Лахно В.А., Мамченко С.М., Криворучко О.В.

БЕЗПЕКА ІНФРАСТРУКТУРИ ХМАРНИХ ОБЧИСЛЕНЬ

НАВЧАЛЬНИЙ ПОСІБНИК

Київ
2025

УДК 04.056.5
Г 96

Рекомендовано до друку Вченою радою Національного університету біоресурсів і природокористування України (протокол __ від _____р.)

Рецензенти:

Остапов Сергій Едуардович, доктор фізико-математичних наук, професор, професор кафедри програмного забезпечення комп'ютерних систем Чернівецького національного університету імені Ю. Федьковича.

Зінченко Ольга Валеріївна, доктор технічних наук, завідувач кафедри штучного інтелекту Державного університету інформаційно-комунікаційних технологій.

Цюцюра Микола Ігорович, доктор технічних наук, професор, професор кафедри комп'ютерних наук НУБіП України.

Г 96 БЕЗПЕКА ІНФРАСТРУКТУРИ ХМАРНИХ ОБЧИСЛЕНЬ: Посібник для студентів ЗВО/ В.А. Лахно, С.М. Мамченко, О.В. Криворучко // - К.: НУБіП України, 2025.- 270 с.

ISBN

Посібник «Безпека інфраструктури хмарних обчислень» знайомить із принципами роботи сучасних хмарних сервісів та підходами до їх безпечного використання. Розглянуто моделі хмар, управління доступом, шифрування, моніторинг і реагування на інциденти. Подано практичні рекомендації щодо роботи з AWS, Azure та GCP, а також побудови гібридних і багатохмарних рішень. Посібник буде корисний для здобувачів освіти, викладачів та фахівців ІТ-сфери, зокрема спеціальностей *F5 «Кібербезпека та захист інформації», F7 «Комп'ютерна інженерія.*

УДК 04.056.5

ISBN

ВІДОМОСТІ ПРО АВТОРІВ

Лахно Валерій Анатолійович

Доктор технічних наук, професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки Національного університету біоресурсів і природокористування України, Україна. Викладає дисципліни: Інтелектуальний аналіз даних, Моделювання комп'ютерних систем, Технології побудови захищених комп'ютерних систем, Методологія організації наукових досліджень з основами інтелектуальної власності, Інтелектуальний аналіз даних.

Коло наукових інтересів: математичне моделювання, безпека комп'ютерних систем та мереж, а також розпізнавання вторгнень.

✉: lva964@nubip.edu.ua

Мамченко Сергій Миколайович

Доктор педагогічних наук, професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки Національного університету біоресурсів і природокористування України, Україна. Викладає дисципліни: Безпека інформації і інформаційно-комінікаційних системах, Адміністрування комп'ютерних мереж, Ризики інформаційної безпеки, Технології адміністрування та експлуатація захищених ІКС.

Коло наукових інтересів: інформаційна безпека, кібербезпека, теорія систем, системний аналіз.

Автор понад 80 наукових праць, у тому числі 3 монографій, 3 підручників та 8 навчальних посібників.

✉: s.mamchenko@nubip.edu.ua

Криворучко Олена Володимирівна

Доктор технічних наук, професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки Національного університету біоресурсів і природокористування України, Україна. Доктор технічних наук, професор. Викладає дисципліни: Управління проектами розробки систем захисту інформації, Інтелектуальні системи, Державні та міжнародні вимоги з кібербезпеки, Методологія організації наукових досліджень з основами інтелектуальної власності.

Коло наукових інтересів: управління проєктами, Product IT, Project IT, інформаційні технології, інтелектуальні системи, захист інформації, інформаційна безпека, аудит інформаційних систем, менеджмент проєктів програмного забезпечення, якість та стандартизація програмного забезпечення

✉: o.kryvoruchko@nubip.edu.ua

Зміст

ПЕРЕДМОВА

Наразі, цифровізація стала невід'ємною частиною майже всіх сфер суспільства: від освіти й науки до бізнесу, від медицини та державного управління, від виробництва дронів до сфер сільського господарства. Головне місце в цьому процесі займають хмарні сервіси та технології, що забезпечують масштабованість, зручність доступу до ресурсів і ефективність використання інформаційних систем. Але розвиток хмарних платформ висуває одне з найважливіших питань - захист даних та безпека інфраструктури.

Потенційні загрози, пов'язані з витоком конфіденційних даних, порушенням цілісності інформації, несанкціонованим доступом та іншими видами кіберінцидентів, обумовлюють потребу у системному підході до побудови та реалізації засобів захисту хмарних сервісів та технологій. Особливої актуальності ці питання набувають у контексті глобалізації кіберпростору та зростання масштабів і складності кібератак.

Слід зазначити, що хмарні сервіси стають привабливою ціллю для кіберзлочинців. Витоки конфіденційної інформації, атаки на віртуальні машини та сховища, порушення правил автентифікації чи управління доступом -лише частина ризиків, із якими стикаються організації та окремі користувачі. У глобальному масштабі кіберзагрози набувають дедалі більшої складності, а масштаби атак можуть завдавати значних економічних та репутаційних втрат.

Питання безпеки хмарних сервісів та технологій нараз є не лише технічним викликом, а й ключовим елементом стратегії розвитку будь-якої IT-інфраструктури. Для України ця тема має особливе значення, адже цифрові рішення активно впроваджуються у сфері державних послуг (наприклад, «Дія»), у бізнесі та в освіті. Водночас в умовах воєнної агресії посилюється актуальність кіберзахисту як критично важливого елементу національної безпеки.

Метою даного посібника є систематизоване подання знань і практичних рекомендацій щодо налаштування захисту хмарних сервісів і технологій. Він орієнтований на студентів закладів вищої освіти, які готуються стати фахівцями у сфері кібербезпеки, інформаційних технологій, комп'ютерних наук та суміжних напрямів.

У структурі посібника логічно вибудувана послідовність матеріалу:

Структура посібника побудована за принципом поступового ускладнення матеріалу:

- ***Розділ 1 Захист інфраструктури хмарних сервісів*** - присвячено питанням захисту інфраструктури хмарних сервісів, зокрема безпеці обчислювальних послуг, сховищ даних і мережевих компонентів.
- ***Розділ 2. Глибинне занурення в IAM, аудит, та шифрування*** - розкриває особливості впровадження систем управління ідентифікацією та доступом (IAM), організації аудиту й моніторингу хмарних середовищ, а також застосування сучасних криптографічних механізмів.

- ***Розділ 3. Управління загрозами та дотримання вимог*** - аналізує характерні загрози хмарним обчисленням, шляхи забезпечення відповідності нормативним вимогам і специфіку взаємодії з постачальниками послуг.
- ***Розділ 4. Розширене використання хмарних сервісів*** - акцентує увагу на розширених аспектах експлуатації хмарних сервісів, включно з управлінням гібридними та багатохмарними середовищами, а також забезпеченням безпеки у масштабованих інфраструктурах.

Посібник поєднує як теоретичні засади, так і практичні інструменти, необхідні для ефективного захисту хмарних сервісів. Його використання сприятиме формуванню у студентів цілісного розуміння архітектури безпеки та навичок, що відповідають сучасним вимогам ІТ-ринку.

Завдяки матеріалам цього керівництва майбутні фахівці отримають можливість:

- опанувати принципи побудови надійної хмарної інфраструктури;
- навчитися впроваджувати стратегії ідентифікації та контролю доступу;
- засвоїти методи моніторингу, аудиту та виявлення загроз;
- зрозуміти особливості нормативного регулювання та взаємодії з провайдерами;
- набути практичних компетентностей для роботи з гібридними й багатохмарними рішеннями.

Посібник покликаний стати базовим довідником і практичним інструментом для студентів, викладачів та всіх, хто цікавиться питаннями безпеки хмарних сервісів та технологій. Він не лише систематизує знання, а й стимулює критичне мислення, формуючи у читачів готовність до реальних викликів у сфері кіберзахисту. Його матеріали сприятимуть підвищенню рівня професійної підготовки майбутніх фахівців та формуванню здатності ефективно діяти в умовах сучасного кіберпростору.

Частка внеску кожного з авторів рівномірна, а саме: Лахно В.А. – розділ 1 та частково розділ 3 , Криворучко О.В. – розділ 2 та частково розділ 1 і 3, Мамченко С.М. – розділ 4 та частково розділ 3.

РОЗДІЛ 1. ЗАХИСТ ІНФРАСТРУКТУРИ ХМАРНИХ СЕРВІСІВ

Після завершення цієї частини ви матимете чітке розуміння того, як захистити основні структурні блоки хмарних сервісів (моделі розгортання та обслуговування в хмарі, обчислення, сховище та мережу).

Ця частина посібника складається з наступних параграфів:

- *1.1. Вступ до хмарної безпеки*
- *1.2. Захист обчислювальних послуг*
- *1. 3. Забезпечення безпеки послуг зберігання даних*
- *1.4. Захист мережевих сервісів*

1.1. Вступ до хмарної безпеки

Світ IT постійно змінюється. Протягом десятиліть підприємства/організації мали придбати фізичне обладнання, встановлювали операційні системи та розгортали програмне забезпечення. Ця рутинна робота вимагала значного постійного обслуговування (розгортання виправлень, резервного копіювання, моніторингу тощо).

Хмара запровадила нову парадигму - тобто можливість використовувати керовані сервіси для досягнення тієї ж мети - запуску програмного забезпечення (від файлових серверів до планування ресурсів підприємства (ERP) або управління взаємовідносинами з клієнтами (CRM) продукти), використовуючи при цьому досвід постачальників гіпермасштабних хмарних послуг.

До відомих випадки використання хмарних обчислень належать наступні:
Нетфлікс - один з найбільших у світі сервісів потокового відео. Він використовує AWS для роботи своїх сервісів потокового медіа.
Мерседес-Бенц - один з найвідоміших автомобільних брендів. Він використовує Azure для проведення своїх досліджень та розробок.
Home Depot - найбільший роздрібний продавець товарів для дому в Сполучених Штатах. Він використовує Google Cloud для роботи своїх інтернет-магазинів.

Слід порівняти різні аспекти хмарних обчислень (від фундаментальних послуг, таких як обчислення, зберігання даних та мережеві технології, до управління відповідністю вимогам та найкращих практик для створення та підтримки великомасштабних середовищ безпечним способом), одночасно розглядаючи різні альтернативи, що загалом пропонуються: Веб-сервіси, Amazon (AWS), Microsoft Azure, та Хмарна платформа Google (GCP).

Не має значення розглядаємо яке підприємство, якої форми власності та напрямку діяльності необхідно розуміти яким чином досягти безпеки в будь-якому з великих постачальників гіпермасштабних хмарних послуг.

Потрібно чітко знати, який хмарний постачальник поширений на конкретному робочому місці або на якому постачальнику хмарних послуг необхідно зосередитись.

Національний інститут стандартів і технологій (НІСТ) визначає хмару як технологію, яка має такі п'ять характеристик (https://www.nist.gov/):

•*Самообслуговування на вимогу*. Припустимо, що необхідно відкрити блог і потрібні обчислювальні ресурси. Замість того, щоб купувати обладнання та чекати, поки постачальник доставить його до офісу, а потім розгортати програмне забезпечення, простішою альтернативою може бути портал самообслуговування, де можна обрати попередньо встановлену операційну систему та систему керування контентом, яку можливо розгорнути самостійно за кілька хвилин.

•*Щоб забезпечити стабільну та масштабовану роботу програмного забезпечення*, яке обслуговує велику кількість кінцевих користувачів, необхідно мати широкий доступ до мережі. Такий рівень доступу, як правило, надається великими постачальниками інтернет-послуг (Інтернет-провайдерами), які здатні обробляти значні обсяги трафіку одночасно.

•*Об'єднання ресурсів*. Припустимо, що тисячі комп'ютерів, які працюють у великій серверній фермі, та дають можливість максимально використовувати їх (застосування процесора, пам'яті та обсягу сховища), замість того, щоб мати один сервер, який використовує лише 10% свого процесора.

•*Швидка еластичність*. Розглядаємо можливість збільшення та зменшення обсягу обчислювальних ресурсів (з одного сервера до тисяч серверів, а потім навпаки - до одного сервера) відповідно до потреб вашої програми чи послуги.

•*Виміряний сервіс*. Розгляньте можливість оплати лише за спожиті ресурси та можливість створення звіту про виставлення рахунків, який показує, які ресурси були використані та скільки ви маєте за них сплатити.

Існує декілька моделей розгортання хмари:

•*Приватна хмара*. Інфраструктура, розгорнута та підтримувана однією організацією. Припустимо, що ми є великою фінансовою організацією (наприклад, банком або страховою організацією), ми хотіли б обслуговувати різні відділи нашої організації (відділ кадрів, ІТ, продажів тощо), і у нас можуть бути нормативні вимоги щодо зберігання даних клієнтів локально - приватна хмара може бути підходящим рішенням.

•*Публічна хмара*. Інфраструктура, розгорнута та підтримувана постачальником послуг для обслуговування кількох клієнтів та організацій, здебільшого доступна через Інтернет.

•*Гібридна хмара*. Поєднання приватної хмари (або локальної хмари) та принаймні однієї інфраструктури публічної хмари. Можна розглядати гібридну хмару як розширення локального центру обробки даних.

•*Мультихмарна модель (Multicloud):* передбачає використання організацією декількох керованих хмарних сервісів (наприклад, програм як послуга - SaaS) або одночасне застосування кількох публічних хмарних інфраструктур (інфраструктура як послуга - IaaS, платформа як послуга -

PaaS). Такий підхід дозволяє гнучко поєднувати можливості різних постачальників і мінімізувати залежність від одного провайдера.

Слід зазначити, що важливою частиною розуміння хмарних технологій є розуміння трьох моделей хмарних сервісів:

- *Інфраструктура як послуга (Інфраструктура як послуга (IAA))*. Це найфундаментальніша модель обслуговування, де клієнт може вибрати розмір віртуальної машини (з точки зору обсягу процесора та пам'яті), вибрати попередньо налаштовану операційну систему та розгорнути програмне забезпечення всередині екземпляра віртуальної машини відповідно до потреб бізнесу (такі послуги, як Amazon EC2, Віртуальні машини Azure, та Обчислювальний сервіс Compute Engine контейнерів Google).
- *PaaS (Platform as a Service*) -це модель хмарного обслуговування, яка надає розробникам платформу для створення, тестування, розгортання та підтримки веб-додатків без необхідності самостійного керування інфраструктурою. Сервіси PaaS охоплюють різноманітні керовані ресурси - від баз даних до повноцінних середовищ виконання додатків. Користувач може імпортувати власний код і запускати його у вже налаштованому середовищі, що спрощує процес розробки та масштабування.
- *Програмне забезпечення як послуга (SaaS).* Це найпоширеніша модель обслуговування - повністю кероване програмне середовище, де клієнт, зазвичай відкриваєте веб-браузер, під час входу в програму та користується послугами. Це можуть бути служби обміну повідомленнями, ERP, CRM, бізнес-аналітика тощо (такі послуги, як Microsoft Office 365, робочі середовища Google, CRM-системи Salesforce, фактори успіху SAP, та Oracle Cloud HCM).

Слід підкреслити таку особливість, що хмарні обчислення змінили традиційний підхід до контролю над даними. Підприємства/організації, які раніше зберігали дані виключно локально (від персональних даних працівників до конфіденційної клієнтської інформації), змушені переосмислити інвестиції в інфраструктуру: від центрів обробки даних, серверів і систем зберігання до мережевого обладнання та рівня програмного забезпечення.

Використання публічних хмарних рішень суттєво трансформувало уявлення про інформаційну безпеку, а саме про її хмарну складову. На відміну від повного локального контролю підприємство/організація розподіляє відповідальність за безпеку з постачальником хмарних послуг, що потребує нових підходів до оцінки ризиків і побудови архітектури безпеки.

Розглянемо приклади ключових відмінностей між локальними рішеннями та хмарними середовищами з погляду безпеки та управління даними (Таблиця 1.1).

Таблиця 1.1 - Порівняння традиційного центру обробки даних та хмарного середовища

Питання	Традиційний центр обробки даних	Хмарне середовище
Хто відповідає за фізичну безпеку?	Підприємство/організація	Постачальник хмарних послуг
Де розміщуються дані?	Локальний центр обробки даних	Центр обробки даних постачальника хмари
Хто контролює доступ до даних?	Підприємство/організація	І організація, і постачальник хмарних послуг
Хто відповідає за управління вразливостями та оновленнями (патчами)?	Підприємство/організація	IaaS - організація PaaS - постачальник хмари SaaS - постачальник хмари
Хто відповідає за реагування на інциденти?	Підприємство/організація	І організація, і постачальник хмарних послуг
Хто несе відповідальність за дотримання вимог законодавства, конфіденційність і регулювання?	Підприємство/організація	І організація, і постачальник хмарних послуг

Багато організацій виявляють обережність або опір при переході до публічного хмарного середовища, мотивуючи це занепокоєнням щодо безпеки. Основною причиною є втрата прямого фізичного контролю над інфраструктурою: сервери, на яких зберігаються дані, можуть розташовуватися за межами території самої організації, а іноді навіть за межами країни чи регіону її діяльності.

Таке розміщення може створювати ризики, пов’язані з юрисдикцією, відповідністю локальному законодавству, конфіденційністю та доступом третіх сторін, включаючи державні органи.

Вступ до хмарної безпеки

Практика показує, що найрозповсюдженіші запитання, які ставить керівництво підприємств/організацій це:

- Чи наші сервери поводяться так само, як якщо б вони були локальними?
- Як захистити мої сервери за межами мого центру обробки даних від витоку даних?
- Як можемо дізнатися, що постачальник хмарних послуг не матиме доступу до наших даних?
- Чи мають наші співробітники достатньо знань для роботи в нових середовищах, таких як публічна хмара?

Можемо зробити висновок, що найочевидніше питання, яке поставатиме - *Чи достатньо безпечна публічна хмара для зберігання моїх даних?* І з досвіду фахівців-практиків, відповідь - *так.*

За своєю суттю, постачальники гіпермасштабних хмарних послуг інвестують мільярди у захист своїх центрів обробки даних, створення безпечних сервісів, навчання співробітників, а також у виявлення інцидентів безпеки та їх швидке усунення.

Причина цього проста: якщо в одному з постачальників гіпермасштабних хмарних послуг станеться порушення безпеки, довіра їхніх клієнтів буде підірвана, і постачальники хмарних послуг збанкрутують.

Врешті решт, хмарна безпека дозволяє підприємству/організації досягти (серед іншого) наступного:

- Зменшена поверхня атаки
- Використання централізованої автентифікації, шифрування даних, служб захисту від DDoS-атак тощо
- Відповідність нормативним вимогам
- Розгортання середовищ відповідно до найкращих практик
- Стандартизація та найкращі практики
- Забезпечення безпеки за допомогою автоматизованих інструментів та сервісів.

Постає питання, що ж таке модель спільної відповідальності.

Коли йде розмова про хмарну безпеку та моделі хмарних сервісів (IaaS/PaaS/SaaS), то чуємо про модель спільної відповідальності, яка намагається провести межу між постачальником хмарних послуг та обов'язками клієнта щодо безпеки.

Як бачимо на рис.1.1, постачальник хмарних послуг завжди відповідає за нижчі рівні - від фізичної безпеки своїх центрів обробки даних до мереж, сховищ, хост-серверів та рівнів віртуалізації.

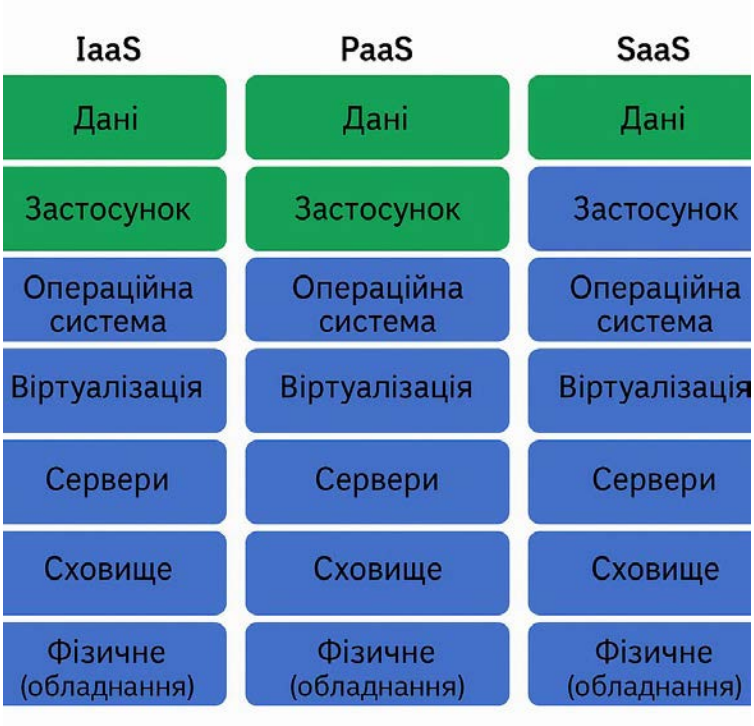

Рисунок 1.1 - Модель спільної відповідальності

AWS та модель спільної відповідальності

Розглядаючи модель спільної відповідальності з точки зору AWS, можемо побачити чітке розмежування між відповідальністю AWS за безпеку з хмари (фізичне обладнання та нижчі рівні, такі як хост-сервери, сховище, база даних та мережа) та відповідальність клієнта за безпеку в хмарі (все, що контролює клієнт) - операційна система, шифрування даних, правила мережевого брандмауера та дані клієнтів). На рис.1.2. зображено AWS та модель спільної відповідальності:

Рисунок 1.2 - AWS та модель спільної відповідальності

Azure та модель спільної відповідальності

Розглядаючи модель спільної відповідальності з точки зору Azure, бачимо різницю між відповідальністю Azure за свої центри обробки даних (фізичні рівні) та відповідальністю клієнта на верхніх рівнях (ідентифікатори, пристрої та дані клієнтів). На середніх рівнях (операційна система, мережеві елементи керування та програми) відповідальність змінюється між Azure та клієнтами залежно від різних типів послуг. На рис.1.3. бачимо Azure та модель спільної відповідальності.

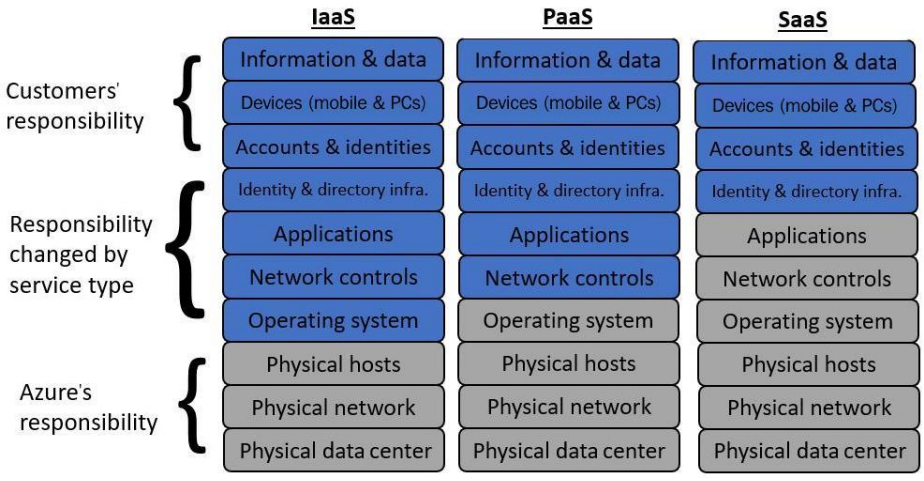

Рисунок 1.3 - Azure та модель спільної відповідальності

Більше інформації про модель спільної відповідальності Azure можна знайти за наступним посиланням: https://surl.li/bbezwc

GCP та модель спільної відповідальності

Розглядаючи модель спільної відповідальності з точки зору GCP, бачимо, що Google створює власне обладнання, що дозволяє компанії контролювати апаратне забезпечення, завантаження та ядро своєї платформи, включаючи шифрування рівня зберігання даних, мережеве обладнання та ведення журналу всього, за що відповідає Google.

Дії, за які відповідає клієнт (рис.1.4), включають все: від гостьової операційної системи до таких речей, як розгортання, використання, політики доступу та контент (дані клієнтів).

Рисунок 1.4 - GCP та модель спільної відповідальності

Розуміння моделі спільної відповідальності дозволяє користувачу у будь-який момент часу розуміти, за які рівні відповідають постачальники хмарних послуг, а за які - клієнт.

Інструменти командного рядка

Одна з речей, яка робить хмарні середовища такими надійними є можливість контролювати майже все за допомогою Інтерфейсу Прикладного Програмування (англ. *Application Programming Interface* - API) або за допомогою командного рядка.

Альтернативою використанню командного рядка для взаємодії з API постачальника хмарних послуг є використання Комплект розробника програмного забезпечення (англ. *Software Development Kit* - SDK) - метод керування діями (від розгортання віртуальної машини до шифрування сховища), запиту інформації від служби (перевірка того, чи ввімкнено аудит для входу клієнтів у нашу веб-програму) тощо.

Командний рядок AWS

AWS CLI можна встановити на Вікна(64 біт), Лінукс як x86, так і ARM-процесори), macOS, і навіть всередині Докерконтейнер.

У документації AWS CLI пояснюється, як встановити інструмент, і надається детальне пояснення того, як його використовувати.

Документацію можна знайти за адресою: https://surli.cc/sbudpi

Інтерфейс командного рядка Azure

Azure CLI можна встановити на Windows, Linux Убунту, Дебіан, РХЕЛ, CentOS, Федора, openSUSE) та macOS.

У документації Azure CLI пояснюється, як встановити інструмент, і надається детальне пояснення того, як його використовувати.

Документацію можна знайти за адресою https://surli.cc/voqbfi

SDK для хмарних сервісів Google

Інструмент командного рядка Google (Командний рядок gcloud) можна встановити на Windows, Linux (Ubuntu, Debian, RHEL, CentOS, Fedora) та macOS.

У документації Google Cloud SDK пояснюється, як встановити інструмент, і надається детальне пояснення того, як його використовувати.

Документацію можна знайти за адресою https://surl.lt/ovyumg

1.2. Захист обчислювальних послуг

У контексті хмарних обчислень, зокрема моделі *інфраструктура як послуга* (Infrastructure as a Service, IaaS), ключовим ресурсом, що привертає найбільшу увагу дослідників та практиків, є обчислювання. Їхній розвиток простежується від використання традиційних віртуальних машин до впровадження керованих баз даних, які працюють на віртуальних машинах серверної частини. Подальша еволюція обчислювальної інфраструктури включає перехід до сучасних обчислювальних архітектур - таких як контейнери і завершується впровадженням безсерверних (serverless) технологій, що забезпечують вищий рівень автоматизації та масштабованості.

В даному розділі маємо розглянуто всі типи обчислювальних сервісів і надати екомендації щодо безпечного розгортання та керування кожним із них. Це розглядатиметься в наступних тема:

- Захист віртуальних машин (автентифікація, контроль доступу до мережі, метадані, доступ до послідовної консолі, керування виправленнями та резервне копіювання).
- Забезпечення безпеки керованих служб баз даних (керування ідентифікаторами, контроль доступу до мережі, захист даних, аудит і моніторинг).
- Захист контейнерів (керування ідентифікаторами, контроль доступу до мережі, аудит та моніторинг, а також відповідність вимогам).

- Захист безсерверних систем/функцій як послуг (керування ідентифікацією, контроль доступу до мережі, аудит та моніторинг, відповідність вимогам та зміна конфігурації).

Технічні вимоги

Основою вивчення даного розділу єбазові розуміння віртуальних машин, що таке керовані бази даних і що таке контейнери (і Kubernetes), а також фундаментальне розуміння безсерверних технологій.

Захист віртуальних машин

Кожен постачальник хмарних послуг має власну реалізацію віртуальних машин (або віртуальних серверів), але зрештою, основна ідея однакова:

1. Виберати тип (або розмір) машини - співвідношення між кількістю віртуальних процесорів та пам'яттю, відповідно до їхніх вимог (загального призначення, оптимізованого для обчислень, оптимізованого для пам'яті тощо).
2. Виберати попередньо встановлений образ операційної системи (від Windows до Linux).
3. Налаштувати сховище (додавання додаткових томів, підключення до служб обміну файлами тощо).
4. Налаштувати параметри мережі (від контролю доступу до мережі до мікросегментації та інших).
5. Налаштувати дозволи для доступу до хмарних ресурсів.
6. Розгорнути застосунок.
7. Розпочати користуватися послугою.
8. Здійснювати поточне обслуговування операційної системи.

Захист Amazon Elastic Compute Cloud (EC2)

Amazon EC2 - це сервіс віртуальної машини Amazon.

Нижче наведено деякі з найкращих практик, які слід пам’ятати:

- Використовуйте лише перевірений AMI під час розгортання екземплярів EC2.
- Використовуйте мінімальну кількість пакетів всередині AMI, щоб зменшити поверхню атаки.
- Використовуйте вбудовані агенти Amazon для екземплярів EC2 (резервне копіювання, керування виправленнями, посилення захисту, моніторинг тощо).

Використовуйте інстанси EC2 нового покоління на базі системи AWS Nitro, яка переносить функції віртуалізації (такі як мережа, сховище та безпека) на виділені програмні та апаратні чіпи. Це дозволяє клієнту отримати набагато кращу продуктивність, значно кращу безпеку та ізоляцію даних клієнтів.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:

Найкращі практики для створення AMI:
https://surl.li/knybsk
*Amazon Linux AMI:*https://surl.li/hvsuzf
Система AWS Nitro: https://surl.li/edmrdi

Найкращі практики автентифікації при роботі з екземплярами Amazon EC2

Amazon Web Services (AWS) не має прямого доступу до віртуальних машин користувачів, що забезпечує високий рівень ізоляції та конфіденційності даних. Важливою складовою безпечного доступу до екземплярів EC2 є належна конфігурація автентифікації на етапі їх розгортання.

Під час створення екземпляра EC2, незалежно від обраної операційної системи (Windows або Linux) користувач має вказати пару криптографічних ключів (public/private key pair). Можна обрати вже існуючу пару ключів або створити нову безпосередньо через майстер розгортання EC2. Генерація ключів відбувається локально на стороні клієнта (в браузері), і AWS не зберігає ці ключі, а отже, не має можливості доступу до вашого інстанса.

У випадку з Linux-екземплярами ця пара ключів використовується для автентифікації через протокол SSH, що дозволяє встановити захищене з'єднання з віртуальною машиною без необхідності використовувати паролі.(*Зверніться до наступного посилання:* https://surl.li/sfmsda)

Для екземплярів Windows пара ключів використовується для отримання вбудованого пароля адміністратора. (*Зверніться до наступного посилання:* https://surl.li/ufzasl)

Рекомендовані практики з безпечного керування ключами доступу до екземплярів EC2

Для забезпечення надійної автентифікації та захисту від несанкціонованого доступу до хмарної інфраструктури важливо дотримуватись низки перевірених практик щодо зберігання та використання криптографічних ключів.

1. ***Захищене зберігання приватних ключів.*** Закриті SSH-ключі мають зберігатися виключно у безпечному середовищі. Одним із рекомендованих сервісів для їх зберігання та керованого доступу є *AWS Secrets Manager*, який забезпечує централізоване, захищене та контрольоване зберігання конфіденційних даних.
2. ***Уникнення зберігання ключів на відкритих хостах.*** Не слід зберігати приватні ключі на бастіонних вузлах або будь-яких екземплярах, що мають пряме підключення до Інтернету. Надійною альтернативою автентифікації без використання SSH-ключів є застосування *AWS Systems Manager* через компонент *Session Manager*, який забезпечує безпечний доступ до інстансів без відкриття портів чи використання ключів.
3. **Інтеграція з Active Directory (AD).** Для централізованого управління обліковими даними та спрощення автентифікації рекомендується приєднувати екземпляри Windows або Linux до домену *Active Directory*

(AD). Це дає змогу автентифікувати користувачів за допомогою корпоративних облікових даних AD, уникаючи використання локальних облікових записів або SSH-ключів.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Дозволити SSH-з'єднання через Session Manager:
https://surl.lu/kbdssi

Найкращі практики для забезпечення мережевого доступу до екземпляра

Доступ до ресурсів та сервісів AWS, таких як екземпляри EC2, контролюється через групи безпеки (на рівні екземпляра EC2) абоперелік керування доступом до мережі(НАКЛ) (на рівні підмережі), які еквівалентні локальному брандмауеру мережі 4-го рівня або механізму контролю доступу.

Як клієнт, ви налаштовуєте такі параметри, як IP-адреса джерела (або CIDR), IP-адреса призначення (або CIDR), порт призначення (або попередньо визначений протокол) та чи є порт TCP чи UDP.

Ви також можете використовувати іншу групу безпеки як джерело або місце призначення в групі безпеки.

Для віддаленого доступу та керування машинами Linux обмежте вхідний мережевий доступ до TCP-порту22.

Для віддаленого доступу та керування комп'ютерами Windows обмежте вхідний мережевий доступ до TCP-порту3389.

Найкращі практики наступні:

- Для протоколів віддаленого доступу (SSH/RDP) доцільно обмежити вихідну IP-адресу (або CIDR) добре відомими адресами. Гарними альтернативами для дозволу протоколів віддаленого доступу до екземпляра EC2 є використання VPN-тунелю, використання бастіонного хоста або використання AWS Systems Manager Session Manager.
- Для протоколів обміну файлами (CIFS/SMB/FTP) обмежте вихідну IP-адресу (або CIDR) добре відомими адресами.
- Встановіть назви та описи для груп безпеки, щоб краще зрозуміти призначення групи безпеки.
- Використовуйте теги (тобто маркування) для груп безпеки, щоб краще зрозуміти, яка група безпеки належить до яких ресурсів AWS.
- Обмежте кількість портів, дозволених у групі безпеки, до мінімально необхідної кількості портів, щоб ваша служба або програма могла функціонувати.

Для отримання додаткової інформації, маєте можливість зверніться до наступних ресурсів:
Групи безпеки Amazon EC2 для екземплярів Linux:
https://surli.cc/xysfey

*Групи безпеки для вашоговіртуальна приватна хмара(ВПК):*https://surl.li/tpjouq
*Менеджер сесій систем AWS:*https://surl.lu/pabgch
Порівняйте групи безпеки та мережеві ACL:
https://surl.lt/vfakog

Найкращі практики для захисту метаданих екземплярів

Метадані екземпляра -це метод отримання інформації про запущений екземпляр, такої як ім'я хоста та внутрішня IP-адреса.

Приклад метаданих про запущений екземпляр можна отримати зсередини екземпляра, відкривши браузер з операційної системи або використовуючи командний рядок за URL-адресою, такою як: http://169.254.169.254/latest/meta-data/ .

Навіть якщо IP-адреса є внутрішньою (тобто до неї неможливо отримати доступ ззовні екземпляра), інформацію за замовчуванням можна отримати локально без автентифікації.

AWS дозволяє вам застосовувати автентифіковані або сеанс-орієнтовані запити до метаданих екземпляра, також відомих як Служба метаданих екземплярів версії 2 (IMDSv2).

Наступна команда використовує інструмент AWS CLI для застосування IMDSv2 *(Instance Metadata Service v2)* до існуючого екземпляра. Ця команда вмикає захищений доступ до метаданих для екземпляра EC2, змушуючи всі запити використовувати токени (IMDSv2). Це важливо для підвищення рівня безпеки в хмарному середовищі AWS.aws ec2 зміна параметрів метаданих екземпляра.

Для отримання додаткової інформації, будь ласка, зверніться до наступного ресурсу:
Налаштуйте службу метаданих екземпляра: https://surl.li/nljref

Найкращі практики для захисту послідовного консольного з'єднання

Для усунення несправностей AWS дозволяє підключатися за допомогою послідовна консоль (схожа концепція до тієї, що ми раніше мали у фізичному світі з мережевим обладнанням) для вирішення проблем з мережею або операційною системою, коли SSH- або RDP-з'єднання недоступні.

Наступна команда використовує інструмент AWS CLI для надання послідовного доступу на рівні облікового запису AWS до певного регіону AWS:

aws ec2 увімкнути доступ до послідовного порту консолі --
region<Код_регіону>

Оскільки цей тип віддаленого підключення надає доступ до вашого екземпляра EC2, рекомендується дотримуватися таких рекомендацій:

- Доступ до послідовної консолі EC2 має бути обмежений групою осіб, які використовують управління ідентифікацією та доступом (Ідентифікація та доступність) ролі.

- Надавайте доступ до послідовної консолі EC2 лише за потреби.
- Завжди встановлюйте пароль користувача на екземплярі, перш ніж дозволити доступ до послідовної консолі EC2.

Для отримання додаткової інформації, будь ласка, зверніться до наступного ресурсу:
Налаштуйте доступ до послідовної консолі EC2:
https://surli.cc/klidug

Найкращі практики для управління виправленнями

Керування виправленнями є важливою частиною кожного випадку поточного обслуговування.

Щоб розгорнути патчі безпеки для екземплярів Windows або Linux стандартним способом, рекомендується використовувати AWS Systems Manager Patch Manager, виконавши такі дії**:**

1. Налаштуйте базову лінію патча.
2. Скануйте екземпляри EC2 на наявність відхилень від базового рівня патчів через запланований інтервал.
3. Встановіть відсутні патчі безпеки на ваші екземпляри EC2.
4. Перегляньте звіти менеджера патчів.

Найкращі практики наступні:

- Використовуйте AWS Systems Manager Compliance, щоб переконатися, що всі ваші екземпляри EC2 оновлені.
- Створіть групу з мінімальними правами IAM, щоб дозволити розгортання виправлень виконувати лише відповідним членам команди.
- Використовуйте теги (тобто маркування) для ваших екземплярів EC2, щоб дозволити групи розгортання патчів для кожного тегу (наприклад, підштовхувати проти розробника середовища).
- Для екземплярів EC2 без збереження стану (де дані сеансу користувача не зберігаються всередині екземпляра EC2) замініть існуючий екземпляр EC2 новим екземпляром, створеним з оновленого образу операційної системи.

Найкращі практики для забезпечення резервних копій

Резервне копіювання є критично важливим для забезпечення можливості відновлення екземпляра EC2 у разі збою або втрати даних. Сервіс AWS Backup автоматично шифрує ваші резервні копії як під час передачі, так і під час зберігання, використовуючи ключі шифрування AWS, які зберігаються у хмарному середовищі.

Для підвищення рівня безпеки додатково використовується служба керування ключами (AWS KMS). Вона надає централізований контроль над створенням, використанням та доступом до ключів шифрування, незалежно від налаштувань шифрування ваших Elastic Block Store (EBS) томів чи знімків.

Найкращі практики наступні:

- Налаштуйте службу AWS Backup з роллю IAM, щоб дозволити доступ до ключів шифрування, що зберігаються в AWS KMS.
- Налаштуйте службу резервного копіювання AWS з роллю IAM, щоб надати доступ до вашого сховища резервних копій.
- Використовуйте теги (тобто маркування) для резервних копій, щоб краще зрозуміти, яка резервна копія належить до якого екземпляра EC2.
- Розгляньте можливість реплікації резервних копій в інший регіон.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:

Захист ваших даних за допомогою AWS Backup:
https://surl.li/ztclks
Створення резервних копій у різних регіонах AWS:
https://surl.li/dhfasb

Захист віртуальних машин Azure

Віртуальні машини Azure - це служба віртуальних машин Azure.

Нижче наведено деякі з найкращих практик, які слід пам’ятати:

- Використовуйте лише перевірені образи під час розгортання віртуальних машин Azure.
- Використовуйте мінімальну кількість пакетів всередині образу, щоб зменшити поверхню атаки.
- Використовуйте вбудовані агенти Azure для віртуальних машин Azure (резервне копіювання, керування виправленнями, посилення захисту, моніторинг тощо).
- Для середовищ із високим рівнем конфіденційності використовуйте конфіденційні обчислювальні образи Azure, щоб забезпечити безпеку та ізоляцію даних клієнтів.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:

Огляд конструктора образів Azure: https://surl.lt/rszqxo
Використання Azure для хмарних конфіденційних обчислень: https://surl.li/vawxjp

Найкращі практики для автентифікації на віртуальній машині

Microsoft не має доступу до віртуальних машин клієнтів.

Неважливо, чи ви оберете розгортати машину з Windows чи Linux, виконавши команду створити віртуальну машину майстра, щоб розгорнути нову машину Linux, за замовчуванням потрібно вибрати або існуючу пару ключів, або створити нову пару ключів.

Цей набір закритих/відкритих ключів генерується на стороні клієнта - Azure не має доступу до цих ключів і тому не може увійти до вашої віртуальної машини Linux.

Для екземплярів Linux пара ключів використовується для входу в систему через протокол SSH.

Для отримання додаткової інформації, будь ласка, зверніться до наступного ресурсу:
Згенеруйте та збережіть SSH-ключі на порталі Azure: https://surl.li/hwfvhb

Для комп'ютерів з ОС Windows, під час запуску створити нову віртуальну машинумайстра, вам буде запропоновано вказати власний обліковий запис адміністратора та пароль для входу в систему через протокол RDP.

Для отримання додаткової інформації, будь ласка, зверніться до наступного ресурсу:
Створення віртуальної машини Windows:
https://surl.lu/xlwvzc

Найкращі практики наступні:

- Зберігайте свої облікові дані в безпечному місці.
- Уникайте зберігання закритих ключів на бастіонному хості (віртуальні машини, безпосередньо підключені до Інтернету).
- Приєднайте екземпляри Windows або Linux до домену AD та використовуйте свої облікові дані AD для входу у віртуальні машини (і повністю уникайте використання локальних облікових даних або ключів SSH).

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
*Лазурний бастіон:*https://surl.li/yysxim
Приєднайте віртуальну машину Windows Server до домену, керованого службами домену Azure AD, за допомогою шаблону Resource Manager: https://surl.lt/lnxihd

Найкращі практики для забезпечення мережевого доступу до віртуальної машини

Доступ до ресурсів і служб Azure, таких як віртуальні машини, контролюється черезгрупи мережевої безпеки, які еквівалентні локальному брандмауеру мережі 4-го рівня або механізму контролю доступу.

Як клієнт, ви налаштовуєте такі параметри, як вихідна IP-адреса (або CIDR), цільова IP-адреса (або CIDR), вихідний порт (або попередньо визначений протокол), цільовий порт (або попередньо визначений протокол), тип порту: TCP чи UDP, а також дію, яку потрібно виконати (дозволити чи заборонити).

Для віддаленого доступу та керування машинами Linux обмежте вхідний мережевий доступ до TCP-порту22. Для віддаленого доступу та керування комп'ютерами Windows обмежте вхідний мережевий доступ до TCP-порту3389.

Найкращі практики наступні:

- Для протоколів віддаленого доступу (SSH/RDP) обмежте вихідну IP-адресу (або CIDR) добре відомими адресами. Гарними альтернативами для дозволу протоколів віддаленого доступу до віртуальної машини Azure є використання VPN-тунелю, використання Azure Bastion або використання Azure Керування привілейованими дентифікаторами (ПІМ), щоб забезпечити своєчасний доступ до віддаленої віртуальної машини.
- Для протоколів обміну файлами (CIFS/SMB/FTP) обмежте вихідну IP-адресу (або CIDR) добре відомими адресами.
- Встановіть назви для груп безпеки мережі, щоб краще зрозуміти призначення групи безпеки.
- Використовуйте теги (тобто маркування) для груп мережевої безпеки, щоб краще зрозуміти, яка група мережевої безпеки належить до яких ресурсів Azure.
- Обмежте кількість портів, дозволених у групі мережевої безпеки, до мінімально необхідної кількості портів, щоб ваша служба або програма могла функціонувати.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
*Групи мережевої безпеки:*https://surli.cc/woliri
Як відкрити порти для віртуальної машини за допомогою порталу Azure:
https://surl.lu/jbygag
*Лазурний бастіон:*https://surl.lu/slddmu
Що таке Azure AD PIM? https://surl.lu/lxgmgm

Найкращі практики для захисту послідовного консольного з'єднання

Для усунення несправностей Azure дозволяє підключатися за допомогою *послідовна консоль* (схожа концепція до тієї, що ми раніше мали у фізичному світі з мережевим обладнанням) для вирішення проблем з мережею або операційною системою, коли SSH- або RDP-з'єднання недоступні.

Наведені нижче команди використовують інструмент Azure CLI, щоб дозволити послідовний доступ для всього рівня підписки *Azure:*

```
Ідентифікатор_підписки=$(показати обліковий запис az --output=json | jq -r .id)
az ресурс invoke-action --action enableConsole \
- - ідентифікатори "/підписки/$subscriptionId/провайдери/Microsoft.SerialConsole/consoleServices/за замовчуванням" --apiversion="2018-05-01"
```

Оскільки цей тип віддаленого підключення розкриває ваші віртуальні машини, рекомендується дотримуватися таких рекомендацій:

- Доступ до послідовної консолі має бути обмежений групою осіб з Автор віртуальної машини роль для віртуальної машини та Діагностика завантаження обліковий запис сховища.
- Завжди встановлюйте пароль користувача на цільовій віртуальній машині, перш ніж дозволити доступ до послідовної консолі.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Послідовна консоль Azure для Linux та для Windows: https://surl.li/buzndx

Найкращі практики для управління виправленнями

Керування виправленнями є важливою частиною кожного випадку поточного обслуговування.

Для стандартного розгортання патчів безпеки для екземплярів Windows або Linux рекомендується використовувати керування оновленнями автоматизації Azure, використовуючи наступний метод:

1. Створіть обліковий запис автоматизації.
2. Увімкніть керування оновленнями для всіх машин з Windows та Linux.
3. Налаштуйте параметри розкладу та опції перезавантаження.
4. Встановіть відсутні патчі безпеки на свої віртуальні машини.
5. Перегляньте стан розгортання.

Найкращі практики наступні:

- Використовуйте мінімальні права для облікового запису, використовуючи керування оновленнями, щоб розгортати виправлення безпеки.
- Використовуйте класифікації оновлень, щоб визначити, які патчі безпеки розгортати.
- Під час використання облікового запису Azure Automation шифруйте конфіденційні дані (наприклад, змінні активи).
- Під час використання облікового запису Azure Automation використовуйте приватні кінцеві точки, щоб вимкнути доступ до загальнодоступної мережі.
- Використовуйте теги (тобто маркування) для ваших віртуальних машин, щоб дозволити визначення динамічних груп віртуальних машин (наприклад, підштовхувати проти розробник середовища).
- Для віртуальних машин без збереження стану (де дані сеансу користувача не зберігаються всередині віртуальної машини Azure) замініть існуючу віртуальну машину Azure новим екземпляром, створеним з оновленого образу операційної системи.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Керування оновленнями автоматизації Azure:
https://surl.li/cxksli
Оновити дозволи керування: https://surl.li/rqacva

Найкращі практики для забезпечення резервних копій

Резервне копіювання є критично важливим для відновлення віртуальної машини.

Служба резервного копіювання Azure шифрує ваші резервні копії під час передачі та в стані спокою за допомогою Azure Key Vault.

Найкращі практики наступні:

- Використовуйте Azureконтроль доступу на основі ролей(RBAC), щоб налаштувати службу резервного копіювання Azure на мінімальний доступ до ваших резервних копій.
- Для конфіденційних середовищ шифруйте дані в стані спокою за допомогою ключів, керованих клієнтом.
- Використовуйте приватні кінцеві точки для захисту доступу між вашими даними та сховищем служби відновлення.
- Якщо вам потрібно, щоб ваші резервні копії відповідали нормативному стандарту, використовуйте Відповідність нормативним вимогам у політиці Azure.
- Використовуйте базові рівні безпеки Azure для резервного копіювання Azure (Тест безпеки Azure).
- Увімкнути м’яке видалення функція захисту резервних копій від випадкового видалення.
- Розгляньте можливість реплікації резервних копій в інший регіон.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Функції безпеки для захисту гібридних резервних копій, що використовують Azure Backup:
https://surl.li/fvjogm
Використовуйте Azure RBAC для керування точками відновлення резервного копіювання Azure:
https://surl.li/rolaix
Контроль відповідності нормативним вимогам політики Azure для резервного копіювання Azure:
https://surl.lu/lebysk
М’яке видалення для резервного копіювання Azure: https://surl.li/yunnbr
Відновлення між регіонами(Загальний капітальний рейтинг (CRR)) для віртуальних машин Azure, що використовують резервне копіювання Azure:
https://surl.li/hyvrxs

Захист екземплярів Google Compute Engine (GCE) та віртуальних машин

GCE -це сервіс віртуальних машин від Google.

