ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТАЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія управління доступом користувачів до сервісів та ресурсів Amazon Web Services»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Марк СКРИЦЬКИЙ
(підпис)

Виконав: здобувач(ка) вищої освіти групи БСДМ-61
СКРИЦЬКИЙ Марк
(прізвище, ім'я)

Керівник д.ф. СОБЧУК Андрій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ABAC – Attribute-Based Access Control

ACL – Access Control List

ACM – Access Control Mechanism

API – Application Programming Interface

AWS – Amazon Web Services

CSP – Cloud Service Provider

IAM – Identity and Access Management

IDaaS – Identity as a Service

IGA – Identity Governance and Administration

MFA – Multi-Factor Authentication

OTP – One-Time Password

PAM – Privileged Access Management

RBAC – Role Based Access Control

SSO – Single Sign-On

ВСТУП

Актуальність дослідження. За оцінками фахівців за 2024 рік хмарні обчислення стали основою IT-інфраструктури сучасних підприємств. Спеціалісти з кібербезпеки та організації стикаються із загрозами, що постійно змінюються. Ці виклики різноманітні й охоплюють усе: від захисту багатохмарних середовищ і забезпечення захисту даних до пом’якшення вразливостей хмари.

Оскільки компанії все більше використовують численні хмарні сервіси, проблема підтримки безпеки на різноманітних платформах стає гострішою.

Керування ідентифікацією та доступом (Identity and Access Management, IAM) надає право адміністраторам дозволяти, хто може виконувати дії з певними ресурсами, надаючи організаціям повний контроль і видимість для централізованого керування ресурсами в хмарі. Для підприємств зі складною організаційною структурою, сотнями робочих груп і багатьма проектами IAM забезпечує єдине уявлення про політику безпеки в усій організації з вбудованим аудитом для полегшення процесів відповідності.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження технології управління доступом користувачів до сервісів та ресурсів Amazon Web Services.

Об’єкт дослідження – управління доступом користувачів до хмарних сервісів та ресурсів організації.

Предмет дослідження – технологія управління доступом користувачів до сервісів та ресурсів Amazon Web Services.

Мета роботи – розробити порядок застосування технології управління доступом користувачів до хмарних сервісів та ресурсів організації та рекомендації щодо його реалізації.

Наукові завдання:

дослідити сутність проблеми забезпечення доступу користувачів до хмарних сервісів та ресурсів організації;

проаналізувати підходи до забезпечення доступу користувачів до хмарних сервісів та ресурсів організації;

проаналізувати існуючі рішення щодо управління доступом користувачів до хмарних сервісів та ресурсів організації;

проаналізувати методи та засоби управління доступом користувачів до сервісів та ресурсів організації Amazon Web Services;

розкрити порядок реалізації технології управління доступом користувачів до сервісів та ресурсів організації Amazon Web Services.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано порядок застосування технології управління доступом користувачів до сервісів та ресурсів управління доступом користувачів до сервісів та ресурсів організації Amazon Web Services організації, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференція «Актуальні проблеми кібербезпеки», яка відбулася 25 жовтня 2024 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО ХМАРНИХ СЕРВІСІВ ТА РЕСУРСІВ ОРГАНІЗАЦІЇ

1.1. Аналіз проблеми забезпечення безпеки хмарних сервісів та ресурсів

Хмарні сервіси – це платформи та програми, які розміщені на віддалених серверах провайдера. Вони дозволяють користувачам завантажувати, зберігати та отримувати постійний доступ до власної інформації з будь-якого пристрою через інтернет [1].

Хмарні рішення у бізнес-сфері позбавляють необхідності купувати та керувати складною IT-інфраструктурою для фізичного зберігання й резервування величезного обсягу даних, є ефективними для автоматизації бізнес-процесів, управління і спільної роботи з документами всередині компанії [1].

Обираючи формат роботи з хмарою, варто розібратись, що таке хмарні сервіси, які є їх види та в чому полягає відмінність. Це дозволить знайти оптимальне рішення саме для вашої компанії.

Наразі існує три види хмарних сервісів:

публічні – є найпопулярнішим варіантом, адже всі технічні рішення, їх підтримку та обслуговування надає провайдер; компанії платять тільки за ті ресурси, які їм потрібні;

приватні – реалізовані на технічній базі компанії, не передбачають глобальний доступ; потребують чималих вкладень;

гібридні – є симбіозом двох попередніх форматів. Частина сервісів розміщена на власних серверах, частина – у хмарі провайдера.

Публічні хмарні сервіси є найбільш поширеними через свою гнучкість, ощадливість, швидкий доступ і високий рівень захисту від зламу та втрати інформації.

Розглянемо основні моделі надання хмарних сервісів:

SaaS – передбачає онлайн-доступ до готових програмних рішень. Клієнтам

не потрібно купувати та інсталювати пакет програм, оновлювати ліцензії тощо.

PaaS – передбачає доступ до програмного середовища. Основною відмінністю від SaaS є більша кількість інструментів та налаштувань, які дозволяють адаптувати платформу під потреби користувача.

IaaS – передбачає надання доступу до обчислювальних потужностей. Клієнт може створювати або завантажувати власні програмні продукти та послуги з використанням серверів провайдера.

Наразі модель SaaS вважається найпоширенішою, адже з нею можливий доступ до сервісів з будь-якого пристрою через інтернет. SaaS найбільше підходить для бізнесу (платформи для управління бізнес-процесами, CRM-системи тощо) [1].

Основними перевагами онлайн-платформ, які надають хмарні сервіси для бізнесу, є [1]:

автоматизація бізнес-процесів – провайдери пропонують сервіси, які дозволяють автоматизувати рутину та скоротити час на виконання низки завдань;

обмін файлами – надання команді швидкого доступу до потрібних файлів, додавши користувача в список. На Google drive можлива спільна робота над редагуванням;

впровадження інновацій – хмарні сервіси включають безліч різноманітних функцій. Це можливість розширити робочий інструментарій команди;

забезпечення безпеки – провідні провайдери використовують найсучасніші технології захисту від зламу, а також надають можливість створювати бекапи.

Загалом кожен керівник має визначити, для чого потрібні хмарні сервіси саме для його організації, адже специфіка різних бізнесів суттєво відрізняється.

У Звіті [2] зазначається, що в епоху, коли хмарні обчислення стали основою IT-інфраструктури, спеціалісти та організації з кібербезпеки стикаються із загрозами, що постійно змінюються. Ці виклики різноманітні й охоплюють усе: від захисту багатохмарних середовищ і забезпечення захисту даних до пом’якшення вразливостей хмари. Але вони також підкреслюють виражену прогалину в навичках у робочій силі з кібербезпеки. Зі збільшенням складності

хмарних екосистем зростає потреба в передових, орієнтованих на хмару стратегіях і навичках кібербезпеки.

Оскільки компанії все більше використовують численні хмарні сервіси, проблема підтримки безпеки на різноманітних платформах стає гострішою. У 2024 році безпека багатохмарних середовищ залишається складним завданням, головним завданням якого є захист даних і конфіденційність, як відзначили 55% учасників опитування. Це незначне збільшення порівняно з 52%, спостережуваним у 2023 році, що свідчить про зростання обізнаності та занепокоєння щодо захисту інформації на різних хмарних платформах. Проблема володіння належними навичками для розгортання та керування рішеннями в усіх хмарних середовищах слідкує за нею, хоча спостерігається зниження з 58% у 2023 році до 51% у 2024 році.

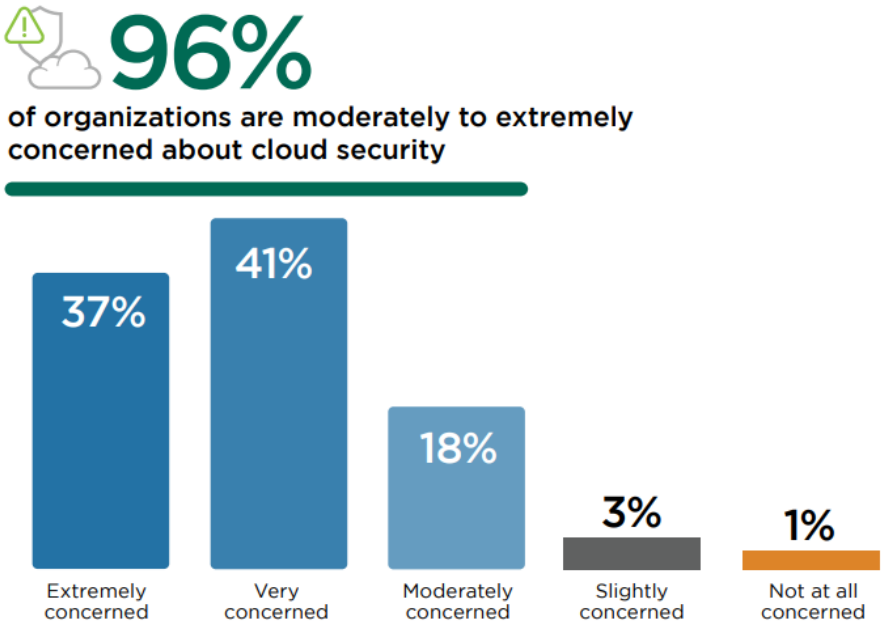

Рис. 1.1. Найбільші проблеми, пов’язані з захистом багатохмарних середовищ [2]

Це падіння може свідчити про покращення навчання або зміщення уваги до інші виникаючі проблеми. Розуміння того, як інтегруються різні рішення (47%), залишається на третьому місці, що свідчить про продовження акценту на згуртованості хмарних сервісів. Подібним чином проблема розуміння варіантів інтеграції послуг (44%) відображає складність забезпечення безперебійної роботи в хмарних середовищах. Управління витратами, пов’язаними з різними хмарними

рішеннями безпеки, викликало значне зростання занепокоєння з 37% у 2023 році до 42% у 2024 році, ймовірно, відображаючи як бюджетні обмеження, так і зростаючі фінансові наслідки мультихмарних стратегій.

Вирішення цих проблем починається з підвищення професійних навичок за допомогою цільової освіти та отримання сертифікатів. Для компаній надзвичайно важливо розробляти інтегровані стратегії безпеки, які зосереджені на захисті даних і безперебійній взаємодії хмарних служб. Оснастивши команди належним досвідом і структурами, організації можуть забезпечити більш безпечну та ефективну багатохмарну екосистему [2].

Стратегічний вибір моделей розгортання хмари є ключовим рішенням для організацій, що впливає на операційну гнучкість, безпеку даних та інтеграцію технологій. Це рішення пов’язане з проблемами хмарної міграції, де міркування щодо конфіденційності даних, бюджету та досвіду відіграють важливу роль у формуванні хмарних стратегій.

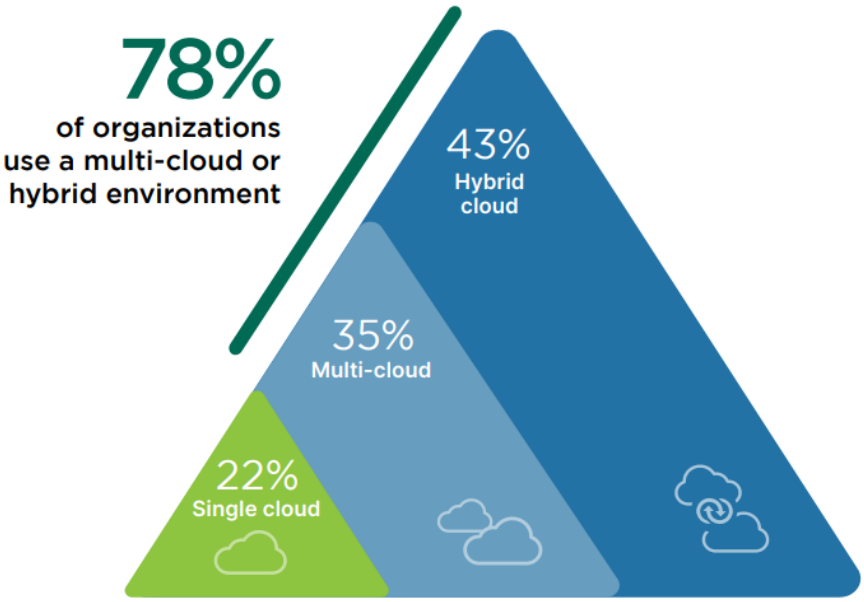

Рис. 1.2. Вибір основної стратегії організацій щодо розгортання хмари [2]

Опитування виявило перевагу моделям гібридної хмари: 43% респондентів прийняли цей підхід, що вказує на його привабливість, оскільки пропонує як масштабованість публічних хмар, так і контроль приватних хмар. Після цього 35% організацій віддають перевагу багатохмарній стратегії, яка використовує

сильні сторони різних хмарних провайдерів для оптимізації продуктивності та зменшення залежності від одного постачальника. Менший сегмент, 22%, обирає єдину хмарну службу, підкреслюючи спрощений підхід, який може запропонувати простоту та легкість керування, але потенційно обмежує гнучкість і надмірність.

Ці переваги підкреслюють необхідність для організацій ретельно розглядати свої хмарні стратегії на основі їхніх конкретних операційних потреб, вимог безпеки та технологічного середовища. Застосування гібридної або мультихмарної стратегії потребує надійної структури для управління складністю, забезпечення захисту даних у різних середовищах і ширших навичок у командах безпеки. Це також пропонує рух до впровадження хмарного розмаїття, зумовлений потребою в гнучкості, стійкості та оптимізації витрат у зусиллях з цифрової трансформації.

Необхідно відмітити, що 59% респондентів опитування [2] підкреслюють важливість IAM в забезпеченні доступу до інформаційних ресурсів лише авторизованим користувачам, мінімізуючи ризик витоку даних.

Майже кожна організація різною мірою використовує хмарні обчислення у своєму бізнесі. Однак із запровадженням хмари виникає необхідність переконатися, що стратегія хмарної безпеки організації здатна захищати від головних загроз для безпеки хмари [3]:

Неправильна конфігурація

Неправильна конфігурація параметрів безпеки хмари є основною причиною витоку хмарних даних. Стратегії керування хмарною безпекою багатьох організацій недостатні для захисту їхньої хмарної інфраструктури.

Цьому сприяє кілька факторів. Хмарна інфраструктура розроблена таким чином, щоб її можна було легко використовувати та надавати можливість легкого обміну даними, що ускладнює організаціям забезпечення доступу до даних лише авторизованим сторонам. Крім того, організації, які використовують хмарну інфраструктуру, також не мають повної видимості та контролю над своєю інфраструктурою, а це означає, що вони повинні покладатися на елементи

керування безпекою, які надає їхній постачальник хмарних послуг (CSP), щоб налаштувати та захистити свої хмарні розгортання. Оскільки багато організацій не знайомі з захистом хмарної інфраструктури та часто мають багатохмарні розгортання – кожне з різним набором засобів безпеки, наданих постачальником, неправильна конфігурація або недогляд у системі безпеки можуть легко залишити хмарні ресурси організації відкритими для зловмисників.

Несанкціонований доступ

На відміну від локальної інфраструктури організації, їх хмарні розгортання знаходяться поза периметром мережі та доступні безпосередньо з загальнодоступного Інтернету. Хоча це є активом для доступності цієї інфраструктури для співробітників і клієнтів, це також полегшує зловмиснику отримання неавторизованого доступу до хмарних ресурсів організації. Неправильно налаштований захист або скомпрометовані облікові дані можуть дозволити зловмиснику отримати прямий доступ, можливо, без відома організації.

Незахищені інтерфейси/API

CSP часто надають своїм клієнтам низку інтерфейсів прикладного програмування (API) та інтерфейсів. Загалом, ці інтерфейси добре задокументовані, щоб зробити їх зручними для використання клієнтами CSP.

Однак це створює потенційні проблеми, якщо клієнт належним чином не захистив інтерфейси своєї хмарної інфраструктури. Документація, розроблена для замовника, також може бути використана кіберзлочинцем для виявлення та використання потенційних методів доступу та викрадання конфіденційних даних із хмарного середовища організації.

Викрадення акаунтів

Багато людей мають надзвичайно слабкий захист паролів, включаючи повторне використання паролів і використання слабких паролів. Ця проблема посилює вплив фішингових атак і витоку даних, оскільки дає змогу використовувати один викрадений пароль для кількох різних облікових записів.

Викрадення облікових записів є однією з найсерйозніших проблем безпеки в хмарі, оскільки організації все більше покладаються на хмарну інфраструктуру

та програми для основних бізнес-функцій. Зловмисник, маючи облікові дані співробітника, може отримати доступ до конфіденційних даних або функцій, а скомпрометовані облікові дані клієнта дають повний контроль над їхнім обліковим записом в Інтернеті. Крім того, у хмарі організаціям часто не вистачає можливості ідентифікувати ці загрози та реагувати на них так само ефективно, як у локальній інфраструктурі.

Відсутність видимості

Хмарні ресурси організації розташовані за межами корпоративної мережі та працюють на інфраструктурі, якою компанія не володіє. Як наслідок, багато традиційних інструментів для досягнення видимості мережі неефективні для хмарних середовищ, а деяким організаціям бракує інструментів безпеки, орієнтованих на хмару . Це може обмежити можливості організації контролювати свої хмарні ресурси та захищати їх від атак.

Зовнішній обмін даними

Хмара створена для полегшення обміну даними. Багато хмар надають можливість явно запросити співавтора електронною поштою або надіслати посилання, яке дає змогу будь-кому, хто має URL-адресу, отримати доступ до спільного ресурсу.

Хоча цей простий обмін даними є перевагою, він також може бути серйозною проблемою безпеки хмари. Використання спільного доступу на основі посилань – популярного варіанту, оскільки це простіше, ніж явно запросити кожного співавтора – ускладнює контроль доступу до спільного ресурсу. Спільне посилання може бути передане комусь іншому, викрадене під час кібератаки або здогадане кіберзлочинцем, що забезпечить несанкціонований доступ до спільного ресурсу. Крім того, обмін на основі посилань унеможливлює скасування доступу лише до одного одержувача спільного посилання.

