

Rendu TP03

Rendu du TP03 effectué par Thomas PEUGNET.

Nous créons l'utilisateur Joanne.

The screenshot shows the AWS IAM console. The URL is [https://console.aws.amazon.com/iamv2/home?#/users/Joanne/setPermissionsBoundary](#). The page title is "Set permissions boundary on Joanne". The main section is titled "Permissions policies (1/1010)" with the sub-instruction "Select policy to set as the permissions boundary." A search bar contains "s3fu". A filter bar shows "1 match" for "All types". A table lists one policy: "AmazonS3FullAccess" (AWS managed). At the bottom right are "Cancel" and "Set boundary" buttons.

Nous nous reconnectons avec Joanne et constatons le résultat suivant:

Resources

You are using the following Amazon EC2 resources in the Europe (Paris) Region:

Instances (running)	0	Auto Scaling Groups	0 API Error	Capacity Reservations	0 API Error
Dedicated Hosts	0 API Error	Elastic IPs	0 API Error	Instances	0 API Error
Key pairs	0 API Error	Load balancers	0 API Error	Placement groups	0 API Error
Security groups	0 API Error	Snapshots	0 API Error	Volumes	0 API Error

Launch instance
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Service health [AWS Health Dashboard](#)

Zones
Zone name | Zone ID
An error occurred
An error occurred retrieving service health information

Instance alarms [View in CloudWatch](#)

Instances in alarm

Scheduled events

EC2 Free Tier [Info](#)
Offers for all AWS Regions.
0 EC2 free tier offers in use

End of month forecast
User: arnawsiam:794038237731:user/Joanne is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:free-tier:us-east-1:794038237731:/GetFreeTierUsage because no permissions boundary allows the freetier:GetFreeTierUsage action

Exceeds free tier
User: arnawsiam:794038237731:user/Joanne is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:free-tier:us-east-1:794038237731:/GetFreeTierUsage because no permissions boundary allows the freetier:GetFreeTierUsage action

View Global EC2 resources

View all AWS Free Tier offers

Account attributes

An error occurred
An error occurred checking for a default VPC

Settings
Data protection and security
Zones
EC2 Serial Console
Default credit specification
EC2 console preferences

Explore AWS

Amazon GuardDuty Malware Protection
GuardDuty now provides agentless malware detection in Amazon EC2 & EC2 container workloads. [Learn more](#)

Nous créons un bucket S3.

Successfully created bucket "bucket-thomas02-12-2024"
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Account snapshot - updated every 24 hours [AWS Regions](#) [View Storage Lens dashboard](#)

General purpose buckets (1) [Info](#) [All AWS Regions](#)

Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
bucket-thomas02-12-2024	Europe (Paris) eu-west-3	View analyzer for eu-west-3	December 2, 2024, 13:26:55 (UTC+01:00)

Nous créons la policy avec le contenu suivant.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": "iam:*",
            "Resource": "*"
        },
        {
            "Sid": "DenyPermBoundaryIAMPolicyAlteration",
            "Effect": "Deny",
            "Action": [
                "iam:DeletePolicy",
                "iam:DeletePolicyVersion",
                "iam>CreatePolicyVersion",
                "iam:SetDefaultPolicyVersion"
            ],
            "Resource": [
                "arn:aws:iam::794038237731:policy/PermissionsBoundary"
            ]
        },
        {
            "Sid": "DenyRemovalOfPermBoundaryFromAnyUserOrRole",
            "Effect": "Deny",
            "Action": [
                "iam>DeleteUserPermissionsBoundary",
                "iam>DeleteRolePermissionsBoundary"
            ],
            "Resource": [
                "arn:aws:iam::794038237731:user/*",
                "arn:aws:iam::794038237731:role/*"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:PermissionsBoundary":
"arn:aws:iam::794038237731:policy/PermissionsBoundary"
                }
            }
        },
        {
            "Sid": "DenyAccessIfRequiredPermBoundaryIsNotBeingApplied",
            "Effect": "Deny",
            "Action": [
                "iam:PutUserPermissionsBoundary",
                "iam:PutRolePermissionsBoundary"
            ],
            "Resource": [
                "arn:aws:iam::794038237731:user/*",

```