Нижче наведено деякі з найкращих практик, які слід пам'ятати:

- Використовуйте лише перевірені образи під час розгортання віртуальних машин Google.
- Використовуйте мінімальну кількість пакетів всередині образу, щоб зменшити поверхню атаки.
- Використовуйте вбудовані агенти GCP для віртуальних машин Google (керування виправленнями, посилення захисту, моніторинг тощо).

Для середовищ із високим рівнем конфіденційності використовуйте зображення Google Confidential Computing, щоб забезпечити безпеку та ізоляцію даних клієнтів.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Перелік загальнодоступних зображень, доступних на GCE: https://surl.li/tzjuum
Конфіденційні обчислення: https://surl.lu/jctoff

Найкращі практики для автентифікації в екземплярі віртуальної машини Google не має доступу до екземплярів віртуальних машин клієнтів. Коли ви запускає тестворити екземпляр майстра, жодних о лікових даних не створюється.

Для екземплярів Linux потрібно вручну створити пару ключів і додати відкритий ключ або до метаданих екземпляра, або до всіх метаданих проекту GCP, щоб увійти до екземпляра машини через протокол SSH.

Для отримання додаткової інформації, будь ласка, зверніться до наступного ресурсу:
Керування SSH-ключами в метаданих: https://surli.cc/wbpbbd

Для екземплярів комп'ютерів з ОС Windows потрібно вручну скинути вбудований пароль адміністратора, щоб увійти до екземпляра комп'ютера через протокол RDP.

Для отримання додаткової інформації, будь ласка, зверніться до наступного ресурсу:
Створення паролів для віртуальних машин Windows: https://surl.lu/fxyhfl

Найкращі практики наступні:

- Зберігайте свої приватні ключі в безпечному місці.
- Уникайте зберігання закритих ключів на бастіонному хості (екземплярах машин, безпосередньо підключених до Інтернету).
- Періодично змінюйте SSH-ключі, що використовуються для доступу до обчислювальних екземплярів.

- Періодично переглядайте відкриті ключі всередині обчислювального екземпляра або метаданих SSH-ключів на рівні проекту GCP та видаляйте непотрібні відкриті ключі.
- Приєднайте екземпляри Windows або Linux до домену AD та використовуйте свої облікові дані AD для входу у віртуальні машини (і повністю уникайте використання локальних облікових даних або ключів SSH).

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Короткий посібник: Приєднання віртуальної машини Windows до домену: https://surl.li/jcvqvn
Короткий посібник: Приєднання віртуальної машини Linux до домену: https://surli.cc/bgqfkq

Найкращі практики для забезпечення мережевого доступу до екземпляра віртуальної машини:
- Доступ до ресурсів та служб GCP, таких як екземпляри віртуальних машин, контролюється через Правила брандмауера VPC, які еквівалентні локальному брандмауеру мережі 4-го рівня або механізму контролю доступу.
- Як клієнт, ви налаштовуєте такі параметри, як вихідна IP-адреса (або CIDR), вихідна служба, вихідні теги, порт призначення (або попередньо визначений протокол), чи є порт TCP чи UDP, чи є напрямок трафіку вхідним чи вихідним, а також дію, яку потрібно виконати (дозволити чи заборонити).
- Для віддаленого доступу та керування машинами Linux обмежте вхідний мережевий доступ до TCP-порту22.
- Для віддаленого доступу та керування комп'ютерами Windows обмежте вхідний мережевий доступ до TCP-порту3389.

Найкращі практики наступні:
- Для протоколів віддаленого доступу (SSH/RDP) обмежте вихідну IP-адресу (або CIDR) добре відомими адресами.
- Для протоколів обміну файлами (CIFS/SMB/FTP) обмежте вихідну IP-адресу (або CIDR) добре відомими адресами.
- Встановіть назви та описи для правил брандмауера, щоб краще зрозуміти призначення групи безпеки.
- Використовуйте теги (тобто маркування) для правил брандмауера, щоб краще зрозуміти, яке правило брандмауера належить до яких ресурсів GCP.
- Обмежте кількість портів, дозволених у правилі брандмауера, до мінімально необхідної кількості портів, щоб ваша служба або програма могла функціонувати.

Для отримання додаткової інформації, будь ласка, зверніться до наступного ресурсу:
Використовуйте менше, ширших наборів правил брандмауера, коли це можливо: https://surl.li/noktvk

Найкращі практики для захисту послідовного консольного з'єднання

Для усунення несправностей GCP дозволяє підключатися за допомогою *послідовна консоль* (схожа концепція до тієї, що ми раніше мали у фізичному світі з мережевим обладнанням) для вирішення проблем з мережею або операційною системою, коли SSH- або RDP-з'єднання недоступні.

Наступна команда використовує Google Cloud SDK для надання послідовного доступу до всього проекту GCP:

*gcloud compute інформація про проект додати метадані *
- - метадані serial-port-enable=TRUE

Оскільки цей тип віддаленого підключення розкриває ваші віртуальні машини, рекомендується дотримуватися цих рекомендацій:

- Налаштуйте вхід на основі пароля, щоб дозволити користувачам доступ до послідовної консолі.
- Вимкнути інтерактивний вхід до послідовної консолі для кожного екземпляра обчислення, коли він не потрібен.
- Увімкнути відключення, коли послідовне консольне з’єднання неактивне.
- Доступ до послідовної консолі має бути обмежений для необхідної групи осіб, які використовують ролі Google Cloud IAM.
- Завжди встановлюйте пароль користувача на цільовому екземплярі віртуальної машини, перш ніж дозволити доступ до послідовної консолі.

Для отримання додаткової інформації, будь ласка, зверніться до наступного ресурсу:
Виправлення неполадок за допомогою послідовної консолі: https://surl.lu/kccdze

Найкращі практики для управління виправленнями

Керування виправленнями є важливою частиною кожного випадку поточного обслуговування.

Для розгортання патчів безпеки для екземплярів на базі Windows або Linux стандартним способом рекомендується використовувати керування патчами операційної системи Google, виконавши такі дії:

- Розгорніть агент конфігурації операційної системи на цільових екземплярах.
- Створіть завдання латки.
- Запустіть розгортання патчів.
- Заплануйте розгортання патчів.
- Перегляньте стан розгортання на панелі керування виправленнями операційної системи.

Найкращі практики наступні:

- Використовуйте мінімальні права для облікових записів, що використовують керування виправленнями операційної системи, для розгортання виправлень безпеки відповідно до ролей Google Cloud IAM.
- Поступово розгортайте патчі безпеки зона за зоною та регіон за регіоном.
- Використовуйте теги (тобто маркування) для ваших екземплярів віртуальних машин, щоб дозволити визначення груп екземплярів віртуальних машин (наприклад, підштовхувати проти розробник середовища).
- Для віртуальних машин без збереження стану (де дані сеансу користувача не зберігаються всередині віртуальної машини Google) замініть існуючу віртуальну машину Google новим екземпляром, створеним з оновленого образу операційної системи.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Керування патчами операційної системи: https://surli.cc/wigfqw
Створення завдань виправлення: https://surl.li/cwlvrm
Найкращі практики для масштабних оновлень операційної системи: https://surl.lu/eelils

Захист керованих служб баз даних

Кожен постачальник хмарних послуг має власну реалізацію керованих баз даних. Згідно з моделлю спільної відповідальності, якщо ми вирішимо використовувати керовану базу даних, постачальник хмарних послуг відповідає за операційну систему та рівні бази даних керованої бази даних (включаючи керування виправленнями, резервне копіювання та аудит).

Якщо у нас є вимога розгорнути певну збірку бази даних, ми завжди можемо розгорнути її всередині віртуальної машини, але відповідно до моделі спільної відповідальності ми будемо контролювати всю операційну систему та обслуговування бази даних (включаючи посилення захисту, резервне копіювання, керування виправленнями та моніторинг).

Кероване рішення для запуску механізму баз даних - або звичайний механізм баз даних, такий як MySQL, PostgreSQL, Microsoft SQL Server, сервер бази даних Oracle, або власні бази даних, такі як Amazon DynamoDB, Azure Cosmos DB або Google Cloud Spanner, але зрештою, основна ідея та сама:

1. Виберіть тип бази даних відповідно до її призначення або випадку використання (реляційна база даних, NoSQL база даних, графова база даних, база даних в оперативній пам'яті та інші).
2. Виберіть механізм баз даних (наприклад, MySQL, PostgreSQL, Microsoft SQL Server або сервер баз даних Oracle).
3. Для реляційних баз даних виберіть тип машини (або розмір) - співвідношення між обсягом віртуального процесора та пам’яті відповідно до їхніх вимог (загального призначення, оптимізована для пам’яті тощо).

4. Виберіть, чи потрібна висока доступність.
5. Розгорніть керований екземпляр бази даних (або кластер).
6. Налаштуйте керування мережевим доступом з вашого хмарного середовища до вашої керованої бази даних.
7. Увімкніть ведення журналу для будь-яких спроб доступу або змін конфігурації у вашій керованій базі даних.
8. Налаштуйте резервні копії керованої бази даних для цілей відновлення.
9. Підключіть свою програму до керованої бази даних та почніть користуватися сервісом.

Існує кілька причин для вибору керованого рішення для баз даних:
- Обслуговування бази даних здійснюється постачальником хмарних послуг.
- Розгортання патчів безпеки здійснюється постачальником хмарних послуг.
- Доступність бази даних знаходиться під відповідальністю постачальника хмарних послуг.
- Резервні копії включено до послуги (до певного обсягу сховища та обсягу історії резервних копій).
- Шифрування під час передачі та зберігання вбудовано як частина керованого рішення.
- Аудит вбудований як частина керованого рішення.

Захист Amazon RDS для MySQL

Amazon Служба реляційних баз даних(РДС) для MySQL - це служба MySQL, керована Amazon.

MySQL підтримує такі типи методів автентифікації:
- Локальна автентифікація за іменем користувача/паролем за допомогою вбудованого механізму автентифікації MySQL.
- Автентифікація бази даних AWS IAM.
- Служба каталогів AWS для автентифікації Microsoft AD.

Найкращі практики наступні:
- Для локального головного користувача MySQL створіть надійний та складний пароль (принаймні 15 символів, що складається з малих та великих літер, цифр та спеціальних символів) і зберігайте пароль у безпечному місці.
- Для кінцевих користувачів, яким потрібен прямий доступ до керованої бази даних, кращим методом є використання сервісу AWS IAM, оскільки він дозволяє централізовано керувати всіма ідентифікаторами користувачів, контролювати їх політику паролів, проводити аудит їхніх

дій (тобтоВиклики API), а у разі підозрілого інциденту безпеки вимкнути ідентифікацію користувача.

- Якщо ви керуєте ідентифікаторами користувачів за допомогою служби каталогів AWS для Microsoft AD (керований AWS Microsoft AD), використовуйте цю службу для автентифікації кінцевих користувачів за допомогою протоколу Kerberos.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Автентифікація бази даних IAM для MySQL: https://surl.li/drewns
Використання автентифікації Kerberos для MySQL: https://surl.lu/dblokp

Найкращі практики для забезпечення мережевого доступу до керованої служби бази даних MySQL

Доступ до керованої служби бази даних MySQL контролюється через *групи безпеки бази даних*, що еквівалентно *групи безпеки* та локальний мережевий брандмауер 4-го рівня або механізм контролю доступу.

Як клієнт, ви налаштовуєте такі параметри, як вихідна IP-адреса (або CIDR) ваших веб-серверів або серверів додатків та цільова IP-адреса (або CIDR) вашої керованої служби бази даних MySQL, а AWS налаштовує порт автоматично.

Найкращі практики наступні:

- Керовані бази даних ніколи не повинні бути доступними з Інтернету або загальнодоступної підмережі - завжди використовуйте приватні підмережі для розгортання ваших баз даних.
- Налаштуйте групи безпеки для веб-серверів або серверів додатків і встановіть групу безпеки як цільовий CIDR під час створення групи безпеки бази даних.
- Якщо вам потрібно керувати службою бази даних MySQL, використовуйте екземпляр EC2 (або бастіонний хост) для віддаленого керування базою даних MySQL або створіть VPN-тунель з віддаленого комп’ютера до керованої бази даних MySQL.
- Оскільки Amazon RDS є керованою службою, вона розташована поза межами VPC клієнта. Альтернативою безпечному доступу з вашого VPC до керованого середовища RDS є використання AWS Private Link, що дозволяє уникнути надсилання мережевого трафіку за межі вашого VPC через захищений канал, використовуючи кінцеву точку інтерфейсу VPC.
- Встановіть назви та описи для груп безпеки бази даних, щоб краще зрозуміти призначення групи безпеки бази даних.
- Використовуйте теги (тобтомаркування) для груп безпеки баз даних, щоб краще зрозуміти, яка група безпеки баз даних належить до яких ресурсів AWS.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
*Контроль доступу до RDS за допомогою груп безпеки:*https://surl.li/sjjkir
Огляд. RDSSecurityGroups.html API Amazon RDS та кінцеві точки інтерфейсу VPC (AWS PrivateLink): https://surl.lu/cgebxc

Найкращі практики захисту даних, що зберігаються в керованій службі баз даних MySQL

База даних призначена для зберігання даних.

У багатьох випадках база даних (і в цьому випадку керована база даних MySQL) може містити конфіденційні дані клієнтів (від роздрібного магазину, що містить дані клієнтів, до конфіденційних даних відділу кадрів організації).

Для захисту даних клієнтів рекомендується шифрувати дані як під час транспортування (коли дані проходять через мережу), щоб уникнути виявлення зовнішньою стороною, так і під час зберігання (дані зберігаються в базі даних), щоб уникнути розкриття даних, навіть внутрішнім адміністратором бази даних.

Шифрування дозволяє вам зберігати конфіденційність та цілісність даних (переконайтеся, що ваші дані не змінені ненадійною стороною).

Найкращі практики наступні:

- Увімкніть шифрування транспортного рівня SSL/TLS 1.2 для вашої бази даних.
- Для середовищ, що не містять конфіденційної інформації, шифруйте дані в стані спокою за допомогою AWS KMS.
- Для чутливих середовищ шифруйте дані в стані спокою за допомогою головний ключ клієнта (ЦМК) управління

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Використання SSL з екземпляром бази даних MySQL: https://surl.li/opdzku
Оновлення програм для підключення до екземплярів бази даних MySQL за допомогою нових сертифікатів SSL/TLS: https://surl.li/pobohp
Виберіть правильні параметри шифрування для сервісів Compute Engine контейнерів баз даних Amazon RDS: https://surl.li/wfnumq
Керівництво ЦМК: https://surl.lt/ckwltx

Найкращі практики проведення аудиту та моніторингу для керованої служби баз даних MySQL

Аудит є важливою частиною захисту даних.

Як і будь-який інший керований сервіс, AWS дозволяє ввімкнути ведення журналу та аудит за допомогою двох вбудованих сервісів:

- *Amazon CloudWatch.* Служба, яка дозволяє реєструвати дії бази даних та піднімати тривогу відповідно до попередньо встановлених порогових значень (наприклад, велика кількість невдалих входів)
- *AWS CloudTrail.* Сервіс, який дозволяє відстежувати активність API (по суті, будь-яку дію, що виконується в рамках API AWS RDS).

Найкращі практики такі:

- Увімкнути тривоги Amazon CloudWatch для високопродуктивного використання (що може свідчити про аномалії в поведінці бази даних).
- Увімкніть AWS CloudTrail для будь-якої бази даних, щоб реєструвати будь-яку діяльність, виконану в базі даних будь-яким користувачем, роллю чи сервісом AWS.
- Обмежте доступ до журналів CloudTrail мінімальною кількістю співробітників - бажано в обліковому записі управління AWS, поза межами доступу ваших кінцевих користувачів (включно з тими, що не входять до компетенції адміністраторів бази даних), щоб уникнути можливого видалення або зміни журналів аудиту.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Використання сповіщень про події Amazon RDS: https://surl.li/vmgubh
Робота з AWS CloudTrail та Amazon RDS: https://surl.lu/pfqupj

Захист бази даних Azure для MySQL

База даних Azure для MySQL - це служба MySQL, керована Azure.
MySQL підтримує такі типи методів автентифікації:

- Локальна автентифікація за іменем користувача/паролем за допомогою вбудованого механізму автентифікації MySQL,
- Автентифікація Azure AD.

Найкращі практики такі:

- Для локального головного користувача MySQL створіть надійний та складний пароль (принаймні 15 символів, що складається з малих та великих літер, цифр та спеціальних символів) і зберігайте пароль у безпечному місці.
- Для кінцевих користувачів, яким потрібен прямий доступ до керованої бази даних, кращим методом є використання автентифікації Azure AD, оскільки це дозволяє централізовано керувати всіма ідентифікаторами користувачів, контролювати їхню політику паролів, проводити аудит їхніх дій (тобто виклики API), а у разі підозрілого інциденту безпеки вимкнути ідентифікацію користувача.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Використовуйте Azure AD для автентифікації за допомогою MySQL: https://surl.lu/ffoxim
Використовуйте Azure AD для автентифікації за допомогою MySQL: https://surli.cc/ohizob

Найкращі практики для забезпечення мережевого доступу до керованої служби бази даних MySQL

Доступ до керованої служби бази даних MySQL контролюється через *правила брандмауера*, що дозволяє налаштувати, яким IP-адресам (або CIDR) дозволено доступ до вашої керованої бази даних MySQL.

Найкращі практики такі:

- Керовані бази даних ніколи не повинні бути доступними з Інтернету або загальнодоступної підмережі - завжди використовуйте приватні підмережі для розгортання ваших баз даних.
- Налаштуйте початкову та кінцеву IP-адреси ваших веб-серверів або серверів додатків, щоб обмежити доступ до керованої бази даних.
- Якщо вам потрібно керувати службою бази даних MySQL, використовуйте віртуальну машину Azure (або бастіонний хост) для віддаленого керування базою даних MySQL або створіть VPN-тунель з віддаленої машини до керованої бази даних MySQL.
- Оскільки База даних Azure для MySQL є керованою службою, вона розташована поза межами клієнтавіртуальна мережа(Віртуальна мережа). Альтернативою безпечному доступу з вашої віртуальної мережі до бази даних Azure для MySQL є використання кінцевої точки служби віртуальної мережі, що дозволяє уникнути надсилання мережевого трафіку за межі вашої віртуальної мережі через захищений канал.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Правила брандмауера сервера бази даних Azure для MySQL: https://surl.li/wjjsty
Використовуйте кінцеві точки та правила служби VNet для бази даних Azure для MySQL: https://surli.cc/abuzko

Найкращі практики захисту даних, що зберігаються в керованій службі баз даних MySQL

База даних призначена для зберігання даних.

У багатьох випадках база даних (і в цьому випадку керована база даних MySQL) може містити конфіденційні дані клієнтів (від роздрібного магазину, що містить дані клієнтів, до конфіденційних даних відділу кадрів організації).

Для захисту даних клієнтів рекомендується шифрувати дані як під час транспортування (коли дані проходять через мережу), щоб уникнути виявлення зовнішньою стороною, так і під час зберігання (дані зберігаються в базі даних), щоб уникнути розкриття даних, навіть внутрішнім адміністратором бази даних.

Шифрування дозволяє вам зберігати конфіденційність та цілісність даних (переконайтеся, що ваші дані не змінені ненадійною стороною).

Найкращі практики такі:

- Увімкніть шифрування транспортного рівня TLS 1.2 для вашої бази даних.

- Для конфіденційних середовищ шифруйте дані в стані спокою за допомогою ключів, керованих клієнтом, що зберігаються в службі Azure Key Vault.
- Зберігайте ключі, якими керує клієнт, у безпечному місці для резервного копіювання.
- Увімкнути м'яке видалення і захист від продувки функції Azure Key Vault, щоб уникнути випадкового видалення ключа (що зашкодить вашій можливості доступу до зашифрованих даних).
- Увімкнути аудит усіх дій, пов'язаних із ключами шифрування.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Шифрування даних бази даних Azure для MySQL за допомогою ключа, керованого клієнтом:
https://surl.li/aohjfe
Базовий рівень безпеки Azure для бази даних Azure для MySQL: https://surl.li/daofoa

Найкращі практики проведення аудиту та моніторингу для керованої служби баз даних MySQL

Аудит є важливою частиною захисту даних.

Як і будь-який інший керований сервіс, Azure дозволяє ввімкнути ведення журналу та аудит за допомогою двох вбудованих сервісів:

- Вбудовані журнали аудиту бази даних Azure для MySQL.
- Журнали монітора Azure.

Найкращі практики такі:

- Увімкнути журнали аудиту для MySQL.
- Використовуйте службу Azure Monitor для виявлення невдалих підключень.
- Обмежте доступ до даних служби Azure Monitor мінімальною кількістю співробітників, щоб уникнути можливого видалення або зміни журналів аудиту.
- Використовуйте розширений захист від загроз для бази даних Azure для MySQL, щоб виявляти аномалії або незвичайну активність у базі даних MySQL.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Журнали аудиту в базі даних Azure для MySQL:
https://surl.lu/nmcrhz
Налаштування та доступ до журналів аудиту для бази даних Azure для MySQL на порталі Azure:
https://surl.li/bfrqsc

Рекомендації щодо оповіщення про метрики за допомогою моніторингу бази даних Azure для MySQL: https://surl.li/gtpxdb
Міркування безпеки для моніторингу даних: https://surl.li/lugyqp

Захист Google Cloud SQL для MySQL

Google Cloud SQL для MySQL - це сервіс MySQL, керований Google.

Рекомендації щодо налаштування IAM для керованої служби баз даних MySQL.

MySQL підтримує такі типи методів автентифікації:

- Локальна автентифікація за іменем користувача/паролем за допомогою вбудованого механізму автентифікації MySQL,
- Автентифікація Google Cloud IAM.

Найкращі практики такі:

- Для локального головного користувача MySQL створіть надійний та складний пароль (принаймні 15 символів, що складається з малих та великих літер, цифр та спеціальних символів) і зберігайте пароль у безпечному місці.
- Для кінцевих користувачів, яким потрібен прямий доступ до керованої бази даних, кращим методом є використання автентифікації Google Cloud IAM, оскільки це дозволяє централізовано керувати всіма ідентифікаторами користувачів, контролювати їхню політику паролів, проводити аудит їхніх дій (тобтоВиклики API), а у разі підозрілого інциденту безпеки вимкнути ідентифікацію користувача.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Створення та керування користувачами MySQL:
https://surl.li/ytzrsr
Користувачі MySQL: https://surl.li/tzblnc
Ролі та дозволи в Cloud SQL: https://surl.lu/iwjctw

Найкращі практики для забезпечення мережевого доступу до керованої служби бази даних MySQL

Доступ до керованої служби бази даних MySQL контролюється за допомогою одного з наступних варіантів:

- Авторизовані мережі: Дозволяє налаштувати, яким IP-адресам (або CIDR) дозволено доступ до вашої керованої бази даних MySQL.
- Проксі-сервер автентифікації Cloud SQL: клієнт, встановлений на стороні вашої програми, який обробляє автентифікацію в базі даних Cloud SQL for MySQL у захищеному та зашифрованому тунелі.

Найкращі практики такі:

- Керовані бази даних ніколи не повинні бути доступними з Інтернету або загальнодоступної підмережі - завжди використовуйте приватні підмережі для розгортання ваших баз даних.
- Якщо можливо, бажано використовувати проксі-сервер автентифікації Cloud SQL.
- Налаштуйте авторизовані мережі для ваших веб-серверів або серверів додатків, щоб надати їм доступ до вашого Cloud SQL для MySQL.
- Якщо вам потрібно керувати службою бази даних MySQL, використовуйте екземпляр віртуальної машини GCE для віддаленого керування базою даних MySQL або хмарну VPN (налаштовує тунель IPSec до пристрою VPN-шлюзу).

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Авторизація в авторизованих мережах: https://surl.li/bglrdm
Підключення за допомогою проксі-сервера Cloud SQL Authentication: https://surl.lu/avgudt
Огляд хмарної VPN: https://surl.lt/vyjyaa

Найкращі практики захисту даних, що зберігаються в керованій службі баз даних MySQL

У багатьох випадках база даних (і в цьому випадку керована база даних MySQL) може містити конфіденційні дані клієнтів (від роздрібного магазину, що містить дані клієнтів, до конфіденційних даних відділу кадрів організації).

Для захисту даних клієнтів рекомендується шифрувати дані як під час транспортування (коли дані проходять через мережу), щоб уникнути виявлення зовнішньою стороною, так і під час зберігання (дані зберігаються в базі даних), щоб уникнути розкриття даних, навіть внутрішнім адміністратором бази даних.

Шифрування дозволяє вам зберігати конфіденційність та цілісність даних (переконайтеся, що ваші дані не змінені ненадійною стороною).

Найкращі практики наступні:

- Застосуйте шифрування транспортного рівня TLS 1.2 до вашої бази даних.
- Для чутливих середовищ шифруйте дані в стані спокою за допомогоюключі шифрування, керовані клієнтом(КМЕК) зберігається всередині служби Google Cloud KMS.
- Під час використання CMEK створіть окремий обліковий запис служби та надайте клієнтам дозвіл на доступ до ключів шифрування в Google Cloud KMS.
- Увімкнути аудит усіх дій, пов’язаних із ключами шифрування.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Налаштування SSL/TLS-сертифікатів: https://surl.li/jfuknb

Шифрування на стороні клієнта: https://surl.li/laxahj
Огляд CMEK: https://surl.li/nxpsnt
Використання CMEK: https://surl.li/lbpkxi

Найкращі практики проведення аудиту та моніторингу для керованої служби баз даних MySQL

Аудит є важливою частиною захисту даних.

Як і будь-який інший керований сервіс, GCP дозволяє ввімкнути ведення журналу та аудит за допомогою журналів аудиту Google Cloud.

Найкращі практики наступні:

- Журнали аудиту активності адміністратора ввімкнено за замовчуванням і не можна вимкнути.
- Явно ввімкнутижурнали аудиту доступу до данихдля реєстрації дій, виконаних у базі даних.
- Обмежте доступ до журналів аудиту мінімальною кількістю співробітників, щоб уникнути можливого видалення або зміни журналів аудиту.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Журнали аудиту: https://surl.li/xovkbm
Журнали хмарного аудиту: https://surli.cc/xsasxw
*Налаштування журналів аудиту доступу до даних:*https://surl.li/mzsyke
Дозволи та ролі: https://surl.li/eqvfat

Закріплення контейнерів

Після віртуальних машин наступним етапом еволюції в еру обчислень є контейнери.

Контейнери поводяться як віртуальні машини, але займають набагато менше місця. Замість того, щоб розгортати програму над цілою операційною системою, ви можете використовувати контейнери для розгортання необхідної програми, маючи лише мінімально необхідні бібліотеки та бінарні файли операційної системи.

Контейнери мають такі переваги над віртуальними машинами:

- Компактний розмір: У контейнері зберігаються лише необхідні бібліотеки та бінарні файли.
- Портативність. Ви можете розробити застосунок всередині контейнера на своєму ноутбуці та запускати його у великих масштабах у робочому середовищі з сотнями або тисячами екземплярів контейнерів.
- Швидке розгортання та оновлення порівняно з віртуальними машинами.

На наступній діаграмі (Рис.1.5) показано архітектурні відмінності між віртуальними машинами та контейнерами:

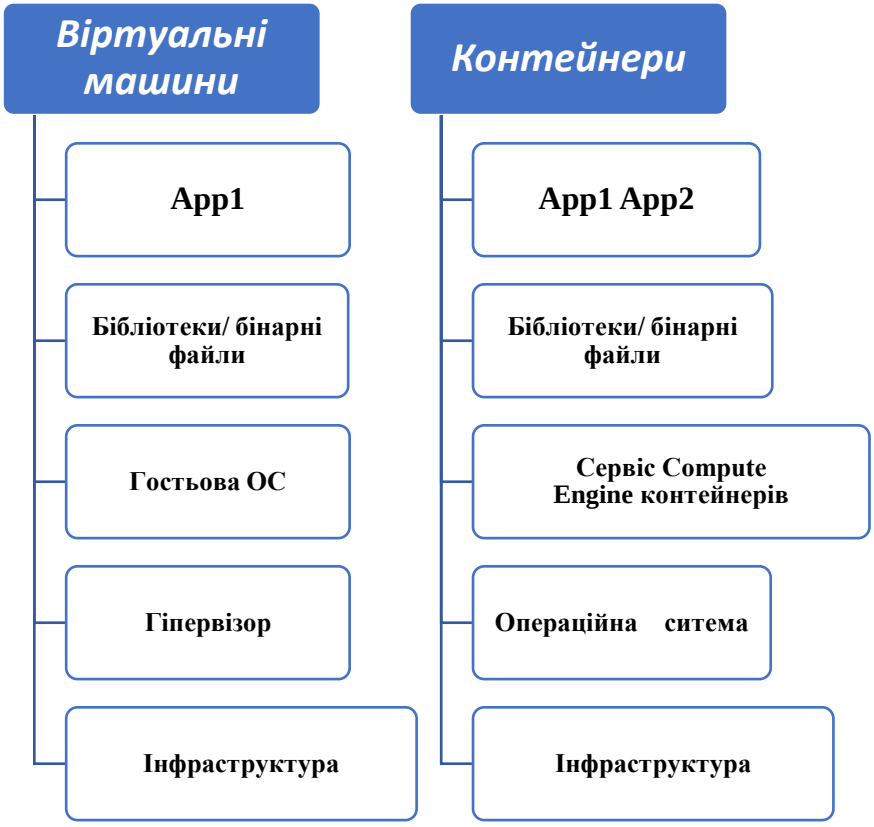

Рисунок 1.5 - Віртуальні машини проти контейнерів

Ця схема (Рис.1.5) наочно демонструє ключову різницю: контейнери не потребують гостьової ОС, що робить їх легшими та швидшими у запуску, на відміну від віртуальних машин.

Якщо ви все ще перебуваєте на етапі розробки, ви можете встановити сервіс Compute Engine контейнерів на свій ноутбук і створити новий контейнер (або завантажити існуючий контейнер) локально, доки не завершите етап розробки.

Коли ви переходите до продакшену та маєте потребу запускати сотні екземплярів контейнерів, вам потрібен оркестратор - механізм (або керована служба) для керування розгортанням контейнерів, моніторингом перевірок справності, переробкою контейнерів тощо.

Docker був прийнятий галуззю як фактичний стандарт для обгортання контейнерів, і за останні кілька років все більше постачальників хмарних послуг почали підтримувати нову ініціативу щодо обгортання контейнерів під назвоюІніціатива «Відкритий контейнер»(ОЦІ).

Kubernetes -це проєкт з відкритим кодом (спочатку розроблений Google), який зараз вважається галузевим стандартом де-факто для оркестрації, розгортання, масштабування та управління контейнерами.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:

Що таке контейнер?: https://surl.lu/zvdgqs

Ініціатива «Відкритий контейнер»: https://surl.li/tmffjg

Підтримка артефактів OCI в Amazon ECR:

https://surl.li/obzlrj
Образи Azure та OCI: https://surl.li/zoeazk
Формат зображення GCP та OCI:
https://surli.cc/leaotq
*Проєкт Kubernetes:*https://surl.lu/xenxgk

Захист служби еластичних контейнерів Amazon (ECS)

ECS -це служба оркестрації контейнерів, керована Amazon. Він може інтегруватися з іншими сервісами AWS, такими як Amazon реєстр еластичних контейнерів (ЕКР) для зберігання контейнерів, AWS IAM для керування дозволами до ECS та Amazon CloudWatch для моніторингу ECS.

Найкращі практики налаштування IAM для Amazon ECS. AWS IAM - це підтримуваний сервіс для керування дозволами на доступ та запуск контейнерів через Amazon ECS.

Найкращі практики такі:

- Надайте мінімальні дозволи IAM для служби Amazon ECS (для запуску завдань, доступу до корзин S3, моніторингу за допомогою подій CloudWatch тощо).
- Якщо ви керуєте кількома обліковими записами AWS, використовуйте тимчасові облікові дані (за допомогою служби токенів безпеки AWS або прийняти роль можливість) керувати ECS у цільовому обліковому записі AWS за допомогою облікових даних з вихідного облікового запису AWS.
- Використовуйте службові ролі, щоб дозволити службі ECS взяти на себе вашу роль і отримати доступ до ресурсів, таких як корзини S3, бази даних RDS тощо.
- Використовуйте ролі IAM для контролю доступу до Amazon еластична файлова система(ЕФС) від ECS.
- Забезпечити виконання багатофакторної автентифікації (МЗС) для кінцевих користувачів, які мають доступ до консолі AWS та виконують привілейовані дії, такі як керування сервісом ECS.
- Забезпечити дотримання умов політики, таких як вимога до кінцевих користувачів підключатися до служби ECS за допомогою захищеного каналу (SSL/TLS), підключатися за допомогою MFA, входити в систему у певні години доби тощо.
- Зберігайте образи контейнерів всередині Amazon ECR та надавайте мінімальні дозволи IAM для доступу та керування Amazon ECR.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Роль IAM екземпляра контейнера Amazon ECS:
https://surl.lu/meusig
Ролі IAM для завдань: https://surl.li/tnkppt
Авторизація на основі тегів Amazon ECS: https://surl.li/mccisz

Використання IAM для керування доступом до даних файлової системи: https://surl.lu/vtddyw
Безпека завдань і контейнерів Amazon ECS: https://surl.li/tqjbkw

Найкращі практики для забезпечення мережевого доступу до Amazon ECS

Оскільки Amazon ECS є керованим сервісом, він розташований поза межами VPC клієнта. Альтернативою безпечному доступу з вашого VPC до керованого середовища ECS є використання AWS Private Link, що дозволяє уникнути надсилання мережевого трафіку за межі вашого VPC через захищений канал, використовуючи кінцеву точку інтерфейсу VPC.

Найкращі практики такі:

- Використовуйте захищений канал (TLS 1.2) для керування Amazon ECS за допомогою викликів API.
- Використовуйте групи безпеки VPC, щоб дозволити доступ з вашого VPC до кінцевої точки Amazon ECS VPC.
- Якщо ви використовуєте AWS Secrets Manager для зберігання конфіденційних даних (таких як облікові дані) з Amazon ECS, використовуйте кінцеву точку Secrets Manager VPC під час налаштування груп безпеки.
- Якщо ви використовуєте AWS Systems Manager для віддаленого виконання команд на Amazon ECS, використовуйте кінцеві точки Systems Manager VPC під час налаштування груп безпеки.
- Зберігайте образи контейнерів в Amazon ECR, а для середовищ, що не містять конфіденційної інформації, шифруйте образи контейнерів в Amazon ECR за допомогою AWS KMS.
- Для чутливих середовищ шифруйте образи контейнерів всередині Amazon ECR за допомогою керування CMK.
- Якщо ви використовуєте Amazon ECR для зберігання образів контейнерів, використовуйте групи безпеки VPC, щоб дозволити доступ з вашого VPC до кінцевої точки VPC інтерфейсу Amazon ECR.
- Закріплення контейнерів.

Для отримання додаткової інформації, будь ласка, зверніться до наступного ресурсу:
*Кінцеві точки VPC інтерфейсу Amazon ECS (AWS Private Link):*https://surl.li/ahnobf

Найкращі практики проведення аудиту та моніторингу в Amazon ECS

Аудит є важливою частиною захисту даних. Як і будь-який інший керований сервіс, AWS дозволяє ввімкнути ведення журналу та аудит за допомогою двох вбудованих сервісів:

- *Amazon CloudWatch*. Сервіс, який дозволяє реєструвати активність контейнерів та піднімати тривогу відповідно до попередньо визначених порогових значень (наприклад, низький рівень ресурсів пам'яті або

високе навантаження на процесор, що вимагає масштабування кластера ECS).
- *AWS CloudTrail.* Сервіс, який дозволяє відстежувати активність API (по суті, будь-яку дію, що виконується в кластері ECS).

Найкращі практики такі:
- Увімкнути сповіщення Amazon CloudWatch для високопродуктивного використання (що може свідчити про аномалію в поведінці кластера ECS).
- Увімкнути AWS CloudTrail для будь-якої дії, що виконується в кластері ECS.
- Обмежте доступ до журналів CloudTrail мінімальною кількістю співробітників - бажано в обліковому записі керування AWS, поза межами доступу ваших кінцевих користувачів (включно з тими, що не входять до компетенції адміністраторів вашого кластера ECS), щоб уникнути можливого видалення або зміни журналів аудиту.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Ведення журналу та моніторинг в Amazon ECS:
https://surl.li/npzmab
*Реєстрація викликів Amazon ECS API за допомогою AWS CloudTrail:*https://surli.cc/hkrgfs

Найкращі практики для забезпечення відповідності вимогам на Amazon ECS

Конфігурація безпеки є важливою частиною вашої інфраструктури. Amazon дозволяє проводити постійні перевірки на відповідність відомим стандартам безпеки (таким як Центр тестів безпеки в Інтернеті).

Найкращі практики такі:
- Використовуйте лише перевірені контейнери образів і зберігайте їх в Amazon ECR - приватному репозиторії для зберігання образів вашої організації.
- Запустіть Docker Bench для безпеки інструментів на регулярній основі для перевірки відповідності CIS Benchmarks для контейнерів Docker.
- Створюйте образи контейнерів з нуля (щоб уникнути шкідливого коду в попередньо налаштованих образах сторонніх розробників).
- Скануйте образи контейнерів на наявність вразливостей у бібліотеках і бінарних файлах і регулярно оновлюйте свої образи.
- Налаштуйте свої образи з кореневою файловою системою лише для читання, щоб уникнути ненавмисного завантаження шкідливого коду на ваші образи.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Docker Bench для безпеки: https://surl.lt/dbrxny
Приватні репозиторії Amazon ECR: https://surli.cc/ztotki

Захист служби Amazon Elastic Kubernetes (EKS)

EKS -це служба оркестрації Kubernetes, керована Amazon. Він може інтегруватися з іншими сервісами AWS, такими як Amazon ECR для зберігання контейнерів, AWS IAM для керування дозволами до EKS та Amazon CloudWatch для моніторингу EKS.

AWS IAM - це підтримуваний сервіс для керування дозволами на доступ та запуск контейнерів через Amazon EKS.

Найкращі практики такі:

- Надайте мінімальні дозволи IAM для доступу та керування Amazon EKS.
- Якщо ви керуєте кількома обліковими записами AWS, використовуйте тимчасові облікові дані (за допомогою служби токенів безпеки AWS або Прийняти Роль можливість) керувати EKS у цільовому обліковому записі AWS за допомогою облікових даних з вихідного облікового запису AWS.
- Використовуйте службові ролі, щоб дозволити службі EKS взяти на себе вашу роль і отримати доступ до ресурсів, таких як корзини S3 та бази даних RDS.
- Для цілей автентифікації уникайте використання токенів облікових записів служби.
- Створіть роль IAM для кожного щойно створеного кластера EKS.
- Створіть обліковий запис служби для кожної новоствореної програми.
- Завжди запускайте програми від імені користувача без прав root.
- Використовуйте ролі IAM для керування доступом до сервісів зберігання даних (таких як Amazon EBS, Amazon EFS та Amazon FSx for Lustre) з EKS.
- Забезпечити багатофакторну автентифікацію (MFA) для кінцевих користувачів, які мають доступ до консолі AWS та виконують привілейовані дії, такі як керування сервісом EKS.
- Зберігайте образи контейнерів всередині Amazon ECR та надавайте мінімальні дозволи IAM для доступу та керування Amazon ECR.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
*Як Amazon EKS працює з IAM:*https://surl.lt/lcmuhp
Ролі IAM для сервісних облікових записів:
https://surl.lu/rlwdlm
Ідентифікація та доступність: https://surli.cc/qrmdix

Найкращі практики для забезпечення мережевого доступу до Amazon EKS

Оскільки Amazon EKS є керованим сервісом, він розташований поза межами VPC клієнта. Альтернативою безпечному доступу з вашого VPC до керованого середовища EKS є використання AWS Private Link, що дозволяє уникнути надсилання мережевого трафіку за межі вашого VPC через захищений канал, використовуючи кінцеву точку інтерфейсу VPC.

Найкращі практики такі:

- Використовуйте TLS 1.2 для керування Amazon EKS за допомогою викликів API.
- Використовуйте TLS 1.2 під час налаштування Amazon EKS за AWS Application Load Balancer або AWS Network Load Balancer.
- Використовуйте TLS 1.2 між вашою площиною керування EKS та робочими вузлами кластера EKS.
- Використовуйте групи безпеки VPC, щоб дозволити доступ з вашого VPC до кінцевої точки Amazon EKS VPC.
- Використовуйте групи безпеки VPC між вашою площиною керування EKS та робочими вузлами кластера EKS.
- Використовуйте групи безпеки VPC для захисту доступу до ваших EKS Pods.
- Вимкніть публічний доступ до вашого сервера API EKS - або використовуйте екземпляр EC2 (або бастіонний хост) для віддаленого керування кластером EKS, або створіть VPN-тунель з віддаленої машини до кластера EKS.
- Якщо ви використовуєте AWS Secrets Manager для зберігання конфіденційних даних (таких як облікові дані) з Amazon EKS, використовуйте кінцеву точку Secrets Manager VPC під час налаштування груп безпеки.
- Зберігайте образи контейнерів в Amazon ECR, а для середовищ, що не містять конфіденційної інформації, шифруйте образи контейнерів в Amazon ECR за допомогою AWS KMS.
- Для чутливих середовищ шифруйте образи контейнерів всередині Amazon ECR за допомогою керування CMK.
- Якщо ви використовуєте Amazon ECR для зберігання образів контейнерів, використовуйте групи безпеки VPC, щоб дозволити доступ з вашого VPC до кінцевої точки VPC інтерфейсу Amazon ECR.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Безпека мережі: https://surl.li/btalbj
Мережа Amazon EKS: https://surl.lt/ecrbzn
Представляємо групи безпеки для Pods: https://surl.lu/eggbbr
Посібники з найкращих практик EKS: https://surl.li/wogeai

Найкращі практики проведення аудиту та моніторингу в Amazon EKS

Аудит є важливою частиною захисту даних.

Як і будь-який інший керований сервіс, AWS дозволяє ввімкнути ведення журналу та аудит за допомогою двох вбудованих сервісів:

- *Amazon CloudWatch.* Служба, яка дозволяє реєструвати активність кластера EKS та піднімати тривогу відповідно до попередньо визначених порогових значень (наприклад, низький рівень ресурсів пам'яті або високе навантаження на процесор, що вимагає масштабування кластера EKS).
- *AWS CloudTrail.* Служба, яка дозволяє відстежувати активність API (по суті, будь-яку дію, що виконується в кластері EKS).

Найкращі практики такі:

- Увімкніть площину керування Amazon EKS під час входу в Amazon CloudWatch - це дозволить вам реєструвати виклики API, аудит та інформацію про автентифікацію з вашого кластера EKS.
- Увімкнути AWS CloudTrail для будь-якої дії, що виконується в кластері EKS.
- Обмежте доступ до журналів CloudTrail мінімальною кількістю співробітників - бажано в обліковому записі керування AWS, поза межами доступу ваших кінцевих користувачів (включно з тими, що не входять до компетенції адміністраторів кластера EKS), щоб уникнути можливого видалення або зміни журналів аудиту.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:

*Журнал керування Amazon EKS:*https://surl.li/ldbcuu

*Аудит та ведення журналу:*https://surl.li/pqrybk

Найкращі практики для забезпечення відповідності вимогам в Amazon EKS

Конфігурація безпеки є важливою частиною вашої інфраструктури. Amazon дозволяє проводити постійні перевірки відповідності відомим стандартам безпеки (таким як CIS Benchmarks).

Найкращі практики такі:

- Використовуйте лише перевірені контейнери образів і зберігайте їх в Amazon ECR - приватному репозиторії для зберігання образів вашої організації.
- Запустіть Docker Bench для безпеки інструментів на регулярній основі для перевірки відповідності CIS Benchmarks для контейнерів Docker.
- Створюйте образи контейнерів з нуля, щоб уникнути шкідливого коду в попередньо налаштованих образах сторонніх розробників.

- Скануйте образи контейнерів на наявність вразливостей у бібліотеках і бінарних файлах і регулярно оновлюйте свої образи.
- Налаштуйте свої образи з кореневою файловою системою лише для читання, щоб уникнути ненавмисного завантаження шкідливого коду на ваші образи.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Аналіз конфігурації та вразливостей в Amazon EKS: https://surli.cc/fwnyoz
Представляємо бенчмарк Amazon EKS для СНД:
https://surl.li/uetbem
Відповідність: https://surl.lu/wziqle
Безпека зображення: https://surl.li/hklqil
Безпека капсули: https://surl.li/maxhfo
кубе-лава: https://surl.lt/ifcuew
Docker Bench для безпеки: https://surli.cc/yjnwbd
Приватні репозиторії Amazon ECR:
https://surl.lu/czmzwc

Захист екземплярів контейнерів Azure (ACI)

ACI - це служба оркестрації контейнерів, керована Azure. Він може інтегруватися з іншими сервісами Azure, такими як реєстр контейнерів Azure (AKP) для зберігання контейнерів, Azure AD для керування дозволами до ACI, Azure Files для постійного сховища та Azure Monitor.

Найкращі практики налаштування IAM для ACI

Хоча ACI не має власного механізму автентифікації, рекомендується використовувати ACR для зберігання образів контейнерів у приватному реєстрі.

ACR підтримує такі методи автентифікації:

- Керована ідентифікація - обліковий запис користувача або системи з Azure AD
- Директор служби - додаток, сервіс або платформа, якій потрібен доступ до ACR

Найкращі практики такі:

- Надайте мінімальні дозволи для доступу та керування ACR за допомогою Azure RBAC.
- Під час передачі конфіденційної інформації (наприклад, секретних даних облікових даних) переконайтеся, що трафік зашифровано під час передачі через захищений канал (TLS).
- Якщо вам потрібно зберігати конфіденційну інформацію (наприклад, облікові дані), зберігайте її всередині служби Azure Key Vault.
- Для конфіденційних середовищ шифруйте інформацію (наприклад, облікові дані) за допомогою ключі, керовані клієнтом, що зберігається всередині служби Azure Key Vault.

- Вимкніть вбудованого адміністратора ACR.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Автентифікація за допомогою ACR: https://surl.li/udbglk
*Ролі та дозволи ACR:*https://surli.cc/beyyah
Зашифруйте реєстр за допомогою ключа, керованого клієнтом: https://surl.lu/uzjdzp

Найкращі практики проведення аудиту та моніторингу в ACI

Як і будь-який інший керований сервіс, Azure дозволяє ввімкнути ведення журналу та аудит за допомогою Azure Monitor for containers - сервісу, який дозволяє реєструвати дії, пов'язані з контейнерами, та піднімати тривогу відповідно до попередньо визначених порогових значень (наприклад, низькі ресурси пам'яті або високе навантаження на процесор, що вимагає масштабування середовища контейнерів).

Найкращі практики такі:

- Увімкніть ведення журналу аудиту для ресурсів Azure за допомогою Azure Monitor, щоб реєструвати дії, пов'язані з автентифікацією, вашого ACR.
- Обмежте доступ до журналів Azure Monitor мінімальною кількістю співробітників, щоб уникнути можливого видалення або зміни журналів аудиту.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Огляд статистики контейнерів: https://surl.li/ulbfrq
Рішення для моніторингу контейнерів у Azure Monitor: https://surli.cc/idcbsv

Найкращі практики для забезпечення відповідності ACI.

Конфігурація безпеки є важливою частиною вашої інфраструктури. Azure дозволяє проводити постійні перевірки відповідності відомим стандартам безпеки (таким як CIS Benchmarks).

Найкращі практики такі:

- Використовуйте лише перевірені контейнери образів і зберігайте їх в ACR - приватному репозиторії для зберігання образів вашої організації.
- Інтегруйте ACR з Центром безпеки Azure для виявлення невідповідних образів (стандарту CIS).
- Створюйте образи контейнерів з нуля (щоб уникнути шкідливого коду в попередньо налаштованих образах сторонніх розробників).
- Скануйте образи контейнерів на наявність вразливостей у бібліотеках і бінарних файлах і регулярно оновлюйте свої образи.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Базовий рівень безпеки Azure для ACI: https://surl.li/dwwdrf
Базовий рівень безпеки Azure для ACR: https://surl.lt/aqpihq
Міркування безпеки для ACI: https://surl.lt/dtokno
Вступ до приватних реєстрів контейнерів Docker в Azure: https://surl.li/rtzqhl

Захист служби Azure Kubernetes (AKS)

AKS -це служба оркестрації Kubernetes, керована Azure. Він може інтегруватися з іншими службами Azure, такими як ACR для зберігання контейнерів, Azure AD для керування дозволами AKS, Azure Files для постійного сховища та Azure Monitor.

Azure AD - це підтримувана служба для керування дозволами на доступ і запуск контейнерів через Azure AKS.

