# Лабораторна робота 3.1: Використання політик на основі ресурсів для захисту S3 Bucket

## Огляд та цілі лабораторії

У цій лабораторній роботі ви дізнаєтеся, як налаштувати дозволи за допомогою політик на основі ідентифікаторів і ресурсів AWS Identity and Access Management (IAM), таких як політики на основі ресурсів, наприклад, політики кошика Amazon Simple Storage Service (Amazon S3). Ви також дізнаєтеся, як політики IAM і ресурсні політики визначають дозволи доступу.

Після виконання цієї лабораторної роботи ви повинні вміти робити наступне:

- Зрозуміти, як використовувати політики на основі ідентифікаційних даних IAM та політики на основі ресурсів для визначення детального контролю доступу до сервісів та ресурсів AWS.
- Опишіть, як користувач IAM може взяти на себе роль IAM, щоб отримати різні дозволи доступу до облікового запису AWS.
- Поясніть, як політики S3 bucket policies і політики на основі ідентичностей IAM, призначені користувачам і ролям IAM, впливають на те, що користувачі можуть бачити або змінювати в різних службах AWS в AWS Management Console.

## Тривалість

Ця лабораторна робота займе приблизно **60 хвилин**.

## Обмеження в роботі AWS

У цьому лабораторному середовищі доступ до сервісів AWS і дії з ними можуть бути обмежені лише тими, які необхідні для виконання інструкцій лабораторної роботи. Ви можете зіткнутися з помилками, якщо спробуєте отримати доступ до інших сервісів або виконати дії, що виходять за рамки описаних у цій лабораторній роботі.

## Сценарій

На наступній схемі показано архітектуру, яка була створена для вас в AWS на *початку* лабораторної роботи.

Лабораторне середовище має три попередньо налаштовані кошики Amazon S3: *bucket1*, *bucket2* і *bucket3*. Середовище також має попередньо налаштовану роль IAM, яка дозволяє доступ до певних кошиків та їхніх об'єктів, коли ця роль прийнята. Ви проаналізуєте різні політики, щоб краще зрозуміти, як вони контролюють ваш рівень доступу.

*Наприкінці* цієї лабораторної роботи ви створите архітектуру, показану на наступній схемі.

# Завдання 1: Доступ до консолі від імені користувача IAM

1. У верхній частині цих інструкцій виберіть **Start Lab**.
   - Лабораторне заняття починається.
   - У верхній частині сторінки відображається таймер, який показує час, що залишився до кінця сеансу.

   **Порада:** Щоб оновити тривалість сеансу в будь-який момент, виберіть **Start Lab** ще раз до того, як таймер дійде до 00:00.

2. Перш ніж продовжити, зачекайте, поки значок кола праворуч від посилання AWS у верхньому лівому куті стане зеленим. Коли лабораторне середовище буде готове, також відобразиться панель Деталі AWS.

   **Попередження:** У цій лабораторній роботі НЕ обирайте посилання AWS для підключення до консолі. Ви отримаєте доступ до консолі не так, як у більшості лабораторних робіт.

3. Увійдіть як користувач IAM на ім'я *devuser*:
   - Виберіть посилання **AWS Details** у верхній частині сторінки.
   - Скопіюйте значення **IAMUserLoginURL** і завантажте його в нову вкладку браузера.
   - Для **імені користувача IAM** введіть `devuser`
   - У полі **Password (Пароль)** введіть значення **IAMUserPassword** з панелі AWS Details (Деталі AWS) на сторінці інструкцій до лабораторної роботи.
   - Виберіть **"Увійти"**.

   Відкриється консоль керування AWS.

   **Попередження:** Щоб уникнути проблем, НЕ змінюйте регіон під час виконання цієї лабораторної роботи, якщо не отримаєте відповідних вказівок.

4. Розташуйте вкладку AWS Management Console так, щоб вона відображалася поруч з цими інструкціями. В ідеалі, ви зможете бачити обидві вкладки браузера одночасно, щоб вам було легше виконувати кроки лабораторної роботи.

