



Звіт до лабораторної роботи №3:
«Створення ІАМ користувача»
з дисципліни «Інтеграція та адміністрування інформаційних систем»

Виконала:
студент групи ІТ-31з
Костюк Тетяна
Прийняв:
Лучкевич М.М.

Зміст

Мета роботи.....	3
Хід виконання роботи.....	4
Висновки	11

Мета роботи

Ознайомитись з сервісом AWS, створити IAM користувача та групу для них. Створити правила поведінки для користувачів та додати policy до групи.

Хід виконання роботи



**Новый аккаунт AWS позволит
ознакомиться с продуктами
уровня бесплатного
пользования.**

Подробнее см. на aws.amazon.com/free.



Зарегистрируйтесь на AWS

Адрес электронной почты
Этот адрес электронной почты будет использоваться
для входа в новый аккаунт AWS.

tetiana.kostiuk.ki.2018@lpnu.ua

Пароль

.....

Подтверждение пароля

.....

Имя аккаунта AWS

Выберите имя для аккаунта. После регистрации это
имя можно будет изменить в настройках вашего
аккаунта.

tkostiuk

Продолжить (шаг 1 из 5)

[Войдите в существующий аккаунт AWS](#)

Рисунок 1 Створення AWS акаунту

per to improve security for this account

Create alias for AWS account 292022959839

Preferred alias

tkostiuk

Must be not more than 63 characters. Valid characters are a-z, 0-9, and - (hyphen).

New sign-in URL

<https://tkostiuk.signin.aws.amazon.com/console>

i IAM users will still be able to use the default URL containing the AWS account ID.

Cancel **Save changes**

Рисунок 2 Зміна URL акаунту

Set password policy

A password policy is a set of rules that define complexity requirements and mandatory rotation periods for your IAM users' passwords. [Learn more](#)

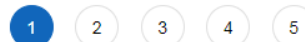
Select your account password policy requirements:

- ☒ Enforce minimum password length

characters
- ☐ Require at least one uppercase letter from Latin alphabet (A-Z)
- ☐ Require at least one lowercase letter from Latin alphabet (a-z)
- ☒ Require at least one number
- ☐ Require at least one non-alphanumeric character (! @ # \$ % ^ & * () _ + - = [] { } | ')
- ☐ Enable password expiration
- ☐ Password expiration requires administrator reset
- ☒ Allow users to change their own password
- ☐ Prevent password reuse

Рисунок 3 Встановлення правил створення паролю для користувачів

Add user



Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name* ✕

✕

[+ Add another user](#)

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

- Select AWS credential type* ☐ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- ☒ **Password - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

- Console password* ☐ Autogenerated password
- ☒ Custom password

☐ Show password

- Require password reset ☒ Users must create a new password at next sign-in

* Required

[Cancel](#)


[Next: Permissions](#)


Рисунок 4 Створення двох нових користувачів


Add user


- 1
- 2
- 3
- 4
- 5

Set permissions

 Add users to group

 Copy permissions from existing user

 Attach existing policies directly

 **Get started with groups**

You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. [Learn more](#)

Create group

Set permissions boundary

Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. [Learn more](#)

Group name

Create policy Refresh

Filter policies Search

Showing 725 results

	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	AdministratorAccess	Job function	None	Provides full access to AWS services and resources.
<input type="checkbox"/>	AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissions while explicitly allowing direct access to resources needed by Amplify applicat...
<input type="checkbox"/>	AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants account administrative permissions. Explicitly allows developers and administrators to gain direct access to resou...
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness resources and access to related AWS Services
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessLifsizeDelegatedAccessPolicy	AWS managed	None	Provide access to Lifesize AVS devices
<input type="checkbox"/>	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None	Provide access to Poly AVS devices
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	AWS managed	None	Provide read only access to AlexaForBusiness services
<input type="checkbox"/>	AmazonAPIGatewayAdministrator	AWS managed	None	Provides full access to create/edit/delete APIs in Amazon API Gateway via the AWS Management Console


Cancel Create group


Рисунок 5 Створення групи "devops" з політикою AdministratorAccess


Add user

- 1
- 2
- 3
- 4
- 5

Set permissions

 Add users to group

 Copy permissions from existing user

 Attach existing policies directly

Add users to an existing group or create a new one. Using groups is a best-practice way to manage users' permissions by job functions. [Learn more](#)

Add user to group

Create group Refresh

Search

Showing 1 result

Group	Attached policies
<input checked="" type="checkbox"/> devops	AdministratorAccess

Set permissions boundary

Рисунок 6 Результат створення групи

Add user

1 2 3 4 5

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
key	12345	×
key1	12345	×
Add new key		

You can add 48 more tags.