Найкращі практики такі:

- Увімкнути інтеграцію Azure AD для будь-якого щойно створеного кластера AKS.
- Надайте мінімальні дозволи для доступу та керування AKS за допомогою Azure RBAC.
- Надайте мінімальні дозволи для доступу та керування ACR за допомогою Azure RBAC.
- Створіть унікального принципала служби для кожного щойно створеного кластера AKS.
- Під час передачі конфіденційної інформації (наприклад, секретних даних облікових даних) переконайтеся, що трафік зашифровано під час передачі через захищений канал (TLS).
- Якщо вам потрібно зберігати конфіденційну інформацію (наприклад, облікові дані), зберігайте її всередині служби Azure Key Vault.
- Для конфіденційних середовищ шифруйте інформацію (наприклад, облікові дані) за допомогою ключі, керовані клієнтом, що зберігається всередині служби Azure Key Vault.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Інтеграція Azure AD, керована AKS:
https://surl.li/bsicst
Найкращі практики для автентифікації та авторизації в AKS: https://surl.lu/gcoblf

Рекомендації щодо забезпечення мережевого доступу до Azure AKS

Azure AKS надає сервісам доступ до Інтернету - саме тому важливо планувати розгортання кожного кластера Azure AKS перед його розгортанням.

Найкращі практики такі:

- Уникайте доступу до площини керування кластера AKS (сервера API) до загальнодоступного Інтернету - створіть приватний кластер із внутрішньою IP-адресою та використовуйте авторизовані діапазони IP-адрес, щоб визначити, які IP-адреси можуть отримати доступ до вашого сервера API.
- Використовуйте службу Azure Firewall для обмеження вихідного трафіку з вузлів кластера AKS на зовнішні адреси DNS (наприклад, оновлення програмного забезпечення із зовнішніх джерел).
- Використовуйте TLS 1.2 для керування Azure AKS за допомогою викликів API.
- Використовуйте TLS 1.2 під час налаштування Azure AKS за Azure Load Balancer.
- Використовуйте TLS 1.2 між площиною керування AKS та вузлами кластера AKS.
- Для невеликих розгортань AKS використовуйте кубенетплагін для реалізації мережевих політик та захисту кластера AKS.
- Для великих розгортань у виробничому середовищі використовуйте плагін Azure CNI Kubernetes для впровадження мережевих політик та захисту кластера AKS.
- Використовуйте групи безпеки мережі Azure для блокування SSH-трафіку до вузлів кластера AKS лише з підмереж AKS.
- Використовуйте мережеві політики для захисту доступу між подами Kubernetes.
- Вимкніть публічний доступ до вашого сервера API AKS - або використовуйте віртуальну машину Azure (або Azure Bastion) для віддаленого керування кластером AKS, або створіть VPN-тунель з віддаленого комп’ютера до кластера AKS.
- Вимкніть або видаліть надбудову маршрутизації HTTP-застосунків.
- Якщо вам потрібно зберігати конфіденційну інформацію (наприклад, облікові дані), зберігайте її всередині служби Azure Key Vault.
- Для конфіденційних середовищ шифруйте інформацію (наприклад, облікові дані) за допомогою ключі, керовані клієнтом, що зберігається всередині служби Azure Key Vault.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Рекомендації щодо підключення до мережі та безпеки в AKS: https://surl.li/zdqhnk
Рекомендації щодо ізоляції кластерів в AKS: https://surl.li/krcope
Створіть приватний кластер AKS: https://surl.lu/npluur

Рекомендації щодо проведення аудиту та моніторингу в Azure AKS

Як і будь-який інший керований сервіс, Azure дозволяє ввімкнути ведення журналу та аудит за допомогою Azure Monitor for containers - сервісу, який дозволяє реєструвати дії, пов'язані з контейнерами, та піднімати тривогу відповідно до попередньо визначених порогових значень (наприклад, низькі ресурси пам'яті або високе навантаження на процесор, що вимагає масштабування середовища контейнерів).

Найкращі практики такі:

- Увімкніть ведення журналу аудиту для ресурсів Azure за допомогою Azure Monitor, щоб реєструвати дії, пов'язані з автентифікацією, вашого ACR.
- Обмежте доступ до журналів Azure Monitor мінімальною кількістю співробітників, щоб уникнути можливого видалення або зміни журналів аудиту.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Огляд ACI: https://surl.lt/acpoel
Рішення для моніторингу контейнерів у Azure Monitor: https://surl.li/dvmqpx

Рекомендації щодо забезпечення відповідності вимогам у Azure AKS

Конфігурація безпеки є важливою частиною вашої інфраструктури. Azure дозволяє проводити постійні перевірки відповідності відомим стандартам безпеки (таким як CIS Benchmarks).

Найкращі практики такі:

- Використовуйте лише перевірені контейнери образів і зберігайте їх в ACR - приватному репозиторії для зберігання образів вашої організації.
- Використовуйте Azure Defender для Kubernetes для захисту кластерів Kubernetes від вразливостей.
- Використовуйте Azure Defender для реєстрів контейнерів, щоб виявляти та усувати вразливості в образах контейнерів.
- Інтегрований реєстр контейнерів Azure з Центром безпеки Azure для виявлення несумісних образів (зі стандартом CIS).
- Створюйте образи контейнерів з нуля (щоб уникнути шкідливого коду в попередньо налаштованих образах сторонніх розробників).
- Скануйте образи контейнерів на наявність вразливостей у бібліотеках і бінарних файлах і регулярно оновлюйте свої образи.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Вступ до Azure Defender для Kubernetes:
https://surl.li/bgqrfj

Використовуйте Azure Defender для реєстрів контейнерів, щоб сканувати образи на наявність вразливостей: https://surli.cc/xvqglv
Базовий рівень безпеки Azure для ACI: https://surli.cc/ckobsl
Базовий рівень безпеки Azure для ACR: https://surl.li/joqurn
*Міркування безпеки для ACI:*https://surl.li/wtxmsy
Вступ до приватних реєстрів контейнерів Docker в Azure: https://surl.lu/grajpq

Захист сервісу Compute Engine контейнерів Google Kubernetes (GKE)

GKE - це служба оркестрації Kubernetes, керована Google. Він може інтегруватися з іншими сервісами GCP, такими як Google Container Registry для зберігання контейнерів, Google Cloud IAM для керування дозволами до GKE, Google Filestore для постійного зберігання та Google Cloud Operations для моніторингу.

Google Cloud IAM - це підтримуваний сервіс для керування дозволами на доступ і запуск контейнерів через GKE.

Найкращі практики такі:

- Надайте мінімальні дозволи для доступу та керування сервісом Google Cloud IAM за допомогою Kubernetes RBAC.
- Використовуйте Групи Google для керування дозволами до вашого кластера GKE.
- Використовуйте пропозицію Google IAM, щоб встановити мінімальні дозволи для вашого кластера GKE.
- Створіть унікальний обліковий запис служби з мінімальними дозволами для будь-якого щойно створеного кластера GKE.
- Забезпечте використання багатофакторної автентифікації (MFA) для будь-якого користувача, якому потрібен доступ для керування вашим кластером GKE.
- Якщо вам потрібно зберігати конфіденційну інформацію (наприклад, облікові дані), зберігайте її всередині служби Google Cloud KMS.
- Для конфіденційних середовищ шифруйте інформацію (наприклад, облікові дані) за допомогою ключів CMEK, що зберігаються в сервісі Google Cloud KMS.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Створення політик IAM: https://surl.lu/qebtko
Забезпечити мінімальні привілеї за допомогою рекомендацій: https://surl.li/lqrrzg
Використовувати облікові записи сервісів Google з найменшими привілеями: https://surl.lu/vvauhs
Таємне управління: https://surl.lu/jrwnyd

Найкращі практики для забезпечення мережевого доступу до GKE

GKE надає сервіси в Інтернет - саме тому важливо планувати розгортання кожного кластера GKE перед його розгортанням.

Найкращі практики такі:

- Створюйте приватні кластери GKE, щоб уникнути доступу до площини керування кластера GKE (сервера API) до публічного Інтернету - використовуйте діапазони IP-адрес псевдонімів, щоб налаштувати, які IP-адреси матимуть доступ до вашого кластера GKE.
- Використовуйте авторизовані мережі, щоб налаштувати, хто може отримати доступ до вашої площини керування кластером GKE.
- Використовуйте мережу, налаштовану на VPC, для захисту доступу між подами Kubernetes.
- Використовуйте мережеві політики для Kubernetes, щоб захистити доступ між подами Kubernetes.
- Використовуйте екрановані вузли GKE як додатковий рівень захисту для вузлів вашого кластера GKE.
- Створіть окремі простори імен для ваших програм відповідно до вимог RBAC.
- Увімкніть пісочницю GKE для кращої ізоляції ваших подів кластера GKE.
- Використовуйте TLS 1.2 для керування кластером GKE за допомогою викликів API.
- Використовуйте TLS 1.2 між вашою площиною керування GKE та вузлами кластера GKE.
- Використовуйте TLS 1.2 під час налаштування кластера GKE за Google Load Balancer.
- Вимкніть публічний доступ до сервера API кластера GKE - використовуйте віртуальну машину Google (або хост Bastion) для віддаленого керування кластером GKE.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Створення приватного кластера:
https://surl.li/sepbvp
Обмежити мережевий доступ до площини керування та вузлів: https://surl.li/brigus
Обмежте трафік між подами за допомогою мережевої політики: https://surl.lu/jszhkx
Безпека мережі: https://surl.li/yenjti

Найкращі практики проведення аудиту та моніторингу в GKE

Як і будь-який інший керований сервіс, Google дозволяє ввімкнути ведення журналу та аудит за допомогою служби Google Cloud Logging - сервісу, який дозволяє проводити аудит дій, пов’язаних із контейнерами.

Найкращі практики такі:

- Увімкніть ведення журналу для будь-якого щойно створеного кластера GKE та інтегруйте елемент із сервісом ведення журналу Google Cloud, щоб реєструвати всі аудиторські дії, пов'язані з вашим кластером GKE.
- Під час використання операційна система, оптимізована для контейнерів зображення, обов'язково надішліть журнали аудиту Linux до служби реєстрації Google Cloud.
- Обмежте доступ до журналів служби ведення журналів Google Cloud мінімальною кількістю співробітників, щоб уникнути можливого видалення або зміни журналів аудиту.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Політика аудиту: https://surl.li/eyplit
Огляд операційного пакету Google Cloud для GKE:
https://surl.lu/tyfalc
Виправлення результатів аналітики стану безпеки: https://surl.li/pxdxtn

Найкращі практики для забезпечення відповідності вимогам у GKE

Конфігурація безпеки є важливою частиною вашої інфраструктури.

Google дозволяє вам проводити постійні перевірки відповідності відомим стандартам безпеки (таким як CIS Benchmarks).

Найкращі практики такі:

- Використовуйте лише перевірені контейнери зображень та зберігайте їх у реєстрі контейнерів Google - приватне сховище для зберігання образів вашої організації.
- Завжди використовуйте останню збірку Kubernetes як на кластері GKE, так і на вузлах кластера.
- Використовуйте аудитор GKE для виявлення неправильних конфігурацій GKE.
- Використовуйте операційні системи, оптимізовані для контейнерів, під час створення нових образів контейнерів для кращої безпеки.
- Створюйте образи контейнерів з нуля (щоб уникнути шкідливого коду в попередньо налаштованих образах сторонніх розробників).
- Скануйте образи контейнерів на наявність вразливостей у бібліотеках і бінарних файлах і регулярно оновлюйте свої образи.
- Використовуйте авторизацію бінарних файлів Google, щоб переконатися, що ви використовуєте лише підписані образи контейнерів від перевірених джерел.
- Використовуйте функцію виявлення загроз контейнерам для виявлення атак на образи контейнерів у режимі реального часу.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Концептуальний огляд виявлення загроз контейнерам: https://surl.lu/xcemos

Аудитор GKE: https://surl.li/ybmdii
Бінарна авторизація: https://surl.lu/lzmakk
Реєстр контейнерів: https://surli.cc/vaijqa

Захист безсерверних систем/функцій як послуг

Хоча назва передбачає відсутність серверів, термін безсерверний або функціонувати як послуга означає, що ви, як клієнт послуги, не відповідаєте за базову обчислювальну інфраструктуру (обслуговування операційної системи, масштабування, керування середовищем виконання тощо) - ви просто імпортуєте свій код (відповідно до мови, що підтримується кожним постачальником хмарних послуг).

На наступній діаграмі (Рис. 1.6) показано архітектурні відмінності між віртуальними машинами, контейнерами та безсерверними системами:

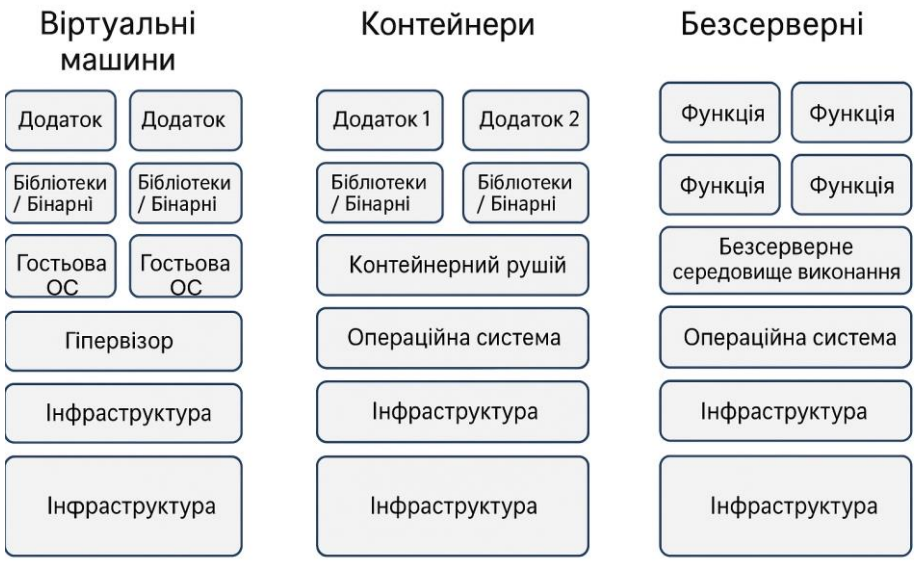

Рисунок 1.6 - Порівняння віртуальних машин, контейнерів та безсерверних систем

Захист AWS Lambda

AWS Lambda - це безсерверний сервіс Amazon.

Він може інтегруватися з іншими сервісами AWS, такими як AWS IAM для керування дозволами до AWS Lambda, Amazon CloudWatch для моніторингу AWS Lambda, а також Amazon S3 та Amazon EFS для постійного зберігання даних.

AWS IAM - це підтримуваний сервіс для керування дозволами на доступ до AWS Lambda.

Найкращі практики такі:

- Надайте мінімальні дозволи IAM для будь-якої щойно створеної функції AWS Lambda (для запуску завдань, доступу до корзин S3, моніторингу за допомогою подій CloudWatch тощо) - порівняйте певну роль IAM з будь-якою щойно створеною функцією AWS Lambda.

- Використовуйте інструменти з відкритим кодом, такі як безсерверний-puresec-cli, щоб створити ролі IAM для вашої функції.
- Уникайте зберігання облікових даних у коді AWS Lambda.
- Якщо вам потрібно зберігати конфіденційні дані (наприклад, облікові дані), використовуйте AWS Secrets Manager.
- Для кращого захисту ваших функцій Lamba налаштуйте AWS Lambda позаду Amazon API Gateway.
- Для чутливих середовищ шифруйте змінні середовища Lambda за допомогою керування CMK.
- Використовуйте TLS 1.2 для шифрування конфіденційних даних у мережі.
- Забезпечити багатофакторну автентифікацію (MFA) для кінцевих користувачів, які мають доступ до API AWS (консолі, CLI та SDK) та виконують привілейовані дії, такі як керування сервісом Lambda.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Політики IAM на основі ідентифікації для Lambda:
https://surl.li/jiddqh
*Найкращі практики безпеки:*https://surl.li/plnzcq
Шифрування змінних середовища Lambda:
https://surl.li/eegtgd
безсерверний-puresec-cli: https://surl.li/dhwjek

Найкращі практики для забезпечення мережевого доступу до AWS Lambda

AWS Lambda можна розгорнути як зовнішній ресурс поза межами вашого VPC або всередині вашого VPC - саме тому важливо планувати розгортання кожної функції Lambda перед розгортанням.

Найкращі практики такі:
- Використовуйте Amazon API Gateway, щоб обмежити доступ до вашої функції Lambda з певної IP-адреси або CIDR.
- Якщо ваша лямбда-функція розташована поза межами VPC, і лямбда-функції потрібен доступ до ресурсів усередині вашого VPC, використовуйте AWS PrivateLink, який дозволяє уникнути надсилання мережевого трафіку за межі вашого VPC через захищений канал, використовуючи інтерфейс Кінцева точка VPC.
- Якщо ваша лямбда-функція розташована всередині вашого VPC, і лямбда-функції потрібен доступ до зовнішніх ресурсів в Інтернеті, використовуйте шлюз NAT, щоб надати вашій лямбда-функції необхідний доступ, не піддаючи лямбда безпосередньо Інтернету.
- Використовуйте TLS 1.2 для шифрування трафіку до та від ваших лямбда-функцій.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
*Захист даних в AWS Lambda:*https://surli.cc/kwyljd
AWS Lambda тепер підтримує AWS PrivateLink:
https://surl.li/stljrw
Налаштування лямбда-функції для доступу до ресурсів у VPC: https://surli.cc/dhtymq
Як надати доступ до Інтернету функції Lambda, підключеній до Amazon VPC?
https://surl.li/ceombd

Найкращі практики проведення аудиту та моніторингу в AWS Lambda

Як і будь-який інший керований сервіс, AWS дозволяє ввімкнути аудит за допомогою сервісу AWS CloudTrail - сервісу, який дозволяє проводити аудит дій, пов'язаних з API.

Найкращі практики такі:

- Увімкніть розширений моніторинг ваших лямбда-функцій.
- Використовуйте Amazon CloudWatch для виявлення піків використання Lambda.
- Використовуйте AWS CloudTrail для моніторингу активності API, пов'язаної з вашою лямбда-функцією.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Використання AWS Lambda з AWS CloudTrail:
https://surl.li/abjalc
Використання AWS Lambda з подіями Amazon CloudWatch: https://surl.li/fvfnpx

Найкращі практики для забезпечення відповідності вимогам, зміни конфігурації та безпечного кодування в AWS Lambda

Безсерверна, або функція як послуга, -це переважно код, що виконується в закритому керованому середовищі.

Як клієнт, ви не можете контролювати базову інфраструктуру - тому вам потрібно інвестувати в безпечне кодування, щоб запобігти проникненню зловмисників у ваш застосунок та заподіянню шкоди, від якої AWS не може захистити.

Найкращі практики такі:

- Дотримуйтесь OWASP 10 найкращих безсерверних рішень проектну документацію під час написання коду лямбда-функції.
- Увімкніть версії у ваших лямбда-функціях, щоб мати змогу повернутися до попереднього коду.

- Використовуйте AWS Signer для підписання коду функції Lambda та переконайтеся, що ви запускаєте лише підписаний код.
- Якщо ви використовуєте Amazon API Gateway перед функціями Lambda, використовуйте авторизатор API Gateway Lambda як додатковий рівень захисту для авторизації доступу до ваших функцій Lambda.
- Використовуйте AWS Config для перевірки змін у ваших лямбда-функціях.
- Використовуйте шаблони оцінювання Amazon Inspector для виявлення невідповідностей або використання старих версій середовища виконання у ваших лямбда-функціях.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Використання AWS Lambda з AWS Config:
https://surl.li/leokay
Версії лямбда-функцій: https://surl.li/ptovby
Використовуйте авторизатори API Gateway Lambda: https://surl.li/snyvot
Налаштування автоматичного оцінювання виконується через лямбда-функцію:
https://surli.cc/mgxvji
Налаштування підписання коду для AWS Lambda:
https://surl.li/gjjisj
Топ-10 безсерверних рішень OWASP: https://surl.li/ygrkxy

Захист функцій Azure

Функції Azure -це функція Azure як послуга.

Вони можуть інтегруватися з іншими службами Azure, такими як Azure AD для керування дозволами на доступ до функцій Azure, Azure Monitor Application Insights для моніторингу функцій Azure та сховище Azure Blob для постійного зберігання.

Найкращі практики такі:

- Увімкніть автентифікацію Azure AD для будь-якої щойно створеної функції Azure, увімкнувши автентифікацію служби додатків Azure.
- Уникайте надання анонімного доступу до вашої функції Azure - вимагайте від клієнтів автентифікації перед використанням функцій Azure.
- Надайте мінімальні дозволи для будь-якої щойно створеної функції Azure за допомогою Azure RBAC.
- Надайте перевагу використанню тимчасових облікових даних для вашої функції Azure - використовуйте Підпис спільного доступу (CAC) токени для виконання цього завдання. Де це можливо, надавайте перевагу використанню клієнтських сертифікатів для автентифікації клієнтів у ваших функціях Azure.

- Щоб дозволити функціям Azure доступ до ресурсів Azure, використовуйте призначену системою керовану ідентифікацію з Azure AD.
- Якщо вам потрібно зберігати конфіденційні дані (наприклад, облікові дані), використовуйте Azure Key Vault.
- Для конфіденційних середовищ зашифруйте налаштування програми Azure Functions за допомогою керування ключами, керованого клієнтом, у Azure Key Vault.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Як використовувати керовані посвідчення для служби програм і функцій Azure: https://surl.lu/wjrxbc
Авторизації функцій Azure: https://surl.li/vhtuoa
Використовуйте посилання на Key Vault для служби програм і функцій Azure: https://surli.cc/wgaduc

Найкращі практики для захисту даних і доступу до мережі до функцій Azure

Функції Azure можуть отримувати доступ до ресурсів у вашій підписці Azure - саме тому важливо планувати розгортання кожної функції Azure перед розгортанням.

Найкращі практики такі:
- Для кращого захисту ваших функцій Azure налаштуйте функцію Azure за шлюзом Azure API.
- Використовуйте TLS 1.2 для шифрування конфіденційних даних у мережі.
- Створіть окремий обліковий запис сховища Azure для будь-якої щойно створеної функції Azure.
- Використовуйте групи безпеки мережі Azure для блокування вихідного трафіку з ваших функцій Azure (коли доступ до Інтернету не потрібен).
- Використовуйте кінцеву точку служби Azure VNet для керування доступом до функцій Azure.
- Використовуйте обмеження статичної IP-адреси служби додатків Azure для керування доступом до функцій Azure.
- Використовуйте стандартний план Azure App Service або преміум-план Azure App Service для налаштування мережевої ізоляції ваших функцій Azure.
- Використовуйте Azure Defender для служби додатків як додатковий рівень захисту для ваших функцій Azure, які мають вхідний доступ з Інтернету.
- Використовуйте брандмауер веб-застосунків Azure як додатковий рівень захисту для ваших функцій Azure, які мають вхідний доступ з Інтернету.

- Вимкніть та заблокуйте використання протоколу FTP з вашими функціями Azure.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Параметри мережі Azure Functions: https://surl.lu/iparjw
Захистіть кінцеву точку HTTP у продакшені: https://surl.li/gsrpqv
Обмеження щодо IP-адрес: https://surl.li/xkbetr
Функції Azure та FTP: https://surl.li/ilzukk
Захистіть свої веб-програми та API: https://surl.li/xoqnho

Найкращі практики проведення аудиту та моніторингу в Azure Functions

Аудит є важливою частиною захисту даних. Як і будь-який інший керований сервіс, Azure дозволяє ввімкнути ведення журналу та аудит за допомогою служби Azure Monitor.

Найкращі практики такі:
- Використовуйте службу Azure Monitor для реєстрації дій, пов'язаних з автентифікацією, у ваших функціях Azure.
- Використовуйте функцію виявлення загроз Центру безпеки (Azure Defender).

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Ведення журналу та виявлення загроз:
https://surl.li/ousmkx
Базовий рівень безпеки Azure для функцій Azure:
https://surl.lu/iezjkb

Найкращі практики для забезпечення відповідності, зміни конфігурації та безпечного кодування у функціях Azure

Безсерверна архітектура, або функція як послуга, -це переважно код, що виконується в закритому, керованому середовищі.

Як клієнт, ви не можете контролювати базову інфраструктуру - тому вам потрібно інвестувати в безпечне кодування, щоб запобігти проникненню зловмисників у вашу програму та заподіянню шкоди, від якої Azure не може захистити.

Найкращі практики такі:
- Дотримуйтесь OWASP 10 найкращих безсерверних рішень документації проєкту під час написання коду Azure Functions.
- Використовуйте базовий рівень безпеки Azure для функцій Azure (Azure Security Benchmark).

- Використовуйте функцію виявлення загроз Центру безпеки (Azure Defender).

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Базовий рівень безпеки Azure для функцій Azure:
https://surli.cc/afsdst
Управління поставою та вразливістю:
https://surl.li/buulqe
Топ-10 безсерверних рішень OWASP: https://surl.li/betkge

Захист функцій Google Cloud

Функції Google Cloud -це функція GCP як послуга. Вони можуть інтегруватися з іншими сервісами GCP, такими як Google Cloud IAM для керування дозволами до Google Cloud Functions, Google Cloud Audit Logs для моніторингу Google Cloud Functions та Google CloudStorage для постійного зберігання даних.

Найкращі практики такі:
- Використовуйте Google Cloud IAM для керування дозволами на доступ до ваших функцій Google Cloud.
- Надайте мінімальні дозволи для доступу та керування сервісом Google Cloud IAM.
- Створіть унікальний обліковий запис служби для кожної новоствореної функції Google Cloud з мінімальними дозволами за допомогою служби Google Cloud IAM.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Авторизація доступу через IAM та автентифікація для виклику:
https://surl.li/gaylbw
Захист доступу за допомогою ідентифікації:
https://surl.li/fcpizm

Найкращі практики для захисту даних і доступу до мережі до Google Cloud Functions

Функції Google Cloud можуть отримувати доступ до ресурсів у вашому проєкті GCP - саме тому важливо планувати розгортання кожної функції Google Cloud перед розгортанням.

Найкращі практики такі:
- Використовуйте налаштування вхідного доступу до функцій Google Cloud, щоб контролювати, яка IP-адреса (або CIDR) може отримати доступ до вашої функції Google Cloud.

- Якщо вам потрібен доступ вашої функції Google Cloud до ресурсів у вашому VPC, використовуйте безсерверний доступ до VPC, щоб обмежити доступ до вашого VPC.
- Якщо ваша функція Google Cloud підключена до вашого VPC та потребує доступу до зовнішніх ресурсів, використовуйте налаштування вихідного потоку Google Cloud Functions, щоб керувати вихідними адресатами.
- Якщо вашій функції Google Cloud потрібен прямий вхідний доступ з Інтернету, використовуйте елементи керування послугами VPC як додатковий рівень захисту, щоб захистити свій периметр від витоку даних.
- Для конфіденційних середовищ шифруйте змінні середовища Google Cloud Functions за допомогою керування CMEK.
- Використовуйте TLS 1.2 для шифрування конфіденційних даних у мережі.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Налаштування безсерверного доступу VPC: https://surl.lu/onfblr
Використання елементів керування сервісом VPC:
https://surl.li/prrzhv
Управління таємницями: https://surl.li/peszvd

Найкращі практики проведення аудиту та моніторингу в Google Cloud Functions

Аудит є важливою частиною захисту даних. Як і будь-який інший керований сервіс, Google дозволяє ввімкнути ведення журналу та аудит за допомогою служби Google Cloud Audit Logs.

Найкращі практики такі:

- Журнали аудиту активності адміністратора ввімкнено за замовчуванням і не можна вимкнути.
- Явно ввімкнути журнали аудиту доступу до даних для реєстрації дій, виконаних у базі даних.
- Обмежте доступ до журналів аудиту мінімальною кількістю співробітників, щоб уникнути можливого видалення або зміни журналів аудиту.

Для отримання додаткової інформації, будь ласка, зверніться до наступних ресурсів:
Використання журналу хмарного аудиту з хмарними функціями: https://surl.lu/kgwbvw

1.3. Забезпечення безпеки послуг зберігання даних

У попередньому параграфі ми розглядали обчислювальні сервіси. Після обчислювальних сервісів, другим за поширеністю ресурсом, про який усі

говорять, є сховище - від об’єктного сховища до блочного сховища (яке також відоме як сховище, підключене до екземпляра), для зберігання файлів.

Ми використовуємо сервіси зберігання даних для зберігання наших даних. Нижче наведено перелік поширених загроз, які можуть вплинути на наші дані, коли вони зберігаються в хмарі:

- Несанкціонований доступ
- Витік даних
- Витік даних
- Втрата даних

Як найкраща практика, нам слід завжди використовувати такі контрзаходи під час зберігання даних у хмарі:

- Списки контролю доступу(ACL; зверніть увагу, що кожен постачальник хмарних послуг має власну реалізацію) та Управління ідентифікацією та доступом(Ідентифікація та доступність даних), щоб обмежити доступ з нашого хмарного середовища до служби зберігання даних
- Шифрування як під час передачі, так і під час зберігання для забезпечення конфіденційності даних
- Аудит для ведення журналу обліку того, хто має доступ до наших даних, і які дії були виконані з нашими даними (наприклад, завантаження, вивантаження, оновлення, видалення тощо)
- Резервні копії або створення знімків, щоб ми могли відновити видалені дані або повернутися до попередньої версії наших даних (наприклад, у разі шифрування наших даних програмою-вимагачем)

У цьому розділі буде розглянуто всі типи служб зберігання даних і надано рекомендації щодо безпечного підключення та використання кожної з них.

У цьому параграфі ми розглянемо такі теми:

1. Забезпечення безпеки зберігання об'єктів
2. Забезпечення безпеки блокового сховища
3. Захист сховища файлів
4. Забезпечення безпеки Інтерфейс зберігання контейнерів (Місце злочину)

Технічні вимоги

Для цього розділу вам потрібно мати фундаментальне розуміння сховища об'єктів, блочного сховища та сховища файлів.

Захист сховища об'єктів

Кожен постачальник хмарних послуг має власну реалізацію сховища об'єктів, але зрештою, основна ідея однакова:

- Об’єктне сховище - це спеціальний тип сховища, призначений для зберігання даних.
- Файли (або об'єкти) зберігаються всередині контейнерів (це логічні поняття, такі як каталоги або логічні контейнери).

- Доступ до файлів на об'єктному сховищі здійснюється або через API протоколу HTTP(S), використовуючи веб-інструменти командного рядка, або програмно за допомогою інструментів SDK.
- Об'єктне сховище не призначене для зберігання операційних систем або баз даних.

Далі ми розглянемо найкращі практики для захисту сервісів зберігання об'єктів від AWS, Azure та GCP.

Захист служби Amazon Simple Storage

Простий сервіс зберігання даних Amazon (Amazon S3) - це сервіс зберігання об’єктів Amazon.

Найкращі практики проведення автентифікації та авторизації для Amazon S3 AWS контролює доступ до корзин S3 за допомогою ACL. Доступ можна контролювати на рівні всіх контейнерів (разом з усіма об'єктами всередині цього контейнера) та на рівні певного об'єкта (наприклад, припустимо, що ви хочете поділитися певним файлом з кількома своїми колегами).

AWS підтримує такі методи доступу до дозволів корзини S3:

- *Політики IAM*. Це дозволяє вам встановити дозволи для дій, дозволених або заборонених для певної особи (наприклад, користувача, групи чи ролі).
- *Політики корзини*. Це дозволяє встановлювати дозволи на рівні корзини S3 - це застосовується до всіх об’єктів у корзині.
- *Точки доступу S3*. Це дає вам можливість надати доступ до S3-бакетів певній групі користувачів або програм.

Крім того, AWS контролює дозволи для ідентифікаційних даних (незалежно від ресурсів, таких як S3) на організаційній основі AWS (їх також називають політики контролю послуг або SCP-об'єкти).

Ефективні дозволи корзини S3 - це сума SCP з дозволами ідентифікації (політики IAM), загальними дозволами ресурсів (політики корзини) та політикою AWS KMS (наприклад, дозвіл на доступ до зашифрованого об’єкта), за умови, що користувачеві не було відмовлено за жодним із попередніх критеріїв.

Перелік найкращих практик, яких слід дотримуватися:

- Створіть групу IAM, додайте користувачів до групи IAM та надайте цільовій групі IAM необхідні дозволи на цільовий корзину S3.
- Використовуйте ролі IAM для сервісів (таких як програми або нелюдські ідентифікаційні дані), яким потрібен доступ до корзин S3.
- Обмежте доступ для користувачів/груп IAM до певного корзини S3, замість використання підстановочних символів для всіх корзин S3 в обліковому записі AWS.
- Видалити стандартні дозволи власника корзини для корзини S3.

- Використовуйте політики IAM для програм (або нелюдських ідентифікаційних даних)/ролей, пов’язаних із сервісами, яким потрібен доступ до корзин S3.
- Увімкнути Видалення багатофакторної автентифікації для відер S3, щоб уникнути випадкового видалення об'єктів з контейнера.
- Надати мінімальні дозволи для S3-бакетів (тобто певний ідентифікатор для певного ресурсу з певними умовами).
- Використовуйте ACL-списки для корзини писати дозволи для групи доставки журналів Amazon S3, щоб ця група мала можливість записувати журнали доступу (для подальшого аналізу).
- Для даних, які потрібно зберігати протягом тривалого часу (через нормативні вимоги), використовуйте блокування об’єкта S3 для захисту даних від випадкового видалення.
- Шифруйте дані в стані спокою за допомогою ключів шифрування, керовані Amazon S3(SSE-S3).
- Для чутливих середовищ шифруйте дані в стані спокою за допомогою ключів шифрування, надані клієнтом(SSE-C).

Для отримання додаткової інформації зверніться до наступних ресурсів:
Керування ідентифікацією та доступом в Amazon S3: https://surl.li/nohvyx
Політики IAM, політики корзин та ACL: https://surli.cc/nwjklu
Чим ролі IAM відрізняються від політик на основі ресурсів: https://surli.cc/tiprhh
Рекомендації щодо превентивної безпеки Amazon S3: https://surl.li/txfzpj
Налаштування поведінки шифрування на стороні сервера за замовчуванням для корзин Amazon S3: https://surl.li/cpylst
Розгляньте шифрування даних у стані спокою: https://surl.li/gcfcka

Найкращі практики для забезпечення мережевого доступу до Amazon S3

Оскільки Amazon S3 є керованим сервісом, він розташований поза межами клієнта.

Перелік найкращих практик, яких слід дотримуватися:

- Якщо немає бізнес-вимоги щодо публічного обміну даними (наприклад, статичний веб-хостинг), зберігайте всі корзини Amazon S3 (всіх рівнів) приватними.
- Щоб захистити доступ з вашого VPC до Amazon S3, використовуйте AWS PrivateLink це утримує трафік всередині магістралі AWS через захищений канал, використовуючи кінцеву точку VPC інтерфейсу.
- Для чутливих середовищ використовуйте політики контейнерів, щоб забезпечити доступ до контейнера S3 з певної кінцевої точки VPC або конкретного VPC.
- Використовуйте політики контейнерів для забезпечення використання шифрування транспорту (лише HTTPS).
- Для чутливих середовищ використовуйте політики контейнерів, щоб вимагати Версію TLS 1.2 як мінімум.

- Шифруйте дані в стані спокою за допомогою SSE-S3.
- Для чутливих середовищ шифруйте дані в стані спокою за допомогою SSE-C.
- Розгляньте можливість використання попередньо підписаних URL-адрес для сценаріїв, коли вам потрібно дозволити зовнішнім користувачам доступ (з певними дозволами, такими як завантаження файлів) до корзини S3 протягом короткого періоду часу, без необхідності створювати користувача IAM.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Конфіденційність міжмережевої мережі:
https://surl.li/ccmurh
AWS PrivateLink для Amazon S3: https://surl.lu/ezitgl
Захист даних за допомогою шифрування: https://surl.li/kxohqw
Налаштування поведінки шифрування на стороні сервера за замовчуванням для корзин Amazon S3: https://surl.li/tgoawm
Розгляньте шифрування даних у стані спокою: https://surl.li/ytjtme
Забезпечити шифрування даних під час передачі: https://surl.lu/gkmnrw
Використання блокування об'єктів S3: https://surl.li/qkscfo

Найкращі практики проведення аудиту та моніторингу для Amazon S3

Аудит є важливою частиною захисту даних. Як і будь-який інший керований сервіс, AWS дозволяє ввімкнути ведення журналу та аудит за допомогою двох вбудованих сервісів:

- *Amazon CloudWatch.* Це сервіс, який дозволяє реєструвати дії зі зберіганням об’єктів та піднімати тривогу відповідно до попередньо визначених дій (наприклад, надмірної кількості дій видалення).
- *AWS CloudTrail.* Це сервіс, який дозволяє вам відстежувати активність API (по суті, будь-яку дію, що виконується на Amazon S3).

Перелік найкращих практик, яких слід дотримуватися:

- Увімкнути сповіщення Amazon CloudWatch про надмірне використання S3 (наприклад, великий обсяг операцій GET, PUT або DELETE у певному корзині S3).
- Увімкніть AWS CloudTrail для будь-якого корзини S3, щоб реєструвати будь-яку активність, виконану на Amazon S3 будь-яким користувачем, роллю чи сервісом AWS.
- Обмежте доступ до журналів CloudTrail мінімальною кількістю співробітників, бажано тими, хто має обліковий запис керування AWS, поза межами ваших кінцевих користувачів (включно з тими, хто не входить до кола ваших користувачів), щоб уникнути можливого видалення або зміни журналів аудиту.

- Увімкнути журнали доступу до сервера S3 для запису всіх дій доступу як доповнення до журналювання на основі API AWS CloudTrail (для цілей майбутньої експертизи).
- Використовуйте Access Analyzer для S3, щоб знайти корзини S3 із публічним доступом або корзини S3, до яких надається доступ із зовнішніх облікових записів AWS.
- Увімкнути моніторинг цілісності файлів, щоб переконатися, що файли не були змінені.
- Увімкнути керування версіями об’єктів, щоб уникнути випадкового видалення (і захиститися від програм-вимагачів).
- Використовуйте інвентаризацію Amazon S3 для моніторингу стану реплікації корзини S3 (наприклад, шифрування як у вихідній, так і в цільовій корзині).

Для отримання додаткової інформації зверніться до наступних ресурсів:
Реєстрація викликів Amazon S3 API за допомогою AWS CloudTrail: https://surl.li/aiqkkn
Реєстрація запитів за допомогою журналу доступу до сервера: https://surl.lu/drirrn
Найкращі практики моніторингу та аудиту Amazon S3: https://surl.li/yjyeih

Захист сховища BLOB-об'єктів Azure

Сховище BLOB-об'єктів Azure - це служба сховища об'єктів Azure.

Рекомендації щодо проведення автентифікації та авторизації для сховища BLOB-блоків Azure

Azure контролює авторизацію для сховища BLOB-об'єктів за допомогою Azure Active Directory.

Для тимчасового доступу до сховища BLOB-об'єктів Azure (тобто для програми або взаємодії, що не здійснюється людиною) ви можете скористатися підписом спільного доступу (CAC).

Перелік найкращих практик, яких слід дотримуватися:

- Створіть групу Azure AD, додайте користувачів до групи AD, а потім надайте цільовій групі AD необхідні дозволи на цільове сховище BLOB-об’єктів.
- Використовуйте авторизацію зі спільним ключем (SAS), щоб надати програмам тимчасовий доступ до сховища BLOB-об’єктів.
- Надайте мінімальні дозволи для сховища BLOB-об'єктів Azure.
- Для даних, які потрібно зберігати протягом тривалого часу (через нормативні вимоги), використовуйте незмінне блокування сховища BLOB-об’єктів, щоб захистити дані від випадкового видалення.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Запобігання авторизації спільного ключа для облікового запису сховища Azure: https://surl.li/oklfcy

Надання обмеженого доступу до ресурсів сховища Azure за допомогою спільних підписів доступу (SAS): https://surl.li/mqahdb
Рекомендації щодо безпеки для сховища BLOB-об'єктів: https://surl.li/bjpvlh

Рекомендації щодо забезпечення мережевого доступу до сховища BLOB-блоків Azure

Оскільки сховище BLOB-об’єктів Azure є керованою хмарною службою, воно фізично розміщується поза межами локального середовища клієнта. Тому надзвичайно важливо забезпечити надійний та безпечний мережевий доступ до цього сховища.

Одним із ключових способів досягнення цього є використання віртуальної мережі (Virtual Network, VNet). Налаштування правил доступу через VNet дозволяє обмежити доступ до BLOB-сховища лише авторизованим ресурсам та службам, що розміщені всередині обраної мережі, зводячи до мінімуму ризики несанкціонованого доступу.

Перелік найкращих практик, яких слід дотримуватися:

- Зберігайте конфіденційність усього сховища Azure Blob (тобто всіх рівнів).
- Щоб захистити доступ із вашої віртуальної мережі до сховища BLOB-об’єктів Azure, використовуйте приватну кінцеву точку Azure, яка запобігає надсиланню мережевого трафіку за межі вашої віртуальної мережі через захищений канал.
- Скасувати примусове використання шифрування транспорту (лише HTTPS) для всього сховища BLOB-об’єктів Azure.
- Для чутливих середовищ потрібна мінімальна версія TLS 1.2 для сховища BLOB-об’єктів Azure.
- Заборонити доступ до облікового запису сховища Azure за замовчуванням у мережі та дозволити доступ лише за попередньо визначених умов, таких як налаштування IP-адрес.
- Шифруйте дані в стані спокою за допомогою Azure Key Vault.
- Для конфіденційних середовищ (наприклад, тих, що містять особисту інформацію, дані кредитних карток, медичні дані тощо) шифруйте дані в стані спокою за допомогою ключів, керовані клієнтом (ЦМК) зберігається всередині Azure Key Vault.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Налаштування брандмауерів та віртуальних мереж сховища Azure: https://surli.cc/bnwdjm
Посібник: Підключення до облікового запису сховища за допомогою приватної кінцевої точки Azure: https://surl.li/xtgosy
Вимагати безпечної передачі для забезпечення безпечних з'єднань: https://surl.li/ewyfja

Застосувати мінімально необхідну версію протоколу TLS (Transport Layer Security) для запитів до облікового запису сховища.:
https://surl.lt/fdfipd
Шифрування сховища Azure для даних у стані спокою: https://surli.cc/mliwwp
Ключі, керовані клієнтом, для шифрування сховища Azure: https://surl.li/zwrdfx

Рекомендації щодо проведення аудиту та моніторингу сховища BLOB-блоків Azure

Azure дозволяє контролювати сховище BLOB-об'єктів за допомогою таких служб:

- *Монітор Azure*. Ця служба реєструє події доступу та аудиту зі сховища BLOB-об'єктів Azure.
- *Центр безпеки Azure.* Ця служба дозволяє відстежувати проблеми відповідності в конфігурації сховища BLOB-об'єктів Azure.

Перелік найкращих практик, яких слід дотримуватися:

- Увімкнути сповіщення журналу за допомогою служби Azure Monitor для відстеження доступу до сховища BLOB-об’єктів Azure та генерування сповіщень (наприклад, про кілька невдалих спроб доступу до сховища BLOB-об’єктів за короткий проміжок часу).
- Увімкнути журналювання сховища Azure для аудиту всіх подій авторизації для доступу до сховища BLOB-об’єктів Azure.
- Реєструйте анонімні успішні спроби доступу, щоб виявити спробу несанкціонованого доступу до сховища BLOB-об’єктів Azure.
- Увімкніть Azure Defender for Storage, щоб отримувати сповіщення безпеки в консолі Центру безпеки Azure.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Моніторинг сховища BLOB-об'єктів Azure: https://surl.li/rktewu
Журнал аналітики сховища Azure: https://surl.li/oemswm
Сповіщення журналу в Azure Monitor: https://surl.li/wbrwbp

Захист хмарного сховища Google

Google CloudStorage - це служба зберігання об’єктів GCP.

Найкращі практики проведення автентифікації та авторизації для Google Cloud Storage.

Доступ можна контролювати на рівні всього контейнера (включно з усіма об'єктами всередині цього контейнера) або на рівні певного об'єкта (наприклад, припустимо, що ви хочете надати спільний доступ до певного файлу кільком своїм колегам).

GCP підтримує такі методи доступу до хмарного сховища:

- Рівномірний доступ на рівні контейнера. Цей метод встановлює дозволи на основі ролі Google Cloud IAM (тобто користувача, групи, домену або публічної).
- Дрібнозернистий. Цей метод встановлює дозволи на основі комбінації Google Cloud IAM та ACL - він застосовується або до всього рівня корзини, або до певного об'єкта.

Перелік найкращих практик, яких слід дотримуватися:

- Створіть групу IAM, додайте користувачів до групи IAM, а потім надайте цільовій групі IAM необхідні дозволи на доступ до цільового хмарного сховища.
- Використовуйте політики IAM для програм, яким потрібен доступ до хмарних сховищ.
- Надайте мінімальні дозволи для хмарних сховищ.
- Використання Служби токенів безпеки, щоб дозволити тимчасовий доступ до хмарного сховища.
- Використовуйте ключі HMAC, щоб надати обліковому запису служби тимчасовий доступ до хмарного сховища.
- Використовуйте підписані URL-адреси, щоб надати зовнішньому користувачеві тимчасовий доступ до хмарного сховища.
- Для даних, які потрібно зберігати протягом тривалого часу (через нормативні вимоги), використовуйте функцію блокування кошика, щоб захистити дані від випадкового видалення.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Управління ідентифікацією та доступом: https://surl.li/tttfiv
Автентифікація хмарного сховища: https://surli.cc/ntkyiv
Списки контролю доступу (ACL):https://surl.li/qjanrq
Політики зберігання та блокування політик зберігання: https://surl.li/gjnzad
API служби токенів безпеки: https://surl.lt/shgder
Ключі HMAC: https://surl.li/ewjcgw
4 найкращі практики для забезпечення конфіденційності та безпеки ваших даних у хмарному сховищі: https://surl.li/pkgjit

Найкращі практики для забезпечення мережевого доступу до Google Cloud Storage

Оскільки Google CloudStorage - це керований сервіс, він розташований поза межами VPC клієнта. Важливо захистити доступ до Google CloudStorage.

Перелік найкращих практик, яких слід дотримуватися:

- Використовуйте TLS для шифрування транспорту (лише HTTPS).
- Зберігайте конфіденційність усіх хмарних сховищ (усіх рівнів).

- Використовуйте елементи керування послугами VPC, щоб дозволити доступ із вашого VPC до хмарного сховища Google.
- Шифруйте хмарні сховища за допомогою ключів шифрування, керованих Google, у Google Cloud KMS.
- Для конфіденційних середовищ (наприклад, тих, що містять особисту інформацію, інформацію про кредитні картки, дані про охорону здоров'я тощо) шифруйте хмарні сховища за допомогою CMK у Google Cloud KMS.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Безпека, ACL та контроль доступу: https://surli.cc/oydwka
Переваги безпеки VPC Service Controls: https://surl.lu/gxlbjc
Увімкнення служб, доступних для VPC: https://surl.li/amvtvu
Ключі шифрування, надані клієнтом: https://surl.li/qalmvw

Найкращі практики проведення аудиту та моніторингу для Google Cloud Storage

Як і будь-який інший керований сервіс, GCP дозволяє ввімкнути ведення журналу та аудит за допомогою журналів аудиту Google Cloud.

Перелік найкращих практик, яких слід дотримуватися:
- Журнали аудиту активності адміністратора ввімкнено за замовчуванням і не можна вимкнути.
- Явно ввімкнути Журнали аудиту доступу до данихдля реєстрації дій, виконаних у Google Cloud Storage.
- Обмежте доступ до журналів аудиту мінімальною кількістю співробітників, щоб уникнути можливого видалення або будь-яких змін, внесених до журналів аудиту.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Журнали хмарного аудиту з хмарним сховищем:
https://surl.li/masmih
Журнали використання та журнали зберігання:
https://surl.li/rxmahd

Захист блокового сховища

Блокове сховище - це схема зберігання, подібна до локальної Мережа зберігання даних(Сан-Франциско). Він дозволяє монтувати том (диск), форматувати його у загальну файлову систему (наприклад, NTFS для Windows або Ext4 для Linux) та зберігати різні файли, бази даних або цілі операційні системи.

Далі ми розглянемо найкращі практики для захисту блокового сховища з AWS, Azure та GCP.

Для отримання додаткової інформації зверніться до наступного ресурсу: *Блокове сховище*: https://surl.li/nqsuxu

Найкращі практики для захисту Amazon Elastic Block Store

Магазин еластичних блоків Amazon(Amazon EBS) - це сховище блоків AWS. Під час роботи з екземплярами EC2 поширеною є необхідність підключити додатковий том для зберігання даних (окремо від тома операційної системи). Це також відоме як блочне сховище.