Внутрішні загрози

Внутрішні загрози є серйозною проблемою безпеки для будь-якої організації. Зловмисник уже має авторизований доступ до мережі організації та деяких конфіденційних ресурсів, які вона містить. Спроби отримати такий рівень

доступу – це те, що відкриває більшість зловмисників до їхньої цілі, що ускладнює для непідготовленої організації виявлення зловмисного інсайдера.

У хмарі виявити зловмисника ще складніше. Завдяки хмарному розгортанню компаніям не вистачає контролю над базовою інфраструктурою, що робить багато традиційних рішень безпеки менш ефективними. Це, а також той факт, що хмарна інфраструктура доступна безпосередньо з загальнодоступного Інтернету та часто страждає від неправильних конфігурацій безпеки, ще більше ускладнює виявлення зловмисників.

Кібератаки

Кіберзлочинність – це бізнес, і зловмисники обирають свої цілі на основі очікуваної прибутковості своїх атак. Хмарна інфраструктура доступна безпосередньо з загальнодоступного Інтернету, часто неналежним чином захищена та містить велику кількість конфіденційних і цінних даних. Крім того, хмара використовується багатьма різними компаніями, а це означає, що успішна атака може бути повторена багато разів з високою ймовірністю успіху. Як наслідок, хмарні розгортання організацій є звичайним об’єктом кібератак.

Атаки на відмову в обслуговуванні

Хмара необхідна для ведення бізнесу багатьма організаціями. Вони використовують хмару для зберігання важливих бізнес-даних і запуску важливих внутрішніх і клієнтських програм.

Це означає, що успішна атака типу «відмова в обслуговуванні» (DoS) проти хмарної інфраструктури, швидше за все, матиме серйозний вплив на низку різних компаній. У результаті DoS-атаки, коли зловмисник вимагає викуп, щоб зупинити атаку, становлять значну загрозу для хмарних ресурсів організації.

Основні проблеми безпеки хмарних сервісів у 2024 році є [3]:

Втрата/витік даних

Хмарні середовища дозволяють легко обмінюватися даними, що зберігаються в них. Ці середовища доступні безпосередньо з загальнодоступного Інтернету та включають можливість легко обмінюватися даними з іншими сторонами через прямі запрошення електронною поштою або шляхом спільного

використання загальнодоступного посилання на дані.

Простота обміну даними в хмарі – хоча це головний актив і ключ до співпраці в хмарі – викликає серйозні занепокоєння щодо втрати або витоку даних. Насправді 69% організацій вказують на це як на найбільшу проблему безпеки хмарних технологій. Обмін даними за допомогою загальнодоступних посилань або налаштування хмарного сховища на загальнодоступне робить їх доступними для будь-кого, хто знає про посилання, і існують спеціальні інструменти для пошуку в Інтернеті цих незахищених хмарних розгортань.

Конфіденційність/конфіденційність даних

Конфіденційність і конфіденційність даних є основною проблемою для багатьох організацій. Положення про захист даних, як-от Загальний регламент ЄС щодо захисту даних (GDPR), Закон про мобільність і доступність медичного страхування (HIPAA), Стандарт безпеки даних індустрії платіжних карток (PCI DSS) та багато інших зобов'язують захистити дані клієнтів і накладають суворі штрафи за збої безпеки. Крім того, організації мають велику кількість внутрішніх даних, необхідних для збереження конкурентної переваги.

Розміщення цих даних у хмарі має свої переваги, але також створює серйозні проблеми з безпекою для 66% організацій. Багато організацій запровадили хмарні обчислення, але їм не вистачає знань, щоб переконатися, що вони та їхні співробітники використовують їх безпечно. У результаті конфіденційні дані знаходяться під загрозою розголошення, про що свідчить величезна кількість порушень хмарних даних.

Випадкове розкриття облікових даних

Фішери зазвичай використовують хмарні програми та середовища як привід для своїх фішингових атак. Зі зростанням використання хмарної електронної пошти (G-Suite, Microsoft 365 тощо) і служб обміну документами (Google Drive, Dropbox, OneDrive) співробітники звикли отримувати електронні листи з посиланнями, які можуть попросити їх підтвердити обліковий запис. облікові дані, перш ніж отримати доступ до певного документа або веб-сайту.

Це дозволяє кіберзлочинцям легко дізнатися облікові дані співробітника для

хмарних сервісів. У результаті випадкове відкриття хмарних облікових даних викликає серйозне занепокоєння для 44% організацій, оскільки це потенційно ставить під загрозу конфіденційність і безпеку їхніх хмарних даних та інших ресурсів.

Реагування на інцидент

Багато організацій мають стратегії реагування на внутрішні інциденти кібербезпеки. Оскільки організація володіє всією внутрішньою мережевою інфраструктурою, а персонал служби безпеки працює на місці, можна заблокувати інцидент. Крім того, це право власності на їх інфраструктуру означає, що компанія, ймовірно, має видимість, необхідну для визначення масштабу інциденту та виконання відповідних дій з усунення.

Завдяки хмарній інфраструктурі компанія має лише часткову видимість і право власності на свою інфраструктуру, що робить традиційні процеси та інструменти безпеки неефективними. У результаті 44% компаній стурбовані своєю здатністю ефективно реагувати на інциденти в хмарі.

Відповідність законодавству та нормам

Правила захисту даних, такі як PCI DSS і HIPAA, вимагають від організацій продемонструвати, що вони обмежують доступ до захищеної інформації (даних кредитних карток, медичних записів пацієнтів тощо). Це може вимагати створення фізично або логічно ізольованої частини мережі організації, яка буде доступна лише для працівників, які мають законну потребу в доступі до цих даних.

Під час переміщення даних, захищених цими та подібними правилами, у хмару досягти та продемонструвати відповідність нормативним вимогам може бути складніше. Завдяки хмарному розгортанню організації мають можливість переглядати та контролювати лише деякі рівні своєї інфраструктури. Як наслідок, 42% організацій вважають відповідність законодавству та нормативним вимогам основною проблемою безпеки хмари та потребують спеціалізованих рішень відповідності хмарі .

Суверенітет даних/перебування/контроль

Більшість хмарних провайдерів мають кілька територіально розподілених центрів обробки даних. Це допомагає підвищити доступність і продуктивність хмарних ресурсів і полегшує для постачальників послуг гарантування того, що вони здатні підтримувати угоди про рівень обслуговування в умовах руйнівних подій, таких як стихійні лиха, відключення електроенергії тощо.

Організації, які зберігають свої дані в хмарі, часто не знають, де насправді зберігаються їхні дані в масиві центрів обробки даних CSP. Це викликає серйозні занепокоєння щодо суверенітету даних, місця проживання та контролю для 37% організацій. З нормативними актами щодо захисту даних, такими як GDPR, які обмежують, куди можна надсилати дані громадян ЄС, використання хмарної платформи з центрами обробки даних за межами затверджених зон може привести організацію до стану невідповідності нормативним вимогам. Крім того, різні юрисдикції мають різні закони щодо доступу до даних для правоохоронних органів і національної безпеки, що може вплинути на конфіденційність даних і безпеку клієнтів організації.

Захист хмари

Хмара надає організаціям ряд переваг; однак він також має свої власні загрози безпеці та проблеми. Хмарна інфраструктура дуже відрізняється від локального центру обробки даних, і традиційні інструменти та стратегії безпеки не завжди здатні ефективно її захистити. Щоб отримати додаткові відомості про головні проблеми та загрози безпеки в хмарі, завантажте звіт про безпеку в хмарі.

1.2. Аналіз моделей, методів та засобів управління доступом користувачів до хмарних сервісів та ресурсів

Управління ідентифікацією та доступом (IAM або IdAM) – це система, що містить інструменти та політики, які компанія використовує для перевірки особи користувача, авторизації контрольованого доступу до ресурсів компанії та перевірки доступу користувачів і пристроїв у своїй IT-інфраструктурі.

Організації використовують технологію IAM, щоб забезпечити потрібним

користувачам правильний доступ до потрібних ресурсів у потрібний час для завершення своєї роботи. Рішення IAM оптимізують робочі процеси та спрощують для користувачів підтверджувати свою особу та безперешкодно переміщатися між програмами протягом робочого дня за допомогою єдиного набору облікових даних для входу. Ці рішення надають організаціям необхідні засоби безпеки, щоб запобігти неавторизованим користувачам отримати доступ до даних і ресурсів компанії. Незважаючи на те, що сучасні інструменти IAM пропонують надійні засоби безпеки та керування користувачами для сучасних організацій, більшість компаній раніше використовували ті чи інші рішення для керування ідентифікацією та доступом [4].

Розглянемо основи IAM.

Каталоги зберігають інформацію про атрибути користувача та права доступу, щоб вони могли перевірити особу користувача перед наданням доступу до ресурсу компанії. Але хоча каталоги надають елементи технології IAM, вони часто обмежені за обсягом і погано інтегруються з сучасними хмарними технологіями, сторонніми інструментами та іншими ресурсами. Виконання дедалі складніших нормативних вимог і керування даними в усьому IT-ландшафті швидко почали вимагати більше IT-підтримки та ресурсів, оскільки їхня інфраструктура продовжувала розвиватися [4].

Коли мова заходить про керування ідентифікацією та доступом порівняно з каталогами (наприклад, Active Directory), IAM є більш надійним рішенням. Деякі сучасні рішення IAM пропонують ідентифікацію як послугу (IDaaS), яка надає технологію IAM як хмарну службу підписки, розміщену третьою стороною. Ці типи рішень підтримують розширену інфраструктуру IT, одночасно зменшуючи ручні робочі процеси для IT-команд, точніше перевіряючи ідентифікацію користувачів і надаючи нові способи керування доступом для великих гібридних робочих сил [4].

Структура IAM компанії демонструє, як її архітектура IAM, включаючи технології, інструменти, процеси, політики та рішення, працюють разом, щоб підтримувати загальну стратегію IAM.

По-перше, структура визначає, які користувачі отримують доступ до ресурсів, коли цим користувачам потрібен доступ і який рівень доступу їм надається. Фреймворк визначає деякі з цих дозволів, починаючи з різниці між користувачем IAM і роллю. Користувач поміщається в одну або кілька груп користувачів, які визначаються роллю або атрибутами, щоб визначити, які політики застосовуються до його доступу. Роль IAM і політика мають подібну відмінність; політики застосовуються до користувача автоматично залежно від того, які ролі та атрибути йому призначено.

Структура IAM також визначає як керувати, відстежувати та контролювати життєвий цикл користувача та доступу. Це охоплює запити на доступ, обробку змін ролі та керування переміщенням співробітників у компанію та з неї. Ці елементи підтримують політику та процедури IT для зменшення та пом’якшення зовнішніх і внутрішніх загроз кібербезпеці [4].

IAM містить модель автентифікації, авторизації та обліку (AAA) як стандартну структуру для технології IAM. Базовими стандартами для кожної системи IAM є автентифікація особи користувача, авторизація доступу відповідно до стратегії керування ідентифікацією та облік використання шляхом моніторингу, реєстрації активності та ведення записів.

Спираючись на структуру AAA, багато організацій створюють структуру IAM зі стратегією та планом дій у таких сферах [4]:

ідентифікація користувача, верифікація та автентифікація;

керування життєвим циклом користувачів і доступу;

методи безпеки для захисту даних і активів компанії;

відстеження та моніторинг активності;

управління робочим процесом аудиту відповідності.

IAM може допомогти організації знизити ризики безпеки, забезпечивши користувачам доступ до ресурсів, необхідних для виконання їх роботи. Складні кроки, задіяні в інструментах IAM, можуть здаватися обмежувальними, але багато з них насправді спрощують робочі процеси користувачів, покращують взаємодію з ними та підвищують продуктивність у всій організації.

Інфраструктури IAM можна повністю налаштувати відповідно до організаційних пріоритетів, які можуть відрізнятися залежно від галузі, розміру компанії або вимог до відповідності. Ось кілька прикладів IAM.

Автентифікація користувача за допомогою інструментів багатофакторної автентифікації (MFA). Після входу користувача, використовуючи свої облікові дані, інструмент MFA запитує другу форму перевірки, щоб підтвердити особу користувача. Інструменти MFA можуть автентифікувати користувача за допомогою запиту відповідей на додаткові питання безпеки, генерації одноразового пароля (OTP) на іншому пристрої або використання біометричних даних, наприклад відбитків пальців. Часто інструменти MFA використовуються разом із системою єдиного входу (SSO) для автентифікації користувача без погіршення взаємодії з ним.

Надання та деініціалізація доступу. IAM спрощує підключення та відключення співробітників за допомогою процесів, призначених для обмеження або дозволу доступу на основі статусу зайнятості та посадової ролі. Новим співробітникам потрібен швидкий доступ, щоб почати навчання та роботу, тому автоматичне надання доступу на основі визначених політик може заощадити IT-спеціалістам час і ресурси. Колишні співробітники, які все ще мають доступ до ресурсів компанії, становлять потенційну загрозу безпеці; важливо швидко деініціалізувати доступ, щоб підтримувати надійну безпеку.

Контроль користувачів для забезпечення належного доступу. Деякі інструменти IAM записують, як користувачі працюють у IT-інфраструктурі організації. Відстежуючи поведінку та дії користувачів, IT-команди можуть швидко виявляти аномальну активність і пом’якшувати можливі порушення з боку неавторизованих користувачів. Журнали також показують, які інструменти використовують ваші співробітники та як вони їх використовують, що може допомогти IT-спеціалістам точніше налаштувати контроль доступу на основі ролей або політики контролю доступу на основі атрибутів і обмежити непотрібний доступ [4].

Оскільки IT-середовища продовжують розширюватися, корпоративні

системи керування доступом до ідентифікаційної інформації стають все більш важливими для захисту бізнес-даних і зменшення впливу кібератак. Збільшення використання хмари, більше інструментів сторонніх розробників і популярність віддаленої роботи створюють нові виклики для компаній – недостатньо лише захистити IT-периметр. Традиційні IT-системи працюють на основі концепції неявної довіри.

Завдяки неявній довірі, коли користувач підтверджує свою особу, увійшовши за допомогою правильних облікових даних, він вважається надійним і дійсним користувачем, який може отримати миттєвий доступ до різних ресурсів, даних і конфіденційної інформації. Це показує, чому скомпрометовані облікові дані становлять такий значний ризик для безпеки організацій: викравши облікові дані, неавторизований користувач може легко отримати доступ до кількох захищених зон на основі прав доступу реального користувача. Без надійних дозволів доступу неавторизований користувач може вільно пересуватися мережею та завдати значно більшої шкоди під час кібератаки. IAM має вирішальне значення для того, щоб допомогти компаніям посилити свої позиції безпеки, одночасно зменшуючи ймовірність і наслідки кібератак. Перевіряючи та автентифікуючи особистість користувача, обмежуючи доступ користувачів і відстежуючи діяльність, компанії можуть захистити свої дані як від зовнішніх, так і від внутрішніх загроз [4].

Оскільки IAM часто впроваджується, щоб допомогти компаніям відповідати вимогам відповідності, хороша система IAM має відповідати надійним стандартам для забезпечення точності. Стандартна структура AAA забезпечує міцну основу, але багато додаткових IT-стандартів було нормалізовано в інструментах і платформах IAM, які посилюють або активують структуру AAA.

Залежно від вашої галузі, конкретних потреб у відповідності та загальної стратегії безпеки ці протоколи та стандарти зазвичай використовуються в системах IAM [4]:

Протокол OAuth 2.0 дозволяє стороннім клієнтам за межами вашої організації отримувати доступ до захищених ресурсів через маркер доступу.

Керований користувачем доступ (User-Managed Access, UMA) працює разом із OAuth 2.0, щоб допомогти контролювати та керувати доступом до ресурсів третіми сторонами.¶

Контроль доступу наступного покоління (Next Generation Access Control, NGAC) або розширена мова розмітки керування доступом (eXtensible Access Control Markup Language, XACML) забезпечують поглиблені можливості контролю доступу та керування політикою для перегляду запитів на доступ.¶

Security Assertion Markup Language (SAML) спрощує веб-систему SSO для відповідності та безпеки за допомогою цифрових підписів замість паролів.¶

Система міждоменного керування ідентифікацією (System for Cross-domain Identity Management, SCIM) ділиться атрибутами користувача між інструментами та автоматизує надання доступу, особливо в хмарних середовищах

У середовищі хмарних обчислень, що швидко розвивається, компанії все більше покладаються на хмарні послуги для підвищення гнучкості, масштабованості та ефективності. Однак, оскільки організації переносять конфіденційні дані та важливі програми в хмару, потреба в надійних заходах безпеки стає першорядною. Керування ідентифікацією та доступом (IAM) відіграє ключову роль у забезпеченні безпечного та сумісного хмарного середовища. Цей блог досліджує тонкощі IAM у хмарних обчисленнях, проливаючи світло на його значення, ключові компоненти та найкращі практики [5].

IAM у хмарних обчисленнях відноситься до структури політик, технологій і процесів, які керують і захищають цифрові ідентифікатори та їхній доступ до хмарних ресурсів. Основна мета полягає в тому, щоб лише авторизовані особи або системи могли отримати доступ до певних ресурсів і щоб вони робили це безпечним способом.

Ключовими компонентами IAM є [5, 7]:

Автентифікація

Автентифікація – це процес перевірки ідентичності користувачів, пристроїв або систем, які намагаються отримати доступ до хмарних ресурсів.

Багатофакторна автентифікація (MFA) додає додатковий рівень безпеки,

вимагаючи від користувачів надання кількох форм ідентифікації.