# Завдання 2: Спроба доступу на рівні читання до сервісів AWS

Тепер, коли ви увійшли в консоль як користувач IAM з іменем *devuser*, ви дізнаєтеся про рівень доступу, який у вас є до декількох сервісів AWS, включаючи Amazon Elastic Compute Cloud (Amazon EC2), Amazon S3 і IAM.

5. Відкрийте консоль Amazon EC2:
   - У меню **Сервіс** виберіть **Обчислення** > **EC2**.
   - На лівій навігаційній панелі виберіть **EC2 Dashboard**.

   Відображається багато повідомлень про помилки API. Це очікувано.

6. Спробуйте виконати деякі дії в консолі Amazon EC2:
   - На лівій навігаційній панелі виберіть **Екземпляри**.

   У списку Екземпляри з'явиться повідомлення *Ви не маєте права виконувати цю операцію*.

   - Виберіть **Запустити екземпляри**
   - Прокрутіть вниз і виберіть у випадаючому списку Ім'я пари ключів.

   З'явиться повідомлення *Ви не маєте права виконувати цю операцію*.

   Зверніть увагу, що ім'я пари ключів є обов'*язковим параметром,* який необхідно вказати, якщо ви хочете запустити екземпляр. Це лише одна з багатьох ознак того, що ви не зможете запустити екземпляр EC2 з правами, наданими вам як користувачеві devuser.

   - На панелі "Підсумки" праворуч натисніть **"Скасувати"**.

7. Щоб дізнатися, до чого можна отримати доступ у консолі Amazon S3, у меню **"Сервіси"** виберіть **"Сховище"** > **"S3"**.

   Задано три відра. Імена відер унікальні, але одне з них містить *bucket1*, друге - *bucket2*, а третє - *bucket3*.

   Зверніть увагу, що у списку кошиків у стовпчику **Доступ** відображається повідомлення Недостатньо дозволів для всіх трьох кошиків. Це очікувана ситуація.

# Завдання 3: Аналіз політики на основі ідентичностей, застосованої до користувача IAM

Ви бачили, як користувач *devuser* IAM не може отримати доступ до певної інформації та дій в консолі Amazon S3 і Amazon EC2. У цьому завданні ви розглянете деталі політики IAM, які застосовуються до користувача *devuser,* щоб зрозуміти, чому ви не можете виконати ці дії.

8. Отримайте доступ до консолі IAM і перегляньте налаштування членства користувачів і груп:
   - У меню **"Служби"** виберіть **"Безпека, ідентичність та відповідність"** > **IAM**.

     На сторінці інформаційної панелі IAM зверніть увагу, що у вас немає прав на перегляд певних частин сторінки. В обох повідомленнях зазначено *Користувач: arn:aws:iam:::user/devuser не має права виконувати: iam:GetAccountSummary на ресурсі: **. Це очікувана ситуація.

   - На лівій навігаційній панелі виберіть **Групи користувачів**.
   - Виберіть назву групи **DeveloperGroup.**

     На вкладці **Користувачі зверніть** увагу, що *devuser* є членом цієї групи IAM.

   - Перейдіть на вкладку **Дозволи.**

     Зверніть увагу, що до цієї групи IAM прив'язано політику IAM з назвою DeveloperGroupPolicy.

     **Примітка:** Коли політику прив'язано до групи, вона застосовується до всіх користувачів IAM, які є членами групи. Отже, наразі ця політика керує вашим доступом до консолі, оскільки ви увійшли як *користувач devuser,* який є членом цієї групи IAM.

9. Ознайомтеся з деталями політики IAM:
   - У нижній частині сторінки виберіть значок плюса зліва від **DeveloperGroupPolicy,** щоб відобразити деталі політики.
   - Перегляньте деталі політики JSON і згадайте рівень доступу, який ви мали для Amazon EC2 і Amazon S3 у попередньому завданні.
   - Зверніть увагу, що політика забороняє будь-які дії з Amazon EC2.
   - Зверніть увагу на дії IAM, дозволені політикою. Коли ви отримали доступ до інформаційної панелі IAM, ви побачили повідомлення про те, що у вас немає дозволу *iam:GetAccountSummary.* Ця дія не дозволена в цьому документі політики. Однак, багато дозволів IAM на рівні читання надаються. Наприклад, ви можете переглянути деталі цієї політики.
   - Зверніть увагу на дії в Amazon S3, дозволені політикою. Жодні дії, пов'язані з об'єктами, не дозволені, але деякі дії, пов'язані зі сховищами, дозволені.