Amazon EBS можна підключити до одного екземпляра EC2 та отримати до нього доступ з операційної системи.

Трафік між вашим екземпляром EC2 та підключеним томом EBS шифрується під час передачі (і автоматично налаштовується та контролюється AWS).

Крім того, том EBS можна налаштувати для шифрування даних у стані спокою для рідкісного сценарію, коли потенційний зловмисник отримує доступ до вашого тому EBS і бажає отримати доступ до ваших даних. Самі дані (на томі EBS та його знімках) доступні лише екземпляру EC2, підключеному до тому EBS.

Наступна команда використовує інструмент AWS CLI для створення зашифрованого тому EBS у певній зоні доступності AWS:

*aws ec2 create-volume *
-- розмір 80
-- зашифровано
-- зона доступності <AWS_AZ_code>

Наступна команда використовує інструмент AWS CLI для ввімкнення шифрування EBS за замовчуванням у певному регіоні AWS:

aws ec2 увімкнути шифрування EBS за замовчуванням --region<Код_регіону>

Перелік найкращих практик для обсягів EBS:

- Налаштуйте шифрування за замовчуванням для кожного регіону, де ви плануєте розгортати екземпляри EC2.
- Шифрувати як завантажувальні томи, так і томи даних.
- Шифруйте кожен том EBS під час створення.
- Шифрувати знімки томів EBS.
- Використовуйте AWS Config для виявлення непідключених томів EBS.
- Використовуйте політику IAM, щоб визначити, хто може підключати, відключати або створювати знімки для томів EBS, щоб мінімізувати ризик витоку даних.
- Уникайте налаштування публічного доступу до знімків томів EBS - переконайтеся, що всі знімки зашифровані.

- Для високочутливих середовищ шифруйте томи EBS за допомогою головний ключ клієнта.
- Встановіть назви та описи для томів EBS, щоб краще розуміти, який том EBS належить до якого екземпляра EC2.
- Використовуйте теги (тобто маркування) для томів EBS, щоб краще зрозуміти, який том EBS належить до якого екземпляра EC2.

Для отримання додаткової інформації зверніться до наступного ресурсу: *Шифрування Amazon EBS*: https://surl.li/wylfyv

Рекомендації щодо захисту керованих дисків Azure

Диски, керовані Azure, - це кероване сховище на рівні блоків Azure. Під час роботи з віртуальними машинами поширеною є практика підключення додаткового тома для зберігання даних (тобто окремо від тома операційної системи). Це також відоме як блочне сховище.

Наведена нижче команда використовує інструмент Azure CLI для шифрування певної віртуальної машини в певній групі ресурсів за допомогою унікального клієнта сховище ключів:

Увімкнути шифрування віртуальної машини az -gМояГрупаРесурсів--ім'яМоя віртуальна машина--diskencryption-keyvaultмійKV

Наведена нижче команда використовує інструмент Azure CLI для відображення стану шифрування певної віртуальної машини в певній групі ресурсів:

шифрування віртуальної машини az show --name"myVM"-г"МояГрупаРесурсів"

Перелік найкращих практик, яких слід дотримуватися:

- Створіть ключі шифрування (всередині служби Azure Key Vault) для кожного регіону, в якому ви плануєте розгортати віртуальні машини.
- На комп'ютерах з ОС Windows шифруйте дані за допомогою технології BitLocker.
- На комп'ютерах з Linux шифруйте дані за допомогою технології dm-crypt.
- Шифруйте як ОС, так і томи даних.
- Шифруйте кожен том даних під час створення.
- Зашифруйте знімки віртуальної машини.
- Використовуйте службу приватних посилань Azure, щоб обмежити експорт та імпорт керованих дисків до вашої мережі Azure.
- Для високочутливих середовищ шифруйте обсяги даних за допомогою ЦМК.
- Встановіть імена для томів дисків Azure, щоб краще розуміти, який том диска належить до якої віртуальної машини.
- Використовуйте теги (тобто маркування) для дискових томів, щоб краще зрозуміти, який дисковий том належить до якої віртуальної машини.

Для отримання додаткової інформації зверніться до наступного ресурсу: *Шифрування на стороні сервера сховища дисків Azure*: https://surl.lu/bdjymt

Найкращі практики для захисту постійного диска Google

Постійний диск Google є частиною блочного сховища GCP.

Наступна команда використовує Google Cloud SDK для шифрування постійного диска в певному проекті GCP у певному регіоні за допомогою певного ключа шифрування:

*обчислювальні диски gcloud *
створити зашифрований диск
- - kms-key \ проекти/[KMS_PROJECT_ID]/місця розташування/[РЕГІОН]/
брелоки/[КЛЮЧ_ДЛЯ_БРЕЖКА]/криптоКлючі/[КЛЮЧ]

Перелік найкращих практик, яких слід дотримуватися:

- Шифруйте як ОС, так і томи даних.
- Шифруйте кожен том даних під час створення.
- Зашифруйте знімки екземпляра машини.
- Для високочутливих середовищ шифруйте постійні диски за допомогою ЦМК всередині
- Google Cloud KMS.
- Встановіть назви для постійних дисків Google, щоб краще розуміти, який постійний диск належить до якого екземпляра машини.
- Використовуйте теги (тобто маркування) для постійних дисків або знімків, щоб ви могли краще зрозуміти, який диск або знімок належить до якого екземпляра машини.

Захист сховища файлів

Сховище файлів - це частина сховища, така як локальне мережеве сховище(НАН).

Кожен постачальник хмарних послуг має власну реалізацію зберігання файлів, але зрештою, основна ідея зберігання файлів описується наступним чином:

- Вони пропонують підтримку поширених протоколів обміну файлами (таких як NFS та SMB/CIFS).
- Вони мають можливість монтувати том із керованої файлової служби до операційної системи для паралельного зберігання та отримання файлів для кількох віртуальних машин.
- Вони мають можливість контролювати дозволи доступу до віддаленої файлової системи.
- Вони забезпечують автоматичне зростання файлової системи.

Захист файлової системи Amazon Elastic

Файлова система Amazon Elastic(Amazon EFS) - це сервіс зберігання файлів Amazon, що базується на протоколі NFS.

Перелік найкращих практик, яких слід дотримуватися:

- Уникайте використання облікового запису root AWS для доступу до ресурсів AWS, таких як Amazon EFS.
- Створіть групу IAM, додайте користувачів до групи IAM, а потім надайте
- цільовій групі IAM необхідні дозволи на цільовому Amazon EFS.
- Використовуйте ролі IAM для федеративних користувачів, сервісів AWS або програм, яким потрібен доступ до Amazon EFS.
- Використовуйте політики IAM, щоб надати мінімально необхідні дозволи для створення томів EFS або доступу та використання Amazon EFS.
- Під час використання політик IAM вкажіть умови (наприклад, вихідну IP-адресу) та дії, які кінцевий користувач може виконувати над цільовою файловою системою, разом із зазначеною умовою.
- Використовуйте політики на основі ресурсів, щоб налаштувати, хто може отримувати доступ до тому EFS та які дії цей кінцевий користувач може виконувати над файловою системою (наприклад, монтувати, читати, записувати тощо).

Для отримання додаткової інформації зверніться до наступних ресурсів:
Керування ідентифікацією та доступом для Amazon EFS: https://surl.lu/veiyml
Робота з користувачами, групами та дозволами на рівні мережевої файлової системи (NFS):
https://surl.lt/blzies
Керовані політики AWS для Amazon EFS:
https://surl.li/ajhqsu
Безпека в Amazon EFS: https://surl.lt/sbgxfb
Огляд керування дозволами доступу до ресурсів Amazon EFS: https://surli.cc/ynavps

Найкращі практики для забезпечення мережевого доступу до Amazon EFS

Оскільки Amazon EFS є керованим сервісом, він розташований поза межами VPC клієнта. Важливо захистити доступ до сервісу Amazon EFS.

Перелік найкращих практик, яких слід дотримуватися:

- Зберігайте Amazon EFS (тобто всі класи сховища) приватними.
- Використовуйте групи безпеки VPC для керування доступом між вашими машинами Amazon EC2 та томами монтування Amazon EFS.
- Щоб захистити доступ з вашого VPC до Amazon EFS, використовуйте AWS PrivateLink, який дозволяє уникнути надсилання мережевого трафіку за

межі вашого VPC через захищений канал, використовуючи кінцеву точку VPC інтерфейсу.

- Використовуйте точки доступу Amazon EFS для керування доступом програм до тому EFS.
- Використовуйте STS для тимчасового доступу до Amazon EFS.
- Використовуйте політику IAM для забезпечення шифрування в стані спокою для файлових систем Amazon EFS. Ви можете зробити це, встановивши значення еластична файлова система: Зашифровано до Правда всередині умови політики IAM.
- Для конфіденційних середовищ використовуйте помічник монтування EFS, щоб примусово ввімкнути шифрування під час передачі за допомогою TLS версії 1.2 під час монтування тома EFS.
- Шифруйте дані в стані спокою за допомогою CMK, керованого AWS, для Amazon EFS.
- Для чутливих середовищ шифруйте дані в стані спокою за допомогою CMK.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Керування мережевим доступом до файлових систем Amazon EFS для клієнтів NFS: https://surl.lu/edljjy
Робота з точками доступу Amazon EFS: https://surl.lu/szdywh
Ізоляція мережі Amazon Elastic File System: https://surli.cc/mihuqt
Шифрування даних в Amazon EFS: https://surli.cc/jkakru

Найкращі практики проведення аудиту та моніторингу для Amazon EFS

Як і будь-який інший керований сервіс, AWS дозволяє ввімкнути ведення журналу та аудит за допомогою двох вбудованих сервісів:

- *Amazon CloudWatch.* Це сервіс, який дозволяє реєструвати дії доступу та піднімати тривогу відповідно до попередньо визначених дій (наприклад, надмірної кількості дій видалення).
- *AWS CloudTrail.* Це сервіс, який дозволяє вам відстежувати активність API (по суті, будь-які дії, що виконуються в Amazon EFS).

Перелік найкращих практик, яких слід дотримуватися:

- Увімкнути сповіщення Amazon CloudWatch про надмірне використання Amazon EFS (наприклад, великий обсяг операцій зберігання або видалення на певному томі EFS).
- Увімкнути використання AWS CloudTrail для будь-якого тому EFS для реєстрації будь-якої активності, виконаної в Amazon EFS API, включаючи будь-яку активність, виконану користувачем, роллю або Сервіс AWS.
- Створіть журнал за допомогою AWS CloudTrail на будь-якому томі EFS для реєстрації подій, таких як запитувана дія, дата та час, запитувані параметри тощо, для доступу до об’єктів, що зберігаються в AWS EFS.

- Обмежте доступ до журналів CloudTrail мінімальною кількістю співробітників, бажано тими, хто має обліковий запис керування AWS, поза межами ваших кінцевих користувачів (включно з тими, хто не входить до кола ваших користувачів), щоб уникнути можливого видалення або зміни журналів аудиту.

Для отримання додаткової інформації зверніться до наступного ресурсу:
Ведення журналу та моніторинг в Amazon EFS: https://surl.lu/tkksjn

Захист файлів Azure

Azure Files -це служба сховища файлів Azure, що базується на протоколі SMB.

Найкращі практики проведення автентифікації та авторизації для файлів Azure

Azure підтримує такі механізми автентифікації та авторизації для керування доступом до файлів Azure:

- Служби домену Active Directory(AD DS). Це схоже на локальний Active Directory з використанням автентифікації Kerberos.
- Служби доменів Azure Active Directory(Azure AD DS). Це додаткова служба до Azure AD, яка дозволяє автентифікуватися у застарілих службах (SMB у випадку Azure Files) та протоколах (Kerberos у випадку Azure Files).

Перелік найкращих практик, яких слід дотримуватися:

- Використовуйте автентифікацію на основі ідентифікації, щоб надати мінімальні дозволи на спільний доступ, доступ до каталогу або файлу в службі Azure Files.
- Для хмарного середовища в Azure (без локальних віртуальних машин) переконайтеся, що всі віртуальні машини приєднані до домену Azure AD, і що всі віртуальні машини підключені до тієї ж віртуальної мережі, що й Azure AD DS.
- Увімкніть автентифікацію Active Directory через SMB, щоб дозволити віртуальним машинам, підключеним до домену, доступ до файлів Azure.
- Уникайте використання ключів облікового запису сховища для автентифікації у Файлах Azure.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Огляд варіантів автентифікації на основі ідентифікації Azure Files для доступу SMB: https://surl.lu/sbaubh
Планування розгортання файлів Azure: https://surl.li/lzdtev

Найкращі практики для забезпечення мережевого доступу до файлів Azure

Оскільки Azure Files - це керована служба, вона розташована поза віртуальною мережею клієнта. Важливо захистити доступ до служби Azure Files.

Перелік найкращих практик, яких слід дотримуватися:

- Оскільки SMB вважається незахищеним протоколом, переконайтеся, що весь доступ до служб Azure Files з локальної мережі проходить через захищений канал, такий як VPN-тунель або службу Express Route.
- Щоб захистити доступ із вашої віртуальної мережі до файлів Azure, використовуйте приватну кінцеву точку Azure,
- яка запобігає надсиланню мережевого трафіку за межі вашої віртуальної мережі через захищений канал.
- Усунути необхідність використання транспортного шифрування (лише HTTPS) для всіх спільних ресурсів Azure Files.
- Для чутливих середовищ потрібна мінімальна версія TLS 1.2 для сховища BLOB-об'єктів Azure.
- Заборонити доступ до облікового запису сховища Azure через мережу за замовчуванням і дозволити доступ лише із заздалегідь визначеного набору IP-адрес.
- Для даних, які потрібно зберігати протягом тривалого часу (через нормативні вимоги), увімкніть функцію м'якого видалення Azure Files, щоб захистити дані від випадкового видалення.
- Шифруйте дані в стані спокою за допомогою Azure Key Vault.
- Для конфіденційних середовищ шифруйте дані в стані спокою за допомогою ключів, керованих клієнтом, що зберігаються в Azure Key Vault.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Рекомендації щодо мережевих функцій Azure Files:
https://surl.li/jarmpm
Запобігання випадковому видаленню спільних файлів Azure: https://surl.lu/ocluxq
Вимагати безпечної передачі для забезпечення безпечних з'єднань: https://surli.cc/grzlgv
Шифрування сховища Azure для даних у стані спокою: https://surl.lu/kownur
Ключі, керовані клієнтом, для шифрування сховища Azure: https://surli.cc/pnunkx

Найкращі практики проведення аудиту та моніторингу для файлів Azure

Аудит є важливою частиною захисту даних.
Azure дозволяє вам контролювати файли Azure за допомогою таких служб:

- *Монітор Azure.* Це реєструє події доступу та аудиту з файлів Azure.
- *Розширений захист від загроз для сховища Azure.* Це дозволяє виявляти аномалію або будь-яку незвичну активність у файлах Azure та обліковому записі сховища Azure.

Перелік найкращих практик, яких слід дотримуватися:

- Увімкнути сповіщення журналу за допомогою служби Azure Monitor для відстеження доступу до файлів Azure та генерування сповіщень (наприклад,

про кілька невдалих спроб доступу до файлів Azure за короткий проміжок часу).

- Увімкніть Azure Defender for Storage, щоб отримувати сповіщення безпеки в консолі Центру безпеки Azure.
- Увімкнути ведення журналу сховища Azure для аудиту всіх подій авторизації для доступу до сховища Azure.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Записи, зареєстровані в журналі: https://surl.li/vypytv
Моніторинг файлів Azure: https://surl.li/awqdpq

Захист файлового сховища Google

Google Filestore -це сервіс зберігання файлів GCP, що базується на протоколі NFS.

Найкращі практики проведення автентифікації та авторизації для Google Filestore

Google Cloud IAM - це підтримуваний сервіс, за допомогою якого можна керувати дозволами на доступ до Google Filestore.

Перелік найкращих практик, яких слід дотримуватися:

- Зберігайте конфіденційність своїх екземплярів Google Filestore.
- Створіть групу IAM, додайте користувачів до групи IAM, а потім надайте цільовій групі IAM необхідні дозволи на цільовий екземпляр Google Filestore.
- Використовуйте ролі IAM для налаштування мінімальних дозволів для будь-якого екземпляра Google Filestore.
- Використовуйте правила безпеки Cloud Firestore, щоб дозволити мобільним клієнтам, веб-клієнтам або безсерверній автентифікації в Google Filestore.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Безпека для бібліотек клієнтського сервера:
https://surl.li/hrihch
Початок роботи з правилами безпеки Cloud Firestore: https://surl.li/diezcm

Найкращі практики для забезпечення мережевого доступу до Google Filestore

Оскільки Google Filestore - це керований сервіс, він розташований поза межами VPC клієнта. Важливо захистити доступ до Google Filestore.

Перелік найкращих практик, яких слід дотримуватися:

- Використовуйте керування доступом на основі IP-адреси, щоб обмежити доступ до Google Filestore.
- Створіть екземпляр Google Filestore на тому ж VPC, що й ваші клієнти.

- Якщо екземпляр Google Filestore розташований за межами вашого VPC, використовуйте правила брандмауера VPC, щоб обмежити доступ між вашим VPC та Google Filestore.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Контроль доступу: https://surl.li/hcyitz
Архітектура: https://surl.li/zgqpqu

Забезпечення безпеки CSI

CSI -це стандартний драйвер для підключення систем оркестрації контейнерів, таких як Kubernetes, до блочного та файлового сховища від різних хмарних постачальників.

Для отримання додаткової інформації зверніться до наступного ресурсу:
Документація інтерфейсу сховища контейнерів (CSI) Kubernetes: https://surli.cc/qfculc

Захист CSI на AWS

Amazon Еластичний сервіс Kubernetes(EKC) має драйвер CSI для таких типів сховищ:

1. Блокове сховище:ЕБС
2. Керований NFS:ЕФС
3. Паралельна файлова система (для робочих навантажень HPC): Amazon FSx для Lustre

Перелік найкращих практик, яких слід дотримуватися:

- Під час створення політики IAM для підключення до драйвера CSI вкажіть назву ресурсу сховища замість використання шаблону підстановки.
- Використовуйте ролі IAM для сервісних облікових записів, щоб обмежити доступ до вашого pod.
- Завжди використовуйте останню версію CSI для обраного типу сховища.
- Під час використання драйвера CSI для EBS та його знімків завжди встановлюйте у файлі конфігурації YAML.
- Під час використання драйвера CSI для EFS завжди встановлюйте (у файлі конфігурації YAML) значення шифрування під час транзиту до Правда.
- Використовуйте Amazon Secrets Manager із драйвером CSI сховища таємниць для зберігання та отримання таємниць (таких як токени, ключі автентифікації SSH, файли конфігурації Docker тощо) до/з ваших подів EKS.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Драйвер CSI для Amazon Elastic Block Store (EBS):
https://surli.cc/tvzcfn
Драйвер Amazon EFS CSI: https://surl.li/pdhxzl
Драйвер Amazon FSx для Lustre CSI: https://surl.li/prhouu

Як використовувати постійне сховище в Amazon EKS?: https://surl.li/yxtujh
Представляємо динамічне забезпечення Amazon EFS CSI: https://surl.li/mviyvw

Захист CSI в Azure

Служба Azure Kubernetes(AKC) має драйвер CSI для таких типів сховищ:

1. Блокове сховище Azure Disk
2. Керовані SMB та NFS файли Azure

Перелік найкращих практик, яких слід дотримуватися:

- Завжди використовуйте останню версію CSI для обраного типу сховища.
- Використовуйте Azure Key Vault із драйвером CSI сховища секретних даних для зберігання та отримання секретних даних (таких як токени, ключі автентифікації SSH, файли конфігурації Docker тощо) до/з ваших подів AKS.
- Використовуйте приватну кінцеву точку для підключення кластера AKS до Azure Files.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Драйвер Azure Disk CSI для Kubernetes: https://surli.cc/ictplz
Використання драйверів інтерфейсу сховища контейнерів Azure (CSI) у службі Azure Kubernetes Service (AKS): https://surli.cc/qwuwde
Використання драйверів інтерфейсу сховища контейнерів файлів Azure (CSI) у службі Azure Kubernetes (AKS): https://surli.cc/plqeok

Захист CSI на GCP

Google Kubernetes Engine має драйвер CSI для таких типів сховищ:

1. Блокове сховище: Постійний диск Google Compute Engine
2. Зберігання об'єктівХмарне сховище Google
3. Керований NFSХмарне сховище файлів Google

Перелік найкращих практик, яких слід дотримуватися:

- Завжди використовуйте останню версію CSI для обраного типу сховища.
- Під час використання драйвера CSI для постійного диска Google укажіть (у файлі YAML) ключ-шифрування-диска-kms ключ, щоб дозволити драйверу CSI використовувати ключ шифрування, керований клієнтом, з Google Cloud KMS.
- Використовуйте ролі Cloud IAM, щоб обмежити доступ з вашого кластера GKE до Google Cloud Filestore.
- Використовуйте Google Secret Manager із драйвером Secret Store CSI для зберігання та отримання таємниць (таких як токени, ключі автентифікації SSH, файли конфігурації Docker тощо) до/з ваших подів GKE.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Драйвер CSI для постійного диска Google Compute Engine: https://surl.li/efqjro

Драйвер CSI для хмарного сховища файлів Google: https://surl.lu/uwnhbx
Драйвер CSI хмарного сховища Google: https://surl.li/vqxkkn
Використання драйвера CSI постійного диска Compute Engine: https://surl.lt/sztmrd

1.4. Захист мережевих послуг

Система доменних імен(ДНС) послуги, мережі доставки контенту(CDN-мережі), віртуальні приватні мережі (VPN-мережі),розподілена відмова в обслуговуванні (DDoS-атак) послуги захисту, та брандмауери веб-застосунків(WAFs).

У цьому розділі буде розглянуто різні мережеві служби та надано рекомендації щодо безпечного підключення та використання кожної з них.

У цьому параграфі ми розглянемо такі теми:

- Захист віртуальних мереж
- Захист DNS-сервісів
- Захист послуг CDN
- Захист VPN-сервісів
- Захист послуг DDoS-захисту
- Забезпечення безпеки послуг WAF

Технічні вимоги

Для цього розділу читачеві необхідно мати фундаментальне розуміння мережевих сервісів, таких як віртуальна приватна хмара(ВПК)/VNET служби та групи безпеки (або списки контролю доступу(ACL)), а також глибоке розуміння VPN, захисту від DDoS-атак та сервісів WAF.

Захист віртуальних мереж

Кожен постачальник хмарних послуг має власну реалізацію віртуальної мережі.

Згідно з моделлю спільної відповідальності, відповідальність за мережу розділена між постачальником хмарних послуг та клієнтом. Фізичний мережевий рівень (тобто доступ між фізичним мережевим обладнанням та фізичними хост-серверами, а також сховищем у центрах обробки даних постачальника хмарних послуг) є відповідальністю постачальника хмарних послуг.

Віртуальні мережі (наприклад Amazon VPC, Віртуальна мережа Azure або Хмарна платформа Google (GCP) ВПК) - це мережевий рівень, за який відповідають клієнти (цей рівень забезпечує доступ між віртуальними серверами, керованими службами зберігання даних, керованими базами даних тощо).

Традиційні локальні мережі мають справу з фізичними з'єднаннями між пристроями в системі: наприклад, такі концепції, як віртуальні локальні мережі

(VLAN) або підмережі, щоб розділити мережу (з пристроями, підключеними до мережі) та створити бар'єри безпеки мережі.

У хмарі мережа базується на програмному забезпеченні (це також відомо як програмно-визначені мережі (Соціально-доступний мережевий продукт (СДН). У хмарі у вас є мікросегментація, а це означає, що ви можете налаштувати дозволити і заперечувати правила контролю доступу між двома екземплярами (навіть якщо вони розташовані в одній підмережі). Ви також зможете проводити аудит і контролювати доступ до ресурсу, такого як API.

Віртуальна мережа - це мережева область у вашому хмарному середовищі, де знаходиться більшість поширених хмарних ресурсів (таких як віртуальні сервери, керовані бази даних тощо). Ці ресурси розділені на кілька мережевих сегментів, які називаються *підмережі*.

У хмарному середовищі кожного клієнта може бути одна або кілька віртуальних мереж, але зрештою основна ідея залишається незмінною. Нижче наведено деякі важливі моменти щодо віртуальних мереж:

- Доступ до підмереж контролюється засобами контролю доступу (наприклад, брандмауерами 4-го рівня).
- Підмережі можуть бути *приватний* (без прямого доступу з Інтернету) або *загальний* (доступ з Інтернету дозволено).
- Якщо вам потрібно дозволити доступ до Інтернету для ресурсів приватної підмережі, вам потрібно налаштувати шлюз NAT.
- Віртуальні мережі можуть бути з'єднані одна з одною за допомогою однорангових з'єднань.

Оскільки кожен постачальник хмарних послуг має власний механізм контролю доступу до мережі, у наступній таблиці 1.2. порівнюються відмінності між механізмами контролю доступу:

Таблиця 1.2 - Механізми контролю доступу

	AWS мережеві ACL	**Групи безпеки AWS**	**Групи мережевої безпеки Azure**	**Правила брандмауера VPC GCP**
Стан (Зі станом / Без стану - Stateful / Stateless)	Беззбережний (Stateless)	Збережний (Stateful)	Беззбережний (Stateless)	Збережний (Stateful)
Місце знаходження (Location)	Рівень підмережі (Subnet level)	Рівень екземпляра (Instance level)	Рівень VM, підмережі, тегування	Рівень екземпляра (Instance level)

Слід пам’ятати:

- *Збережний (Stateful)* - це система пам’ятає попередні з'єднання. Якщо вхідний трафік дозволено -вихідний автоматично також. Відповідно простіше керувати, бо правила працюють обидва боки.
- *Беззбережний (Stateless)* - це система не зберігає стану з'єднання. Треба вказувати окремі правила для вхідного і вихідного трафіку. Відповідно гнучкіша, але складніша в налаштуванні.

Захист віртуальної приватної хмари Amazon

Віртуальна приватна хмара Amazon (Amazon VPC) -це віртуальний мережевий сервіс Amazon.

AWS підтримує такі механізми для захисту доступу до ресурсів усередині VPC:

- Мережеві ACL: Бездержавний механізм для захисту доступу до/від ресурсів на рівні підмережі. Вам потрібно налаштувати правила як для вхідного, так і для вихідного зв'язку. Мережеві ACL підтримують обидва типи дозволити і заперечувати правила.
- Групи безпеки: Механізм захисту доступу до ресурсів на рівні екземпляра з відстеженням стану. Вам потрібно налаштувати правила вхідного зв'язку.
- Мережевий доступ до ресурсу надається комбінацією мережевих ACL на рівні підмережі агрегацією всіх груп безпеки, що діють на ресурс, такий як віртуальна машина (у випадку, якщо кілька груп безпеки дозволяють різний доступ до ресурсу, такого як віртуальна машина).

Ось кілька найкращих практик для забезпечення мережевого доступу до Amazon VPC:

- Під час створення користувацьких мережевих ACL створіть остаточне правило заборони як для вхідного, так для вихідного трафіку для кращого захисту.
- Створюйте підмережі відповідно до функції ресурсу (наприклад, публічні підмережі для веб-серверів, приватні підмережі для серверів баз даних тощо).
- Для протоколів віддаленого доступу (SSH/RDP) обмежте IP-адресу джерела (або Безкласова міждоменна маршрутизація (CIDR)) до відомих джерел.
- Для протоколів обміну файлами (CIFS/SMB/FTP) обмежте IP-адресу джерела (або CIDR) добре відомими джерелами.
- Використовуйте групи безпеки для контролю доступу між публічними ресурсами (такими як балансувальники навантаження або загальнодоступні веб-сервери) та приватними ресурсами (такими як бази даних) та обмежте доступ мінімально необхідними портами/протоколами.
- Встановіть назви та описи для груп безпеки, щоб краще зрозуміти призначення будь-якої групи безпеки.
- Використання тегування (також відомий як маркування) для груп безпеки, щоб краще зрозуміти, які групи безпеки належать до яких ресурсів AWS.

- Для масштабних середовищ з кількома обліковими записами AWS використовуйте Менеджер брандмауера AWS централізовано створювати та забезпечувати виконання груп безпеки VPC.
- Для безпечного доступу з ресурсів у вашому VPC до Керовані послуги AWS(таких як AWS S3, Amazon RDS та інші), а також для утримання трафіку всередині магістралі AWS використовуйте AWS PrivateLinkта налаштуйте групи безпеки VPC, щоб дозволити трафік з вашого VPC до керованих сервісів AWS.
- Щоб дозволити вихідний доступ із внутрішніх ресурсів усередині приватних підмереж до місць призначення в Інтернеті (на основі протоколу IPv4), використовуйте шлюзи NAT або будь-який самостійно розміщений проксі-сервер NAT.
- Щоб дозволити вихідний доступ із внутрішніх ресурсів усередині приватних підмереж до місць призначення в Інтернеті (на основі протоколу IPv6), використовуйте лише вихід інтернет-шлюз.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Мережеві ACL: https://surl.li/zchmrr
Групи безпеки для вашого VPC: https://surl.li/tafopb
Менеджер брандмауера AWS: https://surl.lu/ulnopk
Кінцеві точки інтерфейсу VPC (AWS PrivateLink):
https://surl.li/nbqfjr
NAT-шлюзи: https://surl.li/woohsv
Інтернет-шлюзи лише для виходу: https://surl.li/iwkqtl

Найкращі практики моніторингу Amazon VPC

AWS дозволяє моніторити Amazon VPC за допомогою таких вбудованих сервісів:

- *Amazon CloudWatch.* Це сервіс, який дозволяє вам контролювати компоненти VPC (наприклад, обсяги вхідного/вихідного трафіку).
- *Журнали потоку VPC.* Це сервіс, який дозволяє реєструвати мережеву активність у вашому VPC (наприклад, метадані трафіку, такі як джерело, пункт призначення, порт, позначка часу, розмір, а також дозволяти та забороняти мережеві події). Це корисно як для усунення несправностей, так і для розслідування подій, пов’язаних із безпекою.

Деякі найкращі практики для моніторингу Amazon VPC:

- Увімкнути Журнали CloudWatch для моніторингу активності компонентів VPC та трафіку між вашими ресурсами VPC та кінцевою точкою VPC (керовані сервіси AWS).
- Використання AWS CloudTrail для моніторингу конфігурації VPC.
- Увімкнути Журнали потоку VPC для реєстрації та подальшого аналізу дозволеної та забороненої трафікової активності. У поєднанні з Amazon Guard Duty, ви зможете виявляти аномальну поведінку мережі, таку як

взаємодія з командування та управління (Командування та контроль) мережі, шкідливі IP-адреси тощо.

💻***Примітка!*** *Для масштабних виробничих середовищ увімкніть журнали потоку VPC лише на короткі періоди часу, виключно для усунення несправностей (через високу вартість зберігання та великі обсяги даних, що генеруються журналами потоку VPC).*

- Використання Конфігурація AWS або Центр безпеки AWS для виявлення вхідного доступу до ресурсів усередині вашої VPC через незашифровані протоколи (такі як HTTP замість HTTPS або LDAP замість LDAPS).
- Якщо вам потрібно усунути проблеми з мережею, перехопивши мережевий трафік без переривання роботи виробничих систем, використовуйте Дзеркальне відображення трафіку в Amazon VPC для копіювання мережевого трафіку в реальному часі з мережевого інтерфейсу Хмара еластичних обчислень Amazon (EC2) екземпляр або від балансувальника мережевого навантаження до позасмугового пристрою безпеки.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Використання журналів CloudWatch з кінцевими точками інтерфейсу VPC: https://surl.li/lbdjxk
Реєструйте та контролюйте свій VPC: https://surl.li/gvoecl
Журнали потоку VPC: https://surli.cc/uraqgs
Що таке дзеркалювання трафіку: https://surl.li/ofhucj

Захист віртуальної мережі Azure

Віртуальна мережа Azure (Віртуальна мережа Azure) - це служба віртуальної мережі Azure.

Для захисту ресурсів у віртуальній мережі Azure підтриму єгрупи мережевої безпеки(НСГ) - механізм захисту доступу до ресурсів без урахування стану на рівні віртуальної машини, підмережі або тегування. Вам потрібно налаштувати правила як вхідного, так і вихідного зв’язку для груп підтримки віртуальної мережі (VNet NSG).

Ось кілька найкращих практик, яких слід дотримуватися:

- Створюйте підмережі відповідно до функції ресурсу (наприклад, публічні підмережі для веб-серверів, приватні підмережі для серверів баз даних тощо).
- Для протоколів віддаленого доступу (SSH/RDP) обмежте вихідну IP-адресу (або CIDR) добре відомими джерелами.
- Для протоколів обміну файлами (CIFS/SMB/FTP) обмежте IP-адресу джерела (або CIDR) добре відомими джерелами.
- Використовуйте NSG для контролю доступу між публічними ресурсами (такими як балансувальник навантаження або публічні веб-сервери) та приватними ресурсами (такими як бази даних) та обмежуйте доступ мінімально необхідними портами/протоколами.

- Встановіть назви та описи для груп підтримки клієнтів (ГДЛ), щоб краще зрозуміти їхню мету.
- Використання *тегування* (також відомий як *маркування*) для груп безпеки мережі, щоб краще зрозуміти, які групи безпеки мережі належать до яких ресурсів Azure.
- Використання групи безпеки програм визначити правила доступу на рівні програми (наприклад, правила для дозволу вхідного HTTP-доступу).
- Використовуйте теги послуг для налаштування правил для попередньо визначеної послуги (наприклад, Балансувальник навантаження Azure), замість використання IP-адрес.
- Щоб дозволити вихідний доступ із внутрішніх ресурсів усередині приватних підмереж до місць призначення в Інтернеті, використовуйте NAT віртуальної мережі Azure(або використовуйте NAT-шлюз).
- Для масштабних середовищ з кількома підписками Azure використовуйте Брандмауер Azure централізовано створювати, застосовувати та реєструвати мережеві політики для кількох підписок.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Концепції та рекомендації щодо віртуальної мережі Azure: https://surl.li/cratyz
Групи мережевої безпеки: https://surl.li/evzqzo
Групи безпеки програм: https://surl.lu/atodye
Теги служби віртуальної мережі: https://surl.li/fhhyyq
Що таке NAT віртуальної мережі: https://surl.li/vkfxax
Що таке брандмауер Azure: https://surl.lu/tdttja

Рекомендації щодо моніторингу віртуальної мережі Azure

Azure дозволяє відстежувати мережеву активність за допомогою Спостерігач мережі Azure–сервіс для запису журналів потоків NSG.

Деякі рекомендації щодо моніторингу віртуальної мережі Azure:

- Увімкнути моніторинг мережі Azure Журнали потоку NSG реєструвати та подальший аналіз дозволеної та забороненої трафікової активності.

  💻 ***Примітка!*** *Для масштабних виробничих середовищ увімкніть журнали потоків NSG лише на короткі періоди часу, виключно для усунення несправностей (через високу вартість зберігання та великі обсяги даних, що генеруються журналами потоків NSG).*
- Якщо вам потрібно вирішувати проблеми з мережею шляхом захоплення мережевого трафіку, скористайтеся засобом Azure Network Watcher захоплення пакетів розширення для копіювання мережевого трафіку в реальному часі з віртуальної машини до облікового запису сховища Azure.

  💻 ***Примітка!*** *Для масштабних виробничих середовищ увімкніть розширення захоплення пакетів Network Watcher лише на короткі періоди часу, виключно для усунення несправностей (через вплив на продуктивність цільової віртуальної машини).*

- Для великомасштабних середовищ використовуйте Аналіз трафіку Azure для виявлення загроз безпеці (таких як відкриті порти, вихідний інтернет-трафік програм тощо).
- Використання Політика Azure для виявлення вхідного доступу до ресурсів у вашій віртуальній мережі через незашифровані протоколи (такі як HTTP замість HTTPS або LDAP замість LDAPS).

Для отримання додаткової інформації зверніться до наступних ресурсів:
Реєстрація мережевого трафіку до та з віртуальної машини за допомогою порталу Azure: https://surl.li/zokppe
Вступ до ведення журналу потоків для груп мережевої безпеки: https://surl.li/hcecrw
Що таке спостерігач мережі Azure: https://surl.li/qrqyzk
Керування захопленням пакетів за допомогою Azure Network Watcher за допомогою порталу: https://surl.li/nwkwzv
Аналіз трафіку: https://surl.li/jamuim

Захист Google Cloud VPC

VPC у хмарі Google-це сервіс віртуальних мереж Google.

Найкращі практики для забезпечення мережевого доступу до Google Cloud VPC

Для захисту ресурсів усередині VPC, Google підтримує Правила брандмауера VPC–механізм захисту доступу до ресурсів з урахуванням стану. Вам потрібно налаштувати правила вхідного та вихідного зв'язку, і для кожного правила можна налаштувати дію *дозволити* або *заперечувати*.

Ось кілька найкращих практик для забезпечення мережевого доступу до Google Cloud VPC:

- Створюйте підмережі відповідно до функції ресурсу (наприклад, публічні підмережі для веб-серверів, приватні підмережі для серверів баз даних тощо).
- Для протоколів віддаленого доступу (SSH/RDP) обмежте вихідну IP-адресу (або CIDR) добре відомими джерелами.
- Для протоколів обміну файлами (CIFS/SMB/FTP) обмежте IP-адресу джерела (або CIDR) добре відомими джерелами.
- Використовуйте правила брандмауера VPC для контролю доступу між загальнодоступними ресурсами (такими як балансувальники навантаження або загальнодоступні веб-сервери) та приватними ресурсами (такими як бази даних) та обмежуйте доступ мінімально необхідними портами/протоколами.
- Встановіть назви та описи для правил брандмауера VPC, щоб краще зрозуміти призначення будь-якого правила брандмауера.
- Використання тегування (також відомий як маркування) для правил брандмауера VPC, щоб

- краще зрозуміти, яке правило брандмауера VPC належить до яких ресурсів VPC.
- Використовуйте мережеві теги для налаштування правил для груп ресурсів (наприклад, групи екземплярів обчислювального механізму) замість використання IP-адрес.
- Щоб дозволити вихідний доступ із внутрішніх ресурсів у приватних підмережах до місць призначення в Інтернеті, використовуйте Хмарний шлюз NAT.
- Для масштабних середовищ з кількома проектами Google Cloud VPC використовуйте елементи керування послугами VPC, щоб запровадити обмеження доступу до ресурсів VPC на основі ідентифікації IP-адреси.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Огляд правил брандмауера VPC: https://surl.li/krpxvp
Використання правил брандмауера: https://surl.li/vsceim
Налаштування мережевих тегів: https://surl.li/ydrlxt
Огляд NAT: https://surl.li/pnvrrt

Найкращі практики моніторингу Google Cloud VPC

Google дозволяє вам контролювати Google Cloud VPC за допомогою таких вбудованих сервісів:

- Ведення журналу в хмарі Google. Це сервіс, який дозволяє вам контролювати ваші компоненти VPC.
- Журнали потоку VPC. Це сервіс, який дозволяє вам реєструвати мережеву активність у вашому VPC (наприклад, дозволити і заперечувати мережеві події).

Деякі найкращі практики для моніторингу Google Cloud VPC:

- Увімкніть журнали аудиту VPC для моніторингу активності компонентів VPC та трафіку між ресурсами VPC.
- Зверніть увагу, що журнали аудиту діяльності адміністратора ввімкнено за замовчуванням і їх не можна вимкнути.
- Явно ввімкнути журнали аудиту доступу до даних реєструвати дії у вашій віртуальній віртуальній машині Google Cloud.
- Обмежте доступ до журналів аудиту мінімальною кількістю співробітників (щоб уникнути небажаних змін до журналів аудиту).
- Увімкнути Журнал правил брандмауера для перевірки функціональності правил вашого брандмауера VPC.
- Увімкнути Журнали потоку VPC реєструвати та подальший аналіз дозволеної та забороненої трафікової активності.

💻 ***Примітка!*** *Для масштабних виробничих середовищ увімкніть журнали потоку VPC лише на короткі періоди часу, виключно для усунення несправностей (через високу вартість зберігання та великі обсяги даних, що генеруються журналами потоку VPC).*

- Якщо вам потрібно усунути проблеми з мережею шляхом захоплення мережевого трафіку, використовуйте Дзеркальне відображення пакетів копіювати активний мережевий трафік з екземпляра віртуальної машини обчислювального сервіс Compute Engine контейнерів до групи екземплярів за внутрішнім балансувальником навантаження.

  💻 ***Примітка!*** *Для великомасштабних виробничих середовищ увімкніть дзеркалювання пакетів лише на короткі періоди часу, виключно для усунення несправностей (через високий вплив на продуктивність цільової віртуальної машини).*

Для отримання додаткової інформації зверніться до наступних ресурсів:
Огляд журналювання правил брандмауера: https://surl.li/xnzcyh
Огляд журналів потоку VPC: https://surl.lu/bldmbv
Використання журналів потоку VPC: https://surl.lt/qqxxdo
Інформація про журнал аудиту VPC: https://surli.cc/dtsamp
Огляд дзеркалювання пакетів: https://surl.li/lqwbfv

Захист DNS-сервісів

Кожен хмарний постачальник має власну реалізацію керованих DNS-сервісів - до них належать сервіси для перетворення імен хостів в IP-адреси, різні типи сервісів DNS-записів (такі якПсевдонім,CNAME, та інше), визначення імені хоста для балансування навантаження IP-адресою та інше.

Захист маршруту Amazon Route 53

Amazon Route 53 - це керована служба DNS від Amazon.

Нижче наведено деякі з найкращих практик, яких слід дотримуватися:

- Створіть Управління ідентифікацією та доступом(Ідентифікація та доступність даних) групу, додайте користувачів до групи та надайте цільовій групі необхідні дозволи на користування послугою Route 53.
- Увімкнути Розширення безпеки системи доменних імен(підписання DNSSEC)у будь-якій публічно розміщеній зоні для захисту від атак DNS-спуфінгу.
- Використовуйте новий головний ключ клієнта(ЦМК) для підписання будь-якої щойно створеної публічної зони.
- Переконайтеся, що для будь-якого домену, яким ви керуєте за допомогою Route 53, увімкнено захист конфіденційності, щоб захистити конфіденційність контактної інформації власників доменів.
- Увімкніть блокування передачі доменів Route 53, щоб запобігти передачі ваших доменів до іншого реєстратора.
- Створіть рамки політики відправника(СПФ) запис на вашому домені, розміщеному на Route 53, щоб публічно вказати, які поштові сервери мають право надсилати електронні листи від імені вашого поштового домену.
- Скористайтеся трасою 53Брандмауер DNS-дозволи щоб блокувати загрози на рівні DNS, що походять від вашого VPC.

- Видаліть невикористані DNS-записи з розміщених зон (записи ресурсів, такі як IP-адреси, що підключалися до видаленого ресурсу).
- Використовуйте приватні розміщені зони для керування DNS-записами для внутрішніх ресурсів (таких як ресурси, розташовані всередині приватних підмереж).
- Увімкніть ведення журналу публічних DNS-запитів, щоб мати змогу аналізувати, які публічні DNS-запити щодо ваших доменів були надіслані до Route 53.
- Увімкнути Журнал запитів роутера мати можливість аналізувати таку інформацію, як правила блокування брандмауера DNS Route 53 Resolver.
- Увімкніть Amazon GuardDuty для аналізу журналів DNS та сповіщень про підозрілу активність, таку як активність командного сервера, майнінг біткойнів тощо.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Безпека на маршруті Amazon Route 53: https://surli.cc/rtlcjs
Огляд керування дозволами доступу до ресурсів Amazon Route 53: https://surl.li/fnpswt
Налаштування DNSSEC для домену: https://surl.li/cjobqs
Увімкнення або вимкнення захисту конфіденційності для контактної інформації домену: https://surl.li/niyxqe
Блокування домену для запобігання несанкціонованому перенесенню до іншого реєстратора: https://surl.li/jiumsq
Тип запису SPF: https://surl.li/ruklno
Як працює брандмауер DNS Route 53 Resolver: https://surl.li/nxuaow
Робота з приватними розміщеними зонами: https://surl.lu/debxhj

Захист Azure DNS

Azure DNS– це керована служба DNS Azure.
Нижче наведено деякі з найкращих практик, яких слід дотримуватися:

- Надайте мінімальні дозволи для доступу та керування Azure DNS за допомогою Azure керування доступом на основі ролей(RBAC).
- Видаліть невикористані DNS-записи з розміщених зон (записи ресурсів, такі як IP-адреси, що підключалися до видаленого ресурсу).
- Увімкнути Тільки для читання блокування для будь-якої розміщеної зони, якою ви керуєте за допомогою Azure DNS, щоб захистити від випадкових змін у записах DNS.
- Використовуйте приватні зони DNS для керування записами DNS для внутрішніх ресурсів (таких як ресурси, розташовані всередині приватних підмереж).
- Використання Захисник Azure щоб DNS виявляв підозрілу діяльність, пов’язану з DNS, та надсилав сповіщення про неї.
- Увімкнути ведення журналу DNS та пересилати журналу до Azure Guardian для виявлення підозрілої поведінки в службі Azure DNS.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Базовий рівень безпеки Azure для Azure DNS: https://surl.li/kkbkci
Як захистити зони та записи DNS: https://surl.lu/uihjuc
Як захистити приватні DNS-зони та записи: https://surl.lt/ugdryr
Вступ до Azure Defender для DNS: https://surli.cc/mlkhod

Захист DNS у хмарі Google

Хмарний DNS Google– це керована служба DNS від Google.

Нижче наведено деякі з найкращих практик, яких слід дотримуватися:

- Створіть групу IAM, додайте користувачів до групи та надайте цільовій групі необхідні дозволи на доступ до служби Google Cloud DNS.
- Увімкніть підпис DNSSEC у будь-якій публічно розміщеній зоні для захисту від атак DNS-спуфінгу.
- Видаліть невикористані DNS-записи з розміщених зон (записи ресурсів, такі як IP-адреси, що підключалися до видаленого ресурсу).
- Використовуйте приватні зони Google Cloud DNS для керування записами DNS для внутрішніх ресурсів (таких як ресурси, розташовані всередині приватних підмереж).
- Увімкнути журнали аудиту DNS у хмарі Google для моніторингу активності DNS.
- Зверніть увагу, що журнали аудиту діяльності адміністратора ввімкнено за замовчуванням і їх не можна вимкнути.
- Явно ввімкнути журнали аудиту доступу до даних для реєстрації активності в Google Cloud DNS.
- Обмежте доступ до журналів аудиту мінімальною кількістю співробітників, щоб уникнути небажаних змін до журналів аудиту.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Огляд хмарного DNS: https://surl.li/xqduzi
Найкращі практики DNS: https://surli.cc/hclqcu
Керування конфігурацією DNSSEC: https://surl.li/xcggbc
Огляд розширень безпеки DNS (DNSSEC): https://surl.li/uikjyq
Інформація про журнал аудиту хмарного DNS: https://surl.li/sudrvp
Ведення журналу та моніторинг: https://surl.li/ouwrpj

Захист послуг CDN

Кожен хмарний провайдер має власну реалізацію CDN-сервісу - тобто сервісу для розповсюдження контенту ближче до клієнта по всьому світу.

CDN кешує контент (наприклад, зображення, відео або статичні веб-сторінки) у кількох місцях по всьому світу, дозволяючи клієнтам швидко отримувати контент з місця, розташованого поруч із клієнтом.

CDN також слугують додатковим механізмом захисту від DDoS-атак, будучи одним із перших сервісів, що обслуговують запит клієнта, ще до того, як запит досягне серверів або програм.

Захист Amazon CloudFront

Amazon CloudFront– це керований сервіс CDN AWS.

Нижче наведено деякі з найкращих практик, яких слід дотримуватися:

- Обмежте доступ до вихідних серверів (де зберігається ваш оригінальний контент) лише з сегментів CDN (дозволить трафік лише з сегментів CDN до серверів або служб, які зберігають контент).
- Діліться контентом через протокол HTTPS, щоб зберегти конфіденційність контенту та гарантувати його автентичність.
- Під час розповсюдження контенту через HTTPS використовуйте TLS 1.2 замість старіших протоколів, таких як SSL v3.
- Якщо вам потрібно розповсюджувати приватний контент, використовуйте підписані CloudFront URL-адреси.
- Якщо вам потрібно розповсюджувати конфіденційний контент, використовуйте шифрування на рівні полів як додатковий рівень захисту.
- Використання брандмауер веб-застосунків AWS (ВАФ) для захисту контенту на Amazon CloudFront від атак на рівні додатків (таких як виявлення та блокування бот-трафіку,10
- найкращих атак на програми за версією OWASP, та інше).
- Увімкніть стандартні журнали Cloud Front для цілей ведення журналу аудиту. Зберігайте журнали у спеціальному сховищі Amazon S3 контейнер зі жорстким контролем доступу, щоб уникнути втручання в журнали.