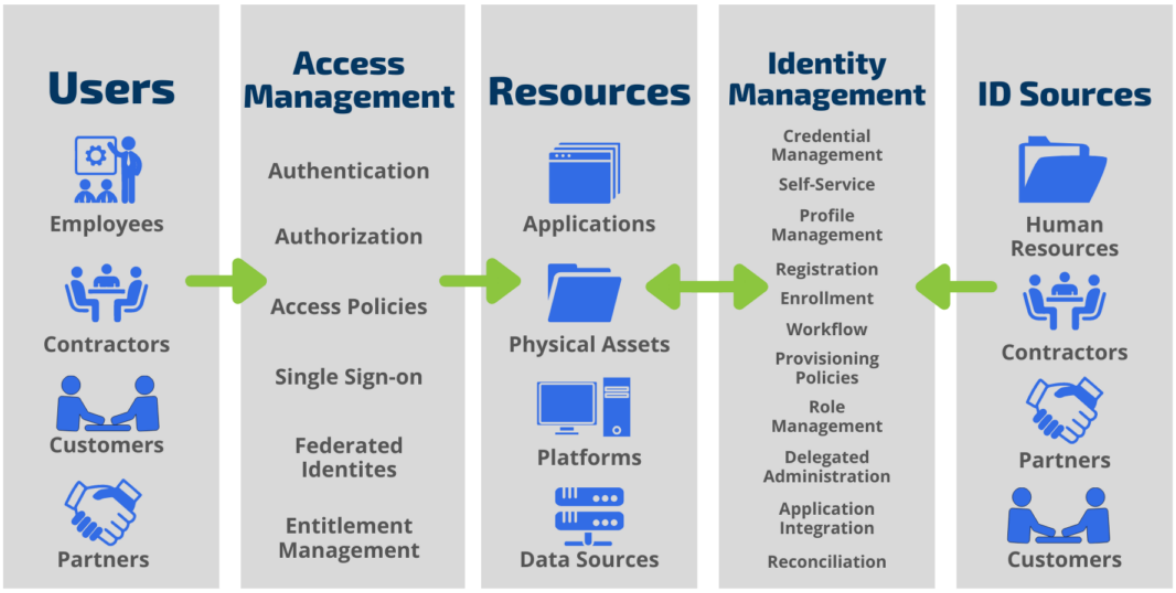

Рис. 1.3. Ключовими компонентами IAM [7]

Авторизація

Авторизація визначає рівень доступу, наданий автентифікованим об’єктам. Він передбачає визначення дозволів і елементів керування доступом на основі ролей, груп або окремих користувачів.

Контроль доступу на основі ролей (RBAC) і контроль доступу на основі атрибутів (ABAC) є поширеними моделями авторизації.

Керування життєвим циклом ідентифікації

IAM включає в себе управління всім життєвим циклом цифрових ідентифікаторів, від створення до дезактивації.

Механізми надання та скасування надання автоматизують процес надання та скасування доступу, коли співробітники приєднуються до організації або залишають її.

Єдиний вхід (SSO)

SSO дозволяє користувачам входити один раз і отримувати доступ до кількох програм або послуг без необхідності повторної автентифікації.

Це покращує взаємодію з користувачем і знижує ризик, пов’язаний із

вразливістю, пов’язаною з паролями.

Аудит і відповідність

Системи IAM містять можливості аудиту для відстеження дій користувачів, змін у дозволах та інших відповідних подій.

Дотримання вимог відповідності, таких як GDPR або HIPAA, є критично важливим для організацій, які обробляють конфіденційні дані.

Перевагами IAM у хмарних обчисленнях є []:

1. Покращена безпека: IAM посилює безпеку, гарантуючи, що лише авторизовані користувачі мають доступ до певних ресурсів. Багаторівнева автентифікація додає додатковий бар’єр проти несанкціонованого доступу.

2. Покращена відповідність: IAM допомагає організаціям дотримуватися нормативних вимог шляхом впровадження механізмів контролю доступу, аудиту та звітності.

3. Підвищення операційної ефективності: автоматизовані процеси керування ідентифікацією оптимізують запити на підключення, відключення та доступ, зменшуючи адміністративні витрати.

4. Зменшення ризиків. Дотримуючись принципів найменших привілеїв і регулярно переглядаючи дозволи на доступ, IAM допомагає зменшити ризик витоку даних і внутрішніх загроз.

1.3. Аналіз існуючих рішень з управління доступом користувачів до хмарних сервісів та ресурсів

У сучасному світі хмарні технології стають невід'ємною частиною розробки веб-додатків. Інтеграція хмарних сервісів дозволяє розробникам створювати більш гнучкі, масштабовані та безпечні додатки.

Хмарні сервіси – це програмні рішення та інфраструктура, що надаються через Інтернет. Вони дозволяють зберігати дані, виконувати обчислення, розгортати додатки та використовувати різні інструменти без необхідності управляти фізичними серверами. Найпопулярніші постачальники хмарних

сервісів включають Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform (GCP) [6].

Популярними хмарними сервісами для інтеграції є [6]:

Amazon Web Services (AWS):

Amazon S3: для зберігання даних;

Amazon EC2: для оренди віртуальних серверів;

Amazon RDS: для керованих баз даних;

AWS Lambda: для серверлесс обчислень;

AWS CodePipeline: для автоматизації CI/CD.

Microsoft Azure:

Azure Blob Storage: для зберігання даних;

Azure Virtual Machines: для оренди віртуальних серверів;

Azure SQL Database: для керованих баз даних;

Azure Functions: для серверлесс обчислень;

Azure DevOps: для автоматизації CI/CD.

Google Cloud Platform (GCP):

Google Cloud Storage: для зберігання даних;

Google Compute Engine: для оренди віртуальних серверів;

Google Cloud SQL: для керованих баз даних;

Google Cloud Functions: для серверлесс обчислень;

Google Cloud Build: для автоматизації CI/CD.

Інтеграція хмарних сервісів у корпоративні веб-додатки відкриває безліч можливостей для покращення продуктивності, безпеки та масштабованості. Використання хмарних платформ дозволяє знизити витрати, прискорити розробку та забезпечити високу доступність ваших додатків. Вибір правильних хмарних сервісів та ефективне їх використання допоможе вам створити надійні та сучасні веб-додатки, що відповідають вимогам користувачів та ринку [6].

Інтеграція хмарних сервісів у корпоративні веб-додатки відкриває безліч можливостей для покращення продуктивності, безпеки та масштабованості. Використання хмарних платформ дозволяє знизити витрати, прискорити розробку

та забезпечити високу доступність корпоративних додатків. Вибір правильних хмарних сервісів та ефективне їх використання допоможе організаціям створити надійні та сучасні веб-додатки, що відповідають вимогам користувачів та ринку.

Управління ідентифікацією та доступом (IAM) є одним із найважливіших, але складних рівнів хмарної безпеки. Крім того, кожен великий хмарний постачальник – Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform (GCP) – обробляє IAM по-різному, вимагаючи від спеціалістів із хмарної безпеки ознайомитися з різними можливостями, обмеженнями та термінологією під час керування IAM у певній ситуації в середовищі. Оскільки хмарна інфраструктура зростає в глибину та ширину, професіонали з хмарної безпеки – навіть якщо вони наразі не працюють у багатохмарному середовищі – захочуть і повинні отримати навички IAM різних CSP [8].

Хмарні ресурси – це всі інструменти та додатки, які утворюють середовище хмарних обчислень. До них належать сервери, бази даних, компоненти для зберігання даних тощо. Розуміння цієї структури важливо для розуміння того, як призначаються дозволи та як ними слід керувати.

Розглянемо, як кожен постачальник хмарних послуг структурує свої хмарні ресурси.

Структура ресурсу в AWS

В AWS основний контейнер називається обліковим записом AWS, який можна налаштувати та використовувати для надання ресурсів. Підприємства зазвичай мають кілька облікових записів AWS. Облікові записи можна консолідувати за допомогою AWS Organizations, хмарної служби AWS.

Питання про те, якою кількістю облікових записів повинен керувати один підрозділ організацій AWS, постійно обговорюється в спільноті інфосектора. Наприклад, деякі вважають, що одного облікового запису достатньо для всіх етапів – таких як розробка, постановка та виробництво – тоді як інші вважають за краще один обліковий запис для кожного етапу програми. В останньому випадку, наприклад, один обліковий запис охоплюватиме Застосунок 1 для його середовища розробки, постановки та виробництва, а інший обліковий запис

охоплюватиме Застосунок 2 для його середовища розробки, постановки та виробництва.

«Кореневий» – це батьківський контейнер для всіх облікових записів організації.

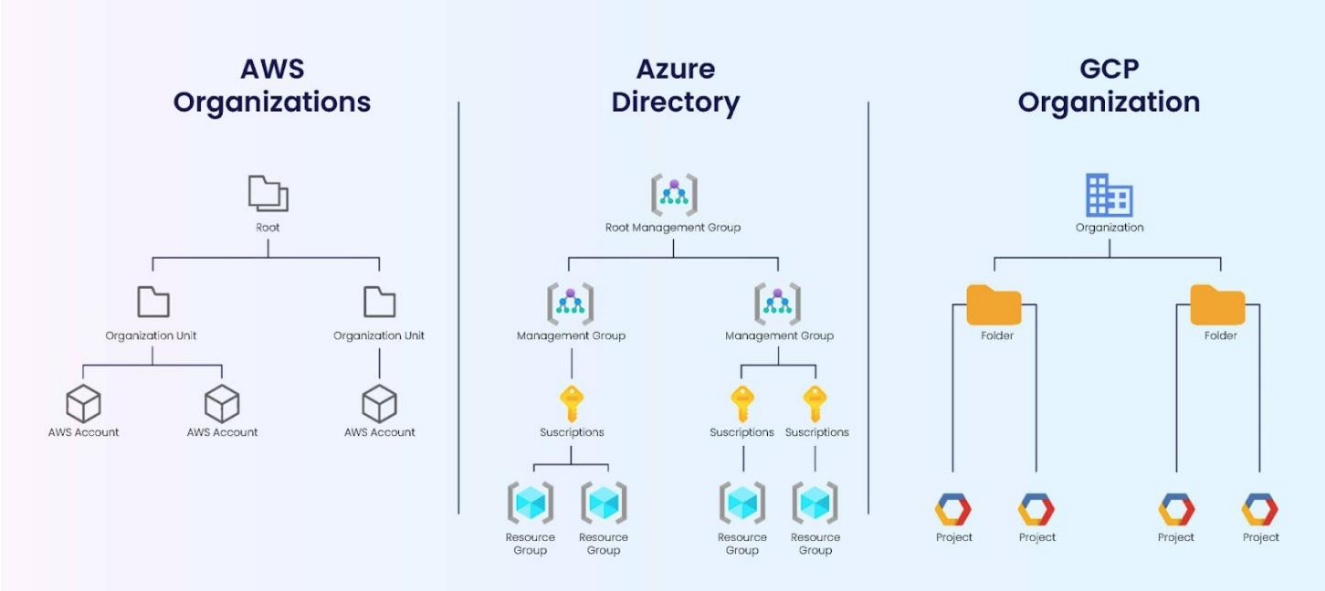

Рис. 1.4. Структура ресурсів у AWS, Azure та GCP [8]

Структура ресурсу в Azure

На відміну від AWS, Azure (і GCP) використовує рольову модель контролю доступу (RBAC), яка спирається на більш методичну структуру ресурсів. На первинному рівні Azure надає базовий контейнер ресурсів, «групу ресурсів». Кожен контейнер групи ресурсів групує всі ресурси, призначені для однієї конкретної програми, тому їх можна надавати та деініціалізувати разом.

Контейнер, який може містити групи ресурсів, є «підпискою». Контейнер, який може містити підписки, є «групою керування» (яка також може містити інші групи керування у вкладеній структурі). Кілька груп керування складаються з «кореневої групи керування». В Azure підписка також є платіжною одиницею.

Структура Azure призначена для узгодження з організаційною структурою підприємства.

Структура ресурсу в GCP

У GCP базовим контейнером є «проект», який містить ресурси для однієї

програми. «Папка» – це контейнер, який може об’єднувати кілька проектів. Папка складається з вкладеної структури на всіх рівнях організації. У GCP проект також є платіжною одиницею.

У той час як моделі Azure і GCP RBAC імітують організаційну структуру, AWS забезпечує меншу структуру та менше можливостей керування своєю структурою ресурсів. Це буде важливо пізніше під час встановлення дозволів для різних рівнів ресурсів.

AWS об’єднує дозволи та ресурси в один файл JSON (так званий політика). Дозволи на ресурси призначаються ідентифікатору за допомогою політики. Це на відміну від Azure і GCP, які відокремлюють набір дозволів від області; кожне призначення передбачає приєднання дозволів і ресурсів до посвідчення.

Крім того, оскільки Azure та GCP дотримуються дозволів RBAC, вони вмикають успадкування. Успадкування означає, що якщо роль має вищий обсяг, вона має ширший набір дозволів.

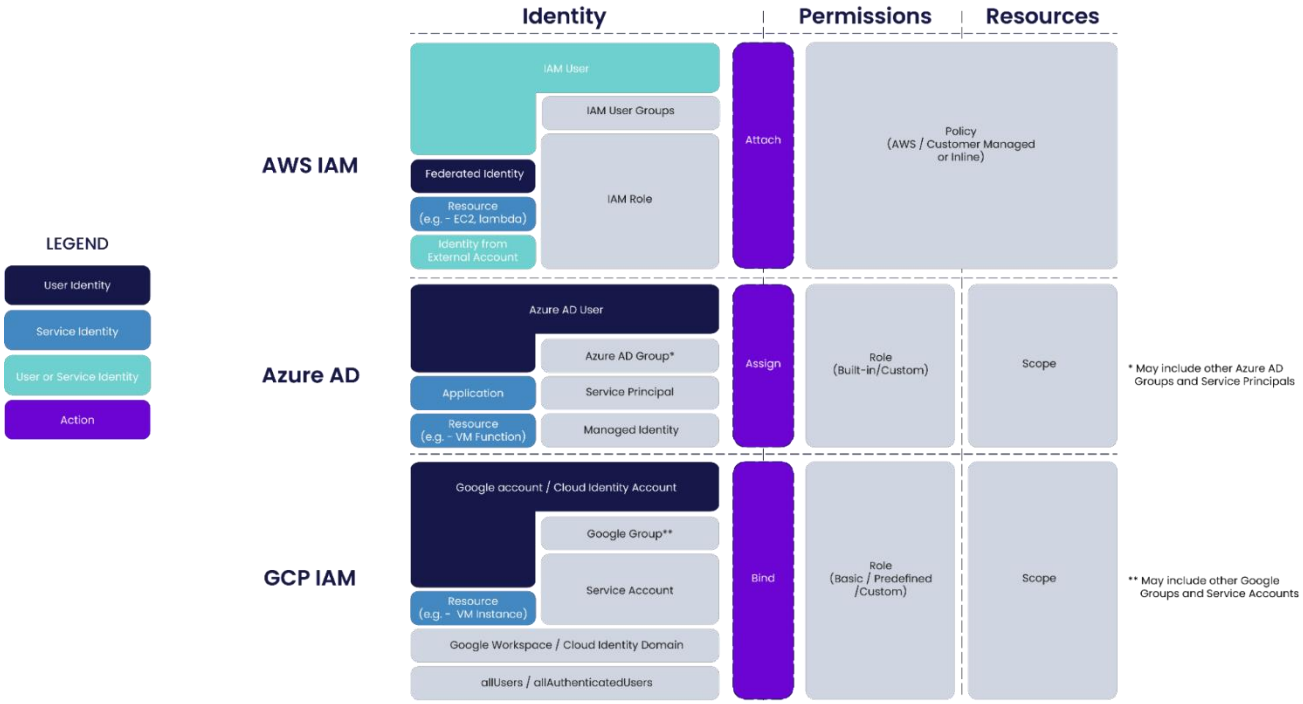

Рис. 1.5. Перелік дозволів у AWS, Azure та GCP [8]

Керування доступом користувачів в AWS

В AWS адміністратори можуть створити ресурс під назвою «IAM user», об’єкт, який представляє ресурс, і політику IAM, яка визначає можливості

доступу. AWS також дозволяє об’єднувати користувачів у «групи користувачів IAM».

Однак використання об’єкта «Користувачі IAM» може стати громіздким, якщо потрібно надати користувачам доступ до кількох облікових записів, оскільки користувачі IAM проживають у певних облікових записах, тому їм потрібен доступ до кількох облікових записів.

В AWS найкраще керувати користувачами через зовнішнього постачальника ідентифікаційної інформації (IdP). За допомогою IdP користувачі представлені через проксі-ідентифікатор, який називається «роллю IAM». Роль IAM дозволяє постачальнику посвідчень делегувати доступ цьому користувачеві.

AWS також представила інструмент AWS, AWS SSO, який забезпечує централізоване керування ідентифікаторами та об’єднання користувачів постачальниками ідентифікаційних даних. Використовуючи «набір дозволів», адміністратори можуть керувати та надавати доступ користувачам в облікових записах AWS. AWS SSO також може автоматично створювати ролі та політики, які до них додаються.

Керування доступом користувачів в Azure

Для керування користувачами Azure пропонує Azure Active Directory (Azure AD) – постачальник ідентифікаційної інформації, за допомогою якого керується користувачами. Це включає створення нових користувачів, запрошення користувачів-гостей або керування їхнім доступом до додатків.

Azure AD також дозволяє керувати користувачами в групах. Користувачі додаються до груп, і групи можуть бути вкладені одна в одну, тобто одну групу можна помістити в іншу, що дуже корисно при призначенні дозволів.

Керування доступом користувачів у GCP

Для IAM у GCP керування користувачами здійснюється через Google Cloud Identity або Google Workspace. Подібно до Azure, GCP дозволяє керувати користувачами та групами, які називаються Google Groups. Крім того, GCP має додаткові сутності, яким можна надати дозволи, зокрема домен, облікові записи служб, автентифікованих користувачів і всіх користувачів.

У GCP слід зауважити, що групи «всі користувачі» та «автентифіковані користувачі» не є специфічними для екземпляра Google Cloud Identity або Google Workspace. Навпаки, вони актуальні для всіх облікових записів Google і користувачів в Інтернеті, тому, по суті, є загальнодоступними.

