

Paul Gillet & Kevin Auberson
Groupe : L04GrC
Date : 28.03.2024

Using IAM user: devuser3

TASK 3: ATTEMPTING WRITE-LEVEL ACCESS TO AWS SERVICES

Explain why you were able to create an S3 bucket but couldn't upload objects to it.

The ability to create an S3 bucket is allowed by the action `s3:CreateBucket`, but uploading objects to the bucket is not permitted because the action `s3:PutObject` is not in the policy.

TASK 4: ASSUMING AN IAM ROLE AND REVIEWING A RESOURCE-BASED POLICY

So, how were you just now able to upload an object to bucket2? The reason will become clear in the next task

Like, we can see on the schema the devuser is part of the DeveloperGroupPolicy who allowed to create a new bucket but not to access objects in "bucket1". Now, this is possible because the "BucketAccessRole" IAM role has the permissions to allow access to "bucket2". Devuser assumes this role and it inherits these permissions.

TASK 6: FIND A WAY TO UPLOAD AN OBJECT TO BUCKET3

Can you upload a file to bucket3?

We can't upload a file to bucket3 because we have "Insufficient permissions to list objects".

Can you view the bucket policy now? Review the bucket policy details. Do you have an idea for how you can upload Image2.jpg to bucket3?

Yes, we can see it.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {
```

```

        "Sid": "S3Write",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::851725581851:role/OtherBucketAccessRole"
        },
        "Action": [
            "s3:PutObject",
            "s3:GetObject"
        ],
        "Resource": "arn:aws:s3:::bucket3-772ade4372b7a3338bf2c99ca077cf00/*"
    },
    {
        "Sid": "ListBucket",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::851725581851:role/OtherBucketAccessRole"
        },
        "Action": "s3:ListBucket",
        "Resource": "arn:aws:s3:::bucket3-772ade4372b7a3338bf2c99ca077cf00"
    }
]
}





```





To upload an image to bucket3 we can maybe try to use an another AWS management tool like the AWS CLI.


TASK 7: DESIGN AND IMPLEMENT PERMISSION POLICIES FOR S3

Create a bucket that at the top level has three folders for internal, private, and public data.

Objects (3) Info




  Copy S3 URI  Copy URL  Download

 Open  Delete  Actions  Create folder

 Upload

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

<input type="checkbox"/>	Name ▲	Type ▼	Last modified ▼	Size ▼
<input type="checkbox"/>	 internal/	Folder	-	-
<input type="checkbox"/>	 private/	Folder	-	-
<input type="checkbox"/>	 public/	Folder	-	-

Creation of the bucket with the three folder at the top level.

An AcmeStaff role that has read access to internal and public data.

Policy:

Specify permissions [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission

Policy editor

```
1 {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Sid": "readAccess",
6             "Effect": "Allow",
7             "Action": [
8                 "s3:Get*",
9                 "s3:List*",
10                "s3:Describe*"
11            ],
12            "Resource": [
13                "arn:aws:s3::acmedata-grc-auberson/internal/*",
14                "arn:aws:s3::acmedata-grc-auberson/public/*"
15            ]
16        }
17    ]
18 }
```

Policy details

Policy name

Enter a meaningful name to identify this policy.

AcmeDataGrcReadAccess



Maximum 128 characters. Use alphanumeric and '+=, @-_' characters.

Description - optional

Add a short explanation for this policy.

Read access to folder internal and public of S3 bucket acmedata-grc-auberson

Maximum 1,000 characters. Use alphanumeric and '+=, @-_' characters.

 This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action t remaining. [Learn more](#) 

Permissions defined in this policy [Info](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach

 Search

Allow (1 of 407 services)

Service	Access level	Resource	Request condition
S3	Limited: Read, List	Multiple	None

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.

Add new tag

You can add up to 50 more tags.

Role:

Step 1 of 3

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.

Use case

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

Service or use case

S3

Choose a use case for the specified service.

Use case

☒ **S3**

Allows S3 to call AWS services on your behalf.

☐ **S3 Batch Operations**

Allows S3 Batch Operations to call AWS services on your behalf.

Add permissions [Info](#)

Permissions policies (1/972) [Info](#)

Choose one or more policies to attach to your new role.

Filter by Type
All types

	Policy name	Type
<input type="checkbox"/>	AcmeDataGrAFullAccess	Customer managed
<input type="checkbox"/>	AcmeDataGrAReadAccess	Customer managed
<input type="checkbox"/>	AcmeDataGrAWriteAccess	Customer managed
<input type="checkbox"/>	AcmeDataGrcFullAccess	Customer managed
<input checked="" type="checkbox"/>	AcmeDataGrcReadAccess	Customer managed
<input type="checkbox"/>	AcmeDataGrcWriteAccess	Customer managed

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and '+=, @- _' characters.

Description

Add a short explanation for this role.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=, @- \[] # \$ % ^ & * () ; ' " < > `

Step 1: Select trusted entities

Trust policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "Service": "s3.amazonaws.com"  
8       },  
9       "Action": "sts:AssumeRole"  
10    }  
11  ]  
12 }
```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AcmeDataGrcReadAccess	Customer managed	Permissions policy