Для отримання додаткової інформації зверніться до наступних ресурсів:

Використання HTTPS з CloudFront: https://surl.li/etykho

Налаштування безпечного доступу та обмеження доступу до контенту: https://surl.lu/ifphpv

Розміщення приватного контенту з підписаними URL-адресами та підписаними файлами cookie: https://surl.lu/swrymv

Використання AWS WAF для контролю доступу до вашого контенту: https://surl.lu/jbbigy

Використання шифрування на рівні поля для захисту конфіденційних даних: https://surl.li/sbbmvx

Налаштування та використання стандартних журналів (журналів доступу): https://surl.li/cfyedw

Ведення журналу та моніторинг в Amazon CloudFront: https://surl.li/tlzbls

Захист Azure CDN

Мережа доставки контенту Azure(CDN) - це керована служба CDN Azure.

Нижче наведено деякі з найкращих практик, яких слід дотримуватися:

- Обмежте доступ до вихідних серверів (де зберігається ваш оригінальний контент) лише з сегментів CDN (дозволить трафік лише з сегментів CDN до серверів або служб, які зберігають контент).

- Надавайте перевагу обміну контентом через протокол HTTPS, щоб зберегти конфіденційність контенту та гарантувати його автентичність.
- Під час розповсюдження контенту через HTTPS надавайте перевагу TLS 1.2 над старішими протоколами, такими як SSL v3.
- Увімкнути журнали Azure CDN для цілей ведення журналу аудиту. Пересилати журнали до Центру безпеки Azure для подальшого розслідування.
- Пересилання журналів Azure CDN до Azure Guardian (керована служба SIEM Azure) для виявлення загроз.

Для отримання додаткової інформації зверніться до наступного ресурсу:
Базовий рівень безпеки Azure для мережі доставки контенту: https://surl.lt/acvhqq

Захист мережі доставки контенту Google Cloud

Хмарна мережа доставки контенту Google CDN– це керований сервіс CDN від Google.

Нижче наведено деякі з найкращих практик, яких слід дотримуватися:

- Обмежте доступ до вихідних серверів (де зберігається ваш оригінальний контент) лише з сегментів CDN (дозволить трафік лише з сегментів CDN до серверів або сервісів, які зберігають контент).
- Діліться контентом через протокол HTTPS, щоб зберегти конфіденційність контенту та гарантувати його автентичність.
- Під час розповсюдження контенту через HTTPS використовуйте TLS 1.2 замість старіших протоколів, таких як SSL v3.
- Якщо вам потрібно розповсюджувати контент, такий як окремі файли, протягом короткого періоду часу, використовуйте підписані URL-адреси.
- Увімкнути журнали аудиту Google Cloud CDN для моніторингу активності CDN.
- Зверніть увагу, що журнали аудиту діяльності адміністратора ввімкнено за замовчуванням і їх не можна вимкнути.
- Явно ввімкнути журнали аудиту доступу до даних для реєстрації активності в Google Cloud CDN.
- Обмежте доступ до журналів аудиту мінімальною кількістю співробітників, щоб уникнути небажаних змін до журналів аудиту.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Функції хмарної CDN: https://surl.lu/autqoy
Огляд підписаних URL-адрес та підписаних файлів cookie: https://surl.li/zjnswo
Інформація про журнал аудиту хмарної CDN: https://surl.li/lsrwcy
Ведення журналу та моніторинг: https://surl.li/bpfhqc

Захист VPN-сервісів

Кожен постачальник хмарних послуг має власну реалізацію VPN-сервісу. VPN дозволяють мережевий доступ до приватних ресурсів через ненадійні мережі.

Нижче наведено деякі поширені концепції VPN-сервісів:

- У поєднанні з брандмауером VPN дозволяє організаціям безпечно отримувати доступ до своїх внутрішніх ресурсів (з обох боків VPN-тунелю) та керувати ними.
- VPN дозволяє корпоративним користувачам підключатися до хмарного середовища своєї організації з корпоративної мережі або з дому.
- З'єднання між VPN та хмарним середовищем зашифроване.
- Підключення до хмарного середовища прозоре (тобто таке ж, як і робота локально з корпоративної мережі).
- VPN може забезпечити використання багатофакторна автентифікація (МЗС) для кінцевих користувачів, які підключаються за допомогою клієнтської VPN.

Захист AWS Site-to-Site VPN

AWS Site-to-Site VPN-це керована послуга, яка дозволяє підключити вашу корпоративну мережу до середовища AWS через захищений канал IPsec.

Нижче наведено деякі з найкращих практик, яких слід дотримуватися:

- Обмежте доступ до ресурсів AWS у вашому середовищі AWS за допомогою груп безпеки Amazon VPC та правил авторизації.
- Для середовищ, що не потребують конфіденційності, використовуйте попередньо надані ключі для автентифікації в міжсайтовому VPN-тунелі.
- Для високочутливих середовищ використовуйте приватний сертифікат від Менеджер сертифікатів AWS(АКМ) Приватний центр сертифікації (Каліфорнія) обслуговування.
- Створіть групу IAM, додайте користувачів до групи та надайте цільовій групі необхідні дозволи на VPN-з'єднання AWS Site-to-Site (прикладом ролі IAM може бути можливість викликати дію API через VPN).
- Рекомендується запланувати період технічного обслуговування та щорічно змінювати попередньо надані ключі або сертифікат для VPN-з'єднання AWS Site-to-Site, щоб уникнути потенційної компрометації.
- Використовуйте Amazon CloudWatch для моніторингу VPN-тунелів (наприклад, він може надсилати тривогу, коли обсяг трафіку в байтах перевищує заздалегідь визначений поріг).
- Використовуйте AWS CloudTrail для моніторингу активності користувачів у сервісі AWS VPN.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Варіанти автентифікації VPN-тунелю типу «сайт-сайт»: https://surl.li/yseebc

Керування ідентифікацією та доступом для AWS Site-to-Site VPN: https://surl.li/gmbshf

Захист VPN-клієнта AWS

VPN-клієнта AWS дозволяє підключатися до середовища AWS з будь-якої точки Інтернету за допомогою Open VPN клієнт у захищеному TLS-каналі.

Нижче наведено деякі з найкращих практик, яких слід дотримуватися:

- Обмежте доступ до ресурсів AWS у вашому середовищі AWS за допомогою груп безпеки VPC та правил авторизації.
- Якщо ви керуєте своїми ідентифікаторами користувачів за допомогою Служба каталогів AWS, використовуйте AWS Client VPNA ctive Directory автентифікація.
- Якщо ви використовуєте SAML 2.0федеративна служба автентифікації, використовуйте AWS Client VPN єдиний вхід автентифікація (автентифікація SAML).
- Для високочутливих середовищ використовуйте AWS Client VPN на основі сертифікатів автентифікація за допомогою АКМ.
- Якщо ви використовуєте автентифікацію на основі сертифікатів AWS Client VPN, використовуйте списки відкликаних сертифікатів клієнта, щоб скасувати доступ співробітникам, які звільнилися організації або яким не потрібен доступ через VPN.
- Використовуйте Amazon CloudWatch для моніторингу VPN-тунелів (наприклад, він може надсилати тривогу, коли обсяг трафіку в байтах перевищує заздалегідь визначений поріг).
- Використовуйте AWS CloudTrail для моніторингу активності користувачів у сервісі AWS VPN.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Обмежте доступ до вашої мережі: https://surl.lu/yocgaf
Автентифікація VPN-клієнта AWS: https://surl.lu/clgxjp
Ведення журналу та моніторинг: https://surl.li/tlquew
Моніторинг клієнтського VPN: https://surl.li/ewfhjo

Захист шлюзу Azure VPN (міжсайтове з'єднання)

Шлюз Azure VPN (*Міжсайтовий зв'язок*)- це керована служба, яка дозволяє підключити корпоративну мережу до середовища Azure через безпечний канал.

Нижче наведено деякі з найкращих практик, яких слід дотримуватися:

- Обмежте доступ до ресурсів Azure у вашому середовищі Azure за допомогою NSG.
- Використовуйте GCMAES 256 алгоритм як для шифрування тунелю IPsec, так і для забезпечення цілісності трафіку, що проходить через тунель.
- Використовуйте попередньо надані ключі для автентифікації в тунелі VPN типу «сайт-сайт».

- Для масштабних середовищ з кількома підписками Azure та кількома шлюзами VPN типу «сайт-сайт» використовуйте брандмауер Azure для централізованого створення, забезпечення дотримання та реєстрації мережевих політик у кількох підписках.
- Використовуйте Azure Monitor для моніторингу VPN-тунелів (наприклад, він може надсилати сповіщення, коли обсяг трафіку в байтах перевищує попередньо визначений поріг).
- Увімкнути захист від DDoS-атак у Azure для захисту вашого VPN-шлюзу від DDoS-атак.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Базовий рівень безпеки Azure для VPN-шлюзу: https://surli.cc/efatod
Моніторинг VPN-шлюзу: https://surl.lt/cxkska

Захист шлюзу Azure VPN (точка-сайт)

Шлюз Azure VPN (*Точка-сайт*) дозволяє підключатися з будь-якої точки Інтернету до середовища Azure через безпечний канал за допомогою клієнта OpenVPN - протокол тунелювання захищених сокетів (SSTP), або обмін ключами Інтернету версії 2(IKEv2) VPN-клієнт.

Нижче наведено деякі з найкращих практик, яких слід дотримуватися:

- Якщо ви керуєте ідентифікаторами користувачів в Azure Active Directory, використовуйте Azure Active Directory для автентифікації користувачів у шлюзі VPN у поєднанні з Azure RBAC, щоб забезпечити мінімальний доступ до ресурсів у вашому середовищі Azure.
- Якщо ви автентифікуєте користувачів через Azure Active Directory, застосуйте багатофакторну автентифікацію (MFA) для своїх кінцевих користувачів.
- Для середовищ з високою чутливістю використовуйте сертифікати для автентифікації в тунелі VPN типу «точка-точка».
- Обмежте доступ до ресурсів Azure у вашому середовищі Azure за допомогою NSG.
- ВикористовуйтеGCMAES256алгоритм як для шифрування тунелю IPSec, так і для забезпечення цілісності трафіку, що проходить через тунель.
- Використовуйте Azure Monitor для моніторингу VPN-тунелів (наприклад, він може надсилати сповіщення, коли обсяг трафіку в байтах перевищує попередньо визначений поріг) та для реєстрації подій, пов’язаних з аудитом (прикладом підозрілої поведінки може бути спроба користувача вперше увійти посеред ночі).
- Увімкніть захист Azure DDoS, щоб захистити ваш VPN-шлюз від DDoS-атак.
- Використання Розширений захист від загроз Azure для виявлення аномальної поведінки користувачів, що підключаються через VPN-тунель типу «точка-точка».

- Використовуйте Центр безпеки Azure для виявлення подій, пов’язаних із безпекою, через VPN-шлюз.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Базовий рівень безпеки Azure для VPN-шлюзу: https://surl.li/dduypr
Про криптографічні вимоги та шлюзи Azure VPN: https://surl.lt/pdhumz
Про VPN-з’єднання типу «точка-точка»: https://surl.lu/rjcelc
Налаштування VPN-з’єднання типу «точка-сайт» за допомогою автентифікації сертифіката Azure: портал Azure: https://surl.li/rhdvxm
Увімкнення багатофакторної автентифікації (MFA) Azure AD для користувачів VPN: https://surli.cc/exqpnw
Моніторинг VPN-шлюзу: https://surl.li/gkcjnv

Захист VPN-сервера Google Cloud

Хмарний VPN від Google-це керована послуга, яка дозволяє підключити вашу корпоративну мережу до середовища GCP через захищений канал (за допомогою тунелю IPSec).

Нижче наведено деякі з найкращих практик, яких слід дотримуватися:

- Обмежте доступ до ресурсів GCP у вашому Google Cloud VPC за допомогою правил брандмауера VPC.
- ВикористовуйтеAES-GCM-16-256 алгоритм як для шифрування тунелю IPSec, так і для забезпечення цілісності трафіку, що проходить через тунель.
- Використовуйте надійний 32-символьний попередньо наданий ключ для автентифікації в тунелі Google Cloud VPN.
- Створіть групу IAM, додайте користувачів до групи та надайте цільовій групі необхідні дозволи на підключення до Google Cloud VPN.
- Використання ведення журналу в хмарі Google для моніторингу активності в сервісі Google Cloud VPN.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Огляд хмарної VPN: https://surl.li/vdgaxl
Генерація надійного попередньо спільного ключа:
https://surli.cc/ufxihb
Підтримувані шифри IKE: https://surl.li/kdyyoj
Налаштування правил брандмауера: https://surl.li/uhsqzg
Найкращі практики для хмарного VPN: https://surl.li/udmqan
Перегляд журналів та показників: https://surl.li/hjklvl

Захист послуг DDoS-захисту

Кожен постачальник хмарних послуг має власну реалізацію керованої служби захисту від DDoS-атак.

Оскільки хмарні провайдери мають дуже велику пропускну здатність, вони можуть пропонувати (як платну послугу) механізми для захисту середовищ клієнтів від DDoS-атак.

Наступні сервіси допомагають запобігти DDoS-атакам:

- Сервіси захисту від DDoS-атак
- Групи автоматичного масштабування в поєднанні з послугами балансування навантаження
- Сервіси CDN
- Послуги WAF

Захист AWS Shield

AWS Shield– це керований сервіс захисту від DDoS-атак Amazon.

Він представлений у двох цінових моделях:

- Стандарт AWS Shield Це стандартний безкоштовний захист від DDoS-атак рівня 7 (HTTP/HTTPS), який надається всім клієнтам.
- Розширений захист AWS. Це пропонує захист від DDoS-атак на рівнях 3/4 (мережевий рівень) та 7 (прикладний рівень) з додатковим захистом для сервісів AWS, таких як DNS (Route 53), CDN (Cloud Front). Еластичне балансування навантаження(ЕЛБ) та послуги віртуальних машин (EC2). Цей ціновий рівень також пропонує підтримку від команди реагування на DDoS-атаки AWS.

Нижче наведено деякі з найкращих практик, яких слід дотримуватися:

- Використовуйте AWS Shield Standard для будь-якого веб-середовища виробництва, яке ви підключаєте до Інтернету.
- Використовуйте AWS Shield Advanced для масштабних виробничих середовищ, які ви підключаєте до Інтернету, щоб краще розуміти атаки.
- Під час використання AWS Shield Advanced зареєструйте еластичну IP-адреса (EIП) адресу як захищене джерело, що дозволяє швидше виявляти атаки.
- Використовуючи AWS Shield Advanced, ви можете генерувати звіти майже в режимі реального часу про атаки на ресурси у вашому(-их) обліковому записі(-ах) AWS.
- Під час поєднання AWS Shield та сервісу AWS WAF використовуйте Amazon CloudWatch для моніторингу вхідних запитів та сповіщень про їх сплеск, щоб отримувати попередні сповіщення про вхідні DDoS-атаки.
- Використання/Керування ідентифікацією та доступом AWS(Ідентифікація та доступність даних), щоб обмежити дозволи для консолі AWS Shield.
- Використовуйте AWS CloudTrail для ведення журналу дій у консолі AWS Shield.

Для отримання додаткової інформації зверніться до наступних ресурсів:

Як працює AWS Shield: https://surl.lu/oubuum

Перегляд DDoS-подій: https://surl.li/nlbtcl
Огляд керування дозволами доступу до ресурсів AWS Shield: https://surl.li/dgsbnn
Інструменти моніторингу: https://surl.li/psfark
Стандарт AWS Shield: https://surl.li/ihbyjg
Розширений захист AWS: https://surl.li/tfionx
Amazon заявляє про пом'якшення найбільшої DDoS-атаки за всю історію спостережень: https://surl.lu/dvkjrt

Захист Azure від DDoS-атак

Захист від DDoS-атак у Azure– це керована служба захисту від DDoS-атак Azure.

Він представлений у двох цінових моделях:

1. Базовий захист від DDoS-атак Azure забезпечує захист від DDoS-атак рівня 3/4 (мережевий рівень) та рівня 7 (HTTP/HTTPS) безкоштовно.
2. Стандарт захисту від DDoS-атак Azure забезпечує захист від DDoS-атак на рівнях 3/4 (мережевий рівень) та 7 (HTTP/HTTPS) з додатковим захистом на рівні віртуальної мережі, а також додатковими можливостями ведення журналу та сповіщень.

Нижче наведено деякі з найкращих практик, яких слід дотримуватися:

- Увімкніть базовий захист Azure DDoS для будь-якого виробничого середовища, до якого ви підключаєтеся до Інтернету.
- Використовуйте стандарт захисту від DDoS-атак Azure для масштабних виробничих середовищ, які ви надаєте доступу до Інтернету, щоб краще розуміти атаки.
- Під час використання стандарту захисту від DDoS-атак Azure увімкніть журнали ресурсів для публічних IP-адрес, щоб швидше виявляти атаки.
- При поєднанні шлюз застосунків Azure за допомогою WAF ви додаєте захист від атак веб-застосунків.
- Використовуйте Azure Monitor для моніторингу та сповіщення про різке збільшення кількості вхідних запитів, щоб отримувати попередження про вхідні DoS-атаки.
- Надсилати журнали захисту від DDoS-атак Azure до Azure Sentinel для подальшого аналізу DDoS-атак.
- Використовуйте Azure Active Directory, щоб обмежити дозволи консолі захисту від DDoS-атак Azure.
- Використовуючи Azure DDoS Protection Standard, ви можете проводити симуляції DDoS-атак на ваші проміжні або виробничі середовища Azure (у години низької активності) за допомогою стороннього рішення від Хмара точок розриву Моделювання дозволить вам краще зрозуміти ефективність планів захисту від DDoS-атак та допоможе навчити ваші команди.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Огляд стандарту захисту від DDoS-атак Azure: https://surli.cc/eujtnz

Перегляд та налаштування сповіщень про захист від DDoS-атак: https://surl.lt/ywbuam
Перегляд та налаштування журналу діагностики DDoS-атак: https://surli.cc/kapkjp
Стандартні функції захисту від DDoS-атак Azure: https://surl.li/mihiyg
Базовий рівень безпеки Azure для стандарту захисту від DDoS-атак Azure: https://surli.cc/mtnngj
Тестування за допомогою симуляцій: https://surl.li/qbqooz

Захист Google CloudArmor

Google CloudArmor - це захист від DDoS-атак, керований Google, і Брандмауер веб-застосунків(ВАФ) обслуговування.

Він представлений у двох цінових моделях:

1. Стандарт Google CloudArmor Це забезпечує захист від об'ємних DDoS-атак і включає попередньо налаштовані правила WAF.
2. Керований захист плюс Це забезпечує захист від об'ємних DDoS-атак, включає попередньо налаштовані правила WAF та адаптивний механізм захисту.

Цей ціновий рівень також пропонує підтримку від команди реагування на DDoS-атаки Google.

CloudArmor захищає програми, розташовані за зовнішнім балансувальником навантаження Google Cloud, який базується на проксі-балансувальниках навантаження HTTP/HTTPS та TCP/SSL.

Нижче наведено деякі з найкращих практик, яких слід дотримуватися:

- Створіть групу IAM, додайте користувачів до групи та надайте цільовій групі необхідні дозволи на CloudArmor.
- Зверніть увагу, що CloudArmor містить попередньо налаштовані правила захисту від поширених атак веб-застосунків.
- Якщо вам потрібно налаштувати власні правила відповідно до вашої програми, створіть власні політики безпеки CloudArmor, щоб дозволити або заборонити трафік до ваших програм за зовнішнім балансувальником навантаження Google Cloud.
- Увімкнути журнали CloudArmor для будь-якої серверної служби, щоб виявляти дозволені або відхилені HTTP/HTTPS-запити.
- Для критично важливих виробничих програм рекомендується підписатися на послугу «Керований захист плюс».
- Для критично важливих виробничих застосувань рекомендується ввімкнути механізм адаптивного захисту CloudArmor для виявлення аномальної активності та створення власної сигнатури для блокування атак на програми за допомогою правил WAF (для атак на програми).
- У сценаріях, коли ви хочете дозволити стороннім партнерам доступ до своїх виробничих програм без необхідності вказувати свою зовнішню IP-адресу

або діапазон IP-адрес, використовуйте списки іменованих IP-адрес CloudArmor для налаштування білого списку дозволених джерел.

- Використовуйте Центр команд безпеки Google сервіс для виявлення аномальної поведінки в трафіку CloudArmor (наприклад, піків трафіку).

Для отримання додаткової інформації зверніться до наступних ресурсів:
Огляд адаптивного захисту Google CloudArmor: https://surl.li/rekwcc
Списки іменованих IP-адрес Google CloudArmor: https://surl.li/jhlhyk
Нові можливості WAF у CloudArmor для локальних та хмарних робочих навантажень: https://surli.cc/ttmudm
Моніторинг політик безпеки Google CloudArmor: https://surl.li/rxqjgj
Висновки Центру управління безпекою: https://surl.lu/srjsba

Забезпечення безпеки послуг WAF

Кожен постачальник хмарних послуг має власну реалізацію служби WAF, тобто брандмауера прикладного рівня з можливостями виявлення та пом'якшення поширених атак на основі HTTP/ HTTPS проти ваших публічно доступних веб-застосунків.

Захист AWS WAF

AWS WAF-це керований сервіс брандмауера веб-застосунків AWS.
AWS WAF пропонує захист від таких типів атак:

- DDoS-атаки 7-го рівня (у поєднанні з AWS Shield)
- Поширені атаки на веб-застосунки
- Боти (трафік, що генерується не людиною)

AWS WAF також дозволяє захистити такі сервіси Amazon:

- Amazon Cloud Front: Керований сервіс CDN від Amazon
- Шлюз Amazon API: Служба керованого шлюзу API Amazon
- Amazon ALBA керує балансувальником навантаження застосунків сервіс (балансувальник навантаження рівня 7)

Нижче наведено деякі з найкращих практик, яких слід дотримуватися:

- Щоб захистити зовнішній веб-ресурс, створіть веб-списки контролю доступу (ACL).
- Під час створення нового правила веб-списку контролю доступу (ACL) змініть назву метрики CloudWatch за замовчуванням на інформативну назву, яка дозволить вам виявити її пізніше під час перегляду журналів
- CloudWatch.
- Використовуйте Amazon CloudWatch для моніторингу активності правил веб-ACL.
- Для захисту від нестандартних типів атак веб-застосунків створіть власні правила.

- Для кращого захисту підпишіться на правила, доступні на AWS Marketplace (створено постачальниками засобів безпеки).
- Для масштабних середовищ з кількома обліковими записами AWS використовуйте AWS Firewall Manager для
- централізованого створення та забезпечення дотримання правил WAF.
- Надсилати журнали AWS WAF до місця призначення Amazon Kinesis Datacервіс для перегляду журналів атак майже режимі реального часу.
- Використовуйте AWS Config, щоб увімкнути ведення журналу для кожного щойно створеного веб-списку контролю доступу (ACL).
- Використовуйте AWS IAM, щоб обмежити дозволи консолі AWS WAF.
- Використовуйте AWS CloudTrail для ведення журналу дій у консолі AWS WAF.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Керівні принципи впровадження AWS WAF: https://surli.cc/vxgcuh
Початок роботи з AWS WAF: https://surl.li/cmmzmx
Огляд керування дозволами доступу до ресурсів AWS WAF: https://surl.lu/knelcx
Ведення журналу та моніторинг в AWS WAF: https://surl.lu/jtlsku

Захист Azure WAF

Брандмауер веб-застосунків Azure(ВАФ) - це служба брандмауера веб-застосунків під керуванням Azure.

Azure WAF інтегровано з такими службами та може бути розгорнуто як їх частина:

- Шлюз застосунків Azure Служба балансування навантаження рівня 7
- Azure Front Door Глобальна служба захисту веб-застосунків від загроз
- CDN Azure Керована CDN

Нижче наведено деякі з найкращих практик, яких слід дотримуватися:

- Розгорніть ліцензію Azure WAF версії 2 у будь-якій щойно відкритій веб-програмі.
- Для масштабних середовищ з кількома підписками Azure та кількома веб-застосунками використовуйте Azure WAF з Front Door для захисту ваших веб-застосунків.
- Після вивчення трафіку для вашої веб-програми (запуск WAF у режимі навчання) налаштуйте Azure WAF у режимі запобігання.
- Для захисту від нестандартних типів атак веб-застосунків створіть власні правила.
- Створюйте власні правила для блокування трафіку, що походить з відомих шкідливих IP-адрес.
- Використовуйте журнали активності Azure як частину служби Azure Monitor для моніторингу змін у правилах Azure WAF.

- Надсилати журнали Azure WAF до Azure Sentinel для виявлення та усунення веб-атак.
- Використовуйте Azure Active Directory, щоб обмежити дозволи консолі Azure WAF.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Базовий рівень безпеки Azure для брандмауера веб-застосунків Azure: https://surl.li/xfvvsg
Базовий рівень безпеки Azure для Application Gateway: https://surl.lt/lojhfs
Що таке брандмауер веб-застосунків Azure на шлюзі застосунків Azure: https://surl.li/qpbmlj
Брандмауер веб-застосунків Azure та політика Azure: https://surl.li/qfqoxe

Підсумки Розділу 1

У Розділі 1 розглянуто визначення таких ключових поняття як *«хмара»*, як основні її моделі розгортання та моделі хмарних сервісів. Особливу увагу приділено концепції моделі спільної відповідальності у хмарних середовищах та її інтерпретації в AWS, Azure і GCP. Також здійснено огляд вбудованих інструментів командного рядка, характерних для кожного з провайдерів.

Окремий акцент зроблено на питаннях безпечної експлуатації віртуальних машин на базі інфраструктури AWS: від процедури входу в систему та захисту мережевого доступу до використання послідовної консолі для усунення несправностей; управління оновленнями та питанням організації резервного копіювання. Розглянуто спектр обчислювальних сервісів AWS, Azure і GCP: від віртуальних машин та керованих баз даних (зокрема MySQL) до контейнерних рішень і безсерверних обчислень (Function as a Service).

Детально проаналізовано засоби керування ідентифікацією та доступом: механізми автентифікації та авторизації, контроль мережевих привілеїв, налаштування аудиту й журналювання, а також дотримання стандартів безпеки та відповідності. Розглянуто сервіси зберігання даних у середовищах AWS, Azure та GCP: від об’єктних сховищ до блокових, файлових і контейнерних систем.

В окремих параграфах зосереджена увага на мережевих сервісах провайдерів: віртуальних приватних мережах, DNS, CDN, VPN, механізмах захисту від DDoS-атак і сервісах WAF. Для кожного типу сервісу наведено найкращі практики налаштування, автентифікації, моніторингу та аудиту. Ефективне управління зазначеними компонентами забезпечує можливість комплексного контролю та відстеження їх функціонування.

Контрольні питання до Розділу 1

1. Що означає термін «зловживання хмарними сервісами»?
2. Які основні наслідки зловживань хмарними ресурсами для клієнтів?
3. Наведіть приклад використання хмарної інфраструктури для DDoS-атак.
4. Як хмарні ресурси можуть використовуватися для майнінгу криптовалют без відома клієнта?
5. Чому зловживання хмарою може призвести до фінансових збитків?
6. Як зловмисники використовують хмарні сервіси для розсилання спаму чи фішингу?
7. Що таке атака методом перебору паролів і як вона може бути реалізована через хмару?
8. Навіщо налаштовувати сповіщення про виставлення рахунків у хмарних сервісах?
9. Як принцип розподілу обов'язків допомагає знизити ризик зловживань?
10. Яку роль відіграють списки контролю доступу (ACL) у запобіганні зловживанням?
11. Як правила мережі та брандмауера можуть обмежувати шкідливий трафік?
12. Чому регулярна зміна облікових даних є ефективним заходом безпеки?
13. Для чого використовуються журнали аудиту у виявленні зловживань?
14. Як сервіси захисту від DDoS допомагають уникнути збоїв у роботі хмарних сервісів?
15. Яким чином WAF захищає від атак на рівні додатків?
16. Чому важливо проводити навчання персоналу щодо правил прийнятного використання хмари?
17. Як Amazon CloudWatch допомагає виявляти ознаки зловживань?
18. Для чого AWS Config використовується у моніторингу безпеки?
19. Яку роль відіграє AWS GuardDuty у виявленні майнінгу криптовалют?
20. Як мережевий брандмауер AWS та VPC ACL захищають від зловживань?
21. Які інструменти Azure допомагають контролювати фінансові витрати на хмарні ресурси?
22. Як Microsoft Defender for Cloud допомагає у виявленні нецільового використання ресурсів?
23. Яку функцію виконують групи безпеки (NSG) в Azure у запобіганні зловживанням?
24. Як Google CloudArmor виявляє та блокує підозрілий трафік?
25. Для чого GCP OS Patch Management використовується у контексті безпеки?

РОЗДІЛ 2. ГЛИБИННЕ ЗАНУРЕННЯ В IAM, АУДИТ ТА ШИФРУВАННЯ

У цій частині посібника ми розглянемо всі тонкощі управління ідентифікацією, аудиту та шифрування.

Ця частина посібника складається з наступних розділів:

- *2.1. Ефективні стратегії впровадження IAM-рішень*
- *2.2. Моніторинг та аудит хмарних середовищ*
- *2.3. Застосування шифрування в хмарних сервісах*

2.1. Ефективні стратегії впровадження IAM-рішень

У цьому парафрафі ми розглянемо різні концепції управління ідентифікацією - від традиційних служб каталогів (на основі протоколу Kerberos у середовищі Microsoft, служб каталогів на основі LDAP, популярних у середовищах, відмінних від Microsoft, і навіть служб каталогів на основі Linux) до сучасних служб каталогів (на основі протоколів SAML або OAuth). - і, нарешті, ми зрозуміємо, як захистити механізми автентифікації на основі Багатофакторна автентифікація(МЗС).

У цьому параграфі ми розглянемо такі теми:

- Вступ до IAM
- Невміння керувати ідентифікаторами
- Захист хмарних сервісів IAM
- Захист служб каталогів
- Налаштування багатофакторної автентифікації

Технічні вимоги

Для цього розділу вам потрібно мати ґрунтовне розуміння управління ідентифікацією та таких концепцій, як Active Directory (AD), протокол Kerberos, SAML проти OAuth 2.0 та MFA.

Нижче наведено приклад діаграми, яка зображує процес автентифікації SAML (Рис.2.1.):

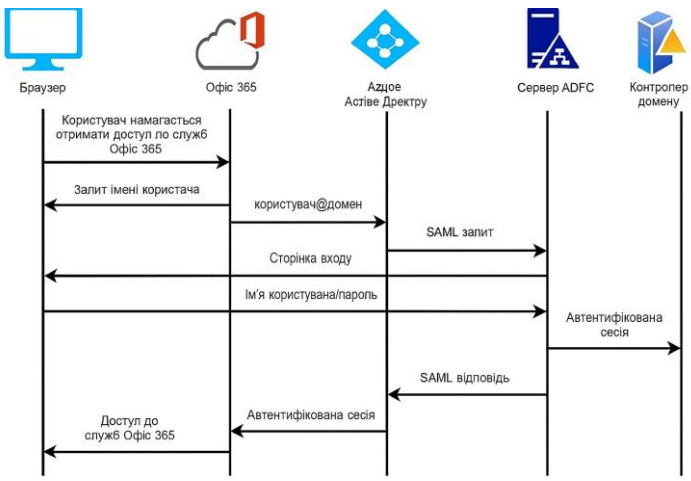

Рисунок 2.1 - Приклад процесу автентифікації SAML для служби Office 365

Вступ до IAM

Управління ідентифікацією та доступом (Ідентифікація та доступність даних) стосується концепції управління всім життєвим циклом користувача, включаючи надання доступу (тобто створення облікового запису), призначення дозволів і, нарешті, скасування надання доступу до облікового запису (тобто, коли людина залишає організацію або обліковий запис більше не потрібен).

Управління доступом складається з таких основних концепцій:

1. *Ідентичність*. Це вказує на користувача, комп'ютер, службу або роль, яка бажає отримати доступ до системи чи програми та виконати дії (від доступу до спільного сховища до запитів до бази даних та отримання інформації).
2. *Автентифікація*. Це процес доведення того, що певна особа (наприклад, користувач) є тим, за кого себе видає (наприклад, надання імені користувача та пароля, що відповідають записам користувача в центральному сховищі користувачів).
3. *Авторизація*. Це процес надання автентифікованій особі (наприклад, користувачеві) дозволів на виконання дій з ресурсом (наприклад, дозвіл користувачеві завантажувати файл до спільного сховища).

Постачальники хмарних послуг використовують інший підхід до IAM:

- AWS IAM. За замовчуванням усі запити неявно відхиляються.
- Azure Active Directory (Azure AD). За замовчуванням користувачі мають мінімальний набір дозволів для доступу до ресурсів.
- GCP. За замовчуванням облікові записи служб мають дозвіл на виклик API Google Cloud.

Найпоширеніша служба каталогів, розгорнута в локальних центрах обробки даних більшості організацій, це Microsoft Active DirectoryЦе центральне сховище для зберігання таких об'єктів, як облікові записи користувачів, облікові записи комп'ютерів, групи тощо.

Найчастіше використовуваним протоколом під час роботи локально з традиційними програмами або службами Windows є Кербероспротокол.

Для отримання додаткової інформації зверніться до наступних ресурсів:
AWS IAM –Визначення того, чи запит дозволено чи відхилено в обліковому записі: https://surl.li/puycnv
Які дозволи користувачів за замовчуванням в Azure Active Directory?: https://surl.li/slcjmz
Облікові записи сервісів GCP за замовчуванням:
https://surl.li/rbbryk
Що таке Active Directory: https://surl.li/tppjzg
Що таке протокол Kerberos: https://surl.li/kyxcys

Невдача в управлінні ідентифікаторами

Перш ніж ми перейдемо до Управління ідентифікацією (Identity and Access Management), розглянемо кілька прикладів невдалого керування ідентифікаторами:

- До організації приєднався новий співробітник. Оскільки у нас немає документованої та автоматизованої Identity and Access Management робочому процесі дозволи працівника були скопійовані з профілю системного адміністратора. Новий працівник не знав, які сайти йому слід переглядати в Інтернеті, і в результаті його заразило програмне забезпечення-вимагач. Це, у свою чергу, «заразило» базу даних продажів, яка була зашифрована, і спричинило простої відділу продажів.
- Працівник зміг створити пароль, який легко вгадати (оскільки на рівні організації не було запроваджено складну політику щодо паролів), і в результаті хакер зміг вгадати пароль працівника та отримати доступ до конфіденційного фінансового звіту.
- Працівник змінив свою роль в організації з IT-відділу на команду розробників, і ми забули оновити його права на виробничих серверах. В результаті працівник тепер має надмірні права доступу та може вносити зміни до виробничої системи.
- Працівник звільнився з організації, а ми забули відключити його обліковий запис. В результаті працівник мав доступ до корпоративної CRM-системи через VPN, який він використовував для експорту контактних даних клієнтів, щоб мати змогу продавати товари свого нового роботодавця.

Захист хмарних сервісів IAM

Кожен хмарний провайдер має власну реалізацію керованих IAM-сервісів, іншими словами, сервіс для управління запитами на автентифікацію та авторизацію.

Перелік термінології AWS IAM:

- *Користувач IAM.* Це особа або програма з дозволом на доступ до ресурсів AWS. Користувач IAM має облікові дані (такі як пароль, ключі доступу та MFA).
- *Група IAM.* Це стосується групи користувачів IAM для спрощення завдання керування дозволами.
- *Роль IAM.* Це вказує на особу, яка має дозвіл на доступ до ресурсів без будь-яких облікових даних. Зазвичай роль IAM призначається групі IAM, користувачеві IAM або обліковому запису служби, який потребує тимчасових дозволів.
- *Обліковий запис служби.* Це стосується спеціального типу користувача IAM, і його метою є надання програмам доступу до ресурсів.
- *Політика IAM.* Це визначення на основі JSON, яке встановлює дозволи для доступу до ресурсів AWS.

Політика, що базується на ресурсах:

- Це прив’язано до ресурсу AWS (наприклад, до корзини Amazon S3).
- Постачальник ідентифікаційних даних: Це стосується можливості керувати ідентифікаторами поза межами AWS, водночас надаючи доступ до ресурсів AWS зовнішнім ідентифікаторам (наприклад, федерація між AWS та Azure AD).

Логіка оцінки політики AWS IAM:

- Політики на основі ідентифікації з політиками на основі ресурсів результатом обох політик є загальна кількість дозволів для обох політик.

Політики на основі ідентифікації з межами дозволів результатом політик на основі ідентифікації з обмеженнями, встановленими межами дозволів, стають ефективні дозволи.

Політики на основі ідентифікації з політиками контролю послуг AWS Organizations. Результатом обох політик (для облікового запису учасника організації) стають чинні дозволи.

Захист AWS IAM

AWS IAM - це сервіс IAM, керований Amazon.

Нижче наведено перелік найкращих практик:

- Вимкніть та видаліть усі ключі доступу й секретні ключі доступу з облікового запису root-користувача AWS.
- Налаштуйте надійний пароль для користувача root облікового запису AWS.
- Увімкнути багатофакторну автентифікацію (MFA) для користувача root облікового запису AWS.
- Уникайте використання облікового запису root AWS. Натомість створіть випадковий пароль для облікового запису root AWS, а в рідкісних випадках, коли потрібен обліковий запис root, скиньте пароль.
- Створіть користувача IAM з повною роллю адміністратора IAM лише для консолі AWS, щоб керувати обліковим записом AWS.
- Увімкнути багатофакторну автентифікацію (MFA) для будь-якого користувача IAM з повною роллю адміністратора IAM.
- Уникайте створення ключів доступу та секретних ключів доступу для користувача IAM з повною роллю адміністратора IAM.
- Створювати користувачів IAM з політиками IAM відповідно до принципу найменших привілеїв.
- Створюйте групи IAM, призначайте дозволи групам і додавайте користувачів IAM до цих груп для легшого керування обліковими записами та дозволами.
- Для обмеженого доступу користувачів створіть керовані політики та призначте ці політики групі користувачів.
- Налаштуйте політику паролів (яка включає мінімальний та максимальний вік пароля, мінімальну довжину пароля та забезпечує використання історії паролів і складних паролів).

- Використовуйте ролі IAM, щоб дозволити програмам, що розгортаються на екземплярах EC2, доступ до ресурсів AWS.
- Використовуйте ролі IAM замість створення ключів доступу та секретних ключів доступу, щоб забезпечити тимчасовий, а не постійний доступ до ресурсів.
- Уникайте вбудовування ключів доступу та секретних ключів доступу в код. Натомість використовуйте рішення для керування секретами, такі як AWS Secrets Manager, для зберігання та отримання ключів доступу.
- Періодично змінюйте ключі доступу, щоб уникнути зловживання ключами з боку зловмисних внутрішніх або зовнішніх користувачів.
- Для високочутливих середовищ або ресурсів налаштуйте політику IAM, щоб обмежити доступ на основі таких умов, як дані, час, багатофакторна автентифікація тощо.
- Для високочутливих середовищ або ресурсів налаштуйте політику IAM, щоб дозволити доступ лише користувачам з увімкненою багатофакторною автентифікацією (MFA).
- Використовуйте AWS IAM Прийняти Роль можливість перемикання між кількома обліковими записами AWS, використовуючи ту саму ідентифікацію IAM.
- Використовуйте межі дозволів IAM, щоб обмежити доступ користувачів IAM до певних ресурсів AWS.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Найкращі практики безпеки в IAM: https://surl.li/eaiudz
Найкращі практики керування ключами доступу AWS: https://surl.lt/oyvipx
AWS: Дозволяє доступ на основі дати та часу:
https://surl.li/utpmoe
Прийняти Роль: https://surl.li/arwmxl
Межі дозволів для об'єктів IAM: https://surli.cc/zwpxoc
Логіка оцінки політики: https://surli.cc/gqflra

Аудит AWS IAM

AWS дозволяє контролювати AWS IAM за допомогою таких вбудованих сервісів:

- *Amazon CloudWatch.* Це сервіс, який дозволяє вам вести журнали аудиту AWS CloudTrail та створювати сповіщення, коли кількість записів у журналі перевищує певний поріг, наприклад, після кількох невдалих входів у систему.
- *AWS CloudTrail.* Це сервіс, який дозволяє вам перевіряти дії, виконані користувачем root облікового запису AWS або будь-яким користувачем IAM.

- *Amazon Guard Duty.* Це сервіс, який використовує машинне навчання для виявлення та сповіщення про неправомірне використання ідентифікаційних даних (на основі журналів AWS CloudTrail).

Нижче наведено перелік найкращих практик:

- Увімкнути AWS CloudTrail у всіх регіонах AWS.
- Обмежте рівень доступу до журналів CloudTrail мінімальною кількістю співробітників - бажано тим, хто має обліковий запис керування AWS, поза межами ваших кінцевих користувачів (включно з користувачами IAM), щоб уникнути можливого видалення або змін до журналів аудиту.
- Використовуйте Amazon Guard Duty для аудиту активності root-користувача облікового запису AWS.
- Використовуйте AWS CloudTrail для аудиту активності користувачів IAM.
- Використовуйте звіти про облікові дані IAM, щоб знаходити користувачів, які не входили в систему протягом тривалого часу.
- Використовуйте симулятор політики IAM, щоб перевірити, які фактичні дозволи має певний користувач IAM (тобто, чи дозволено йому доступ до ресурсів, чи заборонено).
- Використовуйте AWS IAM Access Analyzer для виявлення невикористаних дозволів (як з вашого облікового запису AWS, так і з інших облікових записів) та точного налаштування дозволів для ваших ресурсів AWS.
- Використовуйте AWS IAM Access Analyzer для виявлення секретних даних, до яких можна отримати доступ з-за меж вашого облікового запису AWS та які зберігаються в сервісі AWS Secrets Manager.
- Використовуйте інструмент IAMCTL для порівняння політик IAM між обліковими записами користувачів IAM, щоб виявити будь-які зміни (наприклад, порівнюючи шаблони політик користувачів IAM з політиками одного з ваших інших користувачів IAM).

Для отримання додаткової інформації зверніться до наступних ресурсів:

Керівні принципи аудиту безпеки AWS: https://surl.lu/lqikdb
Реєстрація викликів IAM та AWS STS API за допомогою AWS CloudTrail: https://surli.cc/mqngqz
Моніторинг та контроль дій, що виконуються з урахуванням взятих на себе ролей: https://surli.cc/lwugoj
Типи знахідок GuardDuty IAM: https://surl.li/radutu
Функції аналізу доступу AWS IAM: https://surl.li/rqhyks
Автоматизувати вирішення проблем, пов'язаних з доступом до різних облікових записів IAM Access Analyzer, для ролей IAM: https://surl.lu/yormls
Виявлення, перегляд та усунення ненавмисного доступу до таємниць менеджера таємниць за допомогою аналізатора доступу IAM: https://surl.lt/gdzatb
Отримання звітів про облікові дані для вашого облікового запису AWS: https://surl.li/dxypxd

Тестування політик IAM за допомогою симулятора політик IAM: https://surli.cc/ggvxmn
Новий інструмент IAMCTL порівнює кілька ролей та політик IAM: https://surl.li/dcmsrw

Захист Azure AD

Azure AD - це служба каталогів, керована Azure.
Azure AD підтримує такі типи моделей ідентифікації:

1. Ідентифікація лише для хмари. Обліковий запис користувача створюється всередині клієнта Azure AD та існує лише в хмарі (де доступ до локальної мережі не потрібен).
2. Гібридна ідентичність. Обліковий запис користувача існує як в клієнті Azure AD, так і локально.

Перелік термінології Azure AD:

- *Користувач.* Це особа або програма з дозволом на доступ до ресурсів Azure. Користувач має облікові дані (наприклад, пароль або багатофакторну автентифікацію).
- *Група.* Це група користувачів, яка спрощує керування дозволами.
- *Azure контроль доступу на основі ролей (Azure RBAC).* Це система авторизації з вбудованими дозволами для доступу до ресурсів Azure (наприклад, Власник, Автор, Читач, та інше).

Нижче наведено перелік найкращих практик:

- Налаштуйте надійний пароль для вихідного облікового запису глобального адміністратора Azure AD.
- Увімкнути багатофакторну автентифікацію (MFA) для вихідного облікового запису глобального адміністратора Azure AD.
- Уникайте використання оригінального облікового запису глобального адміністратора Azure AD - зберігайте пароль користувача в безпечному місці.
- Створіть користувача Azure AD з роллю глобального адміністратора для керування Azure AD.
- Увімкніть багатофакторну автентифікацію (MFA) для будь-якого користувача у вашій Azure AD (наприклад, з роллю глобального адміністратора).
- Обмежте кількість глобальних адміністраторів до менш ніж п’яти.
- Використовуйте Azure RBAC, щоб надати користувачам мінімальні дозволи, необхідні для доступу до ресурсів Azure та їх використання.
- Увімкнути Azure AD Керування привілейованими ідентифікаторами(ПІМ) у вашій службі Azure AD для керування своєчасним доступом до ресурсів Azure AD.

- Створюйте групи Azure AD, призначайте дозволи групам і додавайте користувачів до цих груп для легшого керування обліковими записами та дозволами.
- Налаштуйте політику паролів (яка включає мінімальний та максимальний вік пароля, мінімальну довжину пароля та забезпечує використання історії паролів і складних паролів).
- Створіть екстрений обліковий запис (це спеціальні облікові записи користувачів, які не слід використовувати щодня, мають увімкнену багатофакторну автентифікацію та є членами ролі глобального адміністратора), щоб уникнути блокування доступу до Azure AD.
- Використовуйте політику умовного доступу, щоб примусово використовувати багатофакторну автентифікацію (MFA) та визначити розташування, з якого глобальний адміністратор може мати доступ для входу та керування вашою Azure AD (наприклад, мережа вашого офісу).

Для отримання додаткової інформації зверніться до наступних ресурсів:
Моделі ідентифікації Microsoft 365 та Azure Active Directory: https://surli.cc/kvhoiv
Класичні ролі адміністратора підписки, ролі Azure та ролі Azure AD: https://surl.li/fuhrgb
Підвищте рівень доступу для керування всіма підписками Azure та групами керування: https://surl.li/pikrfg
Що таке керування привілейованими ідентифікаторами Azure AD?: https://surl.lu/jcrgxt
Огляд керування доступом на основі ролей в Azure Active Directory: https://surl.lu/vqryfx
Рекомендації щодо ролей Azure AD: https://surl.li/vtrtdj
Політики паролів та обмеження облікових записів у Azure Active Directory: https://surl.li/fobzcy
Керування обліковими записами екстреного доступу в Azure AD: https://surl.li/xingeb
Планування розгортання багатофакторної автентифікації Azure Active Directory: https://surli.cc/ztlgrr

Аудит Azure AD

Azure AD має журнали аудиту, які можуть надати огляд різних системних дій для забезпечення відповідності.

Ось найкращі практики для аудиту Azure AD:

- Використовуйте захист ідентифікаційних даних Azure AD для виявлення будь-яких потенційних вразливостей користувачів Azure AD та надсилання журналів аудиту до вашої системи SIEM.
- Використовуйте звіти Azure AD для виявлення ризикованих користувачів або ризикованих подій входу.

- Використовуйте журнали аудиту Azure AD для перегляду та виявлення подій у вашій службі Azure AD (таких як зміни користувачів або груп, події входу тощо).
- Надсилайте журнали активності Azure AD до служби Azure Monitor для подальшого аналізу.
- Обмежте рівень доступу до даних служби Azure Monitor мінімальною кількістю співробітників, щоб уникнути можливого видалення або зміни журналів аудиту.
- Якщо ви використовуєте службу Azure AD PIM у своєму Azure AD, створіть перевірки доступу, щоб виявити, хто використовував PIM для запиту високих прав на виконання дій.
- Для гібридних середовищ (тобто локальної служби Active Directory, підключеної до Azure AD) використовуйте Microsoft Defender for Identity для виявлення підозрілих дій у вашій локальній службі Active Directory.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Що таке захист особистих даних?: https://surl.lt/cioypu
Що таке Microsoft Defender для ідентифікації?: https://surl.lt/fexwzp
Що таке звіти Azure Active Directory?: https://surli.cc/eskhtl
Журнали аудиту в Azure Active Directory: https://surl.li/aeomas
Аналіз журналів активності Azure AD за допомогою журналів Azure Monitor: https://surli.cc/rbxzec
Створення перевірки доступу до ресурсів Azure та ролей Azure AD у PIM: https://surl.li/ukyfso

Захист Google Cloud IAM

Google Cloud IAM - це служба IAM, керована Google.
Перелік термінології Google Cloud IAM:

- *Елемент*. Це обліковий запис Google (наприклад, користувача), обліковий запис служби (для програм і віртуальних машин) або Cloud Identity з доступом до ресурсів GCP.
- *Користувач*. Це особа або програма (обліковий запис служби) з дозволами на доступ до ресурсів GCP. Користувач має облікові дані (такі як пароль та багатофакторна автентифікація).
- *Група*. Це група користувачів, яка спрощує керування дозволами.
- *Роль*. Це стосується набору дозволів на доступ до ресурсів.
- *Обліковий запис служби*. Це спеціальний тип користувача IAM, який дозволяє програмам отримувати доступ до ресурсів.
- *Політика IAM*. Це визначення на основі JSON, яке встановлює дозволи для доступу до ресурсів GCP.