Отже, хмарний IAM складний сам по собі, не кажучи вже про спроби безпечного керування ним у середовищах різних хмарних постачальників. Платформа автоматизованого аналізу, яка працює в кількох хмарах, може допомогти усунути прогалини в хмарному досвіді, одночасно відстежуючи дозволи для забезпечення безпеки хмари. Це допоможе зменшити ризики хмарної безпеки IAM простим і зрозумілим способом.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО ХМАРНИХ СЕРВІСІВ ТА РЕСУРСІВ AMAZON WEB SERVICES

2.1. Дослідження можливостей використання хмарних сервісів та ресурсів Amazon Web Services

Amazon Web Services (AWS) є дочірньою компанією Amazon, що надає надійну, масштабовану та комплексну платформу хмарних обчислень. Ось більш детальний огляд Amazon Web Services [9]:

великі хмарні послуги: AWS пропонує понад 200 повнофункціональних послуг із центрів обробки даних по всьому світу. Ці послуги включають обчислювальну потужність, зберігання бази даних, доставку вмісту та інші функції, які допомагають бізнесу масштабуватися та рости;

Інфраструктура як послуга (IaaS): модель ціноутворення AWS включає віртуальні сервери (екземпляри EC2) і набір пов’язаних служб, таких як Amazon Virtual Private Cloud (VPC), що дозволяє користувачам створювати ізольовані мережі в хмарі AWS. Amazon Web Services надає віртуальні сервери (примірники EC2) і набір пов’язаних служб, як-от Amazon Virtual Private Cloud (VPC), що дозволяє користувачам створювати ізольовані мережі в хмарі AWS;

Платформа як послуга (PaaS): AWS пропонує кероване середовище для розробки, тестування та розгортання додатків, наприклад Amazon Web Services Elastic Beanstalk, яке спрощує процес розгортання та масштабування веб-додатків і служб;

Програмне забезпечення як послуга (SaaS): AWS також розміщує додатки, якими безпосередньо користуються кінцеві користувачі, наприклад Amazon Chime для спілкування та AWS Work Mail для електронної пошти та календаря;

Глобальна мережа: AWS управляє центрами обробки даних по всьому світу, забезпечуючи високу доступність, резервування та масштабованість. Ця

глобальна присутність дозволяє компаніям розгортати програми та служби поблизу своїх кінцевих користувачів, зменшуючи затримку. Ця глобальна присутність дозволяє компаніям, які використовують AWS, розгортати програми та сервіси поблизу своїх кінцевих користувачів, значно скорочуючи затримку;

безпека та відповідність: AWS відома своєю прихильністю до безпеки. Він пропонує наскрізні функції безпеки та конфіденційності, вбудовані в службу. Amazon Web Services також відповідає різноманітним галузевим стандартам, що робить його життєздатним варіантом для таких секторів, як охорона здоров'я, фінанси та уряд.

Рис. 2.1. Розмаїття додатків AWS [9]

Додатки AWS різноманітні, вони задовольняють різні потреби бізнесу. Ось кілька основних з них [9]:

веб-хостинг і хостинг додатків: компанії можуть використовувати Amazon Web Services для розміщення веб-сайтів і веб-додатків. Використання AWS для недосвідчених користувачів є безпроблемним, коли йдеться про розміщення веб-сайтів і веб-додатків. Такі сервіси, як Amazon EC2 і Amazon S3, забезпечують не тільки масштабованість, але й безпечне середовище для розміщення динамічних веб-сайтів, демонструючи адаптивність моделі ціноутворення AWS;

зберігання та резервне копіювання даних: AWS надає масштабовані рішення для зберігання даних, такі як Amazon S3 і Amazon Glacier. Ці послуги

ідеально підходять для резервного копіювання даних, архівування та аварійного відновлення;

управління базою даних: AWS пропонує служби керованих баз даних, такі як Amazon RDS і Amazon DynamoDB, які забезпечують масштабовані та ефективні рішення для керування реляційними базами даних і базами даних NoSQL;

великі дані та аналітика: для обробки та аналітики великих даних Amazon Web Services пропонує такі послуги, як Amazon EMR (Elastic MapReduce) і Amazon Redshift, які дозволяють компаніям аналізувати та обробляти величезні обсяги даних;

машинне навчання та штучний інтелект: хто використовує AWS для передових технологій? Підприємства, які використовують такі інструменти, як Amazon Web Services SageMaker, стверджують, що AWS для чайників поширюється на машинне навчання та ШІ. AWS надає такі інструменти та платформи, як AWS SageMaker, для машинного навчання та ШІ, що дозволяє компаніям швидко створювати, навчати та розгортати моделі машинного навчання;

Інтернет речей (IoT): AWS IoT Core дозволяє компаніям підключати пристрої IoT до хмари та взаємодіяти з ними безпечно та ефективно;

DevOps і безперервна інтеграція/безперервне розгортання (CI/CD): AWS пропонує низку інструментів для практики DevOps, зокрема Amazon Web Services CodeBuild, AWS CodeDeploy і AWS CodePipeline, що сприяє безперервній інтеграції та безперервному розгортанню;

корпоративні додатки: для розміщення критично важливих корпоративних програм, таких як SAP і Microsoft SharePoint, компанії, які використовують AWS, отримують переваги від надійного та масштабованого середовища.

Ці додатки демонструють універсальність AWS, що робить його придатною платформою для широкого кола бізнес-потреб, від базового веб-хостингу до складного машинного навчання й аналітики великих даних.

Amazon Web Services (AWS) надає широкий спектр послуг, деякі пропозиції

вирізняються неперевершеною зручністю та продуктивністю. Досліджуючи різноманітні програми AWS, компанії знаходять рішення, які задовольняють різноманітні потреби, від базового веб-хостингу до розширеного машинного навчання. Зокрема, найпопулярніші сервіси AWS, такі як Amazon S3 і EC2, є прикладом прагнення платформи до безпечного, масштабованого зберігання даних і обчислювальної потужності.

Рис. 2.2. Найпопулярніші сервіси AWS [9]

Стратегічне використання цих послуг підкреслює економічну ефективність, притаманну моделі ціноутворення AWS, що робить її кращим вибором для безлічі компаній, які використовують AWS по всьому світу, включно з тими, хто користується хмарними службами AWS у Канаді. AWS пропонує широкий спектр послуг, але деякі з них набули популярності завдяки своїй корисності та продуктивності [9]:

Amazon EC2 (Elastic Compute Cloud): EC2 забезпечує масштабовану обчислювальну потужність у хмарі. Це дозволяє користувачам запускати сервери та збільшувати чи зменшувати потужність залежно від їхніх вимог;

Amazon S3 (проста служба зберігання): S3 пропонує масштабоване сховище об’єктів для резервного копіювання даних, архівування та аналітики. Воно відоме

своєю довговічністю, доступністю та масштабованістю;

AWS Lambda: Lambda дозволяє користувачам запускати код без підготовки та керування серверами. Сервіс використовується для створення безсерверних програм і автоматизації завдань;

Amazon RDS (служба реляційної бази даних): RDS полегшує налаштування, роботу та масштабування реляційної бази даних у хмарі. Вона забезпечує економічну ємність із змінним розміром;

Amazon CloudFront: це служба швидкої мережі доставки вмісту (CDN), яка безпечно доставляє дані, відео, програми та API клієнтам у всьому світі з низькою затримкою;

AWS Identity and Access Management (IAM): IAM має вирішальне значення для безпечного керування доступом до сервісів AWS. Він допомагає створювати користувачів і групи AWS і керувати ними, а також використовує дозволи, щоб дозволяти та забороняти їхній доступ до ресурсів AWS.

2.2. Призначення, можливості та функції управління доступом користувачів до хмарних сервісів та ресурсів AWS IAM

AWS Identity and Access Management (IAM) – це веб-сервіс, який допомагає безпечно контролювати доступ до ресурсів AWS. IAM використовується, щоб контролювати, хто автентифікований (ввійшов) і авторизований (має дозволи) на використання ресурсів. Коли вперше створюється обліковий запис AWS, ви починаєте з єдиного входу, який має повний доступ до всіх служб і ресурсів AWS в обліковому записі. Ця особа називається root-користувачем облікового запису AWS, і доступ до нього здійснюється шляхом входу за допомогою адреси електронної пошти та пароля, які ви використовували для створення облікового запису. Наполегливо рекомендується не використовувати користувача root для своїх повсякденних завдань, навіть адміністративних. Натомість необхідно дотримуватися найкращих методів використання лише користувача root для створення першого користувача IAM. Потім надійно заблокуйте облікові дані

користувача root і використовуйте їх для виконання лише кількох завдань керування обліковими записами та службами [10].

AWS IAM забезпечує точний контроль доступу у всіх сервісах AWS. За допомогою IAM ви можете вказати, хто може отримувати доступ до певних сервісів та ресурсів та за яких умов. Завдяки політикам IAM ви керуєте дозволами для співробітників та систем, надаючи дозволи з найменшими привілеями.

Розглянемо приклади використання AWS IAM. Загальний принцип роботи AWS IAM показано на рис. 2.3. За допомогою IAM можна керувати дозволами AWS для співробітників та робочих навантажень. Для співробітників рекомендується використовувати AWS Single Sign-On (AWS SSO), щоб керувати доступом до облікових записів AWS та дозволами в межах облікових записів. З AWS SSO можна легко призначати ролі та політики IAM і керувати ними в масштабах всієї організації. Для робочих навантажень використовуються ролі та політики IAM та надаються лише необхідні дозволи.

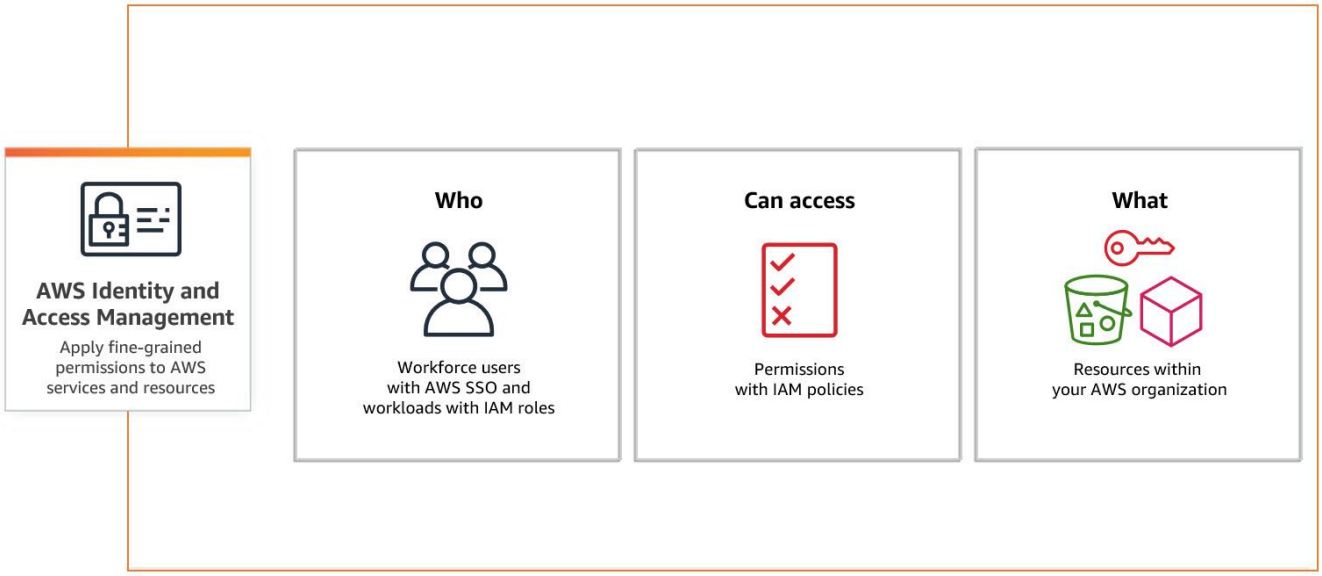

Рис. 2.3. Загальний принцип роботи AWS IAM [10]

Здійснюється точний контроль доступу. Використовуючи політики IAM, надається доступ до певних API сервісів та ресурсів AWS. Ви також можете визначити конкретні умови для надання доступу, наприклад, певна організація AWS або використання певного сервісу AWS.

Встановлюються обмеження дозволів та периметри даних у всій організації

AWS. Завдяки AWS Organizations можна використовувати політики керування сервісами (SCP) для встановлення обмежень дозволів, яким будуть відповідати всі користувачі та ролі IAM в облікових записах організації. Незалежно від того, чи починаєте ви працювати з SCP або вони вже є, можна використовувати консультанта з доступу IAM для того, щоб впевнено обмежувати дозволи.

Створюються дозволи з мінімальними привілеями завдяки IAM Access Analyzer. Досягнення принципу мінімальних привілеїв – це безперервний цикл видачі відповідних точних дозволів у міру появи вимог. IAM Access Analyzer допомагає оптимізувати налаштування, перевірку та уточнення дозволів.

Здійснюється автоматичне масштабування точних дозволів за допомогою ABAC. Управління доступом на основі атрибутів (ABAC) – це стратегія авторизації для створення деталізованих дозволів на базі атрибутів користувача, таких як відділ, робоча роль і назва команди. За допомогою ABAC можна скоротити кількість дозволів, необхідних для точного керування обліковим записом AWS.

Завдяки точним дозволам IAM можна визначати, хто отримує доступ. Потім IAM застосовує ці дозволи до кожного запиту. За замовчанням доступ заборонено та можливий лише в тому випадку, коли вибрано значення «Дозволено».

Розглянемо функції IAM. IAM надає такі функції [10]:

Спільний доступ до облікового запису AWS. Ви можете надати іншим людям дозвіл на адміністрування та використання ресурсів у вашому обліковому записі AWS, не повідомляючи свій пароль або ключ доступу.

Детальні дозволи. Ви можете надавати різні дозволи різним людям для різних ресурсів. Наприклад, ви можете надати деяким користувачам повний доступ до Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB, Amazon Redshift та інших служб AWS. Для інших користувачів ви можете надати доступ лише для читання лише до деяких сегментів S3 або дозволити адмініструвати лише деякі екземпляри EC2 або отримати доступ до вашої платіжної інформації, але нічого іншого.

Безпечний доступ до ресурсів AWS для програм, які працюють на Amazon

EC2. Ви можете використовувати функції IAM для безпечного надання облікових даних для програм, які працюють на екземплярах EC2. Ці облікові дані надають вашій програмі дозволи на доступ до інших ресурсів AWS. Приклади включають сегменти S3 і таблиці DynamoDB.

Багатофакторна автентифікація (MFA). Ви можете додати двофакторну автентифікацію до свого облікового запису та окремих користувачів для додаткової безпеки. З MFA ви або ваші користувачі повинні надати не тільки пароль або ключ доступу для роботи зі своїм обліковим записом, а й код зі спеціально налаштованого пристрою.

Об'єднання ідентифікації. Ви можете дозволити користувачам, які вже мають паролі в інших місцях, наприклад, у вашій корпоративній мережі або у постачальника ідентифікаційних даних в Інтернеті, отримати тимчасовий доступ до вашого облікового запису AWS.

Ідентифікаційна інформація для гарантії. Якщо ви використовуєте AWS CloudTrail, ви отримуєте записи журналу, які містять інформацію про тих, хто зробив запити на ресурси у вашому обліковому записі. Ця інформація заснована на ідентифікаторах IAM.

Відповідність стандарту PCI DSS. IAM підтримує обробку, зберігання та передачу даних кредитних карток продавцем або постачальником послуг, і його було підтверджено як відповідність вимогам Payment Card Industry (PCI) Data Security Standard (DSS).

Інтеграція з багатьма сервісами AWS.

Інтеграція IAM, як і багато інших служб AWS, є узгодженим. IAM досягає високої доступності шляхом реплікації даних на кількох серверах у центрах обробки даних Amazon по всьому світу. Якщо запит на зміну деяких даних успішний, зміна фіксується та безпечно зберігається. Однак зміна має бути відтворена в IAM, що може зайняти деякий час. Такі зміни включають створення або оновлення користувачів, груп, ролей або політик. Рекомендується не включати такі зміни IAM у критичні шляхи коду високої доступності корпоративного додатка. Замість цього внесіть зміни в IAM в окремій підпрограмі

ініціалізації або налаштування, яку ви запускаєте рідше. Також переконайтеся, що зміни були поширені до того, як робочі процеси залежать від них.

Безкоштовне використання. AWS IAM і AWS Security Token Service (AWS STS) – це функції вашого облікового запису AWS, які пропонуються без додаткової плати. З вас стягується плата, лише якщо ви отримуєте доступ до інших служб AWS за допомогою своїх користувачів IAM або тимчасових облікових даних безпеки AWS STS.

Розглянемо, як працює AWS IAM. Перш ніж створювати користувачів, ви повинні зрозуміти, як працює IAM. IAM забезпечує інфраструктуру, необхідну для контролю автентифікації та авторизації для вашого облікового запису. Інфраструктура IAM включає такі елементи (рис. 2.4): умови, принципал, запит, автентифікація, авторизація, дії або операції, ресурси [10].

Ресурси IAM: об’єкти користувача, групи, ролі, політики та постачальники ідентифікаційних даних, які зберігаються в IAM. Як і в інших сервісах AWS, ви можете додавати, редагувати та видаляти ресурси з IAM.

Ідентифікації IAM:

Об’єкти ресурсів IAM, які використовуються для ідентифікації та групування. Ви можете прикріпити політику до ідентифікатора IAM. До них належать користувачі, групи та ролі.

Суб’єкти IAM – об’єкти ресурсу IAM, які AWS використовує для автентифікації. До них належать користувачі та ролі IAM.

Принципал – особа або програма, яка використовує root-користувача облікового запису AWS, користувача IAM або роль IAM для входу та надсилання запитів до AWS. До принципалів належать об’єднані користувачі та передані ролі.

Принципал – головним є людина або додаток, яка може зробити запит на дії або операції по ресурсу AWS. Принципал автентифікується як кореневий користувач облікового запису AWS або сутність IAM для надсилання запитів до AWS. Як найкраща практика, не використовуйте облікові дані користувача root для щоденної роботи. Замість цього створюйте сутності IAM (користувачів і ролей). Ви також можете підтримувати федеративних користувачів або

програмний доступ, щоб дозволити програмі отримати доступ до вашого облікового запису AWS.