```
"arn:aws:iam::794038237731:role/*"
],
{
  "Condition": {
    "StringNotEquals": {
      "iam:PermissionsBoundary": "arn:aws:iam::794038237731:policy/PermissionsBoundary"
    }
  }
},
{
  "Sid": "DenyUserAndRoleCreationWithOutPermBoundary",
  "Effect": "Deny",
  "Action": [
    "iam:CreateUser",
    "iam:CreateRole"
  ],
  "Resource": [
    "arn:aws:iam::794038237731:user/*",
    "arn:aws:iam::794038237731:role/*"
  ],
  "Condition": {
    "StringNotEquals": {
      "iam:PermissionsBoundary": "arn:aws:iam::794038237731:policy/PermissionsBoundary"
    }
  }
}
]
```

The screenshot shows the AWS IAM Policies > PermissionsBoundary page. The policy details are as follows:

- Type: Customer managed
- Creation time: December 02, 2024, 13:32 (UTC+01:00)
- Edited time: December 02, 2024, 13:32 (UTC+01:00)
- ARN: arn:aws:iam::794038237731:policy/PermissionsBoundary

The Permissions tab is selected, showing the following permissions defined in the policy:

- Explicit deny (1 of 433 services):**

Service	Access level	Resource	Request condition
IAM	Limited: Permissions management, Write	Multiple	Multiple
- Allow (1 of 433 services):**

Service	Access level	Resource	Request condition
IAM	Full access	All resources	None

Related consoles links include IAM Identity Center and AWS Organizations.

Nous créons un utilisateur `BadUSER`.

The screenshot shows the AWS IAM Users > Create user page, Step 3: Review and create. The user details are:

- User name: BadUSER
- Console password type: Autogenerated
- Require password reset: No

The Permissions summary shows a single managed policy: `IAMFullAccess`. The Tags section is empty.

At the bottom, there are buttons for Cancel, Previous, and Create user (highlighted).

Nous nous connectons avec et constatons le résultat suivant.

AWS CloudWatch Metrics Dashboard

Recently visited (Info)

No recently visited services

Explore one of these commonly visited AWS services.

EC2 S3 RDS Lambda

Applications (0) (Info)

Region: Europe (Paris)

eu-west-3 (Current Region) Find applications

Name Description Region Originati. ★ ▲

Access denied to servicecatalog>ListApplications

Welcome to AWS

Getting started with AWS (Info)

Learn the fundamentals and find valuable information to get the most out of AWS.

Training and certification (Info)

Learn from AWS experts and advance your skills and knowledge.

What's new with AWS? (Info)

Discover new AWS services, features, and Regions.

AWS Health (Info)

No health data

You don't have permissions to access AWS Health.

Cost and usage (Info)

Current month costs (Info)

Access denied

Cost breakdown (Info)

Access denied

Forecasted month end costs (Info)

Access denied

Savings opportunities (Info)

Access denied

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS CloudWatch Metrics Dashboard

Dashboard

EC2 Global View

Events

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Load Balancing

Load Balancers

Target Groups

Trust Stores

Auto Scaling

Auto Scaling Groups

Resources

You are using the following Amazon EC2 resources in the Europe (Paris) Region:

Instances (running)	0	Auto Scaling Groups	API Error	Capacity Reservations	API Error
Dedicated Hosts	API Error	Elastic IPs	API Error	Instances	API Error
Key pairs	API Error	Load balancers	API Error	Placement groups	API Error
Security groups	API Error	Snapshots	API Error	Volumes	API Error

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance Migrate a server

Note: Your instances will launch in the Europe (Paris) Region

Instance alarms

(User: arnawsiam:794038237731:user/BadUSER is not authorized to perform: cloudwatch:DescribeAlarms on resource: arnawscloudwatch:alarm:arn:3794038237731:alarm:* because no identity-based policy allows the cloudwatch:DescribeAlarms action)

Instances in alarm

Service health

AWS Health Dashboard

An error occurred An error occurred retrieving service health information

Zones

Zone name Zone ID

An error occurred An error occurred retrieving service health information

Enable additional Zones

EC2 Free Tier (Info)

Offers for all AWS Regions.

0 EC2 free tier offers in use

End of month forecast

(User: arnawsiam:794038237731:user/BadUSER is not authorized to perform: freetier:GetFreeTierUsage on resource: arnaws:freetier-east-1:794038237731:/GetFreeTierUsage because no identity-based policy allows the freetier:GetFreeTierUsage action)

View Global EC2 resources

Account attributes

An error occurred An error occurred checking for a default VPC

Settings

Data protection and security

Zones

EC2 Serial Console

Default credit specification

EC2 console preferences

Explore AWS

10 Things You Can Do Today to Reduce AWS Costs