Оцінка політики GCP передбачає наступне:

- Не встановлено політику організації. Застосовується стандартний доступ до ресурсів.

- Спадщина. Якщо вузол ресурсу встановив успадковувати Від Батьків = true, тоді успадковується ефективна політика батьківського ресурсу.

Заборонити успадкування Якщо вузол ієрархії ресурсів має політику, яка має успадковувати Від Батьків = хибність, вона не успадковує політику організації від батьківської.

Узгодження конфліктів політик за замовчуванням політики успадковуються та об'єднуються; однак, ЗАБОРОНИТИ цінності завжди мають пріоритет.

Ось найкращі практики для захисту Google Cloud IAM:

- Використовуйте Google Workspace для створення облікових записів користувачів та керування ними.
- Налаштуйте політику паролів (яка включає мінімальний і максимальний вік пароля, мінімальну довжину пароля та примусове використання історії паролів і складних паролів) у консолі адміністратора Google Workspace.
- Увімкніть багатофакторну автентифікацію (MFA) для будь-якого користувача з високими правами у вашій хмарі Google (наприклад, з роллю власника проекту GCP).
- Створюйте групи IAM, призначайте дозволи групам і додавайте користувачів до цих груп для легшого керування обліковими записами та дозволами.
- Використовуйте сервісні облікові записи, щоб надавати програмам мінімальний доступ до ресурсів Google Cloud.
- Створіть окремий обліковий запис служби для кожної програми.
- У сценаріях, коли вам потрібен лише короткий час для доступу програми до ресурсів, використовуйте короткочасні облікові дані облікового запису служби.
- Вимкніть невикористовувані облікові записи служб.
- Використовуйте облікові записи керованих служб Google для служб (таких як Google Compute Engine), яким потрібен доступ до ресурсів Google (наприклад, Google Cloud Storage).
- Використовуйте рекомендації ролей за допомогою IAM Recommender для забезпечення мінімальних дозволів на доступ до ресурсів Google.
- Обмежте використання ключів облікових записів служби або взагалі уникайте їх, щоб уникнути необхідності надавати доступ до ресурсів Google Cloud поза межею вашого середовища GCP.
- Використовуйте умови IAM, щоб забезпечити місцезнаходження, з якого користувач може отримувати доступ до ресурсів у вашому середовищі Google Cloud (наприклад, у вашій офісній мережі).
- Використовуйте симулятор політик, щоб визначити вплив політики на ваших користувачів.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Огляд Google Cloud IAM: https://surl.lu/slnwqs

Забезпечувати та контролювати вимоги до паролів для користувачів: https://surl.li/ydnjqx
Безпечне використання IAM: https://surl.lu/wefwsf
Отримайте мінімальні привілеї з меншими зусиллями за допомогою IAM Recommender: https://surl.li/yynqwg
Симулятор політики: https://surl.lt/axneig
Огляд умов IAM: https://surl.li/tyhozo

Аудит Google Cloud IAM

Google дозволяє вам контролювати Google Cloud IAM за допомогою Google Cloud Logging.

Ось найкращі практики для аудиту Google Cloud IAM:

- Увімкнути журнали аудиту Cloud IAM для подальшого аналізу журналів, наприклад, відстеження невдалих входів в Active Directory.
- Журнали аудиту активності адміністратора ввімкнено за замовчуванням і не можна вимкнути.
- Явно ввімкнути Журнали аудиту доступу до даних для реєстрації дій, виконаних у Google Cloud IAM.
- Обмежте рівень доступу до журналів аудиту мінімальною кількістю співробітників, щоб уникнути можливого видалення або зміни журналів аудиту за допомогою ролей IAM.
- Використовуйте Policy Analyzer, щоб визначити, яка особа (наприклад, користувач або обліковий запис служби) має доступ до якого ресурсу Google Cloud та тип доступу.
- Використовуйте аналітику облікових записів служб, щоб ідентифікувати невикористані облікові записи служб і ключі облікових записів служб.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Журнал аудиту IAM: https://surl.lu/jcyinf
Моніторинг моделей використання облікових записів та ключів служби: https://surl.li/uqwunh

Захист служб каталогів

Кожен постачальник хмарних послуг має власну реалізацію керованої служби Active Directory. Ця служба дозволяє централізовано керувати ідентифікаторами користувачів та комп’ютерів, приєднувати машини Windows до домену Active Directory, встановлювати політики паролів (такі як довжина пароля, складність пароля тощо) та контролювати доступ до традиційних ресурсів (таких як спільні файлові ресурси Windows, сервери SQL, сервери IIS тощо).

Важливо зазначити, що як клієнт, ви завжди маєте можливість розгортати контролери домену Active Directory на основі віртуальних машин та обслуговувати їх самостійно, як це роблять організації локально (це також відоме

як рішення з власним хостингом). Однак мета цієї посібника -показати вам, як все робиться за допомогою керованих служб, де ви, як клієнт, можете зосередитися на використанні служби IAM (тобто автентифікації та створення ідентифікаційних даних, а потім надавати їм дозволи) без необхідності обслуговування серверів (таких як доступність, керування виправленнями, резервне копіювання тощо).

У наступному розділі ми розглянемо найкращі практики для захисту керованих служб каталогів від AWS, Azure та GCP.

Захист служби каталогів AWS

Служба каталогів AWS -це служба Active Directory, керована Amazon.

Нижче наведено перелік найкращих практик:

- Налаштуйте політику паролів, яка включає мінімальний та максимальний вік пароля, мінімальну довжину пароля та забезпечує використання історії паролів і складних паролів.
- Налаштуйте політику блокування облікового запису, включно з кількістю невдалих спроб входу, тривалістю блокування облікового запису та тим, чи дозволяти скидання блокування облікового запису через певний проміжок часу.
- Щоб уникнути використання привілейованого облікового запису для скидання пароля, скористайтеся Адміністраторами делегованих детальних політик паролів AWS групу, щоб надати команді підтримки дозвіл на скидання паролів.
- Використовуйте MFA для облікових записів з високими привілеями для керування службою каталогів AWS за допомогою сервера RADIUS.
- Створюйте групи Active Directory, додавайте користувачів до груп і надавайте дозволи на доступ до ресурсів (таких як доступ до файлових серверів, серверів входу тощо) групам замість надання дозволів певним користувачам.
- Використовуйте групи безпеки VPC, щоб обмежити доступ з ваших екземплярів EC2 до контролерів домену AWS Directory Service.
- Використовуйте складний пароль для вбудованого облікового запису адміністратора вашої служби каталогів AWS.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Захистіть свій керований каталог Microsoft AD AWS: https://surl.li/dmjfst
Найкращі практики для керованого Microsoft AD від AWS: https://surli.cc/dkpkpe
Новий інформаційний документ *–Доменні служби Active Directory на AWS*: https://surl.li/odorsr

Найкращі практики моніторингу служби каталогів AWS

AWS дозволяє контролювати службу каталогів AWS за допомогою таких вбудованих служб:

- *Amazon CloudWatch*. Цей сервіс дозволяє вам контролювати журнали служби каталогів AWS.
- *AWS CloudTrail*. Цей сервіс дозволяє вам перевіряти дії API, виконані через консоль AWS Directory Service, SDK абоінтерфейс командного рядка(Інтерфейс командного рядка).

Ось найкращі практики:

- Увімкнути пересилання журналів служби каталогів AWS і пересилати журнали Active Directory до Amazon CloudWatch для подальшого аналізу журналів Active Directory, наприклад, відстеження невдалих входів до Active Directory.
- Використовуйте AWS CloudTrail для аудиту активності користувача в службі каталогів AWS за допомогою API.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Реєстрація викликів API служби каталогів AWS за допомогою CloudTrail: https://surl.li/ejswuw

Захист доменних служб Azure Active Directory (Azure AD DS)

Azure AD DS - це служба Active Directory, керована Azure.

Нижче наведено перелік найкращих практик:

- Налаштуйте політику паролів, яка включає мінімальний та максимальний вік пароля, мінімальну довжину пароля та забезпечує використання історії паролів і складних паролів.
- Налаштуйте політику блокування облікового запису, включно з кількістю невдалих спроб входу, тривалістю блокування облікового запису та тим, чи дозволяти скидання блокування облікового запису через певний проміжок часу.
- Вимкнути використання вразливих протоколів, таких як Менеджер локальної мережі Windows New Technology (NTLM).
- Вимкніть використання слабкого шифрування пароля за допомогою алгоритму RC4.
- Забезпечити використання транспортного шифрування TLS 1.2.
- Увімкнути використання можливості бронювання Kerberos для захисту трафіку, що протікає між клієнтом і контролерами домену.
- Якщо у вас є вимога дозволити уособлення від імені іншого користувача для доступу до ресурсів (наприклад, програма, якій потрібен доступ до файлового сервера), увімкніть використання обмежене делегування Kerberos (ККД).
- Використовуйте групи безпеки мережі Azure, щоб обмежити доступ з віртуальних машин до служби Azure AD DS.
- Використовуйте MFA для облікових записів з високими правами для керування службою Azure AD DS.

- Використовуйте складний пароль для вбудованого облікового запису глобального адміністратора вашої служби Azure AD.
- Якщо вам потрібно дозволити доступ до застарілих програм, розгорнутих локально, з Інтернету, використовуйте проксі-сервер програм Azure AD разом з Azure AD DS.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Посилення захисту керованого домену служб домену Azure Active Directory: https://surl.lu/qjovhi
Налаштування обмеженого делегування Kerberos (KCD) у службах доменів Azure Active Directory: https://surl.li/sgpbwo
Базовий рівень безпеки Azure для служб доменів Azure Active Directory: https://surl.li/nrypal
Розгорніть проксі-сервер застосунків Azure AD для безпечного доступу до внутрішніх застосунків у керованому домені служб домену Azure Active Directory.: https://surl.li/gmaupd

Рекомендації щодо моніторингу Azure AD DS

Azure дозволяє надсилати журнали аудиту Azure AD DS до таких місць призначення:

- Сховище Azure. Це лише для архівних цілей.
- Центри подій Azure. Це призначено для надсилання журналів аудиту до зовнішньої системи SIEM для подальшого аналізу.
- Робоча область аналітики журналів Azure. Це для подальшого аналізу з порталу Azure.

Ось найкращі практики:

- Увімкніть аудит Azure AD DS та виберіть, де зберігати журнали аудиту (наприклад, Azure Storage, Azure Event Hubs або робоча область Azure Log Analytics).
- Якщо ви вирішили надсилати журнали аудиту Azure AD DS до робочої області Azure Log Analytics, скористайтеся службою Azure Monitor для запиту журналів (наприклад, невдалих входів, блокувань облікових записів тощо).

Для отримання додаткової інформації зверніться до наступного ресурсу:
Увімкнення аудитів безпеки для служб доменів Azure Active Directory: https://surl.li/foiuot

Захист керованих послуг Google для Microsoft AD

Керована служба Google для Microsoft AD - це служба Active Directory, керована GCP.

Нижче наведено перелік найкращих практик:

- Розгорніть керований Google Microsoft AD у спільній віртуальній машині доступу (VPC), щоб забезпечити доступ до Active Directory з кількох проектів GCP.
- Налаштуйте політику паролів (яка включає мінімальний та максимальний вік пароля, мінімальну довжину пароля та забезпечує використання історії паролів і складних паролів).
- Налаштуйте політику блокування облікового запису (включно з кількістю невдалих спроб входу, тривалістю блокування облікового запису та тим, чи дозволяти скидання блокування облікового запису через певний проміжок часу).
- Щоб уникнути використання привілейованого облікового запису для скидання пароля, скористайтеся Адміністратор обчислювальних екземплярів роль, щоб дозволити вашій команді підтримки скидати паролі.
- Створюйте групи Active Directory, додавайте користувачів до груп і надавайте дозволи на доступ до ресурсів (таких як доступ до файлових серверів, серверів входу тощо) цим групам замість надання дозволів певним користувачам.
- Використовуйте правила брандмауера VPC, щоб обмежити доступ з екземплярів віртуальних машин до керованих контролерів домену Microsoft AD.
- Використовуйте авторизовані мережі, щоб контролювати, яким мережам VPC дозволено доступ до вашої керованої мережі Microsoft AD.
- Для масштабних середовищ з кількома проектами GCP використовуйте елементи керування службами VPC, щоб запровадити обмеження доступу до керованої мережі Microsoft AD на основі ідентифікації IP-адреси.
- Використовуйте складний пароль для вбудованого облікового запису адміністратора вашого керованого Microsoft AD.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Найкращі практики для запуску Active Directory у Google Cloud: https://surl.lt/snxxav
Керований сервіс для Microsoft AD: https://surl.li/mfterf
Керування авторизованими мережами: https://surli.cc/znttui
Доступ до керованого Microsoft AD з вашого VPC: https://surl.li/jnuzys

Найкращі практики моніторингу керованих послуг Google для Microsoft AD

Google дозволяє вам контролювати керований Google Microsoft AD за допомогою Google Cloud Logging.

Нижче наведено перелік найкращих практик:

- Увімкнути Керовані журнали аудиту Microsoft AD для подальшого аналізу журналів Active Directory, такого як відстеження невдалих входів до Active Directory.

- Журнали аудиту активності адміністратора ввімкнено за замовчуванням і не можна вимкнути.
- Явно увімкнути Журнали аудиту доступу до даних для реєстрації дій, виконаних у керованому Google Microsoft AD.
- Обмежте рівень доступу до журналів аудиту мінімальною кількістю співробітників, щоб уникнути можливого видалення або зміни журналів аудиту, використовуючи ролі IAM.

Налаштування багатофакторної автентифікації (MFA)

Кожен постачальник хмарних послуг має власний механізм для забезпечення використання багатофакторної автентифікації (MFA) для захисту спроб автентифікації від потенційних порушень облікових записів.

Нижче наведено перелік найкращих практик:

- Увімкніть багатофакторну автентифікацію (MFA) для користувача root облікового запису AWS.
- Увімкніть багатофакторну автентифікацію (MFA) для будь-якого користувача IAM з високими правами доступу до консолі AWS (наприклад, з роллю адміністратора).
- Увімкнути MFA для доступу до консолі AWS, щоб користувачі мали автентифікуватися за допомогою MFA перед програмним викликом запитів на доступ до API.
- Для середовищ, що не потребують конфіденційності, використовуйте віртуальний пристрій MFA (наприклад, Google Authenticator) для кращого захисту доступу користувачів IAM.
- Для чутливих середовищ використовуйте апаратний пристрій MFA або ключ безпеки U2F (наприклад, Юбікей).
- Уникайте використання SMS як частини MFA (через вразливості в протоколі SMS).

Для отримання додаткової інформації зверніться до наступних ресурсів:
Використання багатофакторної автентифікації (MFA) в AWS: https://surl.li/vdmzdj
Увімкнення віртуального пристрою (консолі) багатофакторної автентифікації (MFA): https://surl.li/azntcv
Увімкнення пристроїв MFA для користувачів в AWS: https://surl.li/nvylgd
Налаштування доступу до API, захищеного MFA: https://surl.li/ffoahg
Багатофакторна автентифікація: https://surl.li/fojdal

Рекомендації щодо налаштування багатофакторної автентифікації (MFA) за допомогою Azure Active Directory

Нижче наведено перелік найкращих практик:

- Увімкніть багатофакторну автентифікацію (MFA) для вихідного облікового запису глобального адміністратора.

- Увімкніть багатофакторну автентифікацію (MFA) для будь-якого користувача з високими привілеями (наприклад, з роллю глобального адміністратора).
- Увімкніть політику умовного доступу, щоб примусово використовувати багатофакторну автентифікацію (MFA) для будь-яких спроб підключення до порталу Azure за межами вашої корпоративної мережі.
- Для середовищ, що не потребують конфіденційної інформації, використовуйте програму Microsoft Authenticator для кращого захисту доступу користувачів Azure AD.
- Для чутливих середовищ використовуйте апаратний пристрій MFA, такий як ключ безпеки FIDO2 або Привіт Windows.
- Уникайте використання SMS як частини MFA (через вразливості в протоколі SMS).
- Налаштувати блокування облікового запису за кількох невдалих спроб входу за допомогою багатофакторної автентифікації (MFA).

Для отримання додаткової інформації зверніться до наступних ресурсів:
Як це працює: Багатофакторна автентифікація Azure AD: https://surl.li/envzcn
Посібник: Захист подій входу користувачів за допомогою багатофакторної автентифікації Azure AD: https://surl.li/remqvp
Планування розгортання багатофакторної автентифікації Azure Active Directory: https://surl.li/vbhciv
Які методи автентифікації та перевірки доступні в Azure Active Directory?: https://surli.cc/xzlbuz
Налаштування параметрів багатофакторної автентифікації Azure AD: https://surl.li/keovfq
Увімкнення багатофакторної автентифікації Azure AD для кожного користувача для захисту подій входу: https://surl.li/xkqxjr

Найкращі практики налаштування багатофакторної автентифікації (MFA) за допомогою Google Cloud:

- GCP безпосередньо не контролює налаштування MFA, оскільки не створює та не керує ідентифікаторами користувачів.
- Ідентифікатори в Google Cloud керуються обліковими записами Google Workspace або Gmail, де ви можете контролювати налаштування багатофакторної автентифікації (MFA), перш ніж надавати обліковий запис ідентифікаторів ресурсам GCP.

Нижче наведено перелік найкращих практик для налаштування багатофакторної автентифікації (MFA) за допомогою Google Cloud:

- Увімкніть багатофакторну автентифікацію (MFA) для будь-якого користувача з високими правами (наприклад, з роллю власника проекту GCP).

- Для середовищ, де не потрібна конфіденційність, використовуйте програму Google Authenticator для кращого захисту доступу ваших користувачів.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Забезпечити єдину багатосторонню професійну угоду (MFA) щодо ресурсів, що належать компанії: https://surl.lu/vraetv
Захистіть свій бізнес за допомогою двоетапної перевірки: https://surli.cc/vswazw
Захистіть свій обліковий запис за допомогою двоетапної перевірки: https://surl.li/eoawcs
Розгорніть двоетапну перевірку: https://surl.li/eqhnap

2.2. Моніторинг та аудит хмарних середовищ

AWS, Azure та Хмарна платформа Google (GCP) мають аналогічні можливості для контролю потоку трафіку та аудиту подій.

Усі служби та засоби контролю безпеки надсилають свої журнали аудиту до центральної служби аудиту для отримання сповіщень та подальшого аналізу (Рис.2.2.).

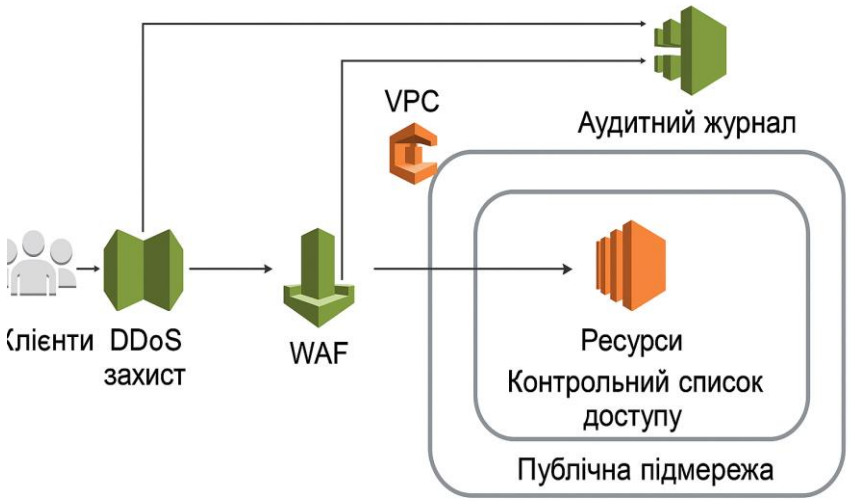

Рисунок 2.2 - Потік трафіку клієнтів

В цьому параграфі будуть розглянуті різні концепції моніторингу та аудиту з точки зору безпеки - від журналів аудиту та виявлення загроз до цифрової криміналістики в хмарних середовищах.

Зосередимось таких питання:

- Проведення моніторингу безпеки та ведення журналів аудиту
- Виявлення загроз та реагування на них
- Проведення реагування на інциденти та цифрової криміналістики

Технічні вимоги

Для цього розділу вам потрібно мати ґрунтовне розуміння журналів аудиту та моніторингу безпеки, виявлення загроз і цифрової криміналістики

Проведення моніторингу безпеки та ведення журналів аудиту

Моніторинг є важливою частиною безпеки в хмарі. Моніторинг у контексті хмарної безпеки полягає у реєстрації дій, що виконуються у ваших хмарних середовищах, таких як події входу користувачів (як успішні, так і невдалі), виконані дії (хто, що робив і коли, і яким був кінцевий результат - успіх чи невдача), документування всіх виконаних дій (також відоме як журнал аудиту), зберігання подій у центральному сховищі з обмеженим доступом до журналів (відповідно до *потрібно знати* концепція), генерування сповіщень відповідно до попередньо налаштованих правил та мати можливість вживати заходів.

В хмарних середовищах усі ресурси базуються на API, що дозволяє нам розгортати ресурси та вносити до них зміни. Ми контролюємо хмарні ресурси (як ми бачили в попередніх розділах) за допомогою засобів контролю безпеки (від груп безпеки через ВАФ. Усі хмарні ресурси можуть надсилати свої журнали аудиту до центральної служби ведення журналу для подальшого аналізу (іноді за замовчуванням, а іноді шляхом ручного ввімкнення ведення журналу аудиту).

Моніторинг безпеки та журнали аудиту за допомогою AWS CloudTrail

AWS CloudTrail– це служба журналу аудиту, керована Amazon. Вона дозволяє відстежувати всю активність користувачів на основі API AWS як з консолі керування AWS, так і через API для подальшого аналізу та кореляції (здебільшого події API, пов’язані з управлінням).

Amazon CloudWatch - це сервіс, керований Amazon, для збору подій, пов’язаних із кінцевими точками хмари (таких як EC2 та Служба реляційних баз даних(РДС).

Конфігурація AWS - це сервіс, який дозволяє відстежувати зміни конфігурації в різних сервісах AWS.

Журнали DNS дозволяють виявляти DNS-запити від вашого віртуальна приватна хмара(ВПК) до командування та управління (Командування та контроль) сервер.

Журнали потоку VPC дозволяють виявляти шкідливий трафік від вашого VPC до командного сервера

Найкращі практики використання AWS CloudTrail

Перелік найкращих практик, яких слід дотримуватися:

- Увімкнення AWS CloudTrail для всіх облікових записів AWS та всіх регіонів AWS.
- Увімкнення реєстрації подій даних (таких як активність на рівні об'єктів S3, виконання AWS Lambda та події на рівні об'єктів DynamoDB).

Важливе зауваження

Рекомендується провести аналіз ризиків цільової служби (наприклад, служби, яка зберігає або обробляє інформацію про кредитні картки, дані про охорону здоров'я тощо), перш ніж увімкнути ведення журналу подій даних, через

порівняння вартості зберігання подій та цінності, яку можна отримати з журналів подій даних.

Увімкнути аналітику CloudTrail для виявлення незвичайної активності, пов'язаної з подіями запису API.

Обмежте доступ до журналів CloudTrail мінімальною кількістю співробітників - бажано в обліковому записі управління AWS, поза межами ваших кінцевих користувачів, щоб уникнути можливого видалення або зміни журналів аудиту

Забезпечити використання Багатофакторна автентифікація(МЗС) для користувачів з доступом до консолі CloudTrail

Надсилати події до журналів CloudWatch для подальшого аналізу активності користувачів (наприклад, видалення файлів з корзини S3, зміни в групі безпеки або вимкнення Екземпляр EC2

Обмежте доступ до журналів CloudTrail, що зберігаються в S3, використовуючи політику корзини S3

Відповідно до галузевого регулювання, ви можете налаштувати зберігання журналів, використовуючи правила управління життєвим циклом об'єктів S3 - архівуйте необхідні журнали протягом потрібного періоду та видаляйте журнали, якщо вони більше не потрібні

Дотримуйтесь певних правил:

1. Увімкнути перевірку цілісності файлів журналів CloudTrail, щоб переконатися, що ваші журнали не були підроблені
2. Під час зберігання журналів CloudTrail у корзині S3, увімкнення функції видалення MFA для запобігання випадковому видаленню журналів CloudTrail
3. Створіть правило конфігурації AWS, яке гарантує надсилання журналів CloudTrail до журналів Amazon CloudWatch
4. Зашифруйте всі журнали CloudTrail, що зберігаються у виділеному корзині S3, за допомогою головного ключа клієнта CMK.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Найкращі практики безпеки в AWS CloudTrail: https://surl.lu/kqwjtw
Реєстрація подій даних для стежок: https://surl.lu/hcvbii
Події журналювання для доріжок: https://surl.lu/dvivfp
Надсилання подій до журналів CloudWatch: https://surli.cc/ramqrq
Як я можу переглядати та відстежувати історію активності облікового запису для певних користувачів IAM, ролей та ключів доступу AWS? https://surl.li/gwwxfh
Увімкнення перевірки цілісності файлів журналу для CloudTrail: https://surl.li/hqahkx
Видалення об'єкта з корзини з увімкненим видаленням MFA: https://surl.li/vrhmca
Увімкнено журнали спостереження за хмарним трасом https://surl.lt/liyjaj
Налаштування ключових політик AWS KMS для CloudTrail: https://surl.li/vpwxxh

Політика корзини Amazon S3 для CloudTrail:
https://surl.li/mavxry

Моніторинг безпеки за допомогою AWS Security Hub

AWS Security Hub - це керований сервіс, який дозволяє агрегувати події та конфігурації з кількох джерел (таких як *Amazon Guard Duty*, *Інспектор Amazon*, *Amazon Macie*, *Аналізатор доступу AWS IAM*, *Системний менеджер AWS*, та *Менеджер брандмауера AWS*) в одну консоль, що дозволяє вам пріоритезувати роботу з подіями безпеки, що надходять з різних джерел. Давайте обговоримо кожне з них:

Amazon Guard Duty. Сервіс, який постійно відстежує журнали CloudTrail, VPC Flow та DNS, а також використовує можливості машинного навчання для виявлення шкідливої діяльності у вашому середовищі AWS.

Інспектор Amazon. Служба оцінки вразливостей для екземплярів EC2 (наприклад, неправильна конфігурація та відсутні патчі)

Amazon Macie. Сервіс, який виявляє та захищає конфіденційну інформацію (наприклад, Особисто ідентифікована інформація (Особиста інформація) на контейнерах S3.

Аналізатор доступу AWS IAM. Сервіс для виявлення непотрібних дозволів IAM (таких як надмірні привілеї) на ресурсах, наданих зовнішніми суб'єктами

Системний менеджер AWS. Сервіс, що дозволяє виконувати автоматизовані завдання на екземплярах EC2 або RDS з центрального розташування (наприклад, вхід у систему та зміна налаштувань у фермі екземплярів EC2).

Менеджер брандмауера AWS. Сервіс для централізованого налаштування правил WAF у великих середовищах

Перелік найкращих практик, яких слід дотримуватися:

- Увімкніть AWS Security Hub для всіх облікових записів AWS та всіх регіонів AWS з одного головного облікового запису AWS у вашій організації AWS
- Надайте мінімальні права для консолі AWS Security Hub та застосуйте багатофакторну автентифікацію (MFA) для користувачів, які мають до неї доступ
- Увімкнути AWS Config для відстеження змін конфігурації та надсилання подій до Центру безпеки AWS

  🗐*Важливе зауваження.* AWS Config може функціонувати незалежно від AWS Security Hub, дозволяє відстежувати історію конфігурації ресурсів та надає як інвентаризацію вашого хмарного середовища в режимі реального часу, так і в історії.
- Увімкніть стандарти AWS Foundational Security Best Practices у Центрі безпеки AWS

  🗐 *Важливе зауваження.* Використовуючи найкращі практики безпеки AWS Foundational Security Best Practices, ви можете виявити служби у вашому середовищі, які відхиляються від найкращих практик безпеки, що відображаються у відомих тестах CIS, таких як використання облікового

запису root, невдача в налаштуванні MFA та невдача в шифруванні даних у стані спокою (наприклад, бази даних RDS та корзини S3).

- Використовуйте аналітику AWS Security Hub для перегляду висновків Security Hub та прийняття рішень щодо належних дій
- Дотримуйтесь інструкцій з виправлення в консолі AWS Security Hub, щоб виправити події безпеки, що виникли в консолі.

🗐 *Важливе зауваження.* Рекомендується вирішити, чи хочете ви використовувати консоль AWS Security Hub для виправлення подій безпеки, чи, у зрілому хмарному середовищі, надсилати події Security Hub до зовнішнього. Інформація про безпеку та управління подіями (CIEM) або система продажу квитків, якою займатиметься команда безпеки.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Контрольні елементи AWS Foundational Security Best Practices: https://surl.li/knbzul
Аналітика в AWS Security Hub: https://surl.lu/uydvin

Моніторинг безпеки та журнали аудиту за допомогою Azure Monitor

Azure дозволяє відстежувати та реєструвати журнали активності користувачів в Azure Monitor, керованій службі збору та моніторингу журналів.

Azure пропонує багаторівневу модель ліцензування:

- *Безкоштовний доступ до Azure AD*. Підтримка базових звітів про безпеку та використання
- *Azure AD Преміум P1*. Підтримка як базових звітів безпеки Azure Active Directory, так і розширених звітів про безпеку та використання.
- *Azure AD Преміум P2*. Підтримка попереднього типу звітів, а також можливість виявлення ризикованих рахунків і розслідування ризикових подій у системі SIEM (таких як Azure Guardian).

Перелік найкращих практик, яких слід дотримуватися:

- Увімкнути ведення журналу активності Azure, надсилаючи журнали активності до робочої області Log Analytics
- Увімкніть ведення журналу ресурсів Azure, створивши діагностичні параметри для кожного ресурсу Azure та надсилаючи журнали до робочої області Log Analytics
- Використовуйте приватне посилання Azure Monitor для захисту доступу з вашої віртуальної мережі до Azure Monitor, що дозволяє уникнути надсилання мережевого трафіку за межі вашої віртуальної мережі через захищений канал.
- Обмежте доступ до журналів монітора Azure мінімальною кількістю співробітників - бажано у виділеному обліковому записі сховища, поза межами доступу ваших кінцевих користувачів, щоб уникнути можливого видалення або зміни журналів аудиту

- Надсилання журналів активності Azure Monitor до Azure Sentinel для подальшого аналізу безпеки
- Для середовищ із високою чутливістю зберігайте дані Log Analytics в обліковому записі сховища, керованому клієнтом, та шифруйте журнали Azure Monitor за допомогою ключа шифрування, керованого клієнтом.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Журналування та аудит безпеки Azure: https://surl.lu/kwnwkk
Журнал активності Azure: https://surli.cc/avdhab
Журнали ресурсів Azure: https://surl.li/watdsv
Ролі, дозволи та безпека в Azure Monitor: https://surl.li/crxgym
Перегляд журналів активності для моніторингу дій з ресурсами: https://surl.lu/retazp
Підключення даних із журналу активності Azure: https://surl.lt/vymzhn
Ключ Azure Monitor, керований клієнтом: https://surl.li/owbdry
Використання облікових записів сховища, керованих клієнтом, в Azure Monitor Log Analytics: https://surl.li/qhmrzr
Використання приватного посилання Azure для підключення мереж до Azure Monitor: https://surl.lu/vhuuao
Azure Private Link запроваджує нові режими та суворо забезпечує ізоляцію мережі.: https://surl.li/cpclsb

Процес моніторингу безпеки та затвердження за допомогою Customer Lockbox

Коли йдеться про хмарні сервіси та модель спільної відповідальності, ми зрозуміли, що як клієнти Інфраструктура як послуга (Інфраструктура як послуга (IAA)), ми контролюємо все всередині віртуальної машини та, серед іншого, відповідаємо за моніторинг активності, що виконується вище рівня операційної системи.

Увімкнено Платформа як послуга (PaaS), ми відповідаємо за моніторинг діяльності, що виконується над рівнем платформи (наприклад, керованої бази даних), та на програмне забезпечення як послуга (SaaS), ми відповідаємо за моніторинг діяльності, що виконується на рівні керованих послуг (за умови, що постачальник SaaS підтримує це).

Що відбувається, коли співробітнику постачальника хмарних послуг потрібен доступ до нашого клієнта, наприклад, у сценарії, коли персонал служби підтримки хоче вирішити запит, який ми надіслали як клієнти, на відновлення об'єкта з поштової скриньки або видаленого файлу зі сховища об'єктів?

Де ми бачимо журнали аудиту такої події, і як ми можемо її взагалі схвалити?

Microsoft пропонує нам спосіб втрутитися в процес, увімкнувши ліцензію на функцію під назвою Скринька для клієнтів.

Скринька клієнта працює в такій послідовності:

- Ми надсилаємо запит до служби підтримки Microsoft і просимо допомоги, яка вимагає доступу до нашого клієнта.
- Заявку призначається інженеру служби підтримки, і оскільки він не має доступу до нашого клієнта, він пересилає заявку менеджеру служби підтримки.
- Після того, як менеджер служби підтримки схвалить запит, призначеній особі, яка затверджує запит, з нашої організації надсилається електронний лист із проханням надати інженеру служби підтримки доступ до нашого клієнта.
- Після схвалення процесу інженер служби підтримки отримує якраз достатньо часу та якраз достатньо доступу для виконання запитуваного завдання.
- Весь процес реєструється в журналах наших орендарів (наприклад, у нашому обмін онлайн-логами) і тимчасові дозволи видаляються.

Перелік найкращих практик, яких слід дотримуватися:

- Придбання ліцензії та активація Customer Lockbox
- Перегляд журналів аудиту, записаних для дій у системі Customer Lockbox
- Підключіть журнали активності Customer Lockbox до Azure Sentinel для цілей аудиту
- Увімкнути сповіщення про аномальну поведінку Customer Lockbox
- Обмежте доступ до журналів Customer Lockbox мінімальною кількістю співробітників - бажано у спеціальному обліковому записі сховища, поза межами доступу ваших кінцевих користувачів, щоб уникнути можливого видалення або зміни журналів аудиту
- Забезпечити використання багатофакторної автентифікації (MFA) для користувачів, які мають доступ до журналів Customer Lockbox
- Призначте співробітника з роллю «Затверджувач замків клієнта» замість використання ролі глобального адміністратора для процесу затвердження

Для отримання додаткової інформації зверніться до наступних ресурсів:
Скринька клієнта в Office 365: https://surl.li/glbmgx
Клієнтський блокувальник для Microsoft Azure: https://surl.li/oykpky
Базовий рівень безпеки Azure для Customer Lockbox для Microsoft Azure: https://surl.lu/pxkxqn
Посада спеціаліста з затвердження клієнтських скриньок тепер доступна: https://surli.cc/hemgao

Моніторинг безпеки та журнал аудиту за допомогою Google Cloud Logging

GCP дозволяє вам відстежувати та реєструвати журнали активності користувачів у Google Cloud Logging, керованій службі збору та моніторингу журналів.

Перелік найкращих практик, яких слід дотримуватися:

- Журнали аудиту активності адміністратора ввімкнено за замовчуванням і не можна вимкнути.
- Явне вмикання журнали аудиту доступу до даних реєструвати дії, виконані в сервісах Google.

  🗐 *Важливе зауваження.* Рекомендується провести аналіз ризиків цільової служби (наприклад, служби, яка зберігає або обробляє інформацію про кредитні картки чи дані про охорону здоров'я) перед увімкненням реєстрації подій даних через вартість зберігання подій порівняно з цінністю, яку можна отримати з журналів подій даних.
- Обмежити доступ до Журнали хмарного ведення журналу мінімальній кількості співробітників - бажано в окремому проекті GCP, поза межами ваших кінцевих користувачів, щоб уникнути можливого видалення або зміни журналів аудиту.
- Обмежте доступ до журналів аудиту мінімальною кількістю співробітників, щоб уникнути можливого видалення або зміни журналів аудиту, використовуючи ролі IAM (а Переглядач журналів для журналів активності адміністратора та Переглядач приватних журналів для журналів доступу до даних).
- Зашифрувати все Журнали хмарного ведення журналу використання CMEK.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Найкращі практики для журналів хмарного аудиту: https://surl.lu/dunvfx
Зберігання журналів вашої організації у сховищі журналів: https://surl.li/qcxjsc
Ролі IAM для функцій, пов'язаних з аудитом: https://surl.lu/ycwrfz

Моніторинг безпеки за допомогою Центру команд безпеки Google

Центр команд безпеки Google - це керований сервіс, який дозволяє агрегувати журнали та конфігурацію з кількох джерел (таких як сервіс Compute Engine контейнерів *додатків Google, Big Query, Хмарний SQL, Хмарне сховище, Хмарна IAM,* та сервіс Compute Engine контейнерів Google Kubernetes (ГКЕ) в єдину консоль, що дозволяє вам визначити пріоритети роботи з налаштування безпеки, відповідності вимогам та загроз.

Перелік найкращих практик, яких слід дотримуватися:
- Використовуйте ролі Cloud IAM, щоб надати мінімальний доступ до консолі Центру команд безпеки Google.
- Журнали аудиту активності адміністратора ввімкнено за замовчуванням і не можна вимкнути.
- Явно ввімкнути журнали аудиту доступу до даних для реєстрації дій, виконаних у Центрі керування безпекою Google.

🗐*Важливе зауваження.* Рекомендується провести аналіз ризиків цільової служби (наприклад, служби, яка зберігає або обробляє інформацію про кредитні картки чи дані про охорону здоров'я) перед увімкненням реєстрації

подій даних через вартість зберігання подій порівняно з цінністю, яку можна отримати з журналів подій даних.

- Використовуйте Центр команд безпеки Google для виявлення та виправлення неправильних конфігурацій у різних службах GCP (таких як правила брандмауера, загальнодоступні хмарні сховища, віртуальні машини з публічною IP-адресою або екземпляри без Захищений рівень сокетів (SSL-сертифікат).
- Підпишіться на Центр командування безпеки отримувати аномальну поведінку ззовні вашого середовища (наприклад, витік облікових даних або аномальну поведінку віртуальної машини).
- Для середовищ, побудованих на контейнерах, увімкнення преміум-рівня Центру команд безпеки Google та використання Виявлення загроз контейнерам сервіс для виявлення атак під час виконання на контейнери та надсилання журналів до Google Cloud Logging.
- Використовуйте Виявлення даних у хмарі DLP можливість перегляду результатів сканування Google Cloud DLP.
- Використання Сканер веб-безпекиу тестових середовищах перед переміщенням програми (наприклад, програми Google App Engine, GKE або Compute Engine) для виявлення вразливостей програми.
- Використовуйте Центр команд безпеки Google для виявлення вразливостей та невідповідностей відповідно до контрольних показників CIS.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Концептуальний огляд центру командування безпеки: https://surl.li/vvddlr
Концептуальний огляд виявлення загроз контейнерів: https://surl.li/gscejv
Огляд веб-сканера безпеки: https://surl.li/ynvrle
Виявлені вразливості: https://surl.li/xgrdza

Процес моніторингу та затвердження безпеки за допомогою засобів прозорості доступу та затвердження доступу

Прозорість доступу Google дозволяє переглядати спроби доступу до вашого проекту та ресурсів GCP співробітниками Google у Google Cloud Logging.

Перелік найкращих практик, яких слід дотримуватися:

- Увімкнути Прозорість доступу щоб розпочати реєстрацію дій, виконаних співробітниками Google у вашому клієнті
- Надайте Переглядач приватних журналів роль користувачеві, якому потрібен мінімальний доступ для перегляду журналів прозорості доступу
- Створіть Паб/Підрядник тема для Схвалення доступу
- Створіть сервісний обліковий запис для процесу затвердження доступу з роллю видавця Pub/Sub та зверніться до служби підтримки Google, надавши їм назву теми Pub/Sub, яку ви раніше створили, а також деталі проекту GCP та ідентифікатор організації GCP, для якої ви хочете отримувати сповіщення.

- Надайте Затвердження доступу роль для користувача, якому потрібен мінімальний доступ для схвалення запитів від інженерів служби підтримки Google
- Забезпечити використання багатофакторної автентифікації (MFA) для користувачів, які мають доступ до будь-якого з них Прозорість доступу або Консоль затвердження доступу/колоди

Для отримання додаткової інформації зверніться до наступних ресурсів:
Прозорість доступу: https://surl.li/elrxeh
Розуміння та використання журналів прозорості доступу: https://surl.lu/snqdqv
Швидкий старт затвердження доступу: https://surl.li/ygvhtp
Затвердження запитів на затвердження доступу: https://surl.lu/lmfuha

Виявлення загроз та реагування на них

Використання Amazon Detective для виявлення загроз Amazon Detective підключається до таких сервісів, як AWS CloudTrail та Amazon VPC Flow Logs, для виявлення подій входу, викликів API та мережевого трафіку. Потім він використовує машинне навчання для виявлення дій поза межами звичайної поведінки, щоб допомогти вам знайти першопричину підозрілої діяльності у вашому середовищі AWS.

Detective Amazon є хмарним еквівалентом сторонніх інструментів, таких як Splunk, який дозволяє запитувати велику кількість журналів та виявляти інциденти, пов'язані з безпекою.

Перелік найкращих практик, яких слід дотримуватися:
- Дозволити доступ до Detective Amazon висновки обмеженій кількості співробітників
- Забезпечити використання багатофакторної автентифікації (MFA) для співробітників, які мають доступ до консолі та журналів Amazon Detective
- Використовуйте Amazon Detective для аналізу активності ролей AWS IAM та надсилання результатів до Amazon Guard Duty
- Використовуйте AWS CloudTrail для реєстрації дій, виконаних на консолі Amazon Detective
- Використовуйте Amazon Detective як частину пошуку загроз реагування на інциденти для виявлення інцидентів, пов’язаних із безпекою, у вашому середовищі AWS

Для отримання додаткової інформації зверніться до наступних ресурсів:
Найкращі практики безпеки для Amazon Detective: https://surl.li/wehuim
Реєстрація викликів API Amazon Detective за допомогою AWS CloudTrail: https://surl.li/ogxxzh

Використання Amazon GuardDuty для виявлення загроз

Amazon Guard Duty-це сервіс моніторингу, який отримує дані з журналів VPC Flow, AWS CloudTrail, журналів подій даних CloudTrail S3 та журналів

DNS. Він використовує машинне навчання для перегляду журналів і сповіщає вас лише про події, які потребують подальшого розслідування, а іноді й дій (наприклад, заміни облікових даних привілейованого облікового запису або налаштування багатофакторної автентифікації, якщо облікові дані були скомпрометовані).

Amazon Guard Duty поєднує можливості машинного навчання з виявленням на основі сигнатур (наприклад, чорні списки дій API або виявлення активності ботів у вашому середовищі AWS). Приклади подій включають події ескалації привілеїв, викрадені облікові дані та вихідний трафік з вашого середовища на зовнішню шкідливу IP-адресу.

Amazon Guard Duty працює з одним обліковим записом AWS або з усією організацією AWS. Щоб уникнути сліпих зон у вашій організації AWS (наприклад, облікових записах AWS або регіонах, де не ввімкнено Guard Duty), рекомендується агрегувати всі журнали Guard Duty за допомогою подій CloudWatch у централізоване корзину S3.

Перелік найкращих практик, яких слід дотримуватися:

- Використовуйте ролі IAM для надання мінімального доступу до консолі GuardDuty
- Забезпечити використання багатофакторної автентифікації (MFA) для користувачів з доступом до консолі GuardDuty
- Увімкнути захист S3 на рівні всієї організації AWS та в корзинах S3, що містять конфіденційну інформацію (наприклад, дані кредитних карток, дані охорони здоров'я), щоб GuardDuty міг відстежувати та шукати шкідливу активність у корзині S3, наприклад, корзину, опубліковану
- Використовуйте події CloudWatch, щоб отримувати сповіщення про результати роботи GuardDuty

Як заходи з відновлення, ви можете обрати одну з наступних альтернатив:

A. Використовуйте CloudWatch для запуску функцій AWS Lambda як заходів щодо усунення недоліків GuardDuty.
B. Надсилання подій з Центру безпеки до AWS Systems Manager та виконання дій (таких як зміна налаштувань на віддалених екземплярах EC2)
C. Надсилати події з Центру безпеки до функцій AWS Lambda для виконання дій (таких як закриття відкритого порту в групі безпеки)

Використовуйте AWS CloudTrail для реєстрації дій, виконаних на консолі Amazon GuardDuty. Забезпечити інтеграцію між Amazon GuardDuty та AWS Security Hub для отримання централізованого огляду всіх інцидентів, пов’язаних із відповідністю вимогам та безпекою, у центральній консолі

Увімкнути інтеграцію між Amazon Detective та Amazon GuardDuty для отримання результатів з Amazon Detective у консоль Amazon GuardDuty

Для отримання додаткової інформації зверніться до наступних ресурсів:
Що таке Amazon GuardDuty?: https://surl.li/ptgycv

Захист Amazon S3 в Amazon GuardDuty: https://surl.li/gtiwkd
Створення власних відповідей на результати GuardDuty за допомогою Amazon CloudWatch Events: https://surl.li/tulcbs
Увімкнення та налаштування інтеграції з AWS Security Hub: https://surl.li/kzqqtj
Виправлення проблем безпеки, виявлених GuardDuty: https://surl.li/ihtwzf
Як використовувати Amazon GuardDuty для виявлення підозрілої активності у вашому обліковому записі AWS: https://surl.li/gwpaml

Моніторинг безпеки за допомогою Microsoft Defender для хмари

Захисник Microsoft для хмари - це централізований сервіс виявлення загроз та захисту від них.

Перелік найкращих практик, яких слід дотримуватися:

- Використовуйте Azure Контроль доступу на основі ролей(RBAC) щоб надати користувачам мінімальні дозволи для використання консолі Microsoft Defender for Cloud
- Використовуйте багатофакторну автентифікацію (MFA) для користувачів із дозволами на доступ до консолі Microsoft Defender for Cloud
- Використовуйте рекомендації Microsoft Defender for Cloud у консолі Центру безпеки, щоб дізнатися, які дії слід виконати для вирішення проблем відповідності у вашому середовищі Azure та їх усунення
- Зменште поверхню атаки у ваших програмах за допомогою адаптивних елементів керування програмами Microsoft Defender for Cloud (таких як виявлення шкідливого програмного забезпечення, непідтримуваних програм і програм, що містять конфіденційні дані)
- Налаштуйте адресу електронної пошти, щоб отримувати сповіщення від Центр реагування на безпеку Microsoft(MSRC (Міністерство кредитної історії США)) коли Microsoft Defender для хмари виявило, що ресурси скомпрометовані
- Автоматично розгортати агент моніторингу на всіх віртуальних машинах, щоб забезпечити моніторинг Microsoft Defender для хмари
- Використовуйте Microsoft Defender for Cloud для перевірки всіх ресурсів у вашому середовищі Azure
- Використовуйте Microsoft Defender for Cloud для моніторингу відповідності вимогам CIS Benchmarks
- Використовуйте Microsoft Defender for Cloud для моніторингу відповідності, наприклад, захисту від DDoS-атак на рівні віртуальної мережі, повного шифрування диска, захисту кінцевих точок і керування виправленнями на віртуальних машинах, конфігурації SQL, як-от аудиту та шифрування в стані спокою, шифрування сховища Azure в стані спокою тощо.
- Використовуйте функцію Microsoft Defender for Cloud під назвою Моніторинг цілісності файлів для виявлення змін у файлах у

конфіденційних середовищах, які не можна підроблювати (наприклад, Стандарт безпеки даних індустрії платіжних карток (PCI DSS) середовища).