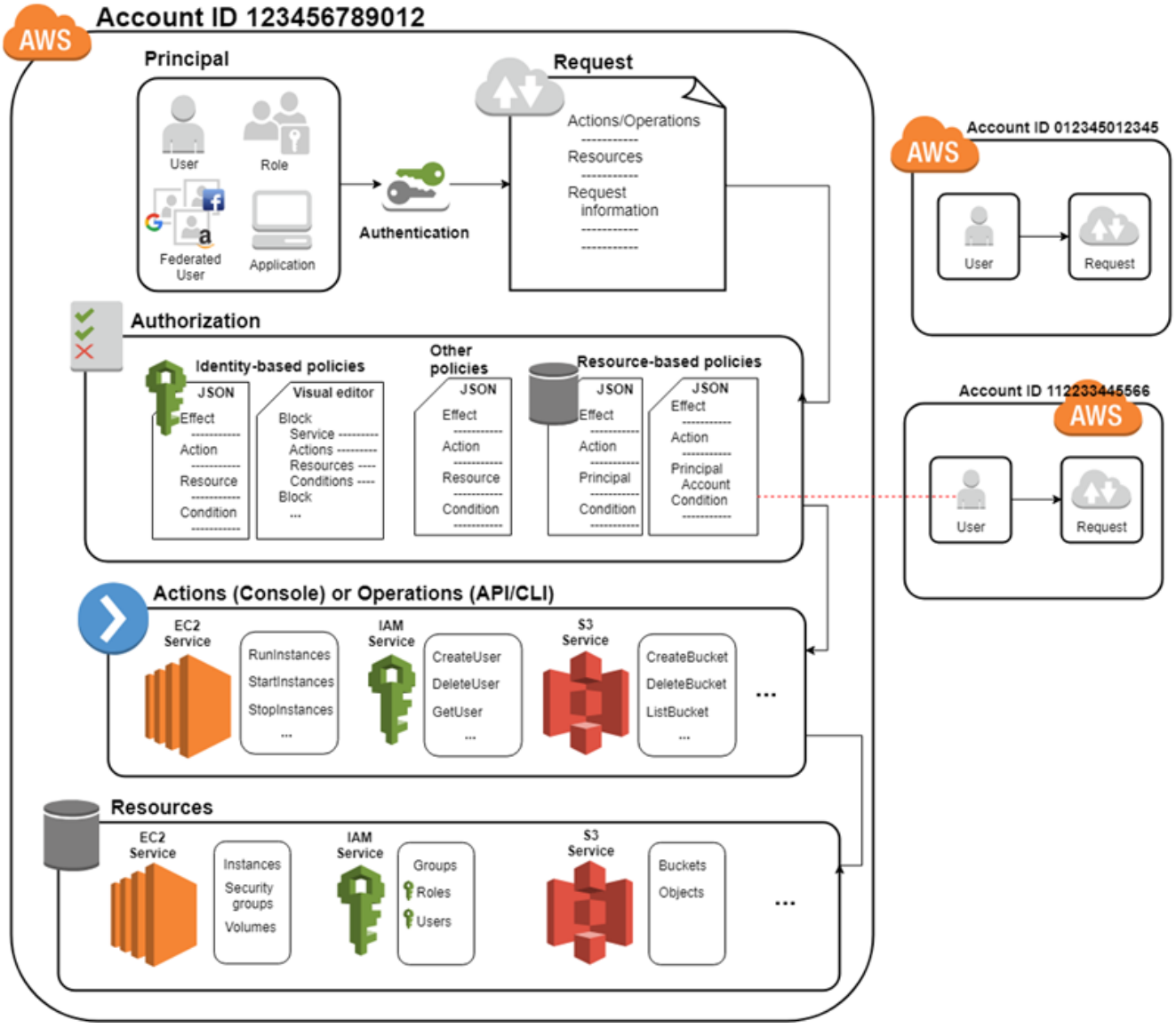

Рис. 2.4. Складові частини системи AWS IAM [10]

Запит: коли принципал намагається використати Консоль керування AWS, API AWS або AWS CLI, цей принципал надсилає запит до AWS. Запит містить таку інформацію [12]:

дії або операції – дії або операції, які хоче виконати принципал. Це може бути дія в Консолі керування AWS або операція в AWS CLI або AWS API;

ресурси – об’єкт ресурсу AWS, на якому виконуються дії або операції;

принципал – особа або програма, яка використовувала об’єкт (користувача чи роль) для відправлення запиту. Інформація про принципала включає політики, пов’язані з сутністю, яку принципал використовував для входу;

дані середовища – інформація про IP-адресу, агент користувача, статус увімкненого SSL або час доби;

дані ресурсу – дані, пов’язані з ресурсом, який запитується. Це може включати таку інформацію, як ім’я таблиці DynamoDB або тег на екземплярі Amazon EC2.

AWS збирає інформацію запиту в контекст запиту , який використовується для оцінки та авторизації запиту.

Автентифікація. Щоб надіслати запит до AWS, принципал має пройти автентифікацію (ввійти в AWS), використовуючи свої облікові дані. Деякі сервіси, такі як Amazon S3 і AWS STS, допускають кілька запитів від анонімних користувачів. Однак вони є винятком із правил.

Щоб пройти автентифікацію з консолі як користувач root, ви повинні увійти, використовуючи свою адресу електронної пошти та пароль. Як користувач IAM, вкажіть ідентифікатор або псевдонім свого облікового запису, а потім ім’я користувача та пароль. Щоб пройти автентифікацію за допомогою API або AWS CLI, потрібно надати ключ доступу та секретний ключ. Від вас також може знадобитися надати додаткову інформацію безпеки. Наприклад, AWS рекомендує використовувати багатофакторну автентифікацію (MFA), щоб підвищити безпеку вашого облікового запису.

Авторизація: ви також повинні бути авторизовані (дозволені) для виконання вашого запиту. Під час авторизації AWS використовує значення з контексту запиту для перевірки правил, які застосовуються до запиту. Потім він використовує політику, щоб визначити, дозволити чи відхилити запит. Більшість політик зберігаються в AWS як документи JSON і вказують дозволи для основних сутностей. Існує кілька типів полісів, що може вплинути на те, чи буде запит авторизований. Щоб надати своїм користувачам дозволи на доступ до ресурсів AWS у власному обліковому записі, вам потрібні лише політики на основі

ідентифікації. Політики на основі ресурсів популярні для надання доступу між обліковими записами. Інші типи політики є розширеними функціями, і їх слід використовувати обережно.

AWS перевіряє кожну політику, яка застосовується до контексту вашого запиту. Якщо одна політика дозволів містить заборонену дію, AWS відхиляє весь запит і припиняє оцінку. Це називається явним запереченням . Оскільки запити відхиляються за замовчуванням, AWS авторизує ваш запит, лише якщо кожна частина вашого запиту дозволена відповідною політикою дозволів. Логіка оцінки запиту в межах одного облікового запису відповідає таким загальним правилам:

За замовчуванням усі запити відхиляються. (Загалом, запити, зроблені з використанням облікових даних root користувача облікового запису AWS для ресурсів облікового запису, завжди дозволені).

Явний дозвіл у будь-якій політиці дозволів (на основі ідентифікаційних даних чи ресурсів) замінює це за замовчуванням.

Існування організації SCP, межі дозволів IAM або політика сеансу перевизначає дозвіл. Якщо існує один або кілька з цих типів політики, усі вони повинні дозволяти запит. В іншому випадку це неявно заперечується. Явна заборона в будь-якій політиці перевизначає будь-які дозволи.

Дії або операції. Після автентифікації та авторизації вашого запиту AWS схвалює дії або операції у вашому запиті. Операції визначаються службою і включають те, що ви можете робити з ресурсом, наприклад перегляд, створення, редагування та видалення цього ресурсу. Наприклад, IAM підтримує приблизно 40 дій для ресурсу користувача, включаючи такі дії: *CreateUser, DeleteUser, GetUser, UpdateUser.*

Ресурси. Після того, як AWS схвалить операції у вашому запиті, їх можна буде виконувати на відповідних ресурсах у вашому обліковому записі. Ресурс – це об’єкт, який існує в службі. Приклади включають екземпляр Amazon EC2, користувача IAM і сегмент Amazon S3. Сервіс визначає набір дій, які можна виконати з кожним ресурсом. Якщо ви створюєте запит на виконання непов’язаної дії з ресурсом, цей запит відхиляється. Наприклад, якщо ви

надсилаєте запит на видалення ролі IAM, але надаєте ресурс групи IAM, запит не виконується.

2.3. Сутність моделі управління доступом користувачів на основі атрибутів в AWS IAM

Контроль доступу на основі атрибутів (ABAC) – це стратегія авторизації, яка визначає дозволи на основі атрибутів. У AWS ці атрибути називаються тегами. Ви можете прикріплювати теги до ресурсів IAM, зокрема до сутностей IAM (користувачів або ролей), а також до ресурсів AWS. Ви можете створити одну політику ABAC або невеликий набір політик для своїх керівників IAM. Ці політики ABAC можуть бути розроблені для того, щоб дозволити операції, коли тег принципала збігається з тегом ресурсу. ABAC корисний у середовищах, які швидко розвиваються, і допомагає у ситуаціях, коли управління політикою стає громіздким [10].

Наприклад, ви можете створити три ролі за допомогою *access-project* ключа тегу. Встановіть значення тегу першої ролі на *Heart*, другої на *Sun*, а третьої на *Lightning* (рис. 2.5). Потім можна використовувати єдину політику, яка надає доступ, якщо роль і ресурс позначено однаковими тегами для *access-project* [12].

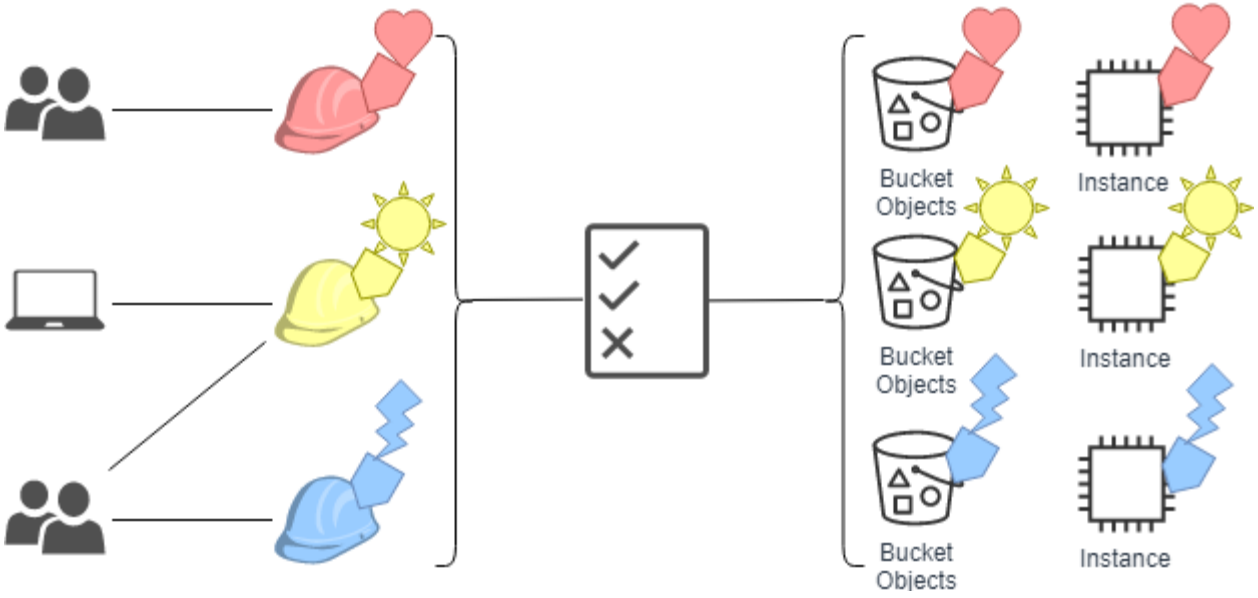

Рис. 2.5. Принцип контролю доступу на основі атрибутів (ABAC) [10]

Порівняння ABAC з традиційною моделлю RBAC [10].

Традиційна модель авторизації, що використовується в IAM, називається керуванням доступом на основі ролей (RBAC). RBAC визначає дозволи на основі службової функції людини, відомої за межами AWS як роль. У AWS роль зазвичай відноситься до ролі IAM, яка є особистістю в IAM, яку ви можете прийняти. IAM містить керовані політики для робочих функцій, які узгоджують дозволи з робочою функцією в моделі RBAC.

У IAM реалізується модель RBAC, створюючи різні політики для різних робочих функцій. Потім ви приєднуєте політики до ідентифікаційних даних (користувачів IAM, груп користувачів або ролей IAM). Як найкраща практика, ви надаєте мінімальні дозволи, необхідні для роботи функції. Це відомо як надання найменших привілеїв. Зробіть це, перерахувавши конкретні ресурси, до яких може отримати доступ службова функція. Недоліком використання традиційної моделі RBAC є те, що коли співробітники додають нові ресурси, ви повинні оновлювати політики, щоб дозволити доступ до цих ресурсів.

Наприклад, припустимо, що у вас є три проекти з іменами *Heart*, *Sun*, і *Lightning*, над якими працюють співробітники. Ви створюєте роль IAM для кожного проекту. Потім ви додаєте політику до кожної ролі IAM, щоб визначити ресурси, до яких може отримати доступ будь-хто, кому дозволено взяти на себе роль. Якщо працівник змінює роботу у вашій компанії, ви призначаєте йому іншу роль IAM. Людей або програм можна призначити на кілька ролей. Однак, *Sun* для проекту можуть знадобитися додаткові ресурси, наприклад, новий сегмент Amazon S3. У цьому випадку ви повинні оновити політику, додану до *Sun* ролі, щоб вказати новий ресурс сегмента. В іншому випадку *Sun* учасники проекту не матимуть доступу до нового сегмента (рис. 2.6).

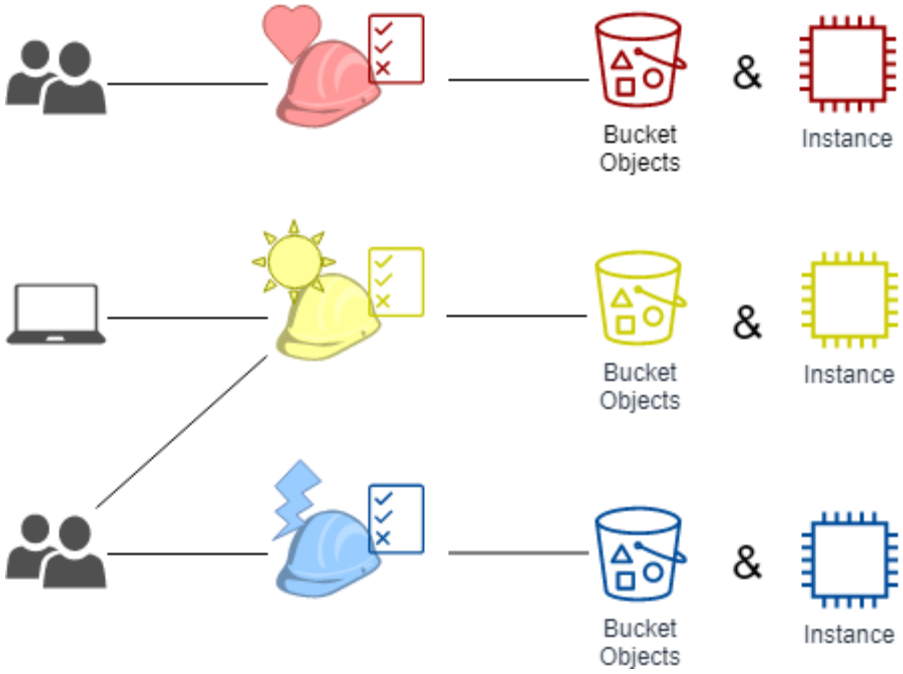

Рис. 2.6. Принцип керуванням доступом на основі ролей (RBAC) [10]

ABAC забезпечує наступні переваги перед традиційною моделлю RBAC [12]:

Інноваційне масштабування дозволів ABAC. Адміністратору більше не потрібно оновлювати існуючі політики, щоб дозволити доступ до нових ресурсів. Наприклад, припустимо, що ви розробили свою стратегію ABAC за допомогою *access-project* тегу. Розробник використовує роль з тегом *access-project = Heart*. Коли учасникам *Heart* проекту потрібні додаткові ресурси Amazon EC2, розробник може створити нові екземпляри Amazon EC2 за допомогою тег *access-project = Heart*. Тоді будь-хто в *Heart* проекті може запускати та зупиняти ці екземпляри, оскільки їхні значення тегу збігаються.

ABAC вимагає менше політик. Оскільки вам не потрібно створювати різні політики для різних робочих функцій, ви створюєте менше політик. Цими політиками легше керувати.

Використовуючи ABAC, команди можуть швидко змінюватися та розвиватися. Це тому, що дозволи для нових ресурсів надаються автоматично на основі атрибутів. Наприклад, якщо ваша компанія вже підтримує проекти *Heart* та з *Sun* використанням ABAC, можна легко додати новий *Lightning* проект.

Адміністратор IAM створює нову роль з тег *access-project = Lightning*. Для підтримки нового проекту змінювати політику не потрібно. Будь-хто, хто має дозвіл на виконання ролі, може створювати та переглядати екземпляри з тегом *access-project = Lightning*. Крім того, член команди може перейти від *Heart* проекту до *Lightning* проекту. Адміністратор IAM призначає користувача іншу роль IAM. Змінювати політику дозволів не потрібно.

Детальні дозволи можливі за допомогою ABAC. Коли ви створюєте політики, найкраще надавати найменші привілеї. Використовуючи традиційний RBAC, ви повинні написати політику, яка надає доступ лише до певних ресурсів. Однак, коли ви використовуєте ABAC, ви можете дозволити дії з усіма ресурсами, але лише якщо тег ресурсу збігається з тегом принципала.

Атрибути співробітників використовуються зі свого корпоративного каталогу за допомогою ABAC. Можна налаштувати свого постачальника ідентифікаторів на основі SAML або веб-посвідчення на передачу тегів сеансу в AWS. Коли співробітники об’єднуються в AWS, їхні атрибути застосовуються до їх результуючого принципала в AWS. Потім можна використовувати ABAC, щоб дозволити або відхилити дозволи на основі цих атрибутів.