An AcmeDataScientist role that has read and write access to all data.

Policy:

Specify permissions [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission

Policy editor

```
1 {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Sid": "fullAccess",  
6             "Effect": "Allow",  
7             "Action": [  
8                 "s3:*Object"  
9             ],  
10            "Resource": [  
11                "arn:aws:s3:::acmedata-grc-auberson/*"  
12            ]  
13        }  
14    ]  
15 }
```


Policy details

Policy name

Enter a meaningful name to identify this policy.

AcmeDataGrcFullAccess

Maximum 128 characters. Use alphanumeric and '+=, @-_' characters.

Description - optional

Add a short explanation for this policy.

Full access to all object of S3 bucket acmedata-grc-auberson

Maximum 1,000 characters. Use alphanumeric and '+=, @-_' characters.

Permissions defined in this policy [Info](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach

 Search

Allow (1 of 407 services)

Service	▲	Access level	▼	Resource	Request condition
S3		Limited: Read, Write		BucketName string like acmedata-grc-auberson, ObjectPath string like All	None

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.

Role:

Step 1 of 3

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.

Use case

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

Service or use case

S3

Choose a use case for the specified service.

Use case

☒ **S3**

Allows S3 to call AWS services on your behalf.

☐ **S3 Batch Operations**

Allows S3 Batch Operations to call AWS services on your behalf.

Add permissions [Info](#)

Permissions policies (1/972) [Info](#)

Choose one or more policies to attach to your new role.

Filter by Type

All types

<input type="checkbox"/>	Policy name 🔗	Type	Description
<input type="checkbox"/>	AcmeDataGrFullAccess	Customer managed	Full access to all data inside acmedata-gra-2 S3 bucket.
<input type="checkbox"/>	AcmeDataGrReadAccess	Customer managed	Read access only to internal and public data inside acmedata-gra-2 S3 bucket.
<input type="checkbox"/>	AcmeDataGrWriteAccess	Customer managed	Grand write permission on internal and private data inside acmedata-gra-2 S3 bucket.
<input checked="" type="checkbox"/>	AcmeDataGrcFullAccess	Customer managed	Full access to all object of S3 bucket acmedata-grc-auberson
<input type="checkbox"/>	AcmeDataGrcReadAccess	Customer managed	Read access to folder internal and public of S3 bucket acmedata-grc-auberson
<input type="checkbox"/>	AcmeDataGrcWriteAccess	Customer managed	Write access on internal and private folder of S3 bucket acmedata-grc-auberson

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and '+=, @-_' characters.

Description

Add a short explanation for this role.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=, @-/[{}!#\$%^&*()~:"'<>`

Step 1: Select trusted entities

Trust policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "Service": "s3.amazonaws.com"  
8       },  
9       "Action": "sts:AssumeRole"  
10    }  
11  ]  
12 }
```

Step 2: Add permissions

Permissions policy summary

Policy name 🔗	Type	Attached as
AcmeDataGrcFullAccess	Customer managed	Permissions policy

An AcmeDataIngester role that has write access to internal and private data.

Policy:

Specify permissions [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission

Policy editor

