# **ПРАКТИЧНА РОБОТА № 5. ВСТУП ДО IAM**

**Мета роботи:** дослідити користувачів, групи та політики в службі AWS Identity and Access Management (IAM).

Для виконання завдань практичної роботи потрібно підключитися до консолі керування AWS.

**Завдання 1. Дослідити користувачів і групи**

У цьому завданні ви дослідите користувачів і групи, які вже були створені для вас в IAM.

1. По-перше, зазначте регіон, у якому ви перебуваєте; наприклад, **N. Virginia**. Регіон відображається у верхньому правому куті сторінки консолі.

Ця інформація може знадобитися вам пізніше.

1. Виберіть меню **«Служби»**, знайдіть служби **«Безпека», «Ідентифікація та відповідність»** і виберіть **IAM**.
2. На панелі навігації ліворуч виберіть **Користувачі**. Для вас створено таких користувачів IAM (якщо немає – створіть користувачівсамостійно):
   * користувач-1
   * користувач-2
   * користувач-3
3. Виберіть ім'я **користувача-1** .
   * Це приведе вас до сторінки зведення для користувача-1. Відобразиться вкладка «Дозволи».
   * Зауважте, що користувач-1 не має жодних дозволів.
4. Виберіть вкладку **Групи**.

Зауважте, що користувач-1 також не є членом жодної групи.

1. Виберіть вкладку **Облікові дані безпеки**.

Зверніть увагу, що користувачеві-1 призначено **пароль консолі**. Надайте йому цю роль. Це дозволяє користувачеві-1 отримати доступ до консолі керування AWS.

1. На панелі навігації ліворуч виберіть **Групи користувачів**. Створіть такі групи (назви англійською):
   * EC2-Admin;
   * Підтримка EC2;
   * S3-підтримка.
2. Виберіть назву групи **EC2-Support**.

Це приведе вас до сторінки зведення для групи **EC2-Support** .

1. Виберіть вкладку **«Дозволи»** .

З цією групою пов’язана керована політика **AmazonEC2ReadOnlyAccess –** підключіть її до групи. Керовані політики – це попередньо створені політики (створені AWS або вашими адміністраторами), які можна прикріпити до користувачів і груп IAM. Коли політику оновлено, зміни в політиці негайно застосовуються до всіх користувачів і груп, долучених до політики.

1. У полі **«Назва політики»** виберіть посилання на політику **AmazonEC2ReadOnlyAccess** .
2. Виберіть вкладку **{} JSON** .
   * Політика визначає, які дії дозволені або заборонені для певних ресурсів AWS. Ця політика надає дозвіл на *перелік* і *опис* (перегляд) інформації про Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing, Amazon CloudWatch і Amazon EC2 Auto Scaling. Ця можливість переглядати ресурси, але не змінювати їх, ідеально підходить для призначення ролі підтримки.
   * Заяви в політиці IAM мають таку базову структуру:
     + **Ефект** повідомляє, дозволити *чи* заборонити *дозволи* .
     + **Дія** вказує виклики API, які можна зробити для служби AWS (наприклад, *cloudwatch:ListMetrics* ).
     + **Ресурс** визначає сферу об’єктів, на які поширюється правило політики (наприклад, конкретне відро Amazon Simple Storage Service [Amazon S3] або екземпляр Amazon EC2; зірочка [ \* ] означає *будь-який ресурс* ).
3. На панелі навігації ліворуч виберіть **Групи користувачів** .
4. Виберіть назву групи **S3-Support** .
5. Виберіть вкладку **«Дозволи»** .

До групи S3-Support долучити політику **AmazonS3ReadOnlyAccess** .

1. У полі **«Назва політики»** виберіть посилання на політику **AmazonS3ReadOnlyAccess** .
2. Виберіть вкладку **{} JSON** .

Ця політика має дозволи на *отримання* та *список* для *всіх* ресурсів в Amazon S3.

1. На панелі навігації ліворуч виберіть **Групи користувачів** .
2. Виберіть назву групи **EC2-Admin** .
3. Виберіть вкладку **«Дозволи»** .

Ця група відрізняється від двох інших. Замість керованої політики група має *вбудовану політику* , яка є політикою, призначеною лише одному користувачеві чи групі. Вбудовані політики зазвичай використовуються для застосування дозволів у певних ситуаціях.

1. У полі **«Назва політики»** виберіть назву політики **EC2-Admin-Policy** .
2. Виберіть вкладку **JSON** .

