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:Put0bject 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 inherit 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.

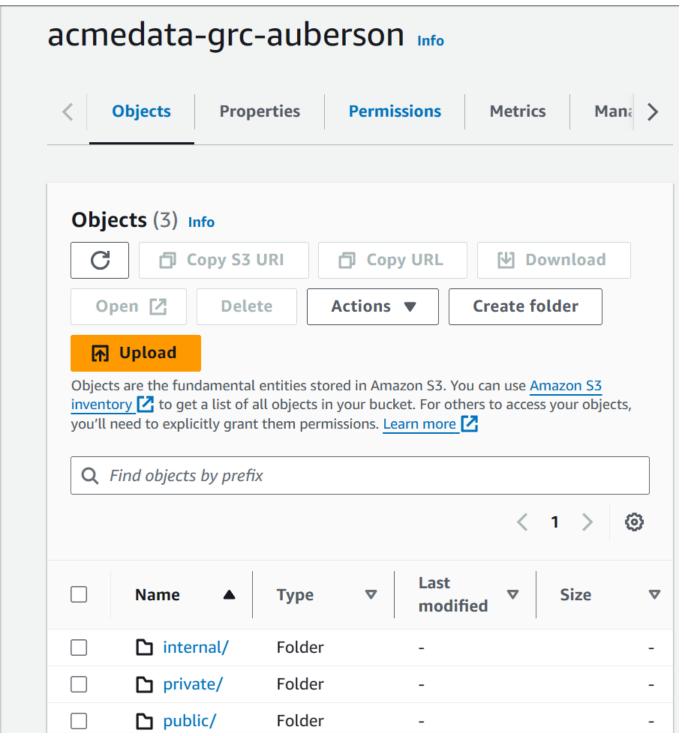
```
{
    "Version": "2012-10-17",
    "Statement": [
    {
```

```
"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"
    1
}
```

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.



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

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

Specify permissions Info

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

Policy editor

```
1 ▼ {
        "Version": "2012-10-17",
       "Statement": [
 3 ▼
4 ▼
            {
 5
                "Sid": "readAccess",
 6
                "Effect": "Allow",
7 ▼
                "Action": [
                    "s3:Get*",
 8
                    "s3:List*",
9
                    "s3:Describe*"
10
11
               ],
12 ▼
               "Resource": [
                    "arn:aws:s3:::acmedata-grc-auberson/internal/*",
13
                    "arn:aws:s3:::acmedata-grc-auberson/public/*"
14
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. (1) 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 Q Search Allow (1 of 407 services) Service Access level **Request condition** Resource Limited: Read, List Multiple None S3 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

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.

Web identity

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

Custom trust policy

Create a custom trust policy to enable 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.

SAML 2.0 federation

Allow users federated with SAML 2.0 from a corporate directory 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.

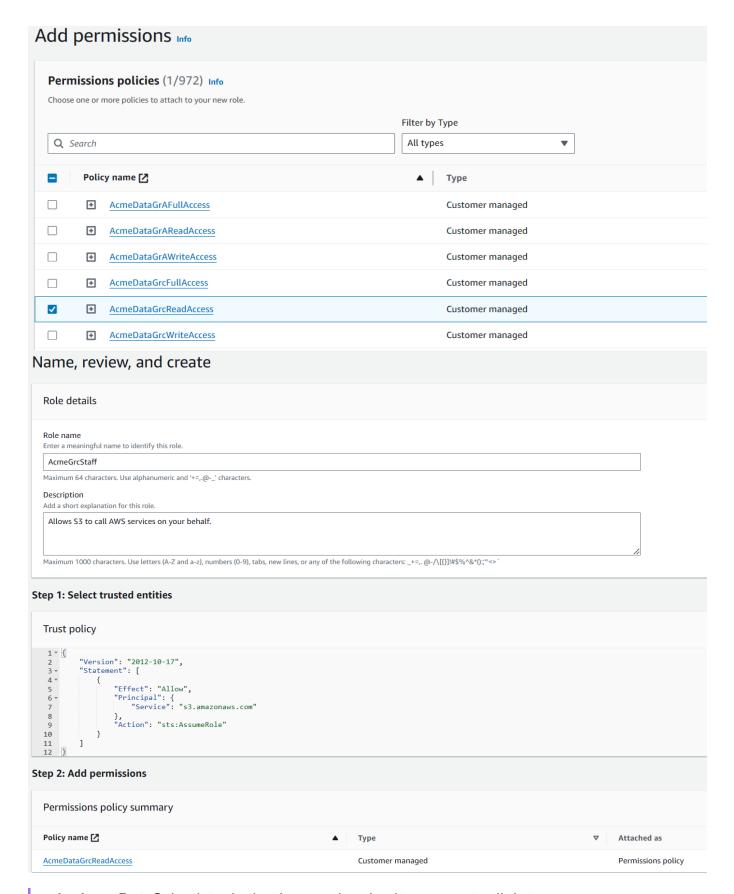
Use case

S3

Allows S3 to call AWS services on your behalf.

S3 Batch Operations

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



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

Specify permissions Info

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

Policy editor