Add user

1 2 3 4 5

Review

Review your choices. After you create the users, you can view and download autogenerated passwords and access keys.

User details

User names	kostiuk1 and kostiuk2
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The users shown above will be added to the following groups.

Type	Name
Group	devops

Tags

The new users will receive the following tags

Key	Value
key	12345
key1	12345

Рисунок 7 Вікно інформації про створення користувачів

Add user

1 2 3 4 5

✓

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://tkostiuk.signin.aws.amazon.com/console>

Download .csv

	User	Email login instructions
▶	✓ kostiuk1	Send email
▶	✓ kostiuk2	Send email

Рисунок 8 Додані користувачі



User groups

1

Users

2

Roles

2

Policies

0

Identity providers

0

Рисунок 9 Результат додавання користувачів і групи

Create policy

1

2

3

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor

JSON

[Import managed policy](#)[Expand all](#) | [Collapse all](#)

▼ S3 (1 action)

[Clone](#) | [Remove](#)

► Service S3

▼ Actions Specify the actions allowed in S3 ?

[Switch to deny permissions](#) ⓘ

close

Q Filter actions

Manual actions (add actions)

☐ All S3 actions (s3:*)

Access level

▼ ☐ List (1 selected)[Expand all](#) | [Collapse all](#)☒ ListAccessPoints ?☐ ListBucketMultipartUploads ?☐ ListMultiRegionAccessPoints ?☐ ListAccessPointsForObjectLambda ?☐ ListBucketVersions ?☐ ListStorageLensConfigurations ?☐ ListAllMyBuckets ?☐ ListJobs ?☐ ListBucket ?☐ ListMultipartUploadParts ?► ☐ Read► ☐ Tagging► ☐ Write► ☐ Permissions management

Character count: 125 of 6 144.

Cancel

Next: Tags

Рисунок 10 Створення нового правила поведінки

Create policy

1

2

3

Review policy

Name* MyPolicy|

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

Description

Maximum 1000 characters. Use alphanumeric and '+-._@-' characters.

Summary

Q Filter

Service ▼

Access level

Resource

Request condition

Allow (1 of 314 services) [Show remaining 313](#)

S3

Limited: List

All resources

None

Tags

Key

Value

No tags associated with the resource.

* Required

Cancel

Previous

Create policy

Рисунок 11 Назва нової політики

Add user

1

2

3

4

5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name* ✕

✕

[+ Add another user](#)

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

- Select AWS credential type*
- ☐ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- ☒ **Password - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

- Console password*
- ☐ Autogenerated password
- ☒ Custom password

☐ Show password

- Require password reset ☒ Users must create a new password at next sign-in

* Required

Cancel

Next: Permissions

Рисунок 12 Створення двох нових користувачів з API ключами

Add user

1

2

3

4

5

✓ Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://tkostiuk.signin.aws.amazon.com/console>

[Download .csv](#)

	User	Email login instructions
▶ ✓	tanya1	Send email
▶ ✓	tanya2	Send email

Users (4) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Delete

Add users

Find users by username or access key

< 1 > ⚙

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	kostiuk1	devops	Never	None	✔ 23 minutes ago	-
<input type="checkbox"/>	kostiuk2	devops	Never	None	✔ 23 minutes ago	-
<input type="checkbox"/>	tanya1	devops	Never	None	✔ 4 minutes ago	-
<input type="checkbox"/>	tanya2	devops	Never	None	✔ 4 minutes ago	-

Рисунок 13 Результат додавання користувачів

Висновки

На цій лабораторній роботі я створила аккаунт Amazon Web Services (AWS), навчилася створювати користувачі, а також групи і правила поведінки(політики) для них.