Ця політика надає дозвіл на *опис* інформації про екземпляри Amazon EC2, а також можливість *запускати* та *зупиняти* екземпляри.

1. Унизу екрана виберіть **«Скасувати»** , щоб закрити політику.

**Бізнес сценарій**

Протягом решти цієї практичної роботи ви працюватимете з цими користувачами та групами, щоб увімкнути дозволи, які підтримують наступний бізнес-сценарій.

Ваша компанія розширює використання служб AWS і використовує багато екземплярів Amazon EC2 і сегментів Amazon S3. Ви хочете надати доступ новим співробітникам залежно від їх посадових функцій, як зазначено в наступній таблиці:

|  |  |  |
| --- | --- | --- |
| Користувач | У групі | Дозволи |
| користувач-1 | S3-підтримка | Доступ до Amazon S3 лише для читання |
| користувач-2 | Підтримка EC2 | Доступ до Amazon EC2 лише для читання |
| користувач-3 | EC2-Admin | Перегляд, запуск і зупинка екземплярів Amazon EC2 |

**Завдання 2. Додати користувачів до груп**

Ви нещодавно найняли *користувача 1* на посаду, де він забезпечуватиме підтримку Amazon S3. Ви додасте їх до групи *S3-Support* , щоб вони успадкували необхідні дозволи за допомогою доданої політики *AmazonS3ReadOnlyAccess* .

Ігноруйте будь-які помилки «не авторизовано», які з’являються під час виконання цього завдання. Вони викликані тим, що ваш обліковий запис лабораторії має обмежені дозволи, і не вплинуть на вашу здатність завершити лабораторію.

### Додайте користувача-1 до групи S3-Support

1. На лівій навігаційній панелі виберіть **Групи користувачів** .
2. Виберіть назву групи **S3-Support** .
3. На вкладці **Користувачі** виберіть **Додати користувачів** .
4. Виберіть **користувача -1** і виберіть **Додати користувачів** .

На вкладці **«Користувачі»** зверніть увагу, що *користувача 1* додано до групи.

### Додайте користувача-2 до групи EC2-Support

Ви найняли *користувача-2* на посаду, де він забезпечуватиме підтримку Amazon EC2. Ви додасте їх до групи *EC2-Support* , щоб вони успадкували необхідні дозволи за допомогою доданої політики *AmazonEC2ReadOnlyAccess* .

1. Використовуйте те, що ви дізналися з попередніх кроків, щоб додати *користувача-2* до групи *EC2-Support* . *Користувач-2* тепер має бути частиною групи *EC2-Support* .

### Додайте користувача-3 до групи EC2-Admin

Ви найняли *користувача-3* як свого адміністратора Amazon EC2 для керування вашими примірниками EC2. Ви додасте їх до групи *EC2-Admin*, щоб вони успадкували необхідні дозволи за допомогою доданої *політики EC2-Admin-Policy* .

1. Використовуйте те, що ви дізналися з попередніх кроків, щоб додати *користувача-3* до групи *EC2-Admin* . *User-3* тепер має бути частиною групи *EC2-Admin* .
2. На панелі навігації ліворуч виберіть **Групи користувачів** .

Кожна група має мати **1** у стовпці **Користувачі**. Це вказує на кількість користувачів у кожній групі. У стовпці «Користувачі» для групи немає 1, перегляньте попередні кроки, щоб переконатися, що кожного користувача призначено групі, як показано в таблиці в розділі «Бізнес-сценарій» .

**Завдання 3. Увійдіть і перевірте користувачів**

У цьому завданні ви перевірите дозволи кожного користувача IAM на консолі.

### Отримайте URL-адресу для входу в консоль

1. На панелі навігації ліворуч виберіть **«Інформаційна панель»** .

Зверніть увагу на **URL-адресу входу для користувачів IAM у цьому** розділі облікового запису вгорі сторінки. URL-адреса для входу виглядає приблизно так: **https://123456789012.signin.aws.amazon.com/console**

Це посилання можна використовувати для входу в обліковий запис AWS, який ви зараз використовуєте.

1. Скопіюйте посилання для входу в текстовий редактор.

### Перевірте дозволи користувача 1

1. Відкрийте приватне або анонімне вікно у своєму браузері.
2. Вставте посилання для входу в приватний браузер і натисніть ENTER.

Тепер ви ввійдете як *користувач-1* , який був найнятий вашим персоналом підтримки зберігання Amazon S3.