10. Збережіть політику у файл на своєму комп'ютері:
    - Щоб скопіювати політику у форматі JSON до буфера обміну, натисніть **Копіювати**.
    - Відкрийте текстовий редактор на локальному комп'ютері та вставте політику, яку ви щойно скопіювали.
    - Збережіть документ політики як `DeveloperGroupPolicy.json` у місці на вашому комп'ютері, яке ви запам'ятаєте.

# Завдання 4: Спроба доступу на рівні запису до сервісів AWS

Будь-яка дія, яку ви намагаєтеся виконати під час взаємодії зі службою AWS, є викликом API, незалежно від того, чи використовуєте ви консоль, інтерфейс командного рядка AWS (AWS CLI) або комплекти розробки програмного забезпечення AWS (SDK). Усі спроби виклику API реєструються в журналах подій AWS CloudTrail.

У цьому завданні ви спробуєте зробити два виклики API, які вимагають доступу на *рівні запису* в Amazon S3. Перша дія полягає у створенні кошика S3, а друга - у завантаженні об'єкта до цього кошика. Після виконання цих двох завдань ви знову проаналізуєте політику, прив'язану до групи IAM, щоб з'ясувати, чому ви змогли або не змогли виконати певні виклики API.

11. Спроба створити відро S3:
    - Перейдіть на консоль Amazon S3.

      **Порада:** Скористайтеся меню **"Сервіс"** або знайдіть `S3 у вікні` пошуку праворуч від меню.

    - Виберіть **Створити відро**
    - У полі **"Ім'я кошика"** введіть свої ініціали, а потім випадкове чотиризначне число, наприклад, *zba1234*.

      **Примітка: За** замовчуванням, нові відра, точки доступу та об'єкти не дозволяють публічний доступ. Занурення у це питання виходить за рамки цієї лабораторної роботи, але важливо зазначити, що це важливо.

    - Для **регіону AWS** виберіть **US East (Північна Вірджинія) us-east-1**.
    - Перегляньте налаштування, а потім виберіть **"Створити кошик"** внизу сторінки.

      Ви успішно створили відро S3.

12. Перейдіть до кошика і спробуйте завантажити об'єкт:
    - Виберіть назву щойно створеного відра.
    - Виберіть **Завантажити,** а потім - **Додати файли**.
    - Знайдіть і виберіть файл **DeveloperGroupPolicy.json, який** ви зберегли раніше.
    - Виберіть **"Завантажити"**.

На екрані з'явиться повідомлення *Помилка завантаження*.

- На вкладці **Файли і папки** в нижній частині сторінки в колонці **Помилка** виберіть посилання **Відмовлено в доступі.**

  У повідомленні йдеться про те, що у *вас немає прав на завантаження файлів і папок*.

- Виберіть **"Закрити"**.
- З хлібних крихт у верхньому лівому кутку сторінки виберіть **Amazon S3**.

13. Ознайомтеся з деталями політики доступу до Amazon S3:
- Поверніться до текстового редактора, куди ви скопіювали документ DeveloperGroupPolicy.json.
- Перегляньте деталі політики, щоб зрозуміти, чому ви змогли створити S3-відро, але не змогли завантажити до нього об'єкти.

  **Підказка: Довідник** з *авторизації послуг містить* список дій, які підтримує кожна служба AWS. Щоб дізнатися про дії в Amazon S3, відкрийте сторінку документації IAM, а потім відкрийте документ *Service Authorization Reference.* У лівій навігаційній панелі розгорніть **Дії, ресурси та ключі умов,** а потім виберіть **Amazon S3**. У розділі Дії, **визначені Amazon S3, у** таблиці перелічено всі можливі дії Amazon S3, які можна надати або заборонити, разом з описом дії.