2.4. Призначення, можливості та функції централізованого управління доступом до облікових записів та додатків AWS Single Sign-On

Єдиний вхід (SSO) – це рішення автентифікації, яке дозволяє користувачам входити в декілька програм і веб-сайтів за допомогою одноразової автентифікації користувача. Враховуючи те, що сьогодні користувачі часто отримують доступ до програм безпосередньо зі своїх браузерів, організації надають пріоритет стратегіям керування доступом, які покращують як безпеку, так і взаємодію з користувачем. SSO забезпечує обидва аспекти, оскільки користувачі можуть отримати доступ до всіх ресурсів, захищених паролем, без повторних входів після перевірки їхньої особи [11].

Використання системи єдиного входу для спрощення входу користувачів приносить користь користувачам і організаціям кількома способами.

Рис. 2.7. Архітектура системи єдиного входу [11]

SSO встановлює довіру між програмою або службою та зовнішнім постачальником послуг, також відомим як постачальник ідентифікаційної інформації (IdP). Це відбувається за допомогою серії кроків автентифікації, перевірки та зв'язку між програмою та централізованою службою SSO. Нижче наведено важливі компоненти рішень SSO.

Служба SSO – це центральна служба, на яку покладаються програми, коли користувач входить у систему. Якщо неавтентифікований користувач запитує доступ до програми, програма перенаправляє його до служби SSO. Потім служба перевіряє автентичність і перенаправляє користувача назад до початкової програми. Служба зазвичай працює на спеціальному сервері політик SSO.

Маркер SSO – це цифровий файл, який містить ідентифікаційну інформацію користувача, наприклад ім'я користувача або адресу електронної пошти. Коли користувач запитує доступ до програми, програма обмінюється маркером SSO зі службою SSO для автентифікації користувача.

Процес SSO виглядає так [11]:

Коли користувач входить у програму, програма генерує маркер SSO та надсилає запит на автентифікацію до служби SSO.

Сервіс перевіряє, чи був користувач попередньо аутентифікований у системі. Якщо так, він надсилає відповідь із підтвердженням автентифікації програмі, щоб надати доступ користувачеві.

Якщо користувач не має підтверджених облікових даних, служба SSO перенаправляє користувача до центральної системи входу та пропонує користувачу надіслати ім’я користувача та пароль.

Після надсилання сервіс перевіряє облікові дані користувача та надсилає позитивну відповідь заявці.

В іншому випадку користувач отримує повідомлення про помилку та повинен повторно ввести облікові дані. Кілька невдалих спроб входу можуть призвести до того, що служба заблокує користувача від подальших спроб протягом фіксованого періоду часу.

Розглянемо види SSO. Існують різні стандарти та протоколи, які використовують рішення SSO для перевірки та автентифікації облікових даних користувача.

SAML або Security Assertion Markup Language – це протокол або набір правил, які програми використовують для обміну інформацією автентифікації зі службою SSO. SAML використовує XML, дружню мову розмітки для браузера, для обміну ідентифікаційними даними користувачів. Служби SSO на основі SAML забезпечують кращу безпеку та гнучкість, оскільки програмам не потрібно зберігати облікові дані користувача у своїй системі.

OAuth або відкрита авторизація – це відкритий стандарт, який дозволяє програмам безпечно отримувати доступ до інформації користувача з інших веб-сайтів, не повідомляючи їм пароль. Замість того, щоб запитувати паролі користувачів, програми використовують OAuth, щоб отримати дозвіл користувача на доступ до захищених паролем даних. OAuth встановлює довіру між програмами через API, що дозволяє програмі надсилати запити автентифікації та

відповідати на них у встановленій структурі.

OpenID – це спосіб використання одного набору облікових даних користувача для доступу до кількох сайтів. Це дозволяє постачальнику послуг взяти на себе роль автентифікації облікових даних користувача. Замість того, щоб передавати маркер автентифікації сторонньому постачальнику ідентифікаційної інформації, веб-додатки використовують OIDC для запиту додаткової інформації та перевірки автентичності користувача.

Kerberos – це система автентифікації на основі квитків, яка дозволяє двом або більше сторонам взаємно перевіряти свою особу в мережі. Він використовує криптографію безпеки для запобігання несанкціонованому доступу до ідентифікаційної інформації, що передається між сервером, клієнтами та Центром розподілу ключів.

Система єдиного входу є розширеним і бажаним рішенням для керування доступом до особистих даних. Після розгортання рішення єдиного входу допомагає організаціям керувати доступом користувачів до корпоративних програм і ресурсів. Рішення SSO спрощує встановлення та запам’ятовування надійних паролів для користувачів програм. Крім того, IT-команда може використовувати інструмент SSO для моніторингу поведінки користувачів, підвищення стійкості системи та зниження ризиків безпеки.

Отже, AWS Single Sign-On дозволяє легко централізовано керувати доступом до кількох облікових записів AWS і бізнес-додатків та надає користувачам доступ до всіх призначених їм облікових записів і програм з одного місця, що забезпечує захищеність корпоративних даних.

3 ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО ХМАРНИХ СЕРВІСІВ ТА РЕСУРСІВ AMAZON WEB SERVICES

3.1. Порядок розгортання рішення AWS IAM

AWS Identity and Access Management (IAM) допомагає безпечно контролювати доступ до Amazon Web Services (AWS) і ресурсів вашого облікового запису. IAM також може зберігати облікові дані вашого облікового запису конфіденційними. За допомогою IAM ви можете створити кількох користувачів IAM під парасолькою свого облікового запису AWS або ввімкнути тимчасовий доступ через об’єднання ідентифікаційних даних із корпоративним каталогом. У деяких випадках ви також можете ввімкнути доступ до ресурсів в облікових записах AWS.

Однак без IAM необхідно створити кілька облікових записів AWS – кожен із власними виставленнями рахунків і підписками на продукти AWS – або співробітники повинні надати доступ до облікових даних безпеки одного облікового запису AWS. Крім того, без IAM не можна контролювати завдання, які може виконувати певний користувач або система, і ресурси AWS, які вони можуть використовувати [10].

На рис. 3.1. показано простий приклад облікового запису AWS з трьома групами. Група – це сукупність користувачів, які мають подібні обов’язки. У цьому прикладі одна група призначена для адміністраторів (вона називається Адміністратори). Також є група розробників і тест група. Кожна група має кілька користувачів. Кожен користувач може бути більш ніж в одній групі, хоча малюнок цього не ілюструє. Не можна розміщувати групи в інших групах. Необхідно використовувати політику для надання дозволів групам [10].

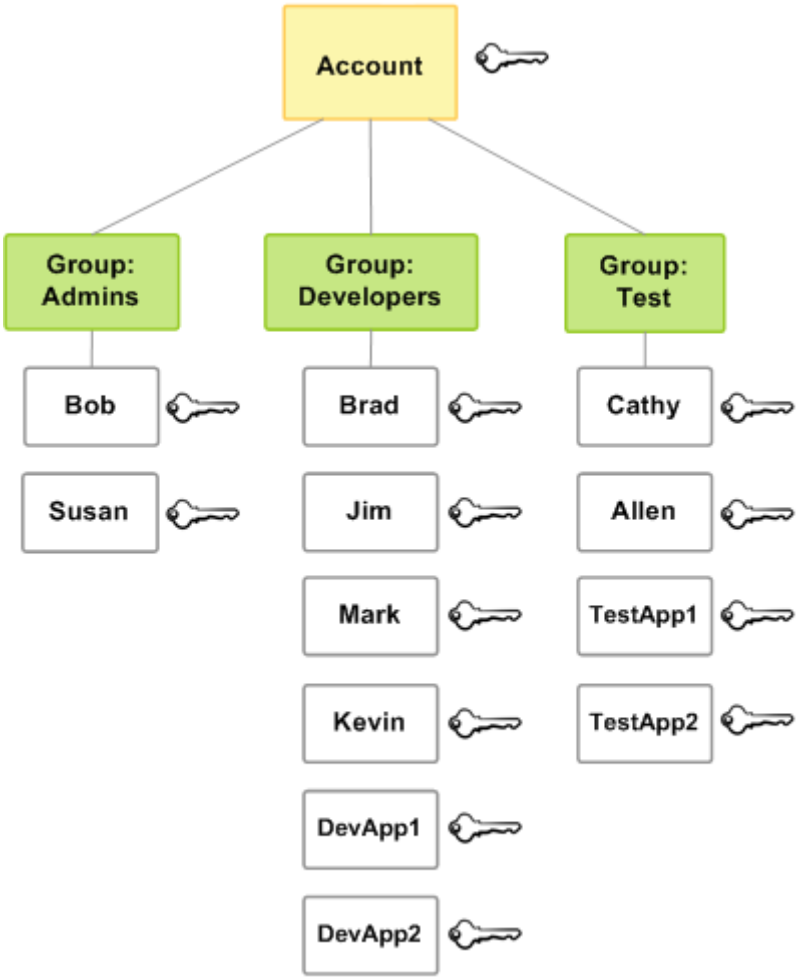

Рис. 3.1. Приклад облікового запису AWS з трьома групами [10]

У наведеній нижче процедурі треба виконувати такі завдання [10]:

створіть групу адміністраторів і надайте групі дозвіл на доступ до всіх ресурсів вашого облікового запису AWS;

створіть собі користувача та додайте його до групи адміністраторів;

створіть пароль для свого користувача, щоб ви могли ввійти в Консоль керування AWS.

Групі адміністраторів надається дозвіл на доступ до всіх доступних ресурсів облікового запису AWS. Доступними ресурсами є будь-які продукти AWS, які ви використовуєте або на які ви зареєструвалися. Користувачі групи адміністраторів також можуть отримати доступ до інформації вашого облікового запису AWS, за винятком облікових даних вашого облікового запису AWS.

Створення першого користувача-адміністратора IAM і групи

користувачів. Як найкраща практика, не використовуйте користувача root облікового запису AWS для виконання будь-яких завдань, де це не потрібно. Натомість створіть нового користувача IAM для кожної особи, якій потрібен доступ адміністратора. Потім зробіть цих користувачів адміністраторами, помістивши користувачів у групу користувачів «Адміністратори», до якої ви приєднаєте керовану політику *AdministratorAccess*.

Після цього користувачі в групі адміністраторів мають налаштувати групи користувачів, користувачів тощо для облікового запису AWS. Вся подальша взаємодія має здійснюватися через користувачів облікового запису AWS та їхні власні ключі, а не через користувача *root*. Однак для виконання деяких завдань керування обліковими записами та службами необхідно ввійти, використовуючи облікові дані користувача *root*.

3.2. Технологія застосування рішення AWS IAM

Розглянемо політики та дозволи в AWS IAM.

Керування доступом в AWS здійснюється, створюючи політики та приєднуючи їх до ідентифікаційних даних IAM (користувачів, груп користувачів або ролей) або ресурсів AWS. Політика – це об’єкт в AWS, який, пов’язаний із ідентифікатором або ресурсом, визначає їхні дозволи. AWS оцінює ці політики, коли принципал IAM (користувач або роль) робить запит. Дозволи в політиках визначають, дозволено чи відхилено запит. Більшість політик зберігаються в AWS як документи JSON. AWS підтримує шість типів політик, які розглядаються нижче.

Політики IAM визначають дозволи для дії незалежно від методу, який ви використовуєте для виконання операції. Наприклад, якщо політика дозволяє *GetUser* дії, то користувач із цією політикою може отримати інформацію про користувача з Консолі керування AWS, AWS CLI або AWS API. Коли ви створюєте користувача IAM, ви можете дозволити консольний або програмний доступ. Якщо доступ до консолі дозволено, користувач IAM може ввійти на

консоль за допомогою імені користувача та пароля. Або якщо програмний доступ дозволено, користувач може використовувати ключі доступу для роботи з CLI або API.

Розглянемо типи політик.

Для використання в AWS доступні наступні типи політики, перераховані в порядку від найбільш часто використовуваних до менш часто використовуваних. Щоб дізнатися більше, перегляньте розділи нижче для кожного типу політики [10].

Політики на основі ідентифікаційних даних – додадаються керовані та вбудовані політики до ідентифікаційних даних IAM (користувачів, груп, до яких належать користувачі, або ролей). Політики на основі ідентифікаційних даних надають дозволи для ідентифікації.

Політики на основі ресурсів – додаються вбудовані політики до ресурсів. Найпоширенішими прикладами політик на основі ресурсів є політики сегмента Amazon S3 і політики довіри ролей IAM. Політики на основі ресурсів надають дозволи принципалу, зазначеному в політиці. Принципали можуть бути в тому ж обліковому записі, що й ресурс, або в інших облікових записах [10].

Межі дозволів – використовується керована політика як межа дозволів для сутності IAM (користувача чи ролі). Ця політика визначає максимальні дозволи, які політика на основі ідентифікаційних даних може надати сутності, але не надає дозволів. Межі дозволів не визначають максимальні дозволи, які політика на основі ресурсів може надати об’єкту.

SCP організацій. Використовується політика керування службами AWS Organizations (SCP), щоб визначити максимальні дозволи для членів облікового запису організації чи організаційного підрозділу (OU). SCP обмежують дозволи, які політика на основі ідентифікаційних даних або політика на основі ресурсів надають сутностям (користувачам або ролям) в обліковому записі, але не надають дозволів [10].

Списки контролю доступу (ACL) – використовуються списки керування доступом, щоб контролювати, які принципали в інших облікових записах можуть

отримати доступ до ресурсу, до якого приєднано ACL. ACL подібні до політик на основі ресурсів, хоча це єдиний тип політики, який не використовує структуру документа політики JSON. ACL – це політики дозволів для кількох облікових записів, які надають дозволи вказаному принципалу. ACL не може надавати дозволи об’єктам в межах одного облікового запису [10].

Політики сеансу застосовуються, коли ви використовуєте AWS CLI або AWS API, щоб взяти на себе роль або як федеративний користувач. Політики сеансу обмежують дозволи, які надають сеансу політика на основі ідентичності ролі або користувача. Політики сеансу обмежують дозволи для створеного сеансу, але не надають дозволи.

Політики на основі ідентифікаційних даних – це документи політики дозволів JSON, які контролюють, які дії може виконувати особа (користувачі, групи користувачів і ролі), на яких ресурсах та за яких умов. Політику на основі ідентифікації можна додатково класифікувати:

керовані політики – окремі політики на основі ідентифікаційних даних, які можна приєднати до кількох користувачів, груп і ролей у своєму обліковому записі AWS. Існує два типи керованих політик:

керовані політики AWS – керовані політики, які створює та керує AWS;

політики, керовані клієнтом – керовані політики, які ви створюєте та керуєте у своєму обліковому записі AWS. Політики, керовані клієнтом, забезпечують більш точний контроль над вашими політиками, ніж політики AWS;

вбудовані політики – політики, які додаються безпосередньо до окремого користувача, групи чи ролі. Вбудовані політики підтримують строгі стосунки один на один між політикою та ідентифікатором. Вони видаляються, коли ви видаляєте ідентифікатор.

Політики на основі ресурсів – це документи політики JSON, які додаються до такого ресурсу, як сегмент Amazon S3. Ці політики надають зазначеному принципалу дозвіл виконувати певні дії над цим ресурсом і визначають, за яких умов це застосовується. Політики на основі ресурсів є вбудованими політиками. Немає політик на основі керованих ресурсів [10].

Щоб увімкнути доступ до кількох облікових записів, ви можете вказати весь обліковий запис або об’єкти IAM в іншому обліковому записі як основний у політиці на основі ресурсів. Додавання принципала для кількох облікових записів до політики на основі ресурсів – це лише половина встановлення довірчих відносин. Якщо принципал і ресурс знаходяться в окремих облікових записах AWS, ви також повинні використовувати політику на основі ідентифікації, щоб надати принципал доступ до ресурсу. Однак, якщо політика на основі ресурсів надає доступ до принципала в тому самому обліковому записі, додаткова політика на основі ідентифікації не потрібна [10].

Сервіс IAM підтримує лише один тип політики на основі ресурсів, яка називається політикою довіри ролі , який додається до ролі IAM. Роль IAM – це і ідентифікатор, і ресурс, який підтримує політику на основі ресурсів. З цієї причини до ролі IAM необхідно приєднати політику довіри та політику на основі ідентифікації. Політики довіри визначають, які основні об’єкти (облікові записи, користувачі, ролі та об’єднані користувачі) можуть взяти на себе цю роль [12].

Межа дозволів – це розширена функція, у якій встановлюється максимальні дозволи, які політика на основі ідентифікаційних даних може надати об’єкту IAM. Коли ви встановлюєте межі дозволів для об’єкта, об’єкт може виконувати лише ті дії, які дозволені як його політиками на основі ідентифікаційних даних, так і його межами дозволів. Політики на основі ресурсів, які визначають користувача або роль як принципала, не обмежені межами дозволів. Явна заборона в будь-якій із цих політик перекриває дозвіл [10].

Політики контролю послуг (SCP)/ AWS Organizations – це сервіс для групування облікових записів AWS, якими володіє ваша компанія, і централізованого керування ними. Якщо ви ввімкнете всі функції в організації, ви зможете застосувати політику керування послугами (SCP) до будь-якого або всіх своїх облікових записів. SCP – це політики JSON, які визначають максимальні дозволи для організації чи організаційного підрозділу (OU). SCP обмежує дозволи для об’єктів в облікових записах учасників, включаючи кожного користувача root облікового запису AWS. Явна заборона в будь-якій із цих політик перекриває

дозвіл [10].

Списки контролю доступу (ACL) – це політики служби, які дозволяють контролювати, які принципали в іншому обліковому записі можуть отримати доступ до ресурсу. ACL не можна використовувати для керування доступом для принципала в межах одного облікового запису. ACL подібні до політик на основі ресурсів, хоча це єдиний тип політики, який не використовує формат документа політики JSON. Amazon S3, AWS WAF і Amazon VPC є прикладами служб, які підтримують списки керування доступом.