1. Увійдіть, використовуючи такі облікові дані:
   * **Ім'я користувача IAM:** користувач-1
   * **Пароль:** Lab-Password1
2. Виберіть меню **«Служби»** та виберіть **S3** .
3. Виберіть назву одного зі своїх відер і перегляньте вміст.

Оскільки цей користувач є частиною групи *S3-Support* в IAM, він має дозволи переглядати список сегментів Amazon S3 і їх вміст.

Тепер перевірте, чи має користувач доступ до Amazon EC2.

1. Виберіть меню **«Служби»** та виберіть **EC2** .
2. На лівій навігаційній панелі виберіть **Екземпляри** .

Ви не бачите жодних екземплярів. Натомість з’явиться повідомлення про помилку, у якому зазначено, що *ви не авторизовані для виконання цієї операції* . Цьому користувачеві не надано жодних дозволів на використання Amazon EC2.

Тепер ви ввійдете як *користувач-2* , який був найнятий вашою особою служби підтримки Amazon EC2.

1. Спочатку вийдіть з консолі *користувача-1 :*
   * У верхньому правому куті сторінки виберіть **user-1** .
   * Виберіть **Вийти** .

### Перевірте дозволи користувача 2

1. Знову вставте посилання для входу в приватний браузер і натисніть ENTER.
2. Увійдіть, використовуючи такі облікові дані:
   * **Ім'я користувача IAM:** користувач-2
   * **Пароль:** Lab-Password2
3. Виберіть меню **«Служби»** та виберіть **EC2** .
4. На панелі навігації ліворуч виберіть **Екземпляри** .
   * Тепер ви можете побачити екземпляр EC2. Однак ви не можете вносити зміни в ресурси Amazon EC2, оскільки у вас є дозволи лише на читання.
   * Якщо ви не бачите екземпляр EC2, можливо, ваш регіон неправильний. У верхньому правому куті сторінки виберіть назву регіону, а потім виберіть регіон, у якому ви були на початку лабораторної роботи (наприклад, **Північна Вірджинія**

).

1. Виберіть примірник EC2.
2. Виберіть меню **«Стан екземпляра»** , а потім виберіть **«Зупинити екземпляр»** .
3. Щоб підтвердити, що ви хочете зупинити екземпляр, виберіть **«Зупинити»** .

З'являється повідомлення про помилку з повідомленням про те, що *ви не маєте прав для виконання цієї операції* . Це демонструє, що політика дозволяє лише переглядати

інформацію без внесення змін.

Потім перевірте, чи може *користувач-2* отримати доступ до Amazon S3.

1. Виберіть меню **«Служби»** та виберіть **S3** .

Повідомлення про помилку говорить про те, що *у вас немає дозволу на створення списку сегментів,* оскільки *користувач-2* не має дозволу на використання Amazon S3.

Тепер ви ввійдете як *користувач-3* , якого було найнято вашим адміністратором Amazon EC2.

1. Спочатку вийдіть з консолі *користувача-2 :*
   * У верхньому правому куті сторінки виберіть **user-2** .
   * Виберіть **Вийти** .

### Перевірте дозволи користувача 3

1. Знову вставте посилання для входу в приватний браузер і натисніть ENTER.
2. Увійдіть, використовуючи такі облікові дані:
   * **Ім'я користувача IAM:** користувач-3
   * **Пароль:** Lab-Password3
3. Виберіть меню **«Служби»** та виберіть **EC2** .
4. На панелі навігації ліворуч виберіть **Екземпляри** .
   * У списку є екземпляр EC2. Як адміністратор Amazon EC2, цей користувач повинен мати дозвіл на *зупинку* екземпляра EC2.
   * Якщо ви не бачите екземпляр EC2, можливо, ваш регіон неправильний. У верхньому правому куті сторінки виберіть назву регіону, а потім виберіть регіон, у якому ви були на початку лабораторної роботи (наприклад, **Північна Вірджинія**).
5. Виберіть примірник EC2.
6. Виберіть меню **«Стан екземпляра»** , а потім виберіть **«Зупинити екземпляр»** .
7. Щоб підтвердити, що ви хочете зупинити екземпляр, виберіть **«Зупинити»** .

Цього разу дію виконано успішно, оскільки *користувач-3* має дозволи на зупинку екземплярів EC2. **Стан екземпляра** змінюється на *«Зупинка»* та починає завершувати роботу.

1. Закрийте приватне вікно браузера.