# Завдання 5: Прийняття на себе ролі IAM та перегляд політики, що базується на ресурсах

У цьому завданні ви спробуєте отримати доступ до *bucket1* і *bucket2, увійшовши в систему* як користувач IAM *devuser.* Ви також спробуєте отримати доступ до кошиків, використовуючи роль, яку було попередньо налаштовано під час налаштування лабораторного середовища.

14. Спробуйте завантажити об'єкт з відер, створених під час налаштування лабораторії:
- У консолі Amazon S3 виберіть ім'я bucket, яке містить **bucket1**.
- Виберіть **Image2.jpg**, а потім натисніть кнопку **Завантажити**.

  З'явиться сторінка помилки AccessDenied.

- Щоб повернутися до консолі Amazon S3, натисніть кнопку "Назад" у вашому браузері.
- З хлібних крихт у верхньому лівому кутку сторінки виберіть **Amazon S3**.
- Спробуйте завантажити файл **Image1.jpg** з *bucket2*.

  Ви отримаєте ту саму помилку.

- Щоб повернутися до консолі Amazon S3, натисніть кнопку "Назад" у вашому браузері.

**Аналіз:** Як показано на наступній діаграмі, з дозволами, які надаються через членство у *DeveloperGroup,* ви змогли створити новий бакет. Однак, ви не можете

отримати доступ до об'єктів у *bucket1* або *bucket2*.

- З хлібних крихт у верхньому лівому кутку сторінки виберіть **Amazon S3**.

15. Прийміть роль IAM *BucketsAccessRole* в консолі:
- У правому верхньому куті сторінки виберіть **devuser**, а потім виберіть Переключити **роль**.
- Якщо з'явиться сторінка Переключити роль, виберіть Переключити **роль.**
- Налаштуйте наступне:
- **Обліковий запис:** Введіть значення **AccountID** з панелі AWS Details на сторінці інструкцій до лабораторної роботи.
- **Роль:** Введіть `BucketsAccessRole`
- **Ім'я для відображення:** Залиште це поле порожнім.
- Виберіть **роль перемикача**

Ви успішно прийняли роль IAM з назвою *BucketsAccessRole,* яка була попередньо налаштована для цього тесту.

**Підказка: Ви** можете визначити, що ви переключилися на роль, подивившись на верхній правий кут консолі. Зверніть увагу, що **BucketsAccessRole відображається** там, де раніше відображався **devuser.**

16. Спробуйте завантажити об'єкт з Amazon S3 ще раз:
- У консолі Amazon S3 виберіть ім'я bucket, яке містить **bucket1**.
- Виберіть **Image2.jpg**, а потім натисніть кнопку **Завантажити**.
- Відкрийте файл, щоб переконатися, що він завантажився.

**Аналіз:** Завантаження пройшло успішно, а це означає, що політика або політики, застосовані до *ролі BucketsAccessRole,* дозволяють дію *s3:GetObject для bucket1*.

17. Перевірте доступ до IAM за допомогою *ролі BucketsAccessRole*:
- Перейдіть до консолі IAM.

**Примітка: Зі зміною** ролей змінилися дозволи, які ви маєте для взаємодії з різними службами AWS. Під час навігації по консолі IAM ви побачите нові повідомлення про помилки, які вказують на те, що ви не авторизовані.

- На лівій навігаційній панелі виберіть **Групи користувачів**.

**Аналіз:** З'явиться повідомлення про помилку. Ви більше не маєте дозволів на перегляд сторінки груп користувачів IAM, оскільки до *ролі BucketsAccessRole* не застосовано дію *iam:ListGroups.*

18. Знову візьміть на себе роль *devuser* і протестуйте доступ до сторінки груп користувачів:
- У правому верхньому куті сторінки виберіть **BucketsAccessRole,** а потім виберіть **Switch back**.
- На лівій навігаційній панелі знову виберіть **Групи користувачів.**

**Аналіз:** Тепер, коли ви скасували *роль BucketsAccessRole*, ви маєте права, призначені користувачеві IAM *devuser* (через членство цього користувача у *групі DeveloperGroup)*. Ви можете знову переглянути сторінку груп користувачів.

19. Проаналізуйте політику IAM, яка пов'язана з *роллю BucketsAccessRole*:
- На лівій навігаційній панелі виберіть **Ролі**.
- Знайдіть `BucketsAccessRole` і виберіть назву ролі, коли вона з'явиться.
- Виберіть стрілку ліворуч від **ListAllBucketsPolicy**.