Explore how to effectively manage your AWS costs without compromising on performance or capacity. Learn more

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS S3 Buckets page. On the left, there's a sidebar with links like 'Amazon S3', 'Buckets', 'Access Grants', 'Access Points', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', 'IAM Access Analyzer for S3', 'Storage Lens', 'AWS Marketplace for S3', and 'Feature spotlight'. The main content area has a heading 'Account snapshot - updated every 24 hours' and a link 'View Storage Lens dashboard'. Below it, there are tabs for 'General purpose buckets' (selected) and 'Directory buckets'. A message says 'General purpose buckets' and 'Buckets are containers for data stored in S3.' There's a search bar 'Find buckets by name' and columns for 'Name', 'AWS Region', 'IAM Access Analyzer', and 'Creation date'. A prominent red-bordered warning message states: 'You don't have permissions to list buckets. After you or your AWS administrator has updated your permissions to allow the s3>ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in Amazon S3.' At the bottom, there are buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'.

Nous allons effectuer une escalade de privilèges avec un nouvel utilisateur `testThomas1`.

The screenshot shows the 'Create user' wizard in the IAM section. The navigation bar at the top includes 'CloudShell', 'Feedback', and links for '© 2024, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'. The main content area is titled 'Review and create' and says 'Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.' It shows a step-by-step progress: 'Step 1 Specify user details' (done), 'Step 2 Set permissions' (done), 'Step 3 Review and create' (selected), and 'Step 4 Retrieve password' (not yet done). Under 'User details', the 'User name' is set to 'testThomas1', 'Console password type' is 'Autogenerated', and 'Require password reset' is 'No'. In the 'Permissions summary' section, the 'Name' is 'AdministratorAccess', 'Type' is 'AWS managed - job function', and 'Used as' is 'Permissions policy'. The 'Tags - optional' section indicates 'No tags associated with the resource' and has a button 'Add new tag'. At the bottom, there are buttons for 'Cancel', 'Previous', and 'Create user' (highlighted).

Nous nous reconnectons avec ce nouvel utilisateur et constatons que nous avons maintenant accès.

The screenshot shows the AWS EC2 Dashboard for the Europe (Paris) Region. On the left, a sidebar lists various EC2 management categories like Instances, Images, and Auto Scaling. The main area displays resource counts: 0 Instances (running), 0 Auto Scaling Groups, 0 Capacity Reservations, 0 Dedicated Hosts, 0 Elastic IPs, 0 Instances, 0 Key pairs, 0 Load balancers, 0 Placement groups, 7 Security groups, 0 Snapshots, 0 Volumes. Below this is a 'Launch instance' section with a 'Launch instance' button and a 'Migrate a server' button. A note says instances will launch in the Europe (Paris) Region. The 'Service health' section shows 'AWS Health Dashboard' and indicates the service is operating normally. The 'Zones' section lists three availability zones: eu-west-3a (euw3-az1), eu-west-3b (euw3-az2), and eu-west-3c (euw3-az3). To the right, there's a 'EC2 Free Tier' summary, an 'Account attributes' section with VPC details, and an 'Explore AWS' section with price-performance information.

Nous appliquons **PermissionsBoundary** à notre utilisateur **BadUSER**.

The screenshot shows the AWS IAM User Details page for 'BadUSER'. The left sidebar includes categories like Access management, Access reports, and Related consoles. The main panel shows a green success message: 'Permissions boundary PermissionsBoundary added.' Below this is the 'BadUSER Info' section with a 'Summary' table. The 'Permissions' tab is selected, showing a table of attached policies: 'Policy name' (IAMFullAccess), 'Type' (AWS managed), and 'Attached via' (Directly). There's also a 'Permissions boundary (set)' section and a 'Generate policy based on CloudTrail events' section with a 'Generate policy' button.

Nous nous reconnectons avec l'utilisateur **BadUSER** et tentons de supprimer permissions boundary.

The screenshot shows the AWS IAM User Details page for a user named 'BadUSER'. The 'Permissions' tab is selected. A modal dialog is displayed in the center of the screen, asking if the user wants to 'Remove permissions boundary?' It includes a 'Cancel' button and a yellow 'Remove boundary' button. The background shows the user's ARN, creation date, console access status, and an access key.

Nous obtenons le retour suivant.

