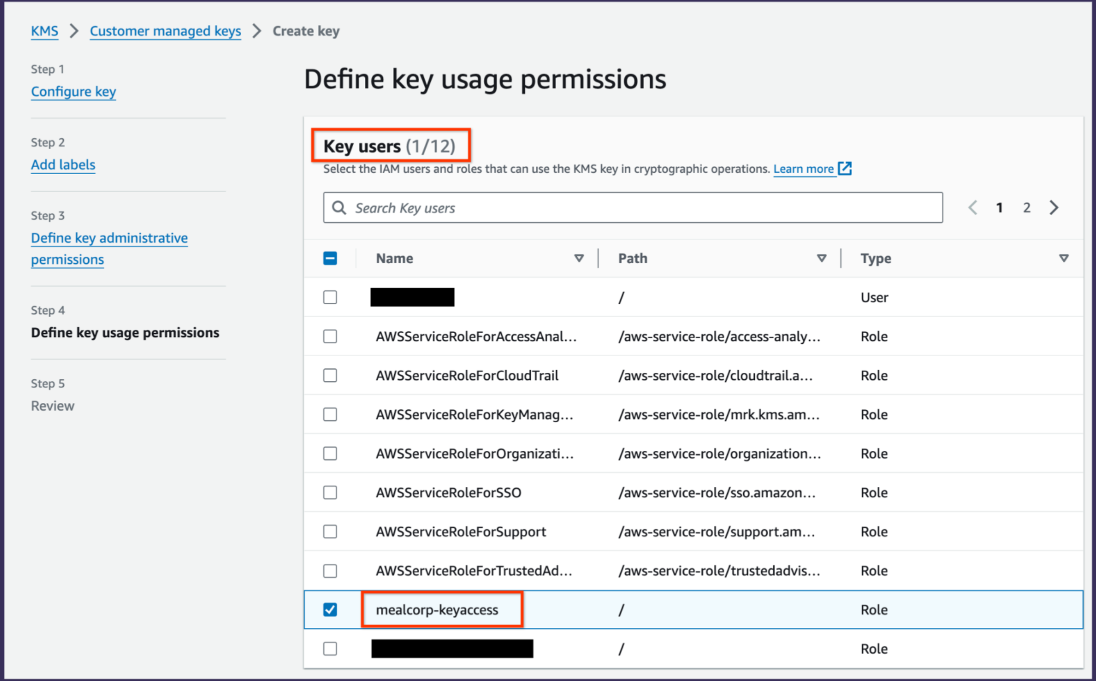
Web identity

Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

Identity provider
storage.googleapis.com/aws_token_bucket/aws_token_testing ▼

Audience
https://meal.corp ▼

Create Encrypt/Decrypt Key



KMS > Customer managed keys > Create key

Step 1
Configure key

Step 2
Add labels

Step 3
Define key administrative permissions

Step 4
Define key usage permissions

Step 5
Review

Define key usage permissions

Key users (1/12)

Select the IAM users and roles that can use the KMS key in cryptographic operations. Learn more

Search Key users

< 1 2 >

☐	Name	Path	Type
☐	[redacted]	/	User
☐	AWSServiceRoleForAccessAnal...	/aws-service-role/access-analy...	Role
☐	AWSServiceRoleForCloudTrail	/aws-service-role/cloudtrail.a...	Role
☐	AWSServiceRoleForKeyManag...	/aws-service-role/mrk.kms.am...	Role
☐	AWSServiceRoleForOrganizati...	/aws-service-role/organization...	Role
☐	AWSServiceRoleForSSO	/aws-service-role/sso.amazon...	Role
☐	AWSServiceRoleForSupport	/aws-service-role/support.am...	Role
☐	AWSServiceRoleForTrustedAd...	/aws-service-role/trustedadvis...	Role
☑	mealcorp-keyaccess	/	Role
☐	[redacted]	/	Role