Політики сеансу – це розширені політики, які ви передаєте як параметр, коли програмно створюєте тимчасовий сеанс для ролі або об'єднаного користувача. Дозволи для сеансу є перетином політик на основі ідентифікації для об'єкта IAM (користувача чи ролі), який використовується для створення сеансу, та політик сеансу. Дозволи також можуть виходити з політики на основі ресурсів. Явна заборона в будь-якій із цих політик перекриває дозвіл [10].

Ви можете створити сеанс ролі та передати політику сеансу програмно за допомогою операцій *AssumeRole*, *AssumeRoleWithSAML*, або *AssumeRoleWithWebIdentityAPI*. Ви можете передати один вбудований документ політики сеансу JSON за допомогою *Policy* параметра. За допомогою цього *PolicyArns* параметра можна вказати до 10 керованих політик сеансу.

Коли ви створюєте сеанс федеративного користувача, ви використовуєте ключі доступу користувача IAM для програмного виклику *GetFederationToken* операції API. Ви також повинні передати політику сеансу. Отримані дозволи сеансу є перетином політики на основі ідентифікації користувача IAM і політики сеансу.

Політика на основі ресурсів може вказувати ARN користувача або роль як принципала. У цьому випадку дозволи з політики на основі ресурсів додаються до політики на основі ролі або ідентифікації користувача перед створенням сеансу. Політика сеансу обмежує загальну кількість дозволів, наданих політикою на основі ресурсів і політикою на основі ідентифікаційних даних. Отримані дозволи сеансу є перетином політик сеансу та політики на основі ресурсів плюс перетин

політик сеансу та політик на основі ідентифікаційних даних (рис. 3.2).

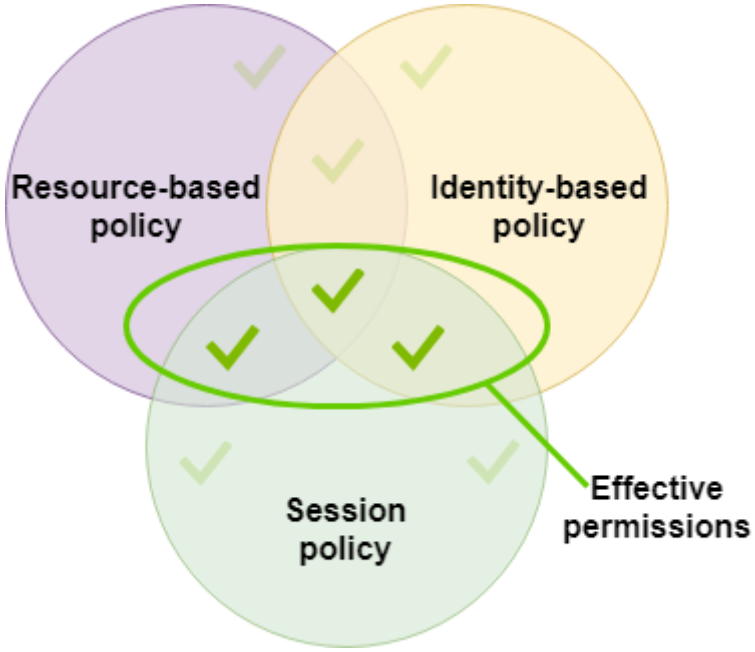

Рис. 3.2. Пояснення формування дозволу [10]

Політика на основі ресурсів може вказати ARN сеансу як принципала. У цьому випадку дозволи з політики на основі ресурсів додаються після створення сеансу. Дозволи політики на основі ресурсів не обмежені політикою сеансу. Отриманий сеанс має всі дозволи політики на основі ресурсів плюс перетин політики на основі ідентифікації та політики сеансу (рис. 3.3).

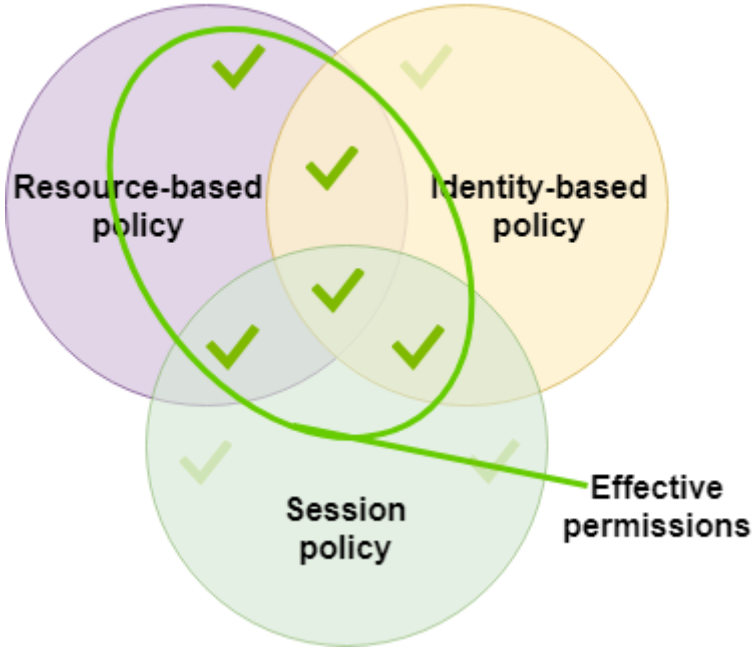

Рис. 3.3. Пояснення формування дозволу [10]

Межа дозволів може встановлювати максимальні дозволи для користувача або ролі, які використовуються для створення сеансу. У цьому випадку дозволи результуючого сеансу є перетином політики сеансу, межі дозволів і політики на основі ідентифікації. Однак межі дозволів не обмежують дозволи, надані політикою на основі ресурсів, яка визначає ARN результуючого сеансу (рис. 3.4).

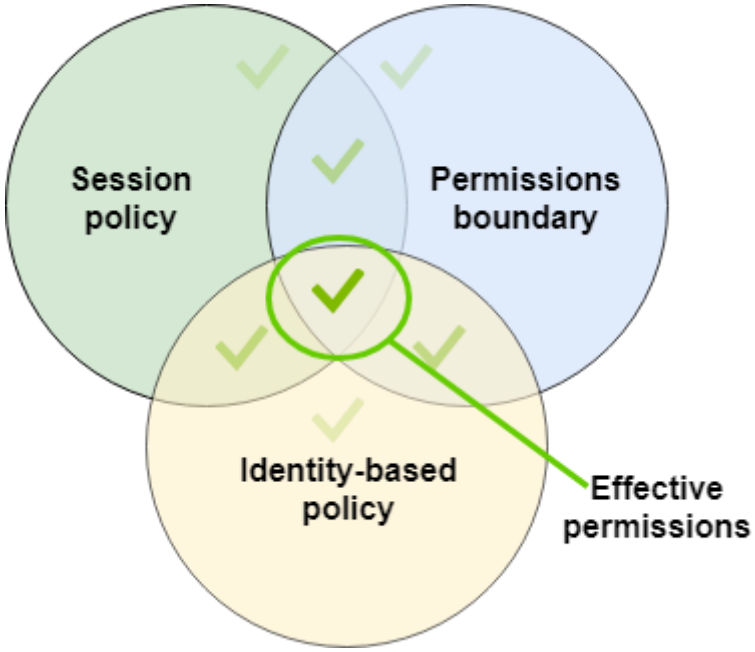

Рис. 3.4. Пояснення формування дозволу [10]

Розглянемо питання управління дозволами IAM.

AWS Identity and Access Management (IAM) забезпечує точне керування доступом, щоб допомогти вам встановити дозволи, які визначають, хто може отримати доступ до ресурсів AWS за яких умов. Необхідно використовувати детальний контроль доступу, щоб захистити ресурси AWS на шляху до досягнення найменших привілеїв [12].

Як це працює: в IAM ви визначаєте, хто може отримати доступ до ваших ресурсів AWS за допомогою політик. Ви додаєте політики до ролей IAM у своїх облікових записах AWS і до ресурсів AWS. Для кожного запиту до AWS IAM авторизує запит, порівнюючи його з вашими політиками, і дозволяє або відхиляє запит (рисунок 3.5).

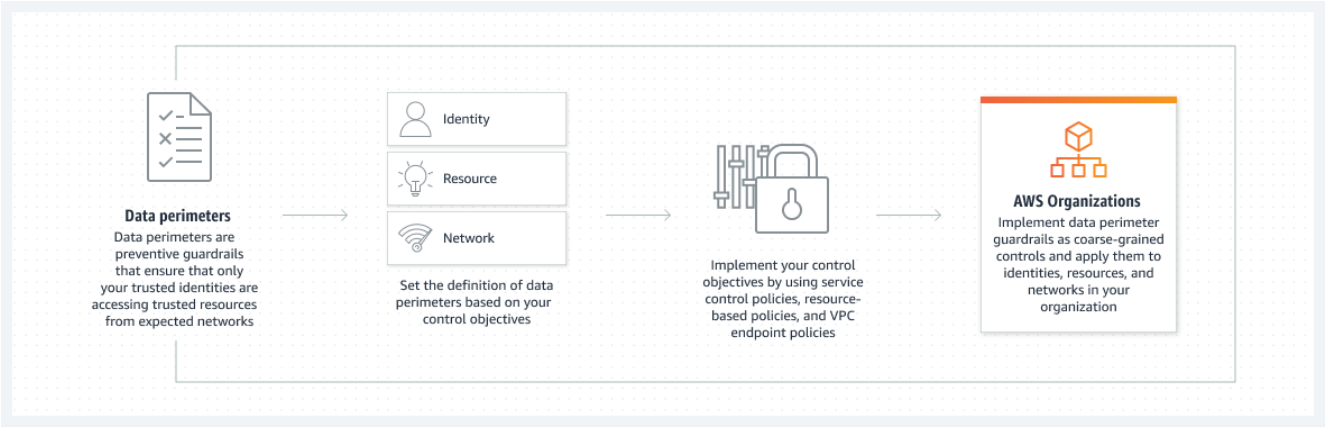

Рис. 3.5. Процес управління дозволами IAM [12]

Мова політики IAM: мова політики IAM, яка називається JSON, дозволяє вам детально виражати вимоги щодо доступу за допомогою дій, ресурсів і елементів умов у політиках.

Типи політик для надання доступу: IAM дає вам можливість додавати політики як до ваших ролей IAM, так і до ресурсів AWS, які підтримують політики на основі ресурсів. Політики на основі ідентифікації та політики на основі ресурсів працюють разом, щоб визначити контроль доступу.

Запобіжні огорожі: запобіжні огорожі допомагають встановити межі максимальних дозволів, доступних для ваших ролей IAM. Ви можете використовувати політики керування службами, межі дозволів і політики сеансу, щоб обмежити дозволи, які можна надати ролі IAM.

Керування доступом на основі атрибутів (ABAC). Використовуйте ABAC для визначення детальних дозволів на основі атрибутів, прикріплених до ролей IAM, наприклад відділів і посад. Надаючи доступ до окремих ресурсів на основі атрибутів, вам не доведеться оновлювати політики для кожного нового ресурсу, який ви додаєте в майбутньому.

3.3. Рекомендації щодо управління доступом користувачів до хмарних сервісів та ресурсів організації

У [13] відмічається, що збільшення як дистанційної роботи, так і зовнішніх

сховищ і послуг швидко розширило довіру до хмари. Хмарні середовища є цінними цілями для зловмисників. Оскільки організації продовжують переміщувати дані та послуги в ці середовища, зловмисники можуть скористатися перевагами загальнодоступних хмар доступу, які часто надають.

Керування ідентифікацією та доступом (IAM) має вирішальне значення для захисту хмарних ресурсів від зловмисників. Однак користувачі можуть легко неправильно налаштувати елементи керування доступом, щоб випадково дозволити відкритий доступ до ресурсів. Такі неправильні конфігурації є поширеними і призвели до масових витоків даних.

Початкові спроби зловмисного доступу до хмарних ресурсів часто спрямовані на облікові дані користувача. Наприклад, соціальна інженерія часто націлена на користувачів у спробі отримати облікові дані або змусити користувачів прийняти push-запити багатофакторної автентифікації (MFA). Зловмисники також можуть спробувати використати зовнішні облікові записи, яким надано доступ до орендаря організації.

Після того, як зловмисники скомпрометують цільове хмарне середовище, вони можуть спробувати надати собі ролі чи ключі або надати нові облікові записи для ескалації привілеїв, збереження або переміщення вбік, націлюючись на хмарні служби, які їх цікавлять, або намагаючись використовувати федеративні ідентифікаційні дані для доступу до жертви локальне середовище.

Управління ідентифікацією

Доступ до облікового запису на основі однофакторної автентифікації (наприклад, лише за паролем або PIN кодом) чутливий до викрадення облікових даних, підробки та повторного використання в кількох системах. Хмарні облікові записи, як правило, доступні у всьому світі, тому вони більш сприйнятливі до певних типів недоліків однофакторної автентифікації.

Багатофакторна автентифікація (MFA) підвищує безпеку облікового запису, краще протистоїть компрометації за рахунок покращення перевірки користувача методи. MFA вимагає двох або більше факторів для входу: те, що користувач знає, має або є. Як правило, це реалізується за допомогою пароля та

другого фактора, який зазвичай базується на випадково введеному числовому маркері, біометричному параметрі (наприклад, відбиток пальця чи розпізнавання обличчя) або фізичному маркері (унікальний апаратний ідентифікатор: смарт-карта, картка загального доступу, тощо).

Багато типів MFA сприйнятливі до методів фішингу. Якщо це можливо, організації повинні використовувати стійкі до фішингу методи MFA, такі як автентифікація Fast Identity Online (FIDO)/WebAuthn на основі відкритих ключів (PK) або MFA на основі інфраструктури відкритих ключів (PKI) (наприклад, картки CAC/PIV).

Стійкий до фішингу MFA зазвичай використовує закритий ключ, прив'язаний до апаратного забезпечення. Якщо пристрій/токен дозволяє експортувати приватний ключ, це впливає на надійність фактора автентифікації, оскільки користувач може експортувати приватний ключ, який потім може бути спільний або іншим чином скомпрометований у разі неправильного поводження.

Організації, які використовують сторонні інструменти MFA, повинні знати про зміни, пов'язані з безпекою, у вибраних інструментах MFA, особливо зміни, які можуть дозволити експортувати ключі.

Керування сертифікатами PKI

Сертифікати можна використовувати в хмарних середовищах різними способами. Два поширені типи сертифікатів PKI, які використовуються в хмарних середовищах, – це клієнтські сертифікати та сертифікати безпеки транспортного рівня (TLS) на стороні сервера.

Клієнтські сертифікати можна використовувати для автентифікації користувачів у хмарній службі (окремо або як частину рішення MFA) або для автентифікації неособових об'єктів (так відомих як «ідентифікатори робочого навантаження» або «ідентифікатори служб») в інших системах. Оскільки організації все частіше розгортають робочі навантаження в хмарі, сертифікатами TLS для цих додатків потрібно належним чином керувати. Належне керування включає безпечне зберігання ключів і періодичну ротацію ключів, а також впровадження відкликання ключів.

Організації, які використовують сертифікати PKI для автентифікації користувачів, повинні підтримувати список довірених центрів сертифікації, дозволяти лише надійні сертифікати, документувати відкликані сертифікати, видаляти користувачів і блокувати доступ, пов’язаний із відкликаними сертифікатами.

Під час розміщення робочих навантажень у хмарі важливо безпечно керувати сертифікатами сервера TLS, які використовуються для захисту веб-зв’язку, і будь-якими клієнтськими сертифікатами, які використовуються для автентифікації між робочими навантаженнями. Деякі хмарні служби автоматично керуватимуть сертифікатами для клієнта, але деякі розгортання використовують сертифікати, якими керує клієнт.

Організаціям, які використовують сервери додатків, якими керує клієнт, слід утримуватися від зберігання закритих ключів у вигляді звичайного тексту на віртуальному екземплярі, на якому розміщено сервер. Натомість сертифікатами слід керувати за допомогою системи керування ключами (KMS), яка функціонує для зберігання зашифрованих ключів, а також контролю та моніторингу доступу до ключів. Системи керування ключами можуть розшифрувати збережені ключі в пам’яті для використання для надання доступу за потреби. Ключі також слід регулярно міняти через автоматичні механізми. Неправильне використання сертифікатів послаблює захист і знижує цілісність системи.

Рекомендації щодо облікових даних

Неправильна конфігурація та неправильне поводження можуть наражати облікові дані користувача на зловживання. Облікові дані хмари ніколи не слід зберігати у вигляді звичайного тексту. За потреби користувачі можуть використовувати інструменти керування секретами (бажано ті, які використовують можливості апаратного модуля безпеки (HSM) для захисту секретних ключів) для керування хмарними обліковими даними (наприклад, менеджери паролів для людських секретів або секретні сховища для облікових даних робочого навантаження). Для подальшого зниження ризику користувачі повинні вимкнути функції, які дозволяють веб-сайтам або додаткам

запам’ятовувати паролі. MFA, як-от одноразові маркери PIN-коду, маркери PKI або смарт-картки, для користувачів і автентифікацію на основі PKI (для робочих навантажень), де це можливо, слід запроваджувати.

У ситуаціях, коли автентифікація на основі PKI технічно неможлива, секретні ключі можуть бути згенеровані, щоб дозволити програмам програмно керувати ресурсами хмари. Під час видачі ключів для додатків, яким потрібно взаємодіяти з хмарою, важливо, щоб вони оброблялися належним чином, оскільки зловмисники розглядають їх як цінні цілі.

Кожен постачальник хмарних послуг (CSP) пропонує різні варіанти отримання цих облікових даних і керування ними, тому найкраще періодично переглядати їхні вказівки. Загалом, найкраще уникати створення ключів із правами root або адміністративними привілеями. Ці ключі слід генерувати лише для короткочасного використання обліковим записам повинні бути надані найменші необхідні привілеї, необхідні для виконання оперативних завдань. Ці облікові дані ніколи не слід включати у звичайний текст у вихідний код програми або вбудовувати у двійкові файли. Натомість їх має безпечно обробляти менеджер секретів і зберігати в зашифрованому вигляді. Якщо для підключення до віртуальних машин, розміщених у хмарі, використовуються пари ключів безпечної оболонки (SSH), приватний ключ слід зберігати в диспетчері секретів і не можна поширювати.