The screenshot shows the AWS IAM User Details page for 'BadUSER'. A red banner at the top indicates an access denial: 'Access denied to iam>DeleteUserPermissionsBoundary'. The 'Permissions' tab is selected, showing one attached policy: 'IAMFullAccess'. A 'You need permissions' message in a red box at the bottom indicates the user lacks the required access to perform the action.

Nous tentons de modifier la politique pour obtenir `AdministratorAccess`.

Permissions policies (1/1010)

Select policy to set as the permissions boundary.

Policy name	Type	Attached entities
<input checked="" type="radio"/> AdministratorAccess	AWS managed - job function	3
<input type="radio"/> AdministratorAccess-Amplify	AWS managed	0
<input type="radio"/> AdministratorAccess-AWSElasticBeanstalk	AWS managed	0
<input type="radio"/> AmazonAPIGatewayAdministrator	AWS managed	0
<input type="radio"/> AmazonSecurityLakeAdministrator	AWS managed	0
<input type="radio"/> AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy	AWS managed	0
<input type="radio"/> AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrator	AWS managed	0
<input type="radio"/> AWS-SSM-RemediationAutomation-AdministrationRolePolicy	AWS managed	0
<input type="radio"/> AWS-SSM-RemediationAutomation-OperationalAccountAdministrator	AWS managed	0
<input type="radio"/> AWSAppSyncAdministrator	AWS managed	0
<input type="radio"/> AWSAuditManagerAdministratorAccess	AWS managed	0
<input type="radio"/> AWSBudgetsActions_RolePolicyForResourceAdministrationWithS...	AWS managed	0
<input type="radio"/> AWSCloud9Administrator	AWS managed	0
<input type="radio"/> AWSGrafanaAccountAdministrator	AWS managed	0
<input type="radio"/> AWSSSOdirectoryAdministrator	AWS managed	0
<input type="radio"/> AWSSQMasterAccountAdministrator	AWS managed	0
<input type="radio"/> AWSSQMemberAccountAdministrator	AWS managed	0

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Nous tentons de recréer un nouvel utilisateur et obtenons le résultat suivant.

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name testThomas2	Console password type Autogenerated	Require password reset Yes
--------------------------	--	-------------------------------

Permissions summary

Name	Type	Used as
AdministratorAccess	AWS managed - job function	Permissions policy
IAMUserChangePassword	AWS managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Previous Create user

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Nous assignons notre **PermissionBoundary** à cet utilisateur et pouvons en effet le créer.

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Step 1
Step 2
Step 3
Step 4 **Retrieve password**

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Console sign-in URL
<https://thomas-peugnet.sigin.aws.amazon.com/console>

User name

Console password
 [Show](#)

[Email sign-in instructions](#)

[Cancel](#) [Download .csv file](#) [Return to users list](#)

Nous pouvons confirmer que l'utilisateur `testThomas2` ne peut pas accéder aux EC2.

EC2 Global View

Resources

You are using the following Amazon EC2 resources in the Europe (Paris) Region:

Instances (running)	0	Auto Scaling Groups	0 API Error	Capacity Reservations	0 API Error
Dedicated Hosts	0 API Error	Elastic IPs	0 API Error	Instances	0 API Error
Key pairs	0 API Error	Load balancers	0 API Error	Placement groups	0 API Error
Security groups	0 API Error	Snapshots	0 API Error	Volumes	0 API Error

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

[Launch instance](#) [Migrate a server](#)

Note: Your instances will launch in the Europe (Paris) Region

Service health

[AWS Health Dashboard](#)

An error occurred

An error occurred retrieving service health information

Zones

Zone name | Zone ID

An error occurred

An error occurred retrieving service health information

[Enable additional Zones](#)

EC2 Free Tier Info

Offers for all AWS Regions.

0 EC2 free tier offers in use

End of month forecast

An error occurred

User: arn:aws:iam::794038237731:user/BadUSER is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:794038237731:GetFreeTierUsage because no id entity-based policy allows the freetier:GetFreeTierUsage action

Exceeds free tier

An error occurred

User: arn:aws:iam::794038237731:user/BadUSER is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:794038237731:GetFreeTierUsage because no id entity-based policy allows the freetier:GetFreeTierUsage action

[View Global EC2 resources](#)

[View all AWS Free Tier offers](#)

Account attributes

An error occurred

An error occurred checking for a default VPC

Settings

Data protection and security
 Zones
 EC2 Serial Console
 Default credit specification
 EC2 console preferences

Explore AWS

10 Things You Can Do Today to Reduce AWS Costs

Explore how to effectively manage your AWS costs without compromising on performance or capacity. [Learn more](#)