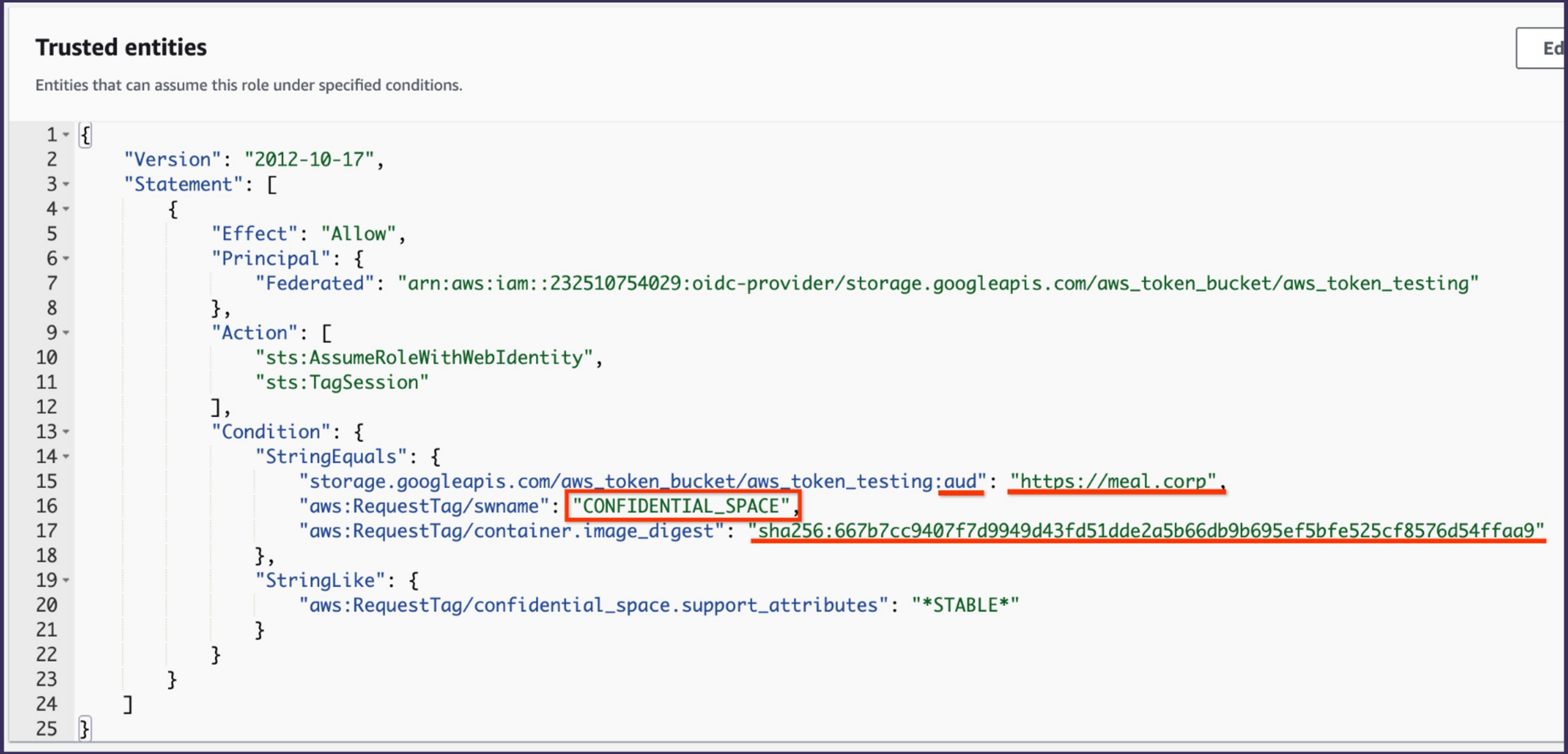
Type: symmetric

Name: mealcorp-datakey

Demo Setup

- Decryption Key in AWS Key Management Service (KMS)
- Policy created to release decryption key
- Sensitive, encrypted data in an S3 bucket
- Run Confidential Space workload