Для отримання додаткової інформації зверніться до наступних ресурсів:
Дозволи в Microsoft Defender для хмари: https://surl.li/oqcnfz
Перегляньте свої рекомендації щодо безпеки: https://surl.lu/icituo
Рекомендації щодо виправлення помилок у Microsoft Defender для хмари: https://surl.li/pspxkv
Автоматизація відповідей на тригери Центру безпеки: https://surl.li/hscten
Використовуйте адаптивні засоби керування програмами, щоб зменшити кількість атак на ваші машини: https://surl.lu/blgwwg
Налаштування сповіщень електронною поштою для сповіщень безпеки: https://surl.lu/mexkjc
Налаштування автоматичного забезпечення для агентів і розширень з Microsoft Defender for Cloud: https://surli.cc/qwvjya
Досліджуйте та керуйте своїми ресурсами за допомогою інвентаризації активів: https://surl.lt/ngwcza
Моніторинг цілісності файлів у Microsoft Defender для хмари: https://surl.lt/jibbav

Використання Azure Sentinel для виявлення загроз

Azure Sentinel -це хмарна служба SIEM, побудована на робочих просторах Azure Log Analytics. Він використовує штучний інтелект (ШІ) для виявлення загроз у вашому середовищі Azure та допомоги у реагуванні на виявлені загрози.

Перелік найкращих практик, яких слід дотримуватися:

- Використовуйте Azure RBAC, щоб надати користувачам мінімальні дозволи для використання Azure Sentinel та розслідування інцидентів у консолі.
- Використовуйте багатофакторну автентифікацію (MFA) для користувачів із дозволами на доступ до консолі Azure Sentinel.
- Використовуйте Azure Monitor для надсилання журналів аудиту Azure Sentinel до робочої області Azure Log Analytics для подальшого аналізу.
- Створіть робочу область Log Analytics для Azure Sentinel і Microsoft Defender for Cloud.
- Використовуйте консоль Azure Sentinel для перегляду інцидентів та їх розслідування, а також граф розслідування для глибшого аналізу інциденту та ресурсів, які були частиною самого інциденту.
- Використовуйте репозиторій Azure Sentinel із попередньо налаштованими плейбуками для автоматичного усунення інциденту (наприклад, блокування IP-адреси, блокування користувача Azure AD або ізоляції віртуальної машини).
- Надсилати журнали Microsoft 365 Defender до Azure Sentinel для подальшого аналізу.
- Інтегруйте продукти сторонніх платформ розвідки загроз у Azure Sentinel для збагачення даних.

- Увімкнути Azure Sentinel. Аналіз поведінки користувачів та сутностей(УЄБА) для виявлення аномальної поведінки користувачів, хостів, IP-адрес і програм у вашому середовищі Azure.
- Для чутливих середовищ додайте додатковий рівень захисту, зашифрувавши дані Azure Sentinel за допомогою CMEK.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Рекомендації щодо використання Microsoft Sentinel: https://surl.li/obnrdj
Базовий рівень безпеки Azure для Azure Sentinel: https://surl.lu/jdwyqp
Дозволи в Azure Sentinel: https://surl.li/xixwfd
Навчальний посібник: Розслідування інцидентів за допомогою Azure Sentinel: https://surli.cc/qnubbn
Посібник: Використання плейбуків із правилами автоматизації в Azure Sentinel: https://surli.cc/httkcp
Інтеграція Microsoft 365 Defender з Azure Sentinel: https://surl.li/hjeiks
Підготовчі дії та передумови для розгортання Azure Sentinel: https://surl.li/ukkazn
Розуміння аналітики загроз у Azure Sentinel: https://surli.cc/vnqlaw
Виявлення складних загроз за допомогою аналітики поведінки користувачів та сутностей (UEBA) в Azure Sentinel: https://surli.cc/pwofsc
Налаштування ключа Azure Sentinel, керованого клієнтом: https://surl.li/ydjswj
Аудит запитів та дій Azure Sentinel: https://surl.lu/xclvdc

Використання Azure Defender для виявлення загроз

Захисник Azure - це служба захисту від загроз для різних типів ресурсів Azure, таких як віртуальні машини, бази даних SQL, контейнери та служби додатків Azure.

Перелік найкращих практик, яких слід дотримуватися:
- Оскільки Azure Defender інтегровано в Microsoft Defender for Cloud, використовуйте Azure RBAC, щоб надати користувачам мінімальні дозволи для використання консолі Microsoft Defender for Cloud.
- Оскільки Azure Defender інтегровано в Microsoft Defender for Cloud, використовуйте MFA для користувачів із дозволами на доступ до консолі Microsoft Defender for Cloud.
- Увімкніть Azure Defender для захисту ваших служб (відповідно до підтримуваних служб Azure Defender)
- Увімкніть Azure Defender на рівні передплати для всіх передплат у вашому середовищі Azure
- Використовуйте вбудований сканер вразливостей Azure Defender для виявлення вразливостей на ваших віртуальних машинах

Для отримання додаткової інформації зверніться до наступних ресурсів:
Вступ до Захисника Azure: https://surl.lt/ixqvtu

Вступ до Azure Defender для серверів: https://surl.li/faftjn
Панель інструментів Azure Defender: https://surl.lu/pipedv

Використання Центру команд безпеки Google для виявлення та запобігання загрозам

Центр команд безпеки Google - це служба виявлення загроз для віртуальних машин і контейнерів. Цей сервіс може сканувати веб-сервери на наявність вразливостей та витоків даних, а також запобігати їм.

Перелік найкращих практик, яких слід дотримуватися:

- Використовуйте найновіші підтримувані версії сервіс Compute Engine контейнерів Google Kubernetes (ГКЕ) версія.
- Увімкнути виявлення загроз контейнерам.
- Увімкнути виявлення загроз віртуальної машини.
- Використовуйте ролі Cloud IAM, щоб надати мінімальний доступ до консолі Центру команд безпеки Google.
- Увімкнути журнали аудиту діяльності адміністратора за замовчуванням.
- Явно ввімкнути журнали аудиту доступу до даних для реєстрації дій, виконаних у Центрі керування безпекою Google.

  🗐 *Важливе зауваження.* Рекомендується провести аналіз ризиків цільової служби (наприклад, служби, яка зберігає або обробляє інформацію про кредитні картки, дані про охорону здоров'я тощо), перш ніж увімкнути ведення журналу подій даних, через порівняння вартості зберігання подій та цінності, яку можна отримати з журналів подій даних.
- Використовуйте хмарне ведення журналу для перегляду результатів роботи Центру команд безпеки Google

Для отримання додаткової інформації зверніться до наступних ресурсів:
Використання виявлення загроз контейнерам: https://surl.lu/nbqkpn
Використання виявлення загроз віртуальної машини: https://surl.li/xscotc
Виправлення недоліків сканера веб-безпеки: https://surl.li/abscem

Проведення реагування на інциденти та цифрової криміналістики

Реагування на інциденти та судова експертиза є складними у хмарних середовищах з кількох причин:

- Усе наше середовище зберігається у фізичному місці, яким керує зовнішній постачальник послуг.
- Усе наше середовище розділене між локальною платформою та хмарним провайдером (також відомим як гібридне хмарне середовище).
- Усе наше середовище розділене між кількома хмарними постачальниками (також відоме як мультихмарне середовище).

Наше хмарне середовище розташоване в кількох регіонах або кількох хмарних облікових записах (наприклад, в обліковому записі AWS, підписках

Azure та проектах GCP), і нам може бракувати видимості всіх ресурсів, розгорнутих у нашому хмарному середовищі, або інформації про те, хто володіє або керує цими обліковими записами.

Згідно з моделлю спільної відповідальності, ми можемо не бачити дії, виконані нашим постачальником хмарних послуг (наприклад, внесення змін до керованої бази даних хмарним інженером або виконання резервного копіювання чи відновлення із SaaS-застосунку).

Наше хмарне середовище може містити хмарні сервіси, про які не знає наш центральний відділ IT або відділ безпеки, або якими керують IT-персонал бізнес-підрозділів чи стороння компанія, про яку нам не відомо.

Віртуальні сервери (і контейнери) можуть існувати протягом коротких періодів часу, перш ніж бути виведеними з експлуатації та стертими.

Національний інститут стандартів і технологій(HICT) визначає такі етапи реагування на інциденти:

- Підготовка. Підготувати актуальну інформацію про контактну особу (яка бере участь у процесі реагування на інциденти), підготувати систему для документування дій з реагування на інциденти, підготувати робоче місце для цілей криміналістики тощо.
- Виявлення та аналіз. Збирати журнали аудиту та журнали керування змінами для виявлення аномалій (таких як кілька невдалих входів або змін у файлах конфігурації, а також аналізувати зібрану інформацію від журналів IDS/IPS до подій пошкодження веб-сайтів тощо).
- Стримування, ліквідація та відновлення. Визначити хост атаки, виконати дії з видалення (наприклад, видалення шкідливого програмного забезпечення із зараженого хоста) та повернути системи до нормальної роботи (повернути чисті хости до робочого режиму).

Для отримання додаткової інформації зверніться до наступного ресурсу: *NIST - Керівництво з обробки інцидентів комп'ютерної безпеки*: https://surl.lt/nbgdic

Реагування на інциденти в AWS

AWS пропонує кілька послуг, які допомагають пройти життєвий цикл реагування на інциденти:

Підготовчий етап:

- Використовуйте NACL та групи безпеки, щоб встановити належні правила доступу до мережі для доступу до вашого середовища AWS.
- Використовуйте AWS Shield для захисту свого середовища від DDoS-атак.
- Використовуйте AWS WAF для захисту вашого середовища від атак на рівні додатків.
- Використовуйте AWS Config для моніторингу змін конфігурації.

- Використовуйте Amazon Inspector для виявлення проблем відповідності, таких як вразливості, що виникають на віртуальних серверах без захисту або системах без виправлень.

Фаза виявлення:

- Використовуйте AWS CloudTrail для реєстрації дій, виконаних через API, для подальшого аналізу.
- Використовуйте журнали Amazon CloudWatch для надсилання сповіщень про поведінку поза звичайною схемою (наприклад, сплеск невдалих входів).
- Використовуйте Amazon GuardDuty для виявлення підозрілої активності в журналах AWS CloudTrail, VPC Flow або DNS.
- Використовуйте журнали потоку VPC для моніторингу мережевої активності.

🗐 *Важливе зауваження:* Для виробничих середовищ увімкніть журнали потоку VPC лише для цілей усунення несправностей. Використовуйте Amazon Macie для виявлення будь-яких витоків конфіденційної інформації (наприклад, даних кредитних карток), що зберігається в корзинах S3

Фаза реагування під час проведення реагування на інциденти та цифрової криміналістики :

- Використовуйте правила AWS Config для автоматичного повернення налаштувань конфігурації до потрібного стану.
- Використовуйте події Amazon CloudWatch для запуску функцій AWS Lambda як запобіжників для автоматичного реагування на події (такі як блокування правила групи безпеки або вимкнення екземпляра EC2).
- Використовуйте AWS Systems Manager для виконання команд на кількох віддалених екземплярах EC2.

Фаза відновлення:

- Використовуйте AWS Backup для відновлення екземпляра EC2 зі старішої резервної копії.
- Використовуйте Магазин еластичних блоків (ЕБС) знімки для відновлення томів EBS.
- Використовуйте шаблони Cloud Formation для перебудови всього середовища AWS з нуля.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Як розпочати роботу з автоматизацією реагування на безпеку в AWS: https://surli.cc/ltaeag
Посібник з реагування на інциденти безпеки AWS: https://surl.li/tjzorn
Як виконати автоматизоване реагування на інциденти в середовищі з кількома обліковими записами: https://surl.lu/urijvj
Реагування на інциденти AWS: https://surl.li/xwnblg *Зразки посібника з реагування на інциденти AWS*: https://surli.cc/szqkbn

Автоматизація безпеки AWS: https://surli.cc/qtnksa

Реагування на інциденти в Azure

Azure пропонує кілька послуг, які допомагають пройти життєвий цикл реагування на інциденти:

Підготовчий етап:

- Використовуйте групи мережевої безпеки, щоб встановити відповідні правила мережевого доступу для доступу до вашого середовища Azure
- Використовуйте захист Azure DDoS для захисту вашого середовища від DDoS-атак.
- Використовуйте Azure WAF (або Azure Application Gateway) для захисту вашого середовища від атак на рівні додатків.
- Використовуйте Azure Monitor та Azure Log Analytics для моніторингу змін конфігурації.

Фаза виявлення:

- Використовуйте Azure Monitor та Azure Log Analytics для реєстрації дій, виконаних через API, для подальшого аналізу.
- Використовуйте Microsoft Defender for Cloud для виявлення проблем відповідності, таких як вразливості, що виникають на віртуальних серверах без захисту або системах без виправлень.
- Використовуйте Azure Sentinel для виявлення атак і реагування на інциденти, отримані з інших служб Azure (таких як Azure Log Analytics або Azure Defender).
- Використовуйте Azure Network Watcher для моніторингу мережевої активності.

  🗐 *Важливе зауваження:* Для виробничих середовищ увімкніть Azure Network Watcher лише для цілей усунення несправностей.
- Використовуйте службу захисту інформації Azure для класифікації даних та виявлення витоку конфіденційної інформації (наприклад, інформації про кредитні картки)

Фаза реагування:

- Використовуйте службу автоматизації Azure для запуску скриптів для автоматичного реагування на події (наприклад, правило групи безпеки блокування або вимкнення віртуального сервера).

Фаза відновлення:

- Використовуйте Azure Backup для відновлення віртуальної машини Azure зі старішої резервної копії.
- Використовуйте знімки дисків Azure для відновлення диска віртуальної машини Azure.

- Використовуйте Azure Resource Manager для відновлення всього середовища Azure з нуля.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Огляд управління інцидентами: https://surl.li/iqomgc
Ланцюг відповідальності комп'ютерної криміналістики в Azure: https://surl.li/oqzdhh

Реагування на інциденти в Google Cloud Platform

GCP пропонує кілька послуг, які допоможуть вам пройти життєвий цикл реагування на інциденти.

Підготовчий етап:

- Використовуйте правила брандмауера, щоб встановити відповідні правила доступу до мережі для доступу до вашого середовища GCP.
- Використовуйте Google CloudArmor для захисту свого середовища від DDoS-атак та атак на рівні додатків.

Фаза виявлення:

- Використовуйте Google Cloud Logging для реєстрування дій, виконаних через API, для подальшого аналізу.
- Використовуйте Центр команд безпеки Google для виявлення проблем відповідності, таких як вразливості, що виникають на віртуальних серверах без захисту або системах без виправлень.
- Використовуйте журнали потоку Google VPC для моніторингу мережевої активності

  🗐 *Важливе зауваження:* Для робочих середовищ увімкніть журнали потоку Google VPC лише для цілей усунення несправностей.
- Використовуйте Google Cloud DLP для класифікації даних та виявлення будь-яких витоків конфіденційної інформації (наприклад, інформації про кредитні картки).

Для отримання додаткової інформації зверніться до наступних ресурсів:
Процес реагування на інциденти з даними: https://surl.li/huivwa
Інциденти для сповіщень на основі показників: https://surl.li/fcwwff

2.3. Застосування шифрування у хмарних сервісах

Оскільки шифрування є поширеною найкращою практикою безпеки, яка використовується для забезпечення конфіденційності даних, і оскільки багато хмарних сервісів вже мають вбудовану підтримку шифрування (на відміну від локальних середовищ, які вимагають значних зусиль для підтримки ключів шифрування), вкрай важливо розуміти, як працює шифрування та як воно реалізовано в різних хмарних сервісах.

Неможливість шифрування конфіденційних даних таких як інформація про кредитні картки, дані про здоров'я тощо. Особисто ідентифікована інформація (Особиста інформація) та інше наражає нас на ризик розкриття даних, а також потенційних позовів з боку клієнтів та регуляторних органів.

В цьому параграфі ми розглянемо такі теми:

- Вступ до шифрування
- Найкращі практики розгортання KMS
- Найкращі практики розгортання служб управління секретами
- Найкращі практики використання шифрування під час передачі
- Найкращі практики використання шифрування в стані спокою
- Використовується шифрування

Технічні вимоги

Для цього підрозділу розділу вам потрібно мати ґрунтовне розуміння криптографічних концепцій, таких як симетричні алгоритми, асиметричні алгоритми, шифрування під час передачі та шифрування в стані спокою.

Вступ до шифрування

Шифрування - це процес перетворення звичайного тексту на зашифрований. Найпростіший спосіб пояснити, чому нам потрібне шифрування, -це уявити собі сценарій, коли ми хочемо передати файл, що містить конфіденційну інформацію (наприклад, медичні записи пацієнтів), між двома комп’ютерами через ненадійну мережу, таку як загальнодоступний Інтернет, не розкриваючи його ненадійною третьою стороною.

Іншим прикладом є веб-сайт роздрібної торгівлі, який обробляє інформацію про кредитні картки своїх клієнтів, коли вони купують товари на веб-сайті.

Щоб слідувати Стандарту безпеки даних індустрії платіжних карток (PCI DSS), стандарт зберігання та обробки інформації про кредитні картки, роздрібна компанія повинна шифрувати всю інформацію про кредитні картки під час передачі та зберігання.

Розглянемо як приклад поширену трирівневу архітектуру - з фронтальними веб-серверами (за балансувальником навантаження для високої доступності), сервером додатків (для обробки бізнес-логіки) та серверною базою даних (для зберігання інформації про покупки).

Щоб захистити інформацію про кредитну картку, нам потрібно зробити наступне:

- Налаштуйте SSL-сертифікат на балансувальнику навантаження (для шифрування під час передачі).
- Налаштуйте SSL-сертифікат на веб-серверах (для шифрування під час передачі).
- Налаштуйте SSL-сертифікат між веб-серверами та сервером застосунків (для шифрування під час передачі).

Якщо сервер застосунків зберігає інформацію про кредитну картку (навіть протягом короткого періоду) на своєму локальному жорсткому диску, нам потрібно налаштувати повне шифрування диска (для шифрування в стані спокою). Налаштуйте повне шифрування бази даних на внутрішній базі даних (для шифрування в стані спокою). Щоб переконатися, що всі ключі шифрування зберігаються безпечно, нам потрібно зберігати їх у захищеному місці.

Нам потрібно зрозуміти наступну термінологію:

- *Відкритий текст*. Оригінальна форма інформації, яку може прочитати людина.
- *Зашифрований текст*. Результат шифрування, що виконується на відкритому тексті - формі інформації, непридатній для читання людиною.
- *Шифрування*. Процес перетворення відкритого тексту в зашифрований.
- *Розшифрування*. Процес перетворення зашифрованого тексту назад у його початкову форму відкритого тексту.
- *Ключ шифрування Рядок*. Рядок, який разом з алгоритмом шифрування може кодувати або декодувати зашифрований текст.
- *Алгоритм шифрування*. Математичний алгоритм, що використовується в криптографії, який разом із ключем шифрування дозволяє нам шифрувати або розшифровувати повідомлення.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Криптографічний алгоритм: https://surl.lu/zmmllc
Огляд криптографії: https://surl.li/mwdovf

Симетричне шифрування

Симетричне шифрування -це спосіб передачі даних між двома сторонами з використанням одного й того ж ключа шифрування як для шифрування, так і для дешифрування.

Симетричне шифрування зазвичай використовується для таких цілей:

- Шифрування даних у стані спокою таких як особиста інформація, інформація про кредитні картки та медична інформація.
- Перевірка того, що відправник повідомлення є тим, за кого себе видає.
- Генерація випадкових чисел як частина криптографічного процесу.

На наступній діаграмі (Рис.2.3.) показано процес перетворення відкритого тексту в шифрований і навпаки за допомогою симетричного шифрування:

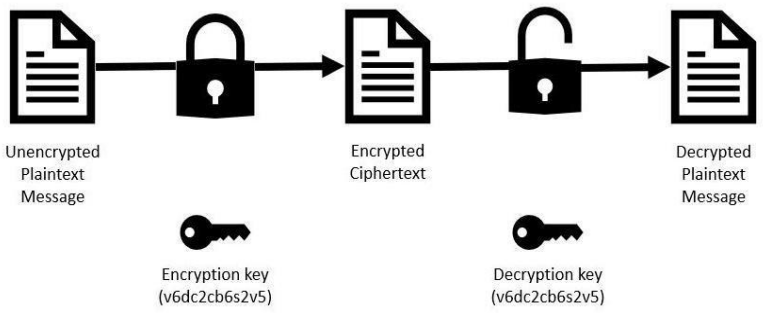

Рисунок 2.3 - Симетричне шифрування

Нижче наведено переваги симетричного шифрування:

- Малий розмір зашифрованого тексту.
- Підходить для передачі великих обсягів даних.
- Низький рівень ресурсів процесора.
- Малий розмір ключа шифрування.
- Швидкий час шифрування порівняно з асиметричним шифруванням.

Нижче наведено недоліки симетричного шифрування:

- Вважається менш безпечним, ніж асиметричне шифрування, оскільки обидві сторони використовують один і той самий ключ шифрування
- Вважається менш конфіденційним, ніж асиметричне шифрування, оскільки обидві сторони використовують один і той самий ключ шифрування

Розширений стандарт шифрування (AES)

AES вважається фактичним стандартом, який сьогодні використовується як у локальних сховищах, так і в публічній хмарі для шифрування в стані спокою. Він був розроблений NIST у 2001 році та постачається зі змінними розмірами ключів - найпоширеніший розмір ключа - 256 біт.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Алгоритм із симетричним ключем: https://surl.li/gshnmd
Розширений стандарт шифрування: https://surl.li/kiyvfg

Асиметричне шифрування

Асиметричне шифрування - це спосіб передачі даних між двома сторонами. Однак, на відміну від симетричного шифрування, в асиметричному шифруванні (також відомому як криптографія з відкритим ключем або шифрування з відкритим ключем), ми використовуємо два різні ключі (приватний та публічний), які пов'язані між собою математично.

В асиметричному шифруванні відкритий ключ може бути переданий будь-кому та використовується для шифрування повідомлення. Закритий ключ має бути надійно захищений та використовується для двох цілей - розшифрування повідомлення та підписання повідомлення для забезпечення його цілісності (повідомлення не було підроблено в процесі).

Асиметричне шифрування зазвичай використовується для таких цілей:

- Створення цифрових підписів
- Розподіл ключів сесій для таких випадків використання, як протокол TLS

На наступній діаграмі (Рис.2.4) показано процес перетворення відкритого тексту в шифрований і навпаки за допомогою асиметричного шифрування:

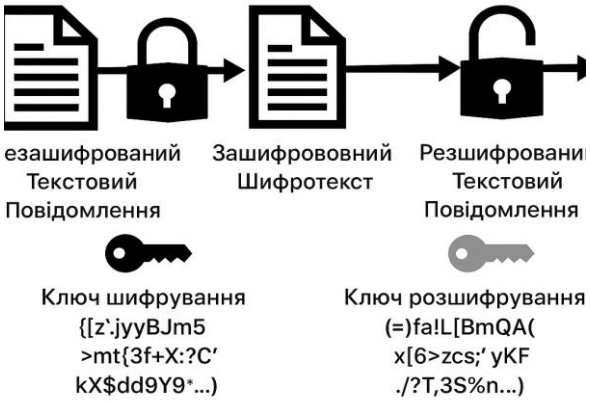

Рисунок 2.4 - Асиметричне шифрування (шифрування з відкритим ключем)

Нижче наведено переваги асиметричного шифрування:

- Великий розмір шифротексту (порівняно із симетричним шифруванням)
- Великий розмір ключа шифрування (наприклад, RSA 2048 біт або вище)
- Вважається набагато безпечнішим за симетричне шифрування, оскільки в процесі використовуються два ключі, і ви не можете розкрити закритий ключ з відкритого ключа
- Вважається більш конфіденційним, ніж симетричне шифрування, оскільки існує два ключі, а для розшифрування повідомлення потрібен закритий ключ (як мається на увазі, він має зберігатися в таємниці).

Нижче наведено недоліки симетричного шифрування:

- Підходить для передачі невеликих обсягів даних
- Високі ресурси процесора
- Повільний час шифрування (порівняно із симетричним шифруванням)

RSA (Rivest-Shamir-Adleman)

RSA - один із найпоширеніших протоколів для шифрування під час передачі, встановлення ключів та цифрових підписів. Безпека RSA базується на розкладанні на множники двох великих простих чисел також відомих як проблема факторингу. Рекомендований розмір ключа починається від 2048 біт або вище.

Криптографія еліптичних кривих (ECC)

ECC здебільшого використовується для ключових угод, цифрових підписів та генераторів псевдовипадкових чисел. Він має малий розмір ключа порівняно з алгоритмом RSA та базується на алгебраїчній структурі еліптичних кривих над скінченними полями. Рекомендовані розміри ключів для ECC становлять 256 бітів для класифікації секретних повідомлень NSA та 384 біти для класифікації надсекретних повідомлень NSA.

Для отримання додаткової інформації зверніться до наступних ресурсів:

Криптографія з відкритим ключем: https://surl.li/grrkmv
RSA (криптосистема): https://surl.li/wvvnhb
Криптографія еліптичних кривих: https://surl.lu/pngxfo

Найкращі практики розгортання KMS

Усі основні постачальники публічних хмарних послуг мають реалізації керованої KMS - захищеного місця (або сховища) для створення, зберігання та отримання ключів шифрування.

Нижче наведено деякі важливі концепції в галузі управління ключами:

- *Ключ шифрування ключа (KEK).* Це використовується для генерації інших ключів шифрування. Ключ шифрування (KEK) зберігається всередині KMS і ніколи не залишає його, оскільки він огортає (шифрує) інші ключі в ієрархії нижче.
- *Ключ шифрування даних (ДЕК).* Це використовується для шифрування самих даних. DEK зберігається поруч із самими даними. KMS зберігають історію DEK та зберігають цю інформацію в метаданих поруч із самими даними, що дозволяє зашифрованій службі знати, яку версію DEK використовувати.
- *Головний ключ шифрування(МЕК).* Це використовується для шифрування та дешифрування DEK під час передачі.
- *Генерація ключів.* Ідея повторного створення нових ключів шифрування, щоб уникнути можливості розкриття ключа третьою стороною через тривале використання статичного ключа шифрування (ключа, який не замінювався дуже давно).

Служба керування ключами AWS (KMS)

AWS KMS - це сервіс керування ключами від Amazon. Це дозволяє генерувати та зберігати криптографічні ключі за стандартом FIPS 140-2.

AWS KMS генерує симетричні ключі шифрування AES256 для шифрування в стані спокою, а також RSA 2048-біт (до 4096 біт) та ECC 256-біт (до 512 біт) для шифрування, цифрового підпису та перевірки підпису.

Приклади поширених сервісів, які використовують AWS KMS:

- *Amazon S3 (зберігання об'єктів).* Захищає від несанкціонованого доступу до сховища об'єктів
- *Amazon EBS (блокове сховище).* Захищає від несанкціонованого доступу до блочного сховища або знімків
- *Amazon RDS (керована реляційна база даних).* Захищає від несанкціонованого доступу до керованих баз даних (зазвичай з операційної системи)

Нижче наведено деякі рекомендації щодо AWS KMS:

- Використовуйте політики IAM для надання доступу до певного ключа шифрування за допомогою API (наприклад, можливість позначати ресурс тегом, але не зчитувати ключ шифрування).
- Для кращого контролю над ключами шифрування вкажіть ARN ключа в політиці IAM.
- Використовуйте API AWS IAM Access Analyzer для виявлення зовнішніх об'єктів, які мають доступ до ключів AWS KMS.
- Використовуйте ключі корзини Amazon S3 для створення унікальних ключів даних для об'єктів у корзині S3, що зменшує кількість запитів між S3 та AWS KMS (забезпечує кращу продуктивність шифрування/дешифрування об'єктів, кешування шифрування ближче до даних та зниження вартості на загальну кількість запитів до AWS KMS).

Щоб захистити доступ з вашого VPC до AWS KMS, використовуйте AWS PrivateLink, який дозволяє уникнути надсилання мережевого трафіку за межі вашого VPC через захищений канал, використовуючи кінцеву точку інтерфейсу VPC.

Використовуйте AWS CloudTrail для реєстрації всіх викликів API, здійснених через AWS KMS.

Використовуйте події Amazon CloudWatch для реєстрації подій, що стосуються імпорту, ротації або видалення ключів CMK. Забезпечити використання багатофакторної автентифікації (MFA) для будь-якого користувача, який має доступ до AWS KMS (за допомогою консолі AWS або API). Для сервісів, що підтримують шифрування у стані спокою, використовуйте керовані ключі AWS, що зберігаються в AWS KMS, для захисту даних у стані спокою.

Для високочутливих середовищ, які підтримують шифрування в стані спокою, використовуйте Головні ключі клієнта(ЦМК) для захисту даних у стані спокою, одночасно контролюючи ключі шифрування.

Для середовищ із високим рівнем конфіденційності шифруйте дані журналів в Amazon CloudWatch за допомогою ключа AWS KMS, керованого клієнтом, і надайте сервісу CloudWatch доступ до ключа шифрування.

Якщо ви використовуєте AWS CMK і маєте ключі шифрування, які ви не використовуєте, вимкніть їх через консоль AWS KMS або через виклик API. Переконайтеся, що ротацію ключів KMS увімкнено для всіх ваших CMK.

Якщо ви використовуєте власний CMK, регулярно змінюйте свої ключі. Ключі, які ми залишаємо незмінними, збільшують ризик їх компрометації неавторизованою особою.

Як найкраща практика, ротуйте всі ключі шифрування кожні 365 днів баланс між безпекою та адміністративними витратами.

Використовуйте теги також відомі як маркування, щоб краще зрозуміти, який CMK належить до якого ресурсу AWS.

Використовуйте симетричне шифрування з AWS KMS для шифрування даних у стані спокою (наприклад, об'єктів всередині Amazon S3).
Використовуйте асиметричне шифрування з AWS KMS для підписання файлів та перевірки того, що вони не були змінені.
Використовуйте AWS Config для моніторингу змін конфігурації AWS KMS.

Перш ніж остаточно закривати обліковий запис AWS, який містить конфіденційні дані, видаліть ключі CMK, щоб уникнути розголошення своїх даних небажаним третім особам. Якщо вам потрібно довести, що ви створили ключі CMK, а не AWS, KMS дозволяє генерувати ключі шифрування локально та імпортувати їх у службу AWS KMS (також відоме як «принеси свій власний ключ»). Недоліком цього є те, що AWS не може ротувати імпортовані ключі.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Головні ключі клієнта (CMK): https://surli.cc/byoxyp
Реєстрація викликів API AWS KMS за допомогою AWS CloudTrail: https://surl.lu/tekepg
Моніторинг за допомогою Amazon CloudWatch: https://surl.li/qlyala
Створення тривоги Amazon CloudWatch для виявлення використання головного ключа клієнта, який очікує видалення: https://surl.lt/nsjvmy
Увімкнення та вимкнення клавіш: https://surl.lu/fwbnpv
Використання політик IAM з AWS KMS: https://surl.lu/iomesd
Підключення до AWS KMS через кінцеву точку VPC: https://surl.li/vfhnnl

Найкращі практики розгортання KMSes 225
Зменшення вартості SSE-KMS за допомогою Amazon S3 Bucket Keys: https://surli.cc/vknhac
Як використовувати API AWS IAM Access Analyzer для автоматизації виявлення публічного доступу до ключів AWS KMS: https://surl.lu/dpqaad
Ротація ключів AWS KMS: https://surl.lt/sqwjrh
Імпорт ключового матеріалу в ключі AWS KMS: https://surl.li/tjlnbt
Шифрування даних журналів у журналах CloudWatch за допомогою служби керування ключами AWS: https://surl.lt/eywcpu

AWS Cloud HSM

AWS Cloud HSM - це хмарна платформа, керована Amazon Модуль апаратної безпеки (HSM). Це HSM, що відповідає стандарту FIPS 140-2 рівня 3. Він призначений для відповідності вимогам регульованих середовищ, таких як банки чи державні установи. Це єдиний ключ для зберігання даних, який діє як спеціалізоване обладнання для одного клієнта. Пристрій HSM є стійким до несанкціонованого доступу, що означає, що будь-яка спроба порушення безпеки фізичного пристрою призведе до стирання всіх ключів. Федеральний стандарт обробки інформації(ФІПС) -це стандарт уряду США для криптографічних модулів (як апаратних, так і програмних).

AWS Cloud HSM генерує симетричні ключі шифрування AES256 для шифрування в стані спокою, а також RSA 2048-біт (до 4096-біт) та ECC 256-біт (до 512-біт) для шифрування, цифрового підпису та перевірки підпису.

Оскільки це апаратний модуль, він містить прискорення TLS/SSL та Oracle Прозоре шифрування бази даних(ТДЕ) прискорення.

Нижче наведено деякі найкращі практики щодо AWS Cloud HSM:

- *Використовуйте* AWS Cloud HSM для розвантаження високоінтенсивних веб-серверів, що обробляють TLS.
- *Використовуйте* AWS Cloud HSM для зберігання PKI вашої організації. Центр сертифікації(Каліфорнія) закритий ключ.
- *Завжди розгортайте* кластер модулів AWS Cloud HSM для забезпечення високої доступності в іншій зоні доступності.
- *Щоб подолати обмеження* можливостей CloudHSM щодо створення нових ключів, додайте ще один модуль Cloud HSM.
- *Створіть групу* IAM, додайте користувачів до цієї групи IAM і надайте цільовій групі IAM необхідні дозволи в AWS Cloud HSM.
- *Забезпечити* використання багатофакторної автентифікації (MFA) для будь-якого користувача з доступом до консолі AWS Cloud HSM.
- *Використання* Утиліта керування Cloud HSM (КМУ) для створення локальних користувачів, які виконують дії безпосередньо на пристрої Cloud HSM (здебільшого для обслуговування пристрою).
- *Використовуйте* політики IAM для надання доступу до ключа шифрування.
- *Для кращого контролю* над ключами шифрування вкажіть ARN ключа в політиці IAM.
- *Створіть приватну* підмережу всередині вашої VPC та розгорніть вузли кластера AWS Cloud HSM всередині цієї приватної підмережі.

Щоб захистити доступ з вашого VPC до AWS Cloud HSM, використовуйте AWS Private Link, який дозволяє уникнути надсилання мережевого трафіку за межі вашого VPC через захищений канал, використовуючи кінцеву точку інтерфейсу VPC.

Використовуйте виділений екземпляр EC2 для підключення до AWS Cloud HSM та керування ним.

Використовуйте групи безпеки для керування доступом між екземпляром EC2 та AWS Cloud HSM.

Згенеруйте SSL-сертифікат для підключення та керування AWS Cloud HSM.

Використовуйте тегування (також відоме як маркування), щоб краще розуміти, який CMK належить до якого ресурсу AWS.

Використовуйте симетричне шифрування з AWS Cloud HSM для шифрування даних у стані спокою (наприклад, об’єктів всередині Amazon S3).

Використовуйте асиметричне шифрування з AWS Cloud HSM для підписання файлів та перевірки їхньої відсутності змін.

Використовуйте AWS CloudTrail для реєстрації всіх викликів API, здійснених через AWS Cloud HSM.
Використовуйте журнали Amazon CloudWatch для моніторингу подій AWS CloudHSM, таких як створення/видалення/зміна пароля для локальних користувачів Cloud HSM або створення/видалення ключів.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Створення адміністративних груп IAM: https://surl.li/qcqmmj
Керування ідентифікацією та доступом для AWS Cloud HSM: https://surl.li/ldiltp
Кінцеві точки AWS Cloud HSM та VPC: https://surli.cc/pwsqfy
Створення приватної підмережі: https://surl.lu/dnjtvr
Переналаштуйте SSL за допомогою нового сертифіката та закритого ключа: https://surli.cc/dmkgws
Найкращі практики для AWS Cloud HSM: https://surl.li/snkypl
Керування двофакторною автентифікацією (2FA) для криптоспеціалістів: https://surl.lu/fduhow
Робота з AWS CloudTrail та AWS Cloud HSM: https://surl.li/syrxhc

Кластери AWS Cloud HSM: https://surl.li/nbozzl
Покращення безпеки вашого веб-сервера за допомогою розвантаження SSL/TLS в AWS Cloud HSM: https://surli.cc/udrowo
Найчастіші запитання щодо AWS Cloud HSM: https://surl.lu/ydugds

Сховище ключів Azure

Azure Key Vault -це служба керування ключами, секретами та сертифікатами. Вона дозволяє створювати та зберігати криптографічні ключі за стандартом FIPS 140-2 рівня 2.

Azure Key Vault генерує RSA 2048-бітний (до 4096-бітний) та ECC 256-бітний (до 512-бітний) для шифрування, цифрового підпису та перевірки підпису.

Нижче наведено приклади поширених служб, які використовують Azure Key Vault:

- *Сховище BLOB-об'єктів Azure (зберігання об'єктів).* Захищає від несанкціонованого доступу до сховища об'єктів
- *Керовані диски Azure (блокове сховище).* Захищає від несанкціонованого доступу до блочного сховища або знімків Azure SQL(керована база даних SQL): Захищає від несанкціонованого доступу до керованих баз даних (зазвичай з операційної системи)

Деякі рекомендації щодо Azure Key Vault:

- *Використовуйте* Azure Key Vault для зберігання ключів облікового запису сховища Azure.
- *Використовуйте* Azure Key Vault для зберігання сертифікатів x509, таких як закритий ключ PKI CA вашої організації.

використання Azure Key Vault.

- *Використовуйте* Azure Key Vault для зберігання паролів замість того, щоб зберігати їх у відкритому тексті в коді чи скриптах (наприклад, скриптах PowerShell).
- *Використовуйте* Azure Key Vault для зберігання секретних кодів клієнтських програм, замість того, щоб зберігати їх у відкритому тексті у вашому коді (наприклад, у коді Java або DotNet).
- *Використовуйте* Azure Key Vault для зберігання SSH-ключів для доступу до віртуальних машин за допомогою SSH, без зберігання SSH-ключів локально на робочому столі.
- *Використовуйте* Azure Key Vault для зберігання рядків підключення до баз даних (замість зберігання облікових даних у відкритому вигляді всередині коду або скриптів).
- *Використовуйте* Azure Key Vault для зберігання ключів доступу до різних служб Azure (зі служби Redis Cache, Azure Cosmos DB, Azure Event Hubs тощо).
- *Використовуйте* Azure Контроль доступу на основі ролей(RBAC) для налаштування мінімального доступу до сховища ключів Azure.

Забезпечити використання багатофакторної автентифікації (MFA) для користувачів, які мають доступ до консолі Azure Key Vault або через API:

- *Використовуйте* Azure AD Керування привілейованими ідентифікаторами(ПІМ) для керування доступом до Azure Key Vault. Для найвищого рівня керування доступом до Azure Key Vault створіть окрему групу AD для кожного Azure Key Vault (наприклад, розділіть їх між Prod та Dev).
- *Використовуйте* кінцеві точки служби віртуальної мережі для керування доступом з вашої віртуальної мережі до сховища ключів Azure.
- *Використовуйте* тегування (тобто позначення), щоб краще розуміти, яке сховище ключів належить до якого ресурсу Azure.

Як найкраща практика, ротуйте всі ключі шифрування кожні 365 днів (баланс між безпекою та адміністративними витратами):

- Увімкнути ведення журналу Azure Key Vault і надсилати журнали до робочої області Azure Log Analytics.
- Пересилати журнали з робочої області Azure Log Analytics до Azure Sentinel для подальшого аналізу.
- Використовуйте аналітику Key Vault (в Azure Monitor) для збору інформації про проблеми з продуктивністю, збоями та затримкою.
- Увімкніть Azure Defender для Key Vault для розширеного захисту від загроз для Azure Key Vault.
- Використовуйте Центр безпеки Azure для моніторингу проблем відповідності, пов’язаних із Azure Key Vault.

- Увімкніть м’яке видалення та захист від очищення, щоб уникнути випадкового видалення ключів.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Рекомендації щодо використання Key Vault: https://surl.li/yolgxz
Кінцеві точки віртуальної мережевої служби для Azure Key Vault: https://surli.cc/rtyhqo
Увімкнути журналювання сховища ключів: https://surl.li/pmdcyg
Моніторинг та оповіщення для Azure Key Vault: https://surl.li/gycwee
Моніторинг служби сховища ключів за допомогою аналітики сховища ключів: https://surl.li/byaoqk
Вступ до Azure Defender для Key Vault: https://surl.li/rvjcmz
Базовий рівень безпеки Azure для Key Vault: https://surl.li/gmfumg
Типи ключів, алгоритми та операції: https://surl.li/qdwxxs
Керування ключами облікового запису сховища за допомогою Key Vault та Azure CLI: https://surl.li/sttisb
Про сертифікати Azure Key Vault: https://surl.li/mextyp
Керування відновленням Azure Key Vault із захистом від м’якого видалення та очищення: https://surli.cc/zaqvgr
Автентифікація в Azure Key Vault: https://surl.li/zwvdqa
Безпека сховища ключів Azure: https://surl.lu/fkdihz

Виділений/керований HSM Azure

Керований HSM Azure та виділений HSM Azure - це керовані хмарні рішення Azure. Модулі апаратної безпеки (HSM). Вони є HSM, що відповідають стандарту FIPS 140-2 рівня 3. Вони призначені для відповідності вимогам регульованого середовища, такого як банки чи державні установи.

Пристрій HSM є стійким до несанкціонованого доступу та захищеним від несанкціонованого доступу, що означає, що будь-яка спроба порушення безпеки фізичного пристрою призведе до стирання всіх ключів.

Федеральні стандарти обробки інформації (ФІПС) -це стандарт уряду США для криптографічних модулів (як апаратних, так і програмних).

Виділений HSM Azure генерує симетричні ключі шифрування AES256 для шифрування в стані спокою, а також RSA 2048-біт (до 4096-біт) та ECC 256-біт (до 512-біт) для шифрування, цифрового підпису та перевірки підпису.

Деякі рекомендації щодо виділеного/керованого HSM Azure:
- Використовуйте керований HSM Azure для зберігання ключів облікового запису сховища Azure.
- Використовуйте керований HSM Azure для зберігання сертифікатів x509, таких як закритий ключ PKI CA вашої організації.
- Використовуйте Azure RBAC для налаштування мінімального доступу до керованого HSM Azure.

- Забезпечити використання багатофакторної автентифікації (MFA) для користувачів, які мають доступ до консолі керованого HSM Azure або через API.
- Регулярно створюйте резервні копії керованого HSM Azure.
- Використовуйте кінцеві точки служби віртуальної мережі для керування доступом з вашої віртуальної мережі до керованого HSM Azure.
- Використовуйте тегування (тобто позначення), щоб краще розуміти, яке сховище ключів належить до якого ресурсу Azure.
- Увімкнути ведення журналу керованого HSM Azure та надсилати журнали до робочої області Azure Log Analytics.
- Пересилати журнали з робочої області Azure Log Analytics до Azure Sentinel для подальшого аналізу.
- Імпортуйте ключі шифрування з локального HSM до керованого HSM Azure (також відомого як принесіть свої власні ключі).
- Імпортуйте свій локальний домен безпеки HSM до керованого HSM Azure, щоб мати змогу спільно використовувати існуючий домен безпеки.
- Увімкніть м'яке видалення та захист від очищення, щоб уникнути випадкового видалення ключів

Для отримання додаткової інформації зверніться до наступних ресурсів:
Документація виділеного HSM Azure: https://surli.cc/fxscic
Що таке керований HSM Azure Key Vault?: https://surl.li/rvhnnf
Часті запитання (FAQ): https://surl.li/xypvut
Загальна доступність: Приватне посилання керованого HSM Azure: https://surl.li/tnaiks
Кероване ведення журналу HSM: https://surl.li/fjstbi
Імпорт ключів, захищених HSM, до керованого HSM (BYOK): https://surl.lt/kxyznn
Про керований домен безпеки HSM: https://surl.li/nxppyb

Служба керування ключами Google Cloud (KMS)

Google Cloud KMS - це служба керування ключами GCP. Вона дозволяє генерувати та зберігати криптографічні ключі за стандартом FIPS 140-2 рівня як програмне рішення або за стандартом FIPS 140-2 рівня 3 як апаратний HSM.

FIPS - це стандарт уряду США для криптографічних модулів (як апаратних, так і програмних).

Пристрій HSM є стійким до несанкціонованого доступу, а це означає, що будь-яка спроба порушення безпеки фізичного пристрою призведе до стирання всіх ключів.

Використовуйте Google Cloud HSM для дотримання вимог регульованих середовищ, таких як банки чи державні установи - за потреби Google також підтримує Розміщені приватні HSM.

Google Cloud KMS генерує симетричні ключі шифрування AES256 для шифрування в стані спокою, а також RSA 2048-біт (до 4096 біт) та ECC 256-біт (до 384 біт) для шифрування, цифрового підпису та перевірки підпису.

Кілька прикладів поширених сервісів, які використовують Google Cloud KMS:

- *Хмарне сховище Google (зберігання об'єктів)*. Захищає від несанкціонованого доступу до сховища об'єктів.
- *Постійний диск Google(блокове сховище)*. Захищає від несанкціонованого доступу до блочного сховища або знімків.
- *Google Cloud SQL(керована реляційна база даних)*. Захищає від несанкціонованого доступу до керованих баз даних (зазвичай з операційної системи).

Деякі рекомендації щодо Google Cloud KMS:

- Використовуйте Google Cloud IAM для керування дозволами до Google Cloud KMS.
- Переконайтеся, що ваша політика Cloud IAM не дозволяє анонімного або публічного доступу до ваших ключів Cloud KMS.
- Використовуйте теги (також відомі як маркування), щоб краще зрозуміти, які ключі Cloud KMS належать до якого ресурсу GCP.

Як найкраща практика, ротуйте всі ключі шифрування кожні 365 днів (баланс між безпекою та адміністративними витратами):

- Увімкнути журнали аудиту Cloud KMS для моніторингу активності Cloud KMS.
- Журнали аудиту активності адміністратора ввімкнено за замовчуванням і не можна вимкнути.
- Явно ввімкнути Аудит доступу до даних журнали для реєстрації дій, що виконуються в Google Cloud KMS.
- Обмежте доступ до журналів аудиту мінімальною кількістю співробітників, щоб уникнути можливого видалення або внесення змін до журналів аудиту.
- Увімкніть автоматичну ротацію ключів, щоб уникнути можливого їхнього злому.
- Якщо ви не використовуєте попередні версії ключів шифрування, вимкніть їх вручну.
- Для високочутливих середовищ, де у вас є локальний HSM, використовуйте Менеджер зовнішніх ключів у хмарі(Хмарне управління EKM) для зберігання ключів шифрування поза центрами обробки даних Google.
- Для масштабних середовищ з кількома проектами GCP використовуйте елементи керування послугами VPC, щоб запровадити обмеження доступу до вашої хмарної KMS на основі вашої ідентифікаційної особи IP-адреса.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Швидкий старт служби керування хмарними ключами: https://surl.li/svrkwv
Глибокий аналіз служби керування ключами в хмарі: https://surl.li/nkdqgb
Використання IAM з Cloud KMS: https://surl.li/zqdyvn
Інформація про журнал аудиту Cloud KMS: https://surl.lt/xkrghk

Розміщений приватний HSM: https://surl.li/kdaxbi
Менеджер зовнішніх ключів у хмарі: https://surli.cc/dvhsra
Обертові ключі: https://surl.li/twktsd
Увімкнення та вимкнення версій ключів: https://surli.cc/tgifkv
Ключі шифрування, керовані клієнтом (CMEK): https://surl.li/tkxprv

Найкращі практики розгортання служб керування секретами

Усі великі постачальники хмарних послуг мають службу управління секретами.

Термін таємниць стосується облікових даних бази даних, ключів API, токенів, імен користувачів/паролів тощо. Фундаментальна концепція служб управління секретами полягає в тому, щоб дозволити вам зберігати таку конфіденційну інформацію в захищеному місці з механізмами авторизації та аудиту, водночас дозволяючи користувачам та обліковим записам служб безпечно отримувати таємниці без необхідності зберігати інформацію у відкритому тексті у файлах конфігурації.

Оскільки хмарне середовище є дуже динамічним, рекомендується мати централізоване та безпечне сховище для зберігання, створення та отримання таємниць.

Команди DevOps можуть скористатися перевагами сервісів управління секретами, перенаправляючи свій код до цих сервісів, замість того, щоб вбудовувати конфіденційну інформацію (таємниці, облікові дані, ключі доступу тощо) у відкритий текстовий код.

Менеджер таємниць AWS

AWS Secrets Manager - це керований сервіс таємниць Amazon.

Деякі сервіси, які підтримують використання таємниць у сервісах AWS:

- Таємниці всередині функцій AWS Lambda,
- Паролі для підключення до Amazon RDS (Aurora, MySQL, PostgreSQL, Oracle, MariaDB та Microsoft SQL Server),
- Таємниці всередині Amazon DocumentDB,
- Таємниці Amazon RedShift.

AWS Secrets Manager дозволяє створювати, зберігати, обертати, маркувати та керувати версіями ваших таємниць. Таємниці, якими керує Менеджер таємниць AWS шифруються та зберігаються в AWS KMS.