Ця політика надає однакову дію *s3:ListAllMyBuckets для* кожного ресурсу. Цей дозвіл дозволяє вам бачити всі S3-баки, коли ви приймаєте *роль BucketsAccessRole*.

- Виберіть стрілку ліворуч від **GrantBucket1Access**.

**Аналіз:** Ця політика дозволяє дії *s3:GetObject*, *s3:ListObjects* та *s3:ListBucket. Зверніть увагу*, що ця політика ***не*** надає доступ до *s3:PutObject.* Дозволені дії надаються лише для певних ресурсів, *bucket1* і всіх об'єктів у *bucket1* (як показано символом ***/*).*** Зірочка (*) є символом підстановки, який вказує на те, що ця дія може відповідати будь-якому значенню.

Завдяки цій політиці, коли ви прийняли *роль BucketsAccessRole*, ви могли бачити і завантажувати об'єкти з *bucket1*.

20. Збережіть копію політики *GrantBucket1Access* на своєму комп'ютері:
- Помістіть курсор на початок рядка 1 в деталях полісу і виберіть всі рядки коду (до рядка 17).
- Скопіюйте політику у форматі JSON до буфера обміну.
- Відкрийте новий текстовий файл на вашому комп'ютері і вставте в нього політику, яку ви щойно скопіювали.
- Збережіть документ політики як `GrantBucket1Access.json` у місці на вашому комп'ютері, яке ви запам'ятаєте.

21. Завершіть аналіз деталей *BucketsAccessRole:*
- Прокрутіть сторінку назад і перейдіть на вкладку **Довірчі відносини.**

Зверніть увагу, що користувач *devuser* IAM в цьому обліковому записі AWS вказаний як довірена особа, яка може взяти на себе цю роль.

Зверніть увагу, що номер облікового запису, який з'являється у верхньому правому куті консолі (після **devuser), збігається з** номером облікового запису у списку **Довірених осіб** (без тире).

**Примітка:** Служба маркерів безпеки AWS (AWS STS) надасть тимчасові облікові дані будь-якій довіреній особі, яка звернеться з проханням взяти на себе цю роль. Ця політика довіри довіряє користувачеві IAM у тому самому обліковому записі. Однак політику довіри можна налаштувати так, щоб довіряти одному або декільком принципалам, навіть в інших облікових записах AWS. Прикладами інших принципалів є служби AWS, ролі IAM і користувачі IAM.

22. Візьміть *роль BucketsAccessRole і* спробуйте завантажити зображення до *bucket2*:
- Щоб знову взяти на себе *роль BucketsAccessRole,* у верхньому правому куті сторінки виберіть **devuser**.
- У розділі **Історія ролей** виберіть **BucketsAccessRole**.
- Перейдіть на консоль Amazon S3.
- Виберіть ім'я відра, яке містить **bucket2**.

  Зверніть увагу, що це відро ще не має файлу Image2.jpg.

- Виберіть **Завантажити,** а потім - **Додати файли**.
- Знайдіть і виберіть файл **Image2.jpg**, який ви завантажили раніше з *відра1*.
- Виберіть **"Завантажити"**.

  Файл успішно завантажено.

- Виберіть **"Закрити"**.

  **Аналіз:** Отримавши *роль BucketsAccessRole*, ви успішно звернулися до *bucket1,* щоб завантажити об'єкт. Потім ви завантажили той самий об'єкт до *bucket2*.

  Ознайомившись з політиками, прикріпленими до *ролі BucketsAccessRole,* ви дізнаєтеся, що дозволи Amazon S3, які були надані цій ролі, були обмежені для *bucket1,* як показано на наступній діаграмі.

- Отже, як ви тільки що змогли завантажити об'єкт до *bucket2*? Причина стане зрозумілою у наступному завданні.

# Завдання 6: Розуміння ресурсно-орієнтованої політики

У цьому завданні ви перевірите політику для кошика, яка пов'язана з *bucket2*.