AWS Policy



Trusted entities

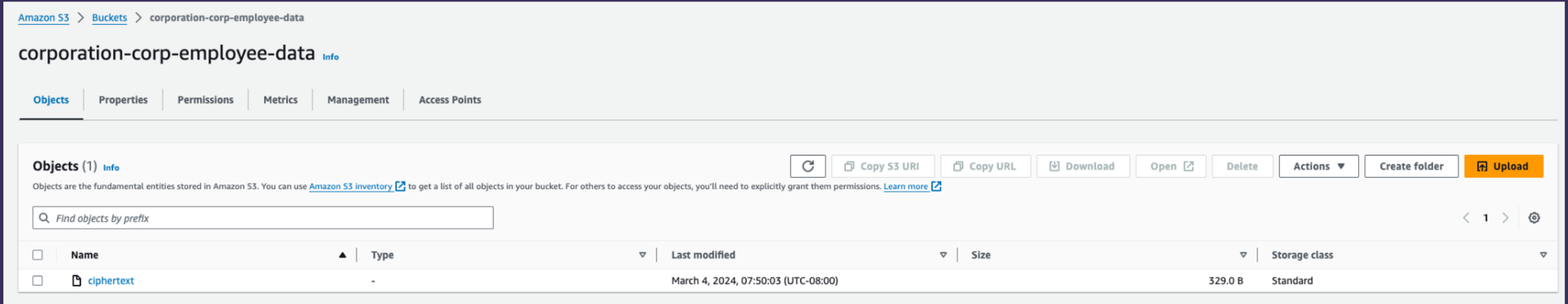
Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::232510754029:oidc-provider/storage.googleapis.com/aws_token_bucket/aws_token_testing"
            },
            "Action": [
                "sts:AssumeRoleWithWebIdentity",
                "sts:TagSession"
            ],
            "Condition": {
                "StringEquals": {
                    "storage.googleapis.com/aws_token_bucket/aws_token_testing:aud": "https://meal.corp",
                    "aws:RequestTag/swname": "CONFIDENTIAL_SPACE",
                    "aws:RequestTag/container.image_digest": "sha256:667b7cc9407f7d9949d43fd51dde2a5b66db9b695ef5bfe525cf8576d54ffaa9"
                },
                "StringLike": {
                    "aws:RequestTag/confidential_space.support_attributes": "*STABLE*"
                }
            }
        }
    ]
}
```

Demo Setup

- Decryption Key in AWS Key Management Service (KMS)
- Policy created to release decryption key
- Sensitive, encrypted data in an S3 bucket
- Run Confidential Space workload

Upload the Data



Amazon S3 > Buckets > corporation-corp-employee-data

corporation-corp-employee-data Info

Objects (1) Info

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

Find objects by prefix

□	Name	Type	Last modified	Size	Storage class
□	ciphertext	-	March 4, 2024, 07:50:03 (UTC-08:00)	329.0 B	Standard

S3 Policy for bucket

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::232510754029:role/mealcorp-keyaccess"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::corporation-corp-employee-data/*"
        }
    ]
}
```

Demo Setup

- Decryption Key in AWS Key Management Service (KMS)
- Policy created to release decryption key
- Sensitive, encrypted data in an S3 bucket
- Run Confidential Space workload

Modify Workload

Workload – Setup CS Client

```
httpClient := http.Client{
    Transport: &http.Transport{
        DialContext: func(_ context.Context, _, _ string) (net.Conn, error) {
            return net.Dial("unix", "/run/container_launcher/teeserver.sock")
        },
    },
}

// Token IPC endpoint
url := "http://localhost/v1/token"
body := `{
        "audience": "https://meal.corp",
        "token_type": "AWS"
    }`
```

Workload – Get CS Token

```
resp, err := httpClient.Post(url, "application/json", strings.NewReader(body))
if err { ... }
tokenbytes, err := io.ReadAll(resp.Body)
if err { ... }
```

Workload – Use CS Token with AWS

```
roleARN := "arn:aws:iam::232510754029:role/mealcorp-keyaccess"

roleProvider := stscreds.NewWebIdentityRoleProviderWithOptions(
  sts, roleARN, "mealcorp", stscreds.FetchTokenPath(tokenPath)
 )

 svc := kms.New(sess, &aws.Config{
     Credentials: credentials.NewCredentials(roleProvider),
 })
```

Summary

More Information

Public Docs - https://cloud.google.com/confidential-computing/confidential-space/docs/confidential-space-overview

Github Repository - https://github.com/google/go-tpm-tools

Q&A