Деякі рекомендації щодо AWS Secrets Manager:

- Створіть групу IAM, додайте облікові записи служб (або аплікативні облікові записи) до групи IAM та надайте цільовій групі IAM необхідні дозволи на AWS Secrets Manager.
- Використовуйте політики IAM для контролю мінімального доступу до секретних даних для ваших користувачів і програм.

- Щоб централізовано зберігати таємниці з кількох регіонів AWS, увімкніть функцію «Секрет репліки» та оновіть ключ шифрування «Секрет репліки».
- Використовуйте тегування (тобто маркування), щоб краще розуміти, який секрет належить до якого ресурсу AWS.
- Переконайтеся, що таємна ротація увімкнено.
- Зберігайте всю конфіденційну інформацію (наприклад, підказки до паролів) у секретних значеннях, які можна отримати з AWS Secrets Manager.
- Використовуйте кешування на стороні клієнта для покращення продуктивності під час зберігання таємниць у сервісі AWS Secrets Manager.
- Уникайте зберігання конфіденційної інформації (наприклад, таємниць) у файлах журналів.
- Запускайте всі ресурси AWS, яким потрібен доступ до AWS Secrets Manager, усередині вашої віртуальної машини.
- Для сервісів, що працюють поза межами вашої VPC, використовуйте AWS CodeBuild для доступу до таємниць із сервісу AWS Secrets Manager.
- Щоб захистити доступ з вашого VPC до AWS Secrets Manager, використовуйте AWS PrivateLink, який дозволяє уникнути надсилання мережевого трафіку за межі вашого VPC через захищений канал, використовуючи кінцеві точки інтерфейсу VPC.
- Використовуйте AWS CloudTrail для моніторингу всіх дій API, що виконуються через AWS Secrets Manager.
- Використовуйте журнали Amazon CloudWatch для моніторингу таємниць, що очікують видалення або ротації таємниць.
- Використовуйте AWS Config для моніторингу змін у ваших секретних даних.
- Для сервісів, що підтримують використання AWS Secrets Manager, шифруйте таємниці за допомогою ключа шифрування AWS Secrets Manager всередині AWS KMS.
- Для середовищ із високим рівнем конфіденційності шифруйте секретні дані за допомогою вашого CMK всередині AWS KMS.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Огляд керування дозволами доступу до таємниць менеджера таємниць: https://surl.li/qmoeqe
Рекомендації щодо роботи з менеджером таємниць AWS: https://surli.cc/uqfcce
Як AWS Secrets Manager використовує AWS KMS: https://surl.lu/fbjeif
Моніторинг використання ваших таємниць AWS Secrets Manager: https://surl.lu/debblf

Менеджер таємниць Google

Google Secret Manager - це служба таємниць, керована GCP, для керування ключами API, паролями, сертифікатами тощо.

Цей сервіс підтримує такі типи таємниць у сервісах GCP:

- Змінні середовища всередині Google Cloud Build,

- Таємниці всередині Google Cloud Code,
- Таємниці функцій Google Cloud,
- Змінні середовища всередині Google Cloud Run,
- Таємниці всередині Google Compute Engine,
- Таємниці всередині сервіса Compute Engine контейнерів Google Kubernetes,
- Таємниці всередині Google Config Connector.

Менеджер таємниць Google дозволяє створювати, зберігати, обертати, позначати та керувати версіями ваших таємниць. Таємниці, якими керує Google Secret Manager, шифруються та зберігаються в Google Cloud KMS.

Деякі рекомендації щодо Google Secret Manager:

- Використовуйте Google IAM та ролі IAM, щоб налаштувати мінімальний доступ до секретних даних як для користувачів IAM, так і для ваших програм.
- Використовуйте IAM Recommender для виявлення ідентифікаційних осіб із надмірними привілеями.
- Використовуйте умови IAM для обмеження доступу до таємниць.
- Якщо у вас є якісь таємниці, якими ви більше не користуєтеся, вимкніть старі версії таємниць перед їх видаленням, щоб уникнути можливості того, що вам може знадобитися стара версія, якщо вона буде знищена, і дані стануть недоступними.
- Увімкнути журнали аудиту Cloud Secret Manager для моніторингу активності Cloud Secret Manager
- Журнали аудиту активності адміністратора ввімкнено за замовчуванням і не можна вимкнути.
- Явно ввімкнути журнали аудиту доступу до даних для реєстрації дій, що виконуються Google Cloud Secret Manager.
- Обмежте доступ до журналів аудиту мінімальною кількістю співробітників, щоб уникнути можливого видалення або внесення змін до журналів аудиту.
- Увімкніть автоматичну ротацію ключів, щоб уникнути можливого їхнього злому.
- Для середовищ з високою чутливістю шифруйте свої таємниці за допомогою Ключі шифрування, керовані клієнтом(CMEK).
- Для масштабних середовищ з кількома проектами GCP використовуйте Елементи керування послугами VPC щоб запровадити обмеження доступу до Cloud Secret Manager на основі ідентифікаційних даних (обліковий запис служби або користувача) або IP-адрес.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Контроль доступу (IAM): https://surl.li/ocbbcs
Забезпечити мінімальні привілеї за допомогою рекомендацій щодо ролей: https://surli.cc/hkfphd
Огляд елементів керування послугами VPC: https://surl.lu/uclkpf

Ведення журналу аудиту секретного менеджера: https://surl.li/qxmjdm
Увімкнення ключів шифрування, керованих клієнтом (CMEK), для Secret Manager: https://surl.li/hxehex
Найкращі практики секретного менеджера: https://surl.li/ttbkju

Найкращі практики використання шифрування під час передачі

Ідея, що лежить в основі шифрування під час передачі полягає в тому, щоб дозволити двом сторонам обмінюватися повідомленнями через публічно доступну мережу безпечним способом, зберігаючи при цьому конфіденційність та цілісність повідомлень.

IPSec - це найпоширеніший протокол для шифрування під час передачі, головним чином для VPN між вузлами та VPN-тунелів. IPSec знаходиться на третьому рівні моделі OSI.

Деякі найкращі практики щодо IPSec:

- Використовуйте протокол IKEv2 для асоціації безпеки (SA).
- Використовуйте AES-GCM для шифрування.
- Використовуйте HMAC-SHA256 (або вище) для забезпечення цілісності.
- Якщо це підтримується як клієнтом, так і сервером, використовуйте автентифікацію на основі сертифіката замість попередньо наданого ключа.
- Використовуйте оновлений VPN-клієнт (щоб уникнути відомих вразливостей).

Для отримання додаткової інформації зверніться до наступних ресурсів:
Безпека інтернет-протоколу (IPSec): https://surl.li/hjpgxb
Посібник з IPSec VPN: https://surl.lu/gmttru

Безпека транспортного рівня (TLS)

TLS є одним з найбільш використовуваних протоколів для шифрування під час передачі даних.
TLS поєднує асиметричне шифрування для узгодження сеансу між клієнтом і сервером (генерація симетричного ключа та копіювання між клієнтом і сервером) із симетричним шифруванням для безпечної передачі повідомлень.

Хоча TLS спирається на TCP (транспортний рівень моделі OSI), він вважається шифруванням прикладного рівня (HTTPS протоколу HTTP) або 7-м рівнем моделі OSI.

Звичайні випадки використання включають веб-браузери (клієнт) та вебсервери (сервер), такі як сайти електронної комерції. У контексті хмарних сервісів майже всі API постачальників хмарних сервісів використовують TLS для шифрування під час передачі.

Деякі найкращі практики щодо TLS:

- Веб-сайти, API або програми, що знаходяться в приватній підмережі або обслуговують внутрішніх співробітників організації, використовують сертифікати, підписані довіреним внутрішнім центром сертифікації.

💻*Примітка!* Як найкраща практика, уникайте використання самопідписаних сертифікатів, оскільки їх неможливо перевірити або довіряти їм.

- Для будь-яких публічно доступних веб-сайтів, API або програм використовуйте сертифікат, підписаний відомим публічним центром сертифікації.
- Переконайтеся, що сертифікат дійсний (ім'я домену відповідає імені DNS) та що термін дії сертифіката не закінчився або його не було відкликано.

Уникайте використання шаблонних сертифікатів - завжди переконайтеся, що назва сертифіката відповідає повному доменному імені сервера.

Уникайте використання сертифікатів з короткими термінами дії (таких як LetsEncrypt сертифікати).

Під час використання Kubernetes використовуйте TLS для шифрування трафіку між подами та взаємної автентифікації сервера та клієнта.

Мінімальна рекомендована версія протоколу TLS -1.2, і якщо у вас є апаратне/програмне забезпечення для її підтримки, рекомендується перейти на TLS 1.3 та відмовитися від підтримки попередніх версій TLS та всіх версій протоколів SSL.

- Вимкніть використання слабких протоколів (будь-яка версія SSL та TLS, нижча за 1.2).
- Вимкніть використання слабких наборів шифрів (таких як 3DES/DES/RC2/IDEA).
- Використовуйте закритий ключ RSA з мінімальним розміром 2048 бітів.
- Використовуйте алгоритм підпису SHA256.
- Увімкнути використання Сувора безпека транспорту (HSTS).
- Увімкнути використання Ідеальна пряма секретність(ВБП).
- Використання ssllabs.com щоб перевірити оцінку вашого протоколу TLS.

Якщо ви бажаєте перевіряти зашифрований трафік у хмарних сервісах, використовуйте SSL-термінацію (для сервісів, які підтримують цю можливість). SSL-термінація дозволяє вам відкривати зашифрований трафік (наприклад, на вашому балансувальнику навантаження або веб-сервері фронтенду) шляхом тимчасового розшифрування трафіку, перевірки його за допомогою пристроїв або програмного забезпечення, що підтримують перевірку трафіку (наприклад, IPS, WAF, запобігання витоку даних тощо), і, нарешті, знову зашифрувати трафік, перш ніж він досягне наступного стрибка (наприклад, між балансувальником навантаження та веб-серверами).

Для отримання додаткової інформації зверніться до наступних ресурсів:
Безпека транспортного рівня: https://surli.cc/lqjdkb
Рекомендації щодо розгортання SSL та TLS: https://surl.li/jipuhl
Посібник з оцінювання SSL-серверів: https://surl.li/iwkpkp
Тест SSL-сервера: https://surl.li/tsybct
Anthos Service Mesh на прикладі: mTLS: https://surl.lu/tlczoc

Найкращі практики використання шифрування в стані спокою

Ідея, що лежить в основі *шифрування в стані спокою* полягає в захисті даних після їх збереження у сховищі чи базі даних, або після того, як до них отримала доступ ненадійна третя сторона.

Робочий процес пояснює процес вилучення зашифрованого об’єкта зі сховища об’єктів:

- DEK зберігається поруч із самим об’єктом, а метадані об’єкта визначають, яку версію ключа шифрування використовувати.
- Весь DEK обгорнутий плівкою KEK.
- Ключовий ключ зберігається всередині служби, керованої ключами.
- Коли надходить запит на доступ до об'єкта, авторизована служба (або програма) надсилає запит до служби керування ключами, щоб знайти KEK та розшифрувати певний DEK.
- Розшифрований DEK надсилається через канал TLS/SSL від KMS до сховища об'єктів. Сам об'єкт розшифровується за допомогою розшифрованого DEK.

На наступній діаграмі показано попередній робочий процес вилучення зашифрованого об'єкта зі сховища об'єктів (Рис.2.5):

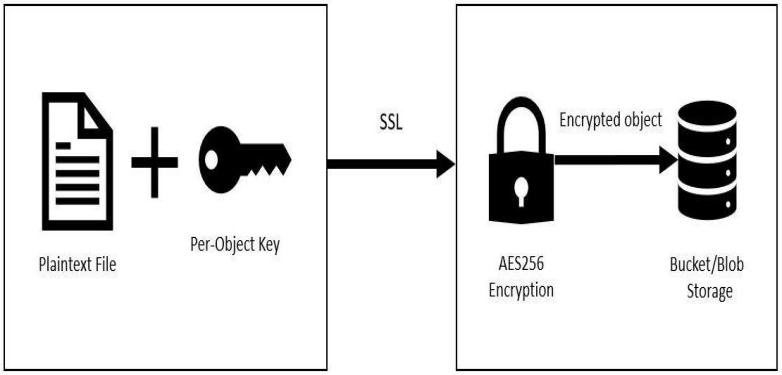

Рисунок 2.5 - Шифрування сховища об’єктів

AWS та шифрування сховища об'єктів

Шифрування на стороні сервера за допомогою керованих ключів Amazon S3 (SSE-S3):

- Шифрування на основі AES256 у стані спокою.
- Ключі шифрування генеруються, ротуються та підтримуються AWS.
- Рекомендовано для всіх шифрувань корзин S3.
- Шифрування на стороні сервера з використанням CMK, що зберігаються в AWS KMS (SSE-KMS):
- Шифрування на основі AES256 у стані спокою.

Ключі шифрування генеруються, ротуються та підтримуються клієнтами, і зберігаються в AWS KMS.

AWS KMS пропонує додатковий рівень контролю, налаштовуючи керування доступом до ключів шифрування. Додатковий журнал аудиту ввімкнено за допомогою AWS CloudTrail для тих, хто використовував CMK. Рекомендовано для високочутливих середовищ, які зберігають конфіденційні дані (такі як особиста інформація, інформація про кредитні картки, дані про охорону здоров'я тощо) у контейнерах S3.

Шифрування на стороні сервера з ключами, наданими клієнтом (SSE-C):

- Коли ви завантажуєте файл, Amazon S3 шифрує його за допомогою
- AES256. Файли шифруються клієнтом перед завантаженням файлу в
- S3. Amazon не має доступу до ключа шифрування.

Для отримання додаткової інформації зверніться до наступного ресурсу:
Захист даних за допомогою шифрування на стороні сервера: https://surli.cc/zliqhq

Шифрування Azure та сховища BLOB-файлів

Сховище BLOB-об'єктів Azure підтримує такі типи ключів шифрування:
Ключі, керовані Microsoft:

- Шифрування на основі AES256 у стані спокою.
- Ключі шифрування генеруються, ротуються та підтримуються Azure. Ключі шифрування зберігаються в сховищі ключів Microsoft. Рекомендовано для всіх типів шифрування сховищ BLOB-об'єктів.

Ключі, керовані клієнтом

- Шифрування на основі AES256 у стані спокою.
- Ключі шифрування генеруються, ротуються та підтримуються клієнтами, і вони зберігаються в Azure Key Vault або Azure Key Vault HSM.
- Azure Key Vault пропонує додатковий рівень контролю, налаштовуючи керування доступом для ключів шифрування.

Рекомендовано для середовищ з високою конфіденційністю, які зберігають конфіденційні дані (такі як особиста інформація, інформація про кредитні картки, дані охорони здоров’я тощо) у сховищі BLOB-об’єктів Azure або файлах Azure.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Шифрування сховища Azure для даних у стані спокою: https://surl.li/qvmufr
Ключі, керовані клієнтом, для шифрування сховища Azure: https://surl.li/edflkf

GCP та шифрування сховища об'єктів

Хмарне сховище Google підтримує такі типи ключів шифрування:
Ключі шифрування, керовані Google:

- Шифрування на основі AES256 у стані спокою
- Ключі шифрування генеруються, ротуються та підтримуються GCP.

Рекомендовано для шифрування всіх сховищ об'єктів.

Ключі шифрування, керовані клієнтом:

- Шифрування на основі AES256 у стані спокою.
- Ключі шифрування генеруються, ротуються та підтримуються клієнтами, і зберігаються в Google Cloud KMS.
- Google Cloud KMS пропонує додатковий рівень контролю, налаштовуючи керування доступом до ключів шифрування.

Ключі шифрування, надані клієнтом:

- Шифрування на основі AES256 у стані спокою.
- Файли шифруються клієнтом перед завантаженням у Google Cloud Storage.
- GCP не має доступу до ключа шифрування.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Ключі шифрування, керовані Google: https://surl.lu/wkcgvn

Шифрування блокового сховища

Під час використання шифрування блочного сховища використовується один ключ шифрування DEK для шифрування всього блочного сховища (також відомого як том диска). Під час використання знімків використовується один ключ шифрування для шифрування всього знімка.

AWS та шифрування блочного сховища

Блокове сховище AWS (EBS) підтримує наступні типи ключів шифрування
Керовані AWS CMK:

- Шифрування на основі AES256 у стані спокою.
- Ключі шифрування генеруються, ротуються та підтримуються AWS.
- Рекомендовано для всіх типів шифрування томів EBS.

Керовані клієнтами CMK:

- Шифрування на основі AES256 у стані спокою.
- Ключі шифрування генеруються, ротуються та підтримуються клієнтами, і зберігаються в AWS KMS.
- AWS KMS пропонує додатковий рівень контролю, налаштовуючи керування доступом до ключів шифрування.
- Використовуйте AWS CloudTrail, щоб перевірити, хто використовував CMK.

Рекомендовано для високочутливих середовищ, які зберігають конфіденційні дані (такі як особиста інформація, інформація про кредитні картки, дані про охорону здоров'я тощо) всередині томів EBS.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Як Amazon Elastic Block Store (Amazon EBS) використовує AWS KMS: https://surli.cc/ugzmwt
Шифрування томів Amazon EBS: https://surl.li/ygzjwz

Шифрування керованих дисків Azure

Керовані диски Azure підтримують такі типи ключів шифрування:

Ключі, керовані платформою:

- Шифрування на основі AES256 у стані спокою.
- Ключі шифрування генеруються, ротуються та підтримуються Azure.

Рекомендовано для всіх керованих дисків, знімків та образів віртуальних машин.

Ключі, керовані клієнтом:

- Шифрування на основі AES256 у стані спокою.
- Ключі шифрування генеруються, ротуються та підтримуються клієнтами, і вони зберігаються в Azure Key Vault або Azure Key Vault HSM.
- Azure Key Vault пропонує додатковий рівень контролю, налаштовуючи керування доступом до ключів шифрування.

Рекомендовано для високочутливих середовищ, які зберігають конфіденційні дані (такі як особиста інформація, інформація про кредитні картки, дані про охорону здоров'я тощо) на керованих дисках, знімках та образах віртуальних машин.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Шифрування на стороні сервера сховища дисків Azure: https://surl.li/woyxss
Використовуйте портал Azure, щоб увімкнути шифрування на стороні сервера з ключами, керованими клієнтом, для керованих дисків: https://surl.lu/urhosw

Шифрування постійних дисків GCP

Постійні диски Google підтримують такі типи ключів шифрування:

- Ключі шифрування, керовані Google:
- Шифрування на основі AES256 у стані спокою.
- Ключі шифрування генеруються, ротуються та підтримуються GCP.

Рекомендовано для всіх постійних дисків.

Ключі шифрування, керовані клієнтом:

- Шифрування на основі AES256 у стані спокою.
- Ключі шифрування генеруються, ротуються та підтримуються клієнтами, і зберігаються в Google Cloud KMS.
- Google Cloud KMS пропонує додатковий рівень контролю, налаштовуючи керування доступом до ключів шифрування.

Рекомендовано для нових постійних дисків у високочутливих середовищах, де зберігаються конфіденційні дані (такі як особиста інформація, інформація про кредитні картки, дані про охорону здоров’я тощо) на постійних дисках Google.

Ключі шифрування, надані клієнтом:

- Шифрування на основі AES256 у стані спокою.

- Файли шифруються клієнтом перед завантаженням на постійний диск Google.
- GCP не має доступу до ключа шифрування.

Повне шифрування бази даних

Під час використання повного шифрування бази даних (іноді його називають Прозоре шифрування даних (ТДЕ), один DEK використовується для шифрування всієї бази даних, журналів, резервних копій та знімків.

DEK деформується KEK, який зберігається в захищеному сховищі (KMS).

Шифрування Amazon RDS

Amazon RDS підтримує наступні типи ключів шифрування:

Керовані AWS CMK.

- Шифрування на основі AES256 у стані спокою.
- Ключі шифрування генеруються, ротуються та підтримуються AWS.

Рекомендовано для звичайного шифрування бази даних RDS.

Керовані клієнтами CMK:

- Шифрування на основі AES256 у стані спокою.
- Ключі шифрування генеруються, ротуються та підтримуються клієнтами, і зберігаються в AWS KMS.
- AWS KMS пропонує додатковий рівень контролю, налаштовуючи керування доступом до ключів шифрування.
- Використовуйте AWS CloudTrail, щоб перевірити, хто використовував CMK.

Рекомендовано для високочутливих середовищ, які зберігають конфіденційні дані (такі як особиста інформація, інформація про кредитні картки, дані про охорону здоров'я тощо) у базах даних RDS.

Для отримання додаткової інформації зверніться до наступного ресурсу:
Шифрування ресурсів Amazon RDS: https://surli.cc/syngju

Прозоре шифрування даних (TDE) Azure SQL

Azure SQL TDE підтримує такі типи ключів шифрування:

Прозоре шифрування даних, кероване сервісом:

- Шифрування на основі AES256 у стані спокою.
- Ключі шифрування генеруються, ротуються та підтримуються Azure.
- Рекомендовано для всіх баз даних Azure SQL.

Прозоре шифрування даних, кероване клієнтом

- Принесіть свій власний ключ.

Шифрування на основі AES256 у стані спокою.

Ключі шифрування генеруються, ротуються та підтримуються клієнтами, і вони зберігаються в Azure Key Vault або Azure Key Vault HSM.

Azure Key Vault пропонує додатковий рівень контролю, налаштовуючи керування доступом до ключів шифрування.

Рекомендовано для середовищ з високою чутливістю, які зберігають конфіденційні дані (такі як особиста інформація, інформація про кредитні картки, дані про охорону здоров'я тощо) всередині Azure SQL.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Прозоре шифрування даних для бази даних SQL, керованого екземпляра SQL та аналітики Azure Synapse: https://surl.li/koxboj
Прозоре шифрування даних Azure SQL з ключами, керованими клієнтом: https://surl.li/zbccfs

Шифрування Google Cloud SQL

Google Cloud SQL підтримує такі типи ключів шифрування:
Ключі шифрування, керовані Google:

- Шифрування на основі AES256 у стані спокою.
- Ключі шифрування генеруються, ротуються та обслуговуються GCP.
- Рекомендовано для всіх SQL-замовлень Google Cloud.

Ключі шифрування, керовані клієнтом:

- Шифрування на основі AES256 у стані спокою.
- Ключі шифрування генеруються, ротуються та підтримуються клієнтами, і зберігаються в Google Cloud KMS.
- Google Cloud KMS пропонує додатковий рівень контролю, налаштовуючи керування доступом до ключів шифрування.
- Рекомендовано для нових постійних дисків у високочутливих середовищах, які зберігають конфіденційні дані (такі як особиста інформація, інформація про кредитні картки, дані про охорону здоров'я тощо) у Google Cloud SQL.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Огляд ключів шифрування, керованих клієнтом (CMEK): https://surl.li/bcplxg
Використання ключів шифрування, керованих клієнтом (CMEK): https://surl.lu/kemscw

Безпека на рівні рядків

Безпека на рівні рядків - це відносно нова концепція, призначена для вирішення питань доступу до спільних ресурсів, таких як бази даних, що обслуговують кількох клієнтів у багатоклієнтському середовищі.

Це дозволяє шифрувати дані більш детально, надаючи дозволи доступу до зашифрованого вмісту на основі рядка, стовпця або поля (залежно від можливостей сервісу).

Щоб отримати додаткові відомості про безпеку на рівні рядків AWS, зверніться до таких ресурсів:
Використання безпеки на рівні рядків (RLS) для обмеження доступу до набору даних в Amazon QuickSight: https://surl.li/wtulwd

Використання шифрування на рівні полів для захисту конфіденційних даних в Amazon Cloud Front: https://surl.lt/fxsgnl

Щоб отримати додаткові відомості про безпеку на рівні рядків Azure, зверніться до таких ресурсів:
Безпека на рівні рядків Azure SQL: https://surl.li/gwfico
Безпека на рівні рядків у провіднику даних Azure: https://surl.li/bjdyol

Використовується шифрування

На цьому етапі ми розуміємо концепцію захисту даних за допомогою шифрування під час передачі та шифрування в стані спокою. Залишилося ще одне місце, де нам потрібно захистити дані - під час їх використання в пам’яті сервера, а саме, під час використання шифрування.

Анклави AWS Nitro

AWS пропонує своїм клієнтам унікальну архітектуру, яка створює ізольоване середовище для зберігання конфіденційної інформації (як-от особисті дані, номери кредитних карток та дані про охорону здоров'я), що відокремлює дані клієнтів від самого екземпляра EC2, використовуючи при цьому AWS KMS для шифрування даних.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Анклави AWS Nitro: https://surl.li/eqyudy
Як AWS Nitro Enclaves використовує AWS KMS: https://surli.cc/wfnkhb

Конфіденційні обчислення Azure

Azure Confidential Computing використовує апаратне забезпечення для ізоляції даних. Дані можна зашифрувати під час використання, запустивши їх у надійне середовище виконання (TI). Azure Confidential Computing базується на обладнанні Intel SGX і підтримує як віртуальні машини Azure, так і службу Azure Kubernetes, що дозволяє клієнтам безпечно зберігати конфіденційну інформацію (наприклад, особисту інформацію, номери кредитних карток, дані про охорону здоров'я тощо).

Для отримання додаткової інформації зверніться до наступних ресурсів:
Конфіденційні обчислення Azure: https://surl.lt/nksntg
Конфіденційні обчислювальні вузли в службі Azure Kubernetes: https://surl.li/ezwajr

Конфіденційні обчислення Google

Служба конфіденційних обчислень Google використовує апаратне забезпечення для ізоляції даних. Дані можна зашифрувати під час використання, запустивши їх у TEE.

Сервіс Google Confidential Computing базується на апаратному забезпеченні AMD SEV (процесори AMD EPYC 2-го покоління) та підтримує як

конфіденційні віртуальні машини Google, так і конфіденційні GKE Google, що дозволяє клієнтам безпечно зберігати конфіденційну інформацію (наприклад, особисті дані, номери кредитних карток та дані про охорону здоров'я).

Для отримання додаткової інформації зверніться до наступних ресурсів:
Використання конфіденційних вузлів GKE: https://surl.lu/bvxgib

Підсумки Розділу 2

У Розділі 2 здійснено комплексний аналіз сервісів керування ідентифікацією та доступом (IAM) у хмарних середовищах AWS, Azure та GCP. Розглянуто еволюцію від керованих служб Active Directory до сучасних систем IAM, а також підкреслено важливість застосування багатофакторної автентифікації (MFA) як засобу додаткового захисту ідентифікаційних даних. Для кожного рішення наведено найкращі практики щодо налаштування, управління обліковими записами, моніторингу та аудиту. Досліджено вбудовані інструменти моніторингу, аудиту, управління загрозами та реагування на інциденти у трьох провідних хмарних платформах. Показано, яким чином вмикається аудит та організовується збір даних із різних джерел подій, що дозволяє проводити комплексний аналіз відповідності та безпеки. Окремо розглянуто сервіси виявлення загроз і механізми їх нейтралізації у масштабованих середовищах, а також представлено основні етапи реагування на інциденти: підготовку, виявлення, реагування та відновлення нормальної роботи систем.

Значну увагу приділено огляду підходів щодо шифрування даних у середовищах AWS, Azure та GCP. Проаналізовано методи шифрування під час передачі даних і в стані спокою, а також варіанти використання клієнтських ключів, що відповідає моделі спільної відповідальності та розширює контроль користувача над інформацією, яка зберігається у хмарі.

Отримані знання щодо моделей IAM, механізмів моніторингу, реагування на інциденти та варіантів шифрування формують цілісне уявлення про практики захисту даних у хмарних середовищах і забезпечують основу для вибору оптимальних рішень у конкретних сценаріях використання.

Контрольні питання до Розділу 2

1. Що таке API та яку роль вони відіграють у хмарних сервісах?
2. Чому публічна доступність API підвищує ризики кіберзагроз?
3. Назвіть чотири основні наслідки використання незахищених API.
4. Наведіть приклад SQL-ін’єкції через уразливий API.
5. Як відсутність перевірки вхідних даних може призвести до витоку даних?
6. Які ризики пов’язані з відсутністю механізмів контролю доступу до API?
7. Чим небезпечне зберігання ключів API у публічних репозиторіях?
8. Що таке безпечний життєвий цикл розробки (SDLC) у контексті API?
9. Чому важливо застосовувати автентифікацію та авторизацію до API?
10. Як перевірка вхідних даних допомагає запобігти атакам на API?
11. Які типи атак на рівні додатків можуть бути спрямовані на API?
12. Для чого проводять перевірку коду API перед розгортанням?
13. Чому необхідно шифрувати дані під час передачі через API?
14. Що дає підписування повідомлень API криптографічним ключем?
15. Як WAF допомагає у захисті API?
16. Яку роль відіграють служби захисту від DDoS в безпеці API?
17. Навіщо встановлювати обмеження швидкості (rate limiting) для API?
18. Як обмеження методів HTTP може знизити ризики атак?
19. Чому важливо моніторити використання API для виявлення аномалій?
20. Як перевірка схеми запитів на стороні сервера знижує ризики?
21. Які можливості AWS API Gateway надає для контролю доступу до API?
22. Як AWS WAF та AWS Shield працюють разом для захисту API?
23. Для чого AWS Secrets Manager використовується у контексті API?
24. Які сервіси Azure можна використати для виявлення атак на API?
25. Як Google CloudArmor захищає API від прикладних і DDoS-атак?

РОЗДІЛ 3. УПРАВЛІННЯ ЗАГРОЗАМИ ТА ДОТРИМАННЯ ВИМОГ

Після завершення цієї частини ви матимете ґрунтовне розуміння поширених загроз у хмарних середовищах та того, як дотримуватися стандартів і правил.

Ця частина посібника складається з наступних параграфів:

- *3.1. Розуміння поширених загроз безпеці хмарних обчислень*
- *3.2. Обробка нормативних актів щодо дотримання вимог*
- *3.3. Взаємодія з постачальниками хмарних послуг*

3.1. Розуміння поширених загроз безпеці хмарних обчислень

Знання загроз, з якими стикається ваша організація під час використання хмарних сервісів, дасть вам розуміння того, на що звертати увагу та як краще захистити свої хмарні середовища заздалегідь. Злом - це радше питання коли а не якщо, тому знання, представлені в цьому розділі, мають допомогти вам підготуватися до такої непередбачуваності.

В цьому розділі ми розглянемо наступні питання:

- Структура MITER ATT&CK.
- Виявлення та усунення порушень даних у хмарних сервісах.
- Виявлення та усунення неправильних конфігурацій у хмарних сервісах.
- Виявлення та зменшення недостатнього IAM у хмарних сервісах.
- Виявлення та зменшення крадіжки облікових записів у хмарних сервісах.
- Виявлення та зменшення внутрішніх загроз у хмарних сервісах.
- Виявлення та зменшення ризиків небезпечних API у хмарних сервісах.
- Виявлення та зменшення зловживань хмарними сервісами.

Технічні вимоги

Для цього розділу читач повинен мати ґрунтовне розуміння концепцій інформаційної безпеки. До них належать (але не обмежуються): *загрози*, *пом'якшення*, *витоки даних*, *неправильні конфігурації*, *викрадення облікового запису*, та інші.

Структура MITRE ATT&CK

MITRE ATT&CK Фреймворк -це база знань про методи злому. Хмарна матриця MITRE ATT&CK містить загальний потік кібератак:

- Початковий доступ
- Виконання
- Наполегливість
- Ескалація привілеїв
- Ухилення від оборони

- Доступ до облікових даних
- Відкриття
- Бічний рух
- Колекція
- Ексфільтрація
- Вплив

Розуміння методів атак дозволяє нам зрозуміти результати атак. Наприклад, використання *зловживання повноваження ми* дозволяє зловмиснику отримати постійний доступ до нашої системи.

Ще один приклад атаки –*виявлення хмарного сховища об'єктів*, який може використовувати зловмисник для отримання доступу до всіх об'єктів у екземплярі хмарного сховища.

Огляд усіх методів атак дозволить нам зрозуміти, які засоби контролю безпеки ми можемо впровадити для зменшення потенційних атак у нашому хмарному середовищі, будь то вбудовані інструменти безпеки з AWS, Azure або GCP, чи зовнішні інструменти сторонніх розробників.

Для отримання додаткової інформації зверніться до наступних ресурсів:
MITRE ATT&CK, Хмарна матриця: https://surl.li/goucrx
MITRE ATT&CK, матриця IaaS: https://surl.li/vserqs
MITRE ATT&CK, SaaS Matrix: https://surl.li/zayudb
Як покращити виявлення та пошук загроз у хмарі AWS за допомогою матриці MITRE ATT&CK: https://surl.li/sxuhhx

Виявлення та усунення порушень даних у хмарних сервісах

А витік даних, як випливає з назви, - це несанкціонований доступ до даних організації. Це може призвести до розкриття персональних даних клієнтів або співробітників і завдати шкоди репутації організації. Через модель спільної відповідальності хмарних обчислень нам потрібно по-іншому ставитися до витоків даних. Наприклад, ми не контролюємо фізичне зберігання наших даних. Це створює іншу модель загрози порівняно з традиційним локальним центром обробки даних, яким ми керуємо. Витоки даних більш імовірні під час роботи з публічними хмарними сервісами, оскільки в цьому випадку ми не контролюємо фізичне зберігання наших даних. Чи означає це, що зберігання наших даних у хмарі робить їх більш схильними до витоків даних? Це залежить від моделі хмарного сервісу та від зрілості постачальника хмарних послуг. Згідно з *модель спільної відповідальності*, при використанні інфраструктура як послуга(Інфраструктура як послуга (IAA)) рішення, ми (клієнти) відповідаємо за впровадження більшості заходів безпеки надопераційна система(ОС).

У платформі як послуга (PaaS) контексті ми покладаємося на постачальника хмарних послуг з точки зору посилення захисту ОС, керування виправленнями та резервного копіювання, але в PaaS дуже часто ми можемо переглядати

журнали аудиту та встановлювати відповідні дозволи для тих, хто має доступ до сервісу на рівні програми.

У програмні забезпечення як послуга(SaaS) контексті, все стає складніше. Немає стандарту для SaaS, тобто будь-хто, хто розгортає програму на віртуальній машині або знаходиться на публічному IaaS, може оголосити себе постачальником SaaS.

Залежно від рівня зрілості SaaS-провайдера, ми можемо мати можливість додавати засоби контролю безпеки (наприклад, шифрування даних у стані спокою), налаштовувати надійну автентифікацію (наприклад, SAML з багатофакторна автентифікація (МЗС)), підключення до журналів аудиту через REST API та інші.

Перш ніж говорити про витоки даних, спробуємо зосередитися на тому, які дані ми зберігаємо в хмарі.

Нижче наведено кілька прикладів даних, які ми можемо зберігати в хмарі:

1. *Публічні дані.* Дані, які ми можемо безпечно зберігати на загальнодоступних вебсайтах. Якщо такі дані будуть розкриті анонімними користувачами, це не зашкодить нашій організації (це можуть бути новинні сайти, курси валют, фізична адреса організації з *Зв'яжіться з нами* веб-сторінка тощо).

2. *Інтелектуальна власність/комерційна таємниця.* Це дані, які ми повинні зберігати в безпеці, оскільки їх розголошення зашкодить нашому бізнесу та вплине на нашу здатність отримувати дохід (прикладами інтелектуальної власності можуть бути дані фармацевтичної компанії, яка розробляє ліки від COVID-19, дані стартапу, який розробляє нову технологію для безпечної автентифікації без використання паролів тощо).

3. *Особисто ідентифікована інформація (Особиста інформація).* Включає будь-яку інформацію, що дозволяє ідентифікувати особу (наприклад, контактні дані, інформацію про кредитні картки, дані про здоров’я тощо).

Типові наслідки витоків даних

Внаслідок витоку даних з нашими даними може статися низка речей. Порушення конфіденційності може включати розкриття фінансових даних клієнтів або даних про охорону здоров'я, які потім можуть бути використані хакерами.

Цілісність даних. Це може включати доступ до основних систем банку та маніпулювання фінансовою інформацією клієнта; в результаті клієнт може помітити зміну балансу свого рахунку.

Наявність. Одним із наслідків витоку даних може бути використання програм-вимагачів, які шифрують дані цілі, роблячи їх недоступними.

Деякі з елементи керування що дозволяє нам зменшити витоки даних:

- *Мережевий рівень.* Налаштування контролю доступу (мережа Списки контролю доступу (ACL), групи безпеки тощо) для контролю доступу до наших ресурсів.

- *Шифрування.* Впроваджуйте шифрування під час передачі та зберігання. Це дозволяє нам завжди зберігати конфіденційність наших даних.
- *Аудит.* Дозволяє нам відстежувати, хто отримував доступ (або намагався отримати доступ) до наших ресурсів, і які дії були здійснені (наприклад, через API) пов'язані з ресурсами.
- *Управління загрозами.* Дозволяє нам переглядати журнали та виявляти потенційні загрози для наших сервісів.
- *Стратегія відновлення.* Підготуйте план аварійного відновлення. Наприклад, технічні резервні копії та знімки томів, баз даних і процесів. Він також повинен включати процедури відновлення даних (наприклад, які системи відновлювати в першу чергу, як автоматизувати відновлення за допомогою інфраструктури як коду тощо).

Деякі з найкращих практик:

- Використовуйте безпечний життєвий цикл розробки Вбудуйте це як частину вашого процесу розробки - це включає такі елементи керування, як наведено нижче
- Аутентифікація та авторизація: Забезпечте доступ до вашої програми та даних.
- Перевірка вхідних даних Перевірте та підтвердьте, які рядки та/або дані можна вставляти у вашу програму та базу даних сервера.
- Атаки на рівні додатків Виявлення та зменшення наслідків атак, таких як атаки з впровадженням коду, міжсайтовий скриптинг та інші.
- Використання списків контролю доступу: Встановіть правила мережі/брандмауера, щоб налаштувати, хто може отримувати доступ до ваших ресурсів (як для вхідного, так і для вихідного мережевого трафіку)
- Використовуйте журнали аудиту: Вони дозволяють вам контролювати доступ до ресурсів та виконані дії.
- Перевірте цілісність ваших даних Переконайтеся, що збережені дані не були змінені.
- Використовуйте управління змінами Перевірте наявність відхилень від попередньо налаштованих параметрів (наприклад, служби, що мають публічний доступ, або сервери, які можуть потребувати посилення захисту тощо).
- Використовуйте класифікацію даних Поєднайте це з послугами витоку даних, щоб допомогти виявити витік даних.
- Використовуйте шифрування Забезпечте конфіденційність ваших даних під час передачі та зберігання.

Налаштування політик для всієї організації. Наприклад, використовуйте успадковані політики, які визначають, хто має доступ до яких ресурсів і які дії можна виконувати з ресурсами, забезпечуйте аудит, забезпечуйте шифрування тощо.

Використовуйте резервні копії Це дозволяє відновити ваші дані та програми після витоку даних.

Загальні сервіси AWS для допомоги у виявленні та усуненні наслідків порушень даних

Деякі поширені сервіси AWS, які можна використовувати для зменшення витоків даних:

- Використання Amazon VPC елементи керування (наприклад, мережеві ACL та групи безпеки) та Мережевий брандмауер AWS налаштувати правила вхідного та вихідного доступу до мережі.
- Використання AWS IAM щоб налаштувати, хто може автентифікувати та отримувати доступ до ваших програм, ресурсів і даних.
- Використання AWS KMS шифрувати ваші дані, щоб запобігти витокам даних.
- Використання Менеджер таємниць AWS щоб захистити ваші таємниці (ключі доступу, паролі, облікові дані тощо) від витоків даних.
- Використання AWS CloudTrail для виявлення активності API (для користувачів, комп'ютерів блікових записів служб тощо), яка може свідчити про витік даних.
- Використання Amazon CloudWatch реєструвати та сповіщати про підозрілу діяльність, яка перевищує певні порогові значення (наприклад, кілька невдалих спроб входу).
- Використання Amazon Guard Duty для виявлення порушень даних.
- Використання Журнали потоку AWS VPC для перевірки мережевої активності, яка може свідчити про порушення даних.
- Використання Конфігурація AWS для виявлення змін конфігурації у вашому середовищі та хмарних ресурсах.
- Використання Detective Amazonки виявити першопричину витоку даних.
- Використання Резервне копіювання AWS для відновлення вашого середовища після витоку даних.

Загальні служби Azure для допомоги у виявленні та усуненні наслідків порушень даних

Деякі поширені служби Azure, які можна використовувати для зменшення витоків даних:

- Використання групи безпеки мережі Azure (НСГ) для налаштування правил вхідного та вихідного доступу до мережі.
- Використання Azure Active Directory (AD), щоб налаштувати, хто може автентифікувати та отримувати доступ до ваших програм, ресурсів і даних.
- Використання сховища ключів Azure зашифрувати ваші дані, щоб запобігти витокам даних.

- Використання конфіденційних обчислень Azure щоб захистити ваші дані від витоків даних.
- Використання Монітор Azurei та Аналіз журналів для виявлення підозрілих дій, які можуть свідчити про витік даних.
- Використання Захисник Azure (раніше відомий як Розширений захист від загроз Azure) для виявлення неправильних конфігурацій, які можуть призвести до витоку даних.
- Використання Спостерігач мережі Azure для перевірки мережевої активності, яка може свідчити про порушення даних.
- Використання Центр безпеки Azure для сприяння у виявленні порушень даних.
- Використання Azure Guardian зіставити кілька джерел даних для сприяння виявленню порушень безпеки даних.
- Використання Резервне копіювання Azure для відновлення вашого середовища після витоку даних.

Загальні послуги GCP для сприяння виявленню та усуненню наслідків порушень даних

Деякі поширені сервіси GCP, які можна використовувати для зменшення витоків даних:

- Використання Правила брандмауера GCP VPC налаштувати правила вхідного та вихідного доступу до мережі.
- Використання Google Cloud IAM щоб налаштувати, хто може автентифікувати та отримувати доступ до ваших програм, ресурсів і даних.
- Використання Google Cloud KMS зашифрувати ваші дані, щоб запобігти витокам даних.
- Використання Менеджер таємниць Google щоб захистити ваші таємниці (ключі доступу, паролі, облікові дані тощо) від витоків даних.
- Використання Конфіденційні обчислення GCP щоб захистити ваші дані від витоків даних.
- Використання Ведення журналу в хмарі Google для виявлення підозрілих дій, які можуть свідчити про витік даних.
- Використання Журнали потоку GCP VPC для перевірки мережевої активності, яка може свідчити про порушення даних.
- Використання Центр керування безпекою хмари Google зіставити кілька джерел даних для сприяння виявленню порушень безпеки даних.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Майже 80% компаній зазнали витоку хмарних даних за останні 18 місяців: https://surl.li/ynnvqf

Виявлення та усунення неправильних конфігурацій у хмарних сервісах

Неправильні конфігурації є поширеною загрозою під час використання хмарних сервісів. Згідно з *модель спільної відповідальності* Деякі поширені причини неправильної конфігурації хмарних сервісів, які підпадають під відповідальність клієнта, наведені нижче:

- Брак знань з експлуатації хмарних сервісів.
- Людська помилка.
- Налаштування за замовчуванням залишаються в незахищеному стані.
- Великі та складні середовища розгортаються за дуже короткий час.
- Швидкі та некеровані зміни в хмарних середовищах.

Кілька поширених прикладів неправильних конфігурацій у хмарних сервісах:

- Надто широкі політики IAM (або політики контролю доступу на основі ролей) - наприклад, дозволи за замовчуванням, які дозволяють користувачам виконувати дії з конфіденційними ресурсами, або наявність більшої кількості дозволів, ніж потрібно для виконання їхніх щоденних завдань.
- Сховище об'єктів є загальнодоступним для будь-кого в Інтернеті.
- Знімки та образи віртуальних машин публічно доступні будь-кому в Інтернеті.
- Бази даних є загальнодоступними для будь-кого в Інтернеті.
- Віртуальні сервери публічно доступні будь-кому в Інтернеті, хто їх використовує Безпечна оболонка(SSH) або Протокол віддаленого робочого столу(ПРП) порти.

Непатчені сервери та бази даних

Деякі найкращі практики для виявлення та усунення неправильних конфігурацій у хмарних середовищах:

- Використовуйте політики конфігурації організації для забезпечення бажаних конфігурацій, таких як зашифроване сховище, блокування публічного доступу до ресурсів тощо.
- Безпека у великомасштабних середовищах).
- Використовуйте інфраструктуру як код для автоматизації та стандартних конфігурацій.
- Використання Управління станом безпеки хмари(CSPM) для виявлення неправильних конфігурацій.
- Скануйте на наявність неправильних конфігурацій (таких як використання вразливих компонентів) як частину процесу збірки.
- Використання управління змінами перевірити наявність відхилень від попередньо налаштованих параметрів (наприклад, служби, які можуть мати публічний доступ, або сервери, які можуть потребувати посилення захисту тощо).

- Обмежте доступ до виробничих середовищ до необхідного мінімуму (як за допомогою мінімальних дозволів, так і за допомогою мережевого контролю доступу) - не дозволяйте розробникам або кінцевим користувачам доступ до виробничих середовищ.
- Проводити навчання співробітників щодо правильного використання різних хмарних сервісів.
- Перегляньте, які ідентифікаційні дані у вашій організації потребують доступу до хмарних ресурсів, і керуйте ними за потреби.

В наступному розділі ми розглянемо поширені сервіси від AWS, Azure та GCP, які дозволять вам виявляти та усувати неправильні конфігурації.

Загальні сервіси AWS для допомоги у виявленні та усуненні помилок у конфігураціях

Деякі сервіси AWS, які можуть зменшити кількість помилок у конфігураціях:

- Використання AWS IAM щоб налаштувати, хто може автентифікувати та отримувати доступ до ваших програм, ресурсів і даних.
- Використання Аналізатор доступу AWS IAM для виявлення користувачів, які давно не використовували свої облікові записи, наприклад, для доступу до кількох облікових записів в AWS із публічним доступом до таких ресурсів, як Amazon S3та AWS KMS.
- Використовуйте Amazon GuardDuty для виявлення неправильних конфігурацій, таких як AWS EC2намагається отримати доступ командно-контрольний (Командування та контроль) мережі, загальнодоступний для Інтернету контейнер S3 та багато іншого.
- Використання Конфігурація AWS виявляти зміни конфігурації у вашому середовищі та хмарних ресурсах і порівнювати їх з відповідними політиками відповідності.
- Використання Центр безпеки AWS відстежувати події з кількох сервісів AWS та виявляти неправильні конфігурації, що не відповідають стандартам політики.
- Використання Інспектор AWS Amazon для виявлення неправильних конфігурацій, таких як відхилення від Центру інтернет-безпеки (СНД) посилення тестів безпеки, відсутність патчів безпеки тощо.
- Використання Менеджер аудиту AWS для виявлення неправильних конфігурацій, що не відповідають стандартам відповідності.
- Використання Довірений радник AWS переглянути поширені помилки конфігурації безпеки.
- Використання Диспетчерська вежа AWS централізовано застосовувати конфігурації на всіх рівнях організації AWS (наприклад, блокування публічного доступу S3, блокування можливостей користувачів, таких як розгортання віртуальних серверів тощо).

- Використання AWS Cloud Formation розгортати нові хмарні середовища стандартизованим способом.

Загальні служби Azure для допомоги у виявленні та усуненні помилок конфігурації

Деякі служби Azure, які можуть зменшити кількість неправильних конфігурацій:

- Використання Azure AD щоб налаштувати, хто може автентифікувати та отримувати доступ до ваших програм, ресурсів і даних.
- Використовуйте Активність у Azure журнал, який є частиною Azure Monitor, щоб виявити, які дії були виконані у вашому середовищі Azure.
- Використання Захисник Microsoft для хмари для виявлення неправильних конфігурацій безпеки в різних сервісах Azure.
- Використання Консультант Azure переглянути поширені помилки конфігурації безпеки.
- Використання Політика Azurei Групи керування Azure централізовано застосовувати конфігурації на всій Орендар Azure рівні (наприклад, блокування публічного доступу до сховища BLOB-об'єктів, блокування можливостей користувачів, таких як розгортання віртуальних серверів тощо).
- Використання Диспетчер ресурсів Azure розгортати нові середовища стандартним способом.

Загальні сервіси GCP для допомоги у виявленні та усуненні помилок у конфігураціях

Деякі поширені сервіси GCP, які можна використовувати для зменшення помилок у конфігураціях:

- Використання Google Cloud IAM щоб налаштувати, хто може автентифікувати та отримувати доступ до ваших програм, ресурсів і даних.
- Використання Ведення журналу в хмарі Google щоб виявити, які дії були виконані у вашому середовищі GCP.
- Використання Центр керування безпекою хмари Google для виявлення неправильних конфігурацій безпеки в різних сервісах GCP.
- Використання Менеджер ресурсів GCP централізовано застосовувати конфігурації для