```
1 ▼ {
 2
        "Version": "2012-10-17",
       "Statement": [
 3 ▼
            {
 5
              "Sid": "fullAccess",
              "Effect": "Allow",
 6
               "Action": [
                   "s3:*Object"
 8
 9
              ],
        "Resource": [
10 ▼
                   "arn:aws:s3:::acmedata-grc-auberson/*"
11
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 Q Search Allow (1 of 407 services) Service Access level Resource **Request condition** BucketName| string like Limited: Read, Write **S**3 |acmedata-grc-auberson, None ObjectPath| string like |All

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.

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.

Web identity

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

Custom trust policy

Create a custom trust policy to enable 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.

SAML 2.0 federation

Allow users federated with SAML 2.0 from a corporate directory 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.

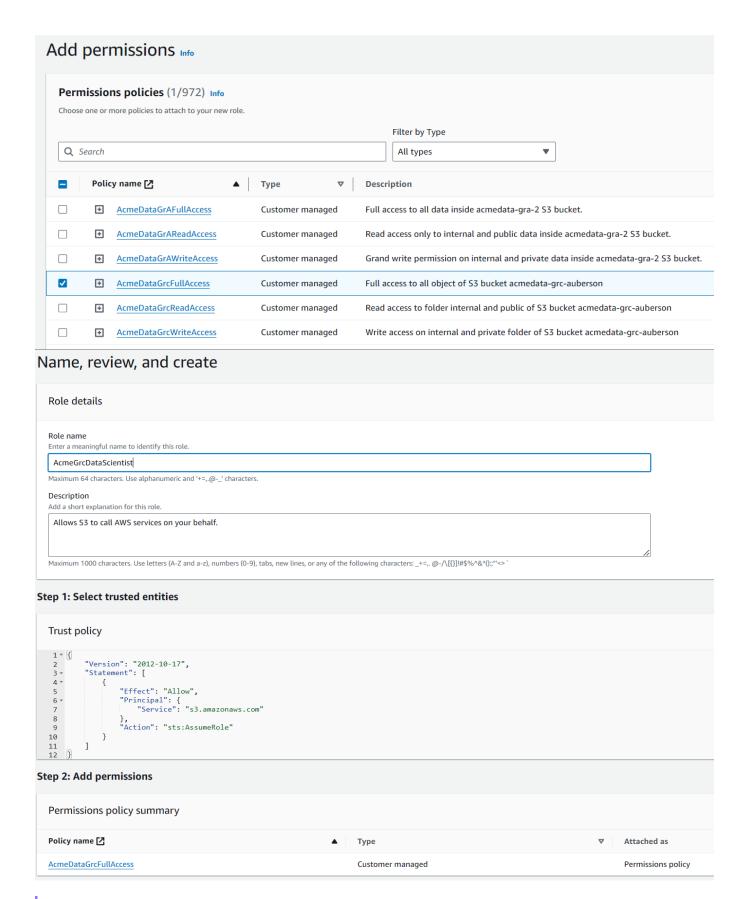
Use case

S3

Allows S3 to call AWS services on your behalf.