23. Зверніть увагу на деталі політики bucket, яка застосовується до *bucket2*:
- На сторінці деталей для *bucket2* перейдіть на вкладку **Дозволи.**
- У розділі **Політика для ковша** перегляньте політику, яку застосовано до *ковша2*.

Політика має два твердження.

Перший ідентифікатор оператора (SID) - *S3Write*. Основною є IAM роль *BucketsAccessRole, яку* ви обрали. Цій ролі дозволено викликати дії *s3:GetObject* і *s3:PutObject* на ресурсі, яким є *bucket2*.

Другий SID - *ListBucket*. Основна роль - *BucketsAccessRole*. Ця роль має право викликати дію *s3:ListBucket* на ресурсі, яким є *bucket2*.

**Аналіз:** Тепер ви повинні краще розуміти, як політики на основі ресурсів (наприклад, політики S3 bucket) і політики на основі ролей (політики, пов'язані з ролями IAM) можуть взаємодіяти і використовуватися разом.

У цьому тесті рольові *політики, прив'*язані до ролі IAM *BucketsAccessRole,* надали *s3:GetObject* і *s3:ListBucket* доступ до *bucket1* і об'єктів у ньому. Ці рольові політики явно не дозволяли доступ до *bucket2, але* вони також не забороняли доступ явно.

На наступній діаграмі показано, як політики, застосовані до користувача IAM, ролі IAM та кошика, визначали, які дії ви могли виконувати.

Потім, все ще маючи *роль BucketsAccessRole*, ви спробували завантажити об'єкт до *bucket2,* і вам вдалося це зробити. Це здавалося дивним, виходячи з політик IAM, які ви переглянули. Однак, після того, як ви переглянули *політику на основі ресурсів* (в даному випадку, політику для кошика), яка була прикріплена до кошика, ваш доступ став зрозумілим. Ця політика надає доступ, включно з дією *s3:PutObject,* до *bucket2* принципалу *BucketsAccessRole.*

# Завдання з викликом

Ваше завдання полягає у тому, щоб знайти спосіб завантажити файл Image2.jpg у *відро3*.

24. Спробуйте завантажити файл від імені *користувача devuser* без обраної ролі:
    - Зніміть *роль BucketsAccessRole*.
    - Спробуйте завантажити файл Image2.jpg, який ви завантажили з *відра1 на* початку цієї лабораторної роботи, до *відра3*.

      Не вдалося завантажити.

    - Перевірте, чи пов'язано політику ковша з *ковшем3*. Можливо, це дасть вам деяку підказку про те, як виконати це завдання.

      Ви не можете переглянути політику відра.

25. Візьміть *роль BucketsAccessRole і* спробуйте виконати дії з попереднього кроку:

- Чи можете ви завантажити файл до *bucket3*?
- Чи можете ви переглянути політику відер зараз? Ознайомтеся з деталями тарифної політики. У вас є ідея, як можна завантажити Image2.jpg до *bucket3*?
- Ви розібралися, як завантажити файл? Якщо так, то вітаємо!

## Надсилайте свої роботи

26. Щоб зафіксувати свій прогрес, натисніть кнопку **"Надіслати" вгорі** цієї інструкції.

27. Коли з'явиться відповідний запит, виберіть **"Так"**.

    Через кілька хвилин з'явиться панель оцінок, яка покаже, скільки балів ви заробили за кожне завдання. Якщо результати не з'являться через пару хвилин, виберіть **"Оцінки"** у верхній частині цієї інструкції.

    **Порада:** Ви можете надсилати свою роботу кілька разів. Після того, як ви змінили свою роботу, натисніть кнопку **Надіслати** ще раз. Ваша остання робота буде записана для цієї лабораторії.

28. Щоб знайти детальний відгук про вашу роботу, виберіть **Звіт про подачу**.

## Лабораторія завершена

Вітаю! Ви виконали завдання.

29. У верхній частині цієї сторінки виберіть **Завершити лабораторну роботу,** а потім виберіть **Так,** щоб підтвердити, що ви хочете завершити лабораторну роботу.

    Панель повідомлень вказує на завершення роботи лабораторії.

30. Щоб закрити панель, натисніть кнопку **Закрити** у верхньому правому куті.