Організаціям слід вимагати від адміністраторів підключатися до хмарних ресурсів за допомогою робочих станцій із привілейованим доступом (PAW), які мають бути захищені відповідно до встановлених передових практик, вимагати MFA та виконувати ретельне журналювання. Адміністраторам часто потрібен доступ до хмарних ресурсів через такі протоколи, як SSH, які не завжди підтримують ці елементи керування. Організаціям легше контролювати PAW, належним чином загартовувати та контролювати. PAW можуть застосовувати MFA для всіх дій адміністратора, навіть якщо протокол його не підтримує, і спрощують аудит дій адміністратора. Це спрощує захист і реєстрацію на робочих станціях, ніж на некерованих пристроях. Деякі CSP пропонують PAW як послугу,

щоб полегшити впровадження цієї функції безпеки.

Федерація ідентичності

Організації, які працюють у хмарних середовищах, зазвичай об’єднують ідентифікатори для спрощення керування ідентифікаціями в різних середовищах. Системи, які об’єднують ідентифікаційні дані від локальних до хмарних середовищ, часто націлені на зловмисники, щоб забезпечити переміщення між середовищами.

Захист і моніторинг серверів об’єднання ідентифікаційних даних має вирішальне значення для загальної безпеки. Системи виявлення кінцевих точок і реагування повинні використовуватися на серверах об’єднання ідентифікаційних даних для виявлення спроб використання, а зміни повинні регулярно перевірятися для виявлення потенційної компрометації.

Необхідно захищати сертифікати та ключі, які використовуються для федерації ідентифікації, за допомогою апаратного модуля безпеки (HSM). Організації також повинні впроваджувати принципи сегментації мережі, щоб максимально ізолювати ці чутливі сервери.

Керування доступом

Управління умовним контекстним доступом

Хоча безпечні паролі, маркери входу та MFA корисні для захисту облікових записів користувачів, зловмисники все одно можуть скомпрометувати облікові дані користувача.

Одним із способів обмежити вплив таких компромісів є впровадження політик для забезпечення умовного доступу на основі додаткового контексту. Цей контекст виражається в політиках, які часто можуть бути встановлені для хмарних орендарів, щоб обмежити можливість користувача входити в систему, якщо попередньо визначений набір умов не виконується. Наприклад, відмова від спроб входу з-за меж дозволеного географічного розташування на основі їхніх адрес Інтернет-протоколу (IP). Ці елементи керування можуть бути особливо корисними для захисту привілейованих облікових записів або облікових записів із широким/конфіденційним доступом, вимагаючи від адміністраторів входу в ці

облікові записи з локального об’єкта організації.

Організації повинні ретельно переглянути та перевірити свої конфігурації умовного доступу та застосування, щоб запобігти використанню просунутими зловмисниками прогалин у цих політиках.

Зашифровані канали доступу до ресурсів

Контроль доступу важливий під час зберігання хмарних даних. Несанкціонований доступ може погіршити загальну безпеку та негативно вплинути на роботу.

Необхідно призначати дозволи відповідно до потреб авторизованого користувача для доступу до рівня даних, необхідних для виконання завдання. Постійно перевіряйте призначення доступу та адміністративних привілеїв, щоб переконатися, що вони відповідають принципу найменших привілеїв. Необхідно увімкнути моніторинг і журналювання запитів на доступ і змін політики. Необхідно досліджувати аномальну активність і запити. Необхідно шифрувати дані в стані спокою та під час передачі, безпечно зберігаючи та керуючи криптографічними ключами. Використовуйте захищені протоколи, такі як TLS1.2 або вище, використовуючи алгоритми з Commercial National Security Algorithm (CNSA) Suite 2.0, коли це можливо, і CNSA Suite 1.0 як мінімум для підключення клієнтів до хмарних ресурсів.

Розподіл обов'язків

Розподіл обов’язків є важливою концепцією, коли йдеться про захист хмарних ресурсів. NIST визначає розподіл обов’язків як «принцип, згідно з яким жодному користувачеві не повинно бути надано достатніх привілеїв для самостійного використання системи неправильно».

Одним із способів цього можна досягти, вимагаючи керування двома особами для виконання особливо чутливих операцій.

Інший метод полягає в розподілі ролей адміністратора для контролю доступу до ресурсів і керування ними. Наприклад, адміністратори керування доступом KMS з необхідними привілеями для надання доступу до ключів, що захищають конфіденційні дані або можливості, не повинні мати можливість

надавати собі доступ для використання цих виданих ключів. Хоча в деяких випадках користувачі повинні мати можливість створювати власні ключі шифрування, керувати ними та використовувати їх, це важливий метод підвищення безпеки конфіденційних організаційних даних.

Крім того, слід обмежити доступ для запису до резервних копій, щоб допомогти протистояти тактиці, методам і процедурам програм-вимагачів (TTP), які використовуються зловмисники для цільового резервного копіювання даних. Один із способів зменшити ризик порушення безпеки даних у хмарному середовищі – створити окремі облікові записи керування резервним копіюванням для адміністраторів, яким потрібен доступ до резервних копій. Ці запобіжні заходи обмежують вплив, який може зробити учасник внутрішньої загрози або зловмисники, який має облікові дані доступу, у скомпрометованому хмарному середовищі.

Захист даних користувачів

Пристрої користувачів є звичайним вектором атаки для зловмисників, щоб отримати доступ до хмарного середовища організації. Користувачам хмарних технологій важливо дотримуватися правил кібергігієни щодо пристроїв, які вони використовують для доступу до хмарних ресурсів. Користувачі повинні:

оновлювати та виправляти ОС і додатки;

утримуватися від відкриття електронних листів і веб-посилань від невідомих сторін, щоб мінімізувати можливості;

не сприяти фішингу та зараження шкідливим програмним забезпеченням.

Змінюйте та видаляйте параметри за замовчуванням (наприклад, паролі за замовчуванням і облікові записи користувачів за замовчуванням). Відстежуйте облікові записи на наявність незрозумілих дій. Перевірте URL-адреси, щоб перевірити наявність змінених URL-адрес, призначених для переспрямування користувачів на підроблені веб-сайти.

Розгляньте ризики та переваги дозволу користувачам отримувати доступ до хмарних ресурсів із некерованих пристроїв, наприклад із власного пристрою чи персонального комп’ютера.

Контроль привілеїв

Неналежним чином обмежений доступ користувачів і програм може призвести до надмірного розкриття конфіденційних даних і сприяти зловмисному переміщенню через хмару.

Необхідно дотримуватися принципу найменших привілеїв і обмежувати облікові записи лише ресурсами, необхідними для виконання функцій місії. Надаючи привілеї, пам’ятайте, що багато постачальників хмарних технологій використовують ієрархічні схеми дозволів, тому надання користувачу або групі привілейованого доступу до ресурсу надасть їм однаковий рівень доступу до вкладених ресурсів, тобто надання доступу до «Папки» або «Організаційний підрозділ» надає доступ до всіх ресурсів цього підрозділу.

Різні постачальники та служби хмари можуть пропонувати різні методи контролю доступу. Найпоширеніші методи: контроль доступу на основі ролей (RBAC) і контроль доступу на основі атрибутів (ABAC). Більшість CSP пропонують гібрид двох підходів, доповнюючи ролі умовами на основі атрибутів для забезпечення умовного доступу.

За допомогою RBAC організації можуть призначати привілеї ролям, а потім призначати користувачам роль або ролі, надаючи їм відповідні привілеї. Коли привілеї, призначені для ролі, змінюються, оновлення впливає на всіх, кому призначено цю роль.

ABAC є ключовим елементом нульової довіри (Zero Trust) у стовпі ідентифікації/користувача. Цей метод використовується для керування доступом до даних шляхом призначення атрибутів ресурсам і користувачам, забезпечуючи більш точний захист ресурсів політикою, ніж використання лише політик RBAC.

Один із способів керування корпоративними дозволами та виявлення дрейфу – це кодифікація дозволів. Цей підхід, відомий як «політика як код», корисний для керування дозволами на підприємстві, оскільки його можна використовувати для створення завідомо доброго стану налаштувань дозволів, його можна перевіряти та контролювати версії, а також можна використовувати для виявлення дрейфу.

Необхідно розглядати можливість впровадження практики безпеки Just-in-Time (JIT), коли розширений привілейований доступ до програм або системи обмежується заздалегідь визначеними періодами для визначені види діяльності. Підвищення привілеїв за допомогою JIT має реєструватися та може вимагати виправдання, якщо потрібно, для кращого відстеження та перевірки запитів на привілеї. Нарешті, уникайте використання привілейованих облікових записів для повсякденної діяльності, натомість використовуйте привілейований обліковий запис лише для обслуговування, оновлень, операцій керування обліковими записами, операцій пошуку загроз тощо, для яких потрібен привілейований доступ.

Періодично перевіряйте конфігурації IAM, щоб підтвердити, що користувачам надано лише необхідні привілеї. Багато CSP пропонують послуги, які відстежуватимуть невикористані привілеї, щоб допомогти адміністраторам адаптувати облікові записи до найменших привілеїв, необхідних користувачам для виконання своїх повсякденних обов’язків. Однак важливо враховувати випадковий або надзвичайний («розбити скло») доступ під час видалення, здавалося б, невикористаних дозволів.

Захист служби метаданих хмарного екземпляра Службу метаданих хмарного екземпляра (IMDS) можна запитувати у віртуальних екземплярів у хмарі для отримання загальної інформації про клієнта. Однак цю послугу також можна використовувати для отримання різноманітної інформації, включаючи облікові дані IAM, які зловмисники можуть використовувати для отримання додаткового доступу до хмарного клієнта.

Точна реалізація хмарної IMDS залежить від CSP. Як правило, зловмисники запитують IMDS, використовуючи вразливість підробки запитів на стороні сервера (SSRF) у програмі, яку організації-клієнти обслуговують публічно, з примірника, що працює в хмарі та має доступ до IMDS.

Використовуйте усталені найкращі практики для захисту додатків, як-от дезінфекція введених користувачами та розгортання брандмауерів веб-додатків. Ці методи можуть завадити методам SSRF, які можуть використовувати програму

для запиту IMDS і повернення облікових даних зловмиснику. Використовуйте найновішу доступну версію IMDS, оскільки вона може запровадити додаткові заходи безпеки. Обмежте доступ до IMDS для екземплярів або облікових записів, яким це не потрібно. IMDS кожного CSP може працювати дещо інакше; отже, важливо переглянути рекомендації постачальника щодо передової практики щодо їх IMDS, щоб вжити всіх можливих запобіжних заходів для запобігання неправильному використанню послуги.

Кращі практики

Для організацій, які працюють у хмарі, важливо переконатися, що співробітники розуміють ризики, які виникають через неправильне керування ідентифікацією та доступом. Щоб зменшити ризик інциденту кібербезпеки, організації повинні дотримуватися таких передових практик:

щодо керування ідентифікацією:

вимагати використання стійкого до фішингу MFA для облікових записів користувачів;

не зберігайте сертифікати TLS сервера у вигляді звичайного тексту на віртуальному екземплярі, на якому розміщено веб-сервер; натомість використовуйте менеджер секретів;

обережно поводьтеся з сертифікатами користувача PKI, щоб запобігти несанкціонованому збиранню, і негайно відкликайте скомпрометовані або непотрібні сертифікати;

використовуйте секретні ключі лише тоді, коли це необхідно, і надавайте їх для короткострокового доступу з найменшими необхідними привілеями.

захистить сервери федерації ідентифікації та перевірте федерацію ідентифікації, щоб виявити спроби зловмисників зловживати довірчими відносинами.

щодо керування доступом:

використовуйте політики керування доступом на основі контексту та переглядайте політики перед розгортанням і періодично після розгортання, щоб виявити потенційні прогалини. Подумайте над тим, щоб адміністратори мали

доступ до хмарних ресурсів за допомогою PAW. Обмежте використання адміністративних облікових записів і використовуйте JIT, щоб обмежити привілейований доступ і покращити відстеження привілейованих дій в орендарі;

підключайтеся до хмарних ресурсів через зашифрований канал за допомогою безпечних протоколів, таких як TLS 1.2 або новішої версії, і схвалених CNSA наборів шифрів (бажано CNSA Suite 2.0);

призначайте привілеї відповідно до найкращих практик контролю доступу, ретельно застосовуючи принципи розподілу обов’язків і найменших привілеїв, а також перевіряйте призначення привілеїв і запити на доступ;

розгляньте можливість використання політики як коду, щоб забезпечити покращене відстеження та перегляд політик керування доступом, і часто перевіряйте на дрейф;

захистить хмарну IMDS, обмеживши користувачів/сервіси з привілеями надсилати запити до IMDS, використовуючи найновішу версію, запровадивши найкращі практики постачальників і запровадивши найкращі практики для захисту програм, розміщених у хмарі, і запобігання вразливостям SSRF.

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми управління доступом користувачів до хмарних сервісів та ресурсів організації як складової частини забезпечення кібербезпеки її інформаційної системи, встановлена сутність завдань управління доступом.

Amazon Web Services (AWS) – це найпоширеніша у світі хмарна платформа з найширшими можливостями, що надає понад 200 повнофункціональних сервісів для центрів обробки даних. Тому, AWS широко застосовується у сучасних організаціях. Даний момент визначає необхідність централізованого управління доступом користувачів до хмарних сервісів та ресурсів організації.

Проаналізовано існуючі технології управління доступом користувачів до хмарних сервісів та ресурсів організації. Досліджена технологія управління доступом користувачів до хмарних сервісів та ресурсів організації на прикладі Amazon Web Services.

Визначено методи та засоби управління доступом користувачів до хмарних сервісів та ресурсів Amazon Web Services. Встановлено основні функції та принципи роботи сервісу AWS IAM. AWS IAM забезпечує точний контроль доступу у всіх сервісах AWS. За допомогою IAM надається доступ до певних сервісів та ресурсів за відповідними умовами. Завдяки політикам IAM здійснюється управління дозволами для співробітників та систем, надаючи дозволи з найменшими привілеями. Використовуючи політики IAM, надається доступ до певних API сервісів та ресурсів AWS. Також визначаються конкретні умови для надання доступу, наприклад, певна організація AWS або використання певного сервісу AWS.

Визначена сутність моделі управління доступом користувачів на основі атрибутів в AWS IAM. Управління доступом на основі атрибутів (ABAC) – це стратегія авторизації для створення деталізованих дозволів на базі атрибутів користувача, таких як відділ, робоча роль і назва команди. За допомогою ABAC

можна скоротити кількість дозволів, необхідних для точного керування обліковим записом AWS.

Досліджено призначення, можливості та функції централізованого управління доступом до облікових записів та додатків AWS Single Sign-On. Даний сервіс забезпечує створення або підключення посвідчення співробітників і централізовано керуєте доступом всієї організації до AWS. Контролюється як доступ тільки до своїх облікових записів AWS, так і до хмарних додатків. AWS Single Sign-On – це єдиний адміністративний інтерфейс для точного визначення, налаштування та надання доступу. Корпоративні користувачі отримують портал користувача для доступу до всіх призначених облікових записів AWS або хмарних додатків.

У роботі запропоновано порядок розгортання та застосування технології управління доступом користувачів до хмарних сервісів та ресурсів на прикладі рішення AWS IAM. Розроблено рекомендації фахівцям з кібербезпеки щодо застосування технології управління доступом користувачів до хмарних сервісів та ресурсів організації.

Таким чином, правильна реалізація технології управління доступом користувачів до хмарних сервісів та ресурсів організації як складової частини забезпечення кібербезпеки її інформаційної системи, має забезпечити ефективний захист корпоративних даних та кібербезпеку інформаційної системи організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Ірина Онен. Що таке хмарні сервіси та їх переваги для бізнес-сфери. mcCloud, 25.04.2024 URL: https://mccloud.ua/shcho-take-khmarni-servisy/

2. 2024 Cloud Security Report. Cybersecurity Insiders. URL: https://www.isc2.org/-/media/5C011B9E35624F309CB4D00EA1A22FED.ashx

3. Top 15 Cloud Security Issues, Threats and Concerns. Check Point. URL: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/

4. The Definitive Guide to Identity and Access Management (IAM). Strongdm. URL: https://www.strongdm.com/ebooks/identity-and-access-management-ebook

5. Team Ciente. Identity and Access Management (IAM) in Cloud Computing. Jan 19, 2024. URL: https://medium.com/@ciente/identity-and-access-management-iam-in-cloud-computing-2777481525a4

6. Інтеграція хмарних сервісів у ваші веб-додатки: можливості та переваги. REDSTONE, 2024. URL: https://redstone.agency/blog/intehratsiia-khmarnykh-servisiv-u-vashi-veb-dodatky-mozhlyvosti-ta-perevahy/

7. Understanding Key Identity and Access Management Components. Braxton-Grant Technologies. URL: https://braxtongrant.com/understanding-key-identity-and-access-management-components/

8. AWS, Azure and GCP: The Ultimate IAM Comparison. Team Tenable. URL: https://www.tenable.com/blog/aws-azure-and-gcp-the-ultimate-iam-comparison

9. What is AWS? Complete Guide to Amazon Web Services. GoGeekz. URL: https://gogeekz.com/what-is-aws-complete-guide-to-amazon-web-services/

10. AWS Identity and Access Management. User Guide. 2024. URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/iam-ug.pdf

11. What is SSO (Single-Sign-On)? AWS. URL: https://aws.amazon.com/what-is/sso/

12. IAM Fine-Grained Access Control. AWS. URL:

https://aws.amazon.com/iam/features/manage-permissions/?nc1=h_ls

13. Use Secure Cloud Identity and Access Management Practices. NSA & CISA, March 2024 Ver. 1.0. URL: https://www.cisa.gov/news-events/alerts/2024/03/07/cisa-and-nsa-release-cybersecurity-information-sheets-cloud-security-best-practices

14. Скрицький Марк Єрвандович. Технологія управління доступом користувачів до сервісів та ресурсів Amazon Web Services. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». Державний університет інформаційно-комунікаційних технологій. 25 жовтня 2024. Тези доповідей. С. 157-160. https://duikt.edu.ua/uploads/p_2661_48963150.pdf

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)