S3 Batch Operations

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



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

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",
                  "Effect": "Allow",
 6
                  "Action": [
 7 ▼
                      "s3:PutObject",
 8
 9
                      "s3:DeleteObject",
                      "s3:RestoreObject",
10
                      "s3:ReplicateObject"
11
12
                  ],
                  "Resource": [
13 ▼
                      "arn:aws:s3:::acmedata-grc-auberson/internal/*",
14
15
                      "arn:aws:s3:::acmedata-grc-auberson/private/*"
16
17
          ]
18
19
      }
```

Policy name Enter a meaningful name	to identify this policy.		
AcmeDataGrcWriteA			
Maximum 128 characters.	Use alphanumeric and '+=,.@' characters.		
Description - optional Add a short explanation for	or this policy.		
Write access on inter	nal and private folder of S3 bucket acmo	edata-grc-auberson	
Maximum 1,000 character	s. Use alphanumeric and '+=,.@' characters.		
Maximum 1,000 character	s. Use alphanumeric and '+=,.@' characters.		
Permissions defi	ned in this policy Info		
Permissions defi		lowed or denied. To define permissions for an	IAM identity (user, user group, or role), att
Permissions defi	ned in this policy Info	lowed or denied. To define permissions for an	IAM identity (user, user group, or role), att
Permissions defined in this	ned in this policy Info s policy document specify which actions are all	lowed or denied. To define permissions for an	IAM identity (user, user group, or role), att
Permissions defined in thi	ned in this policy Info s policy document specify which actions are all	lowed or denied. To define permissions for an ▼ Resource	IAM identity (user, user group, or role), att

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.

Web identity

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

Custom trust policy

Create a custom trust policy to enable 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.

SAML 2.0 federation

Allow users federated with SAML 2.0 from a corporate directory 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.

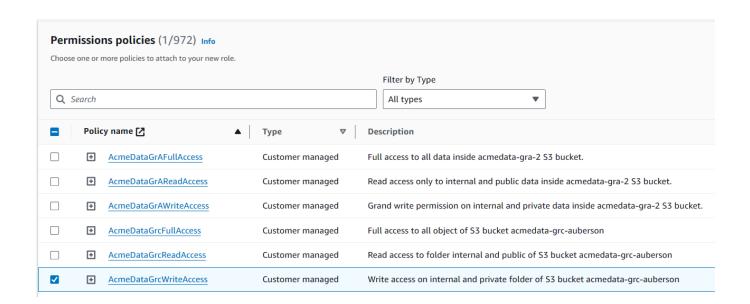
Use case

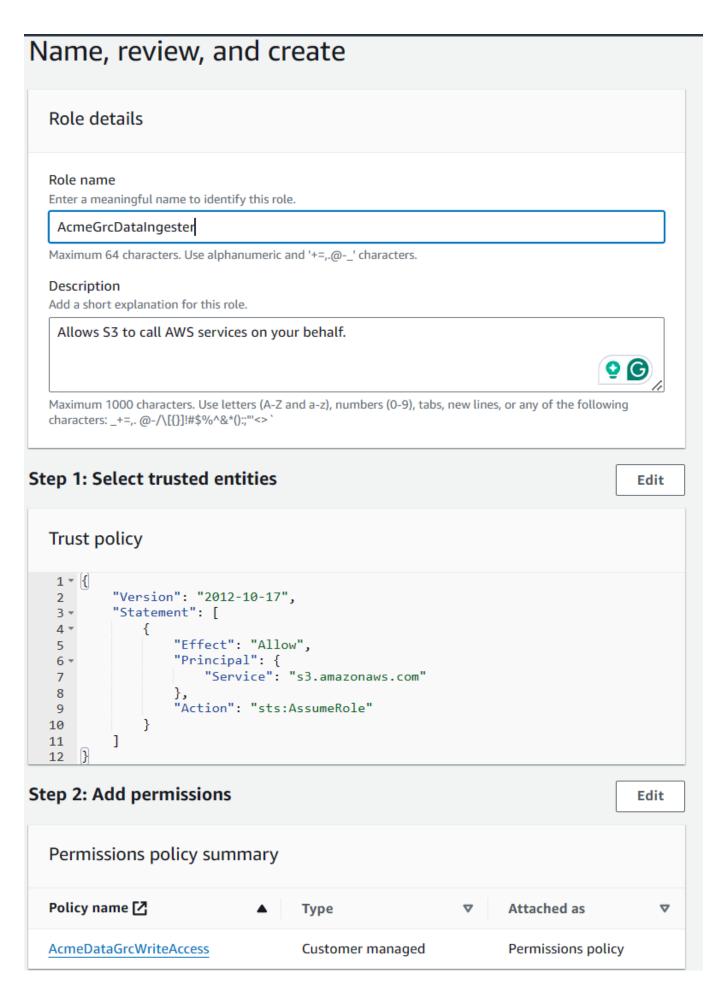
S3

Allows S3 to call AWS services on your behalf.

S3 Batch Operations

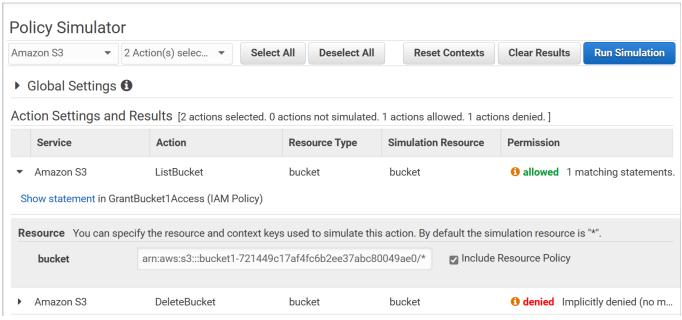
Allows S3 Batch Operations to call AWS services on your behalf.





TASK 8: SIMULATING POLICY EVALUATION

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



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.

Résultat:

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