```
1 ▼ {
2     "Version": "2012-10-17",
3     "Statement": [
4     {
5         "Sid": "writeAccess",
6         "Effect": "Allow",
7         "Action": [
8             "s3:PutObject",
9             "s3:DeleteObject",
10            "s3:RestoreObject",
11            "s3:ReplicateObject"
12        ],
13        "Resource": [
14            "arn:aws:s3:::acmedata-grc-auberson/internal/*",
15            "arn:aws:s3:::acmedata-grc-auberson/private/*"
16        ]
17    }
18 ]
19 }
```

Policy details

Policy name

Enter a meaningful name to identify this policy.

AcmeDataGrcWriteAccess

Maximum 128 characters. Use alphanumeric and '+=, @-_' characters.

Description - optional

Add a short explanation for this policy.

Write access on internal and private folder of S3 bucket acmedata-grc-auberson

Maximum 1,000 characters. Use alphanumeric and '+=, @-_' characters.

Permissions defined in this policy [Info](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach this policy to the identity.

 Search

Allow (1 of 407 services)

Service	▲	Access level	▼	Resource	Request condition
S3		Limited: Write		Multiple	None

Role:

Step 1 of 3

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.

Use case

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

Service or use case

S3

Choose a use case for the specified service.

Use case

☒ **S3**

Allows S3 to call AWS services on your behalf.

☐ **S3 Batch Operations**

Allows S3 Batch Operations to call AWS services on your behalf.

Permissions policies (1/972) Info

Choose one or more policies to attach to your new role.

Q

Search

Filter by Type

All types

	Policy name	Type	Description
<input type="checkbox"/>	AcmeDataGrAFullAccess	Customer managed	Full access to all data inside acmedata-gra-2 S3 bucket.
<input type="checkbox"/>	AcmeDataGrAReadAccess	Customer managed	Read access only to internal and public data inside acmedata-gra-2 S3 bucket.
<input type="checkbox"/>	AcmeDataGrAWriteAccess	Customer managed	Grand write permission on internal and private data inside acmedata-gra-2 S3 bucket.
<input type="checkbox"/>	AcmeDataGrcFullAccess	Customer managed	Full access to all object of S3 bucket acmedata-grc-auberson
<input type="checkbox"/>	AcmeDataGrcReadAccess	Customer managed	Read access to folder internal and public of S3 bucket acmedata-grc-auberson
<input checked="" type="checkbox"/>	AcmeDataGrcWriteAccess	Customer managed	Write access on internal and private folder of S3 bucket acmedata-grc-auberson

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and '+,.,@-_' characters.

Description

Add a short explanation for this role.



Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,., @-/ \[] ! # \$ % ^ & * () ; ' " < > `

Step 1: Select trusted entities

[Edit](#)


Trust policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "Service": "s3.amazonaws.com"  
8       },  
9       "Action": "sts:AssumeRole"  
10    }  
11  ]  
12 }
```

Step 2: Add permissions

[Edit](#)

Permissions policy summary

Policy name 	Type	Attached as
AcmeDataGrcWriteAccess	Customer managed	Permissions policy

TASK 8: SIMULATING POLICY EVALUATION

How did you modify the ListBucket request so that it is allowed for the OtherBucketAccessRole?

Policy Simulator

Amazon S3 2 Action(s) selec... **Select All** **Deselect All** **Reset Contexts** **Clear Results** **Run Simulation**

► Global Settings ⓘ

Action Settings and Results [2 actions selected. 0 actions not simulated. 1 actions allowed. 1 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
Amazon S3	ListBucket	bucket	bucket	allowed 1 matching statements. Show statement in GrantBucket1Access (IAM Policy)
Resource You can specify the resource and context keys used to simulate this action. By default the simulation resource is "*".				
bucket		<input type="text" value="arn:aws:s3:::bucket1-721449c17af4fc6b2ee37abc80049ae0/*"/>		<input checked="" type="checkbox"/> Include Resource Policy
Amazon S3	DeleteBucket	bucket	bucket	denied Implicitly denied (no m...

We add resource with the name of the bucket.

Create a new policy, by copying and modifying the GrantBucket1Access policy, that explicitly denies access to a bucket. Using the New Policy mode of the simulator, create a request that will be denied explicitly. Copy the policy into the report and make a screenshot of the simulator showing the explicit deny of the request.

```
{
  "Statement": [
    {
      "Action": [
        "s3:*"
      ],
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::bucket1-721449c17af4fc6b2ee37abc80049ae0/*",
        "arn:aws:s3:::bucket1-721449c17af4fc6b2ee37abc80049ae0"
      ]
    }
  ],
  "Version": "2012-10-17"
}
```

Résultat:

▶ Amazon S3	ListBucket	bucket	bucket	 denied 1 matching statements.
▶ Amazon S3	DeleteBucket	bucket	bucket	 denied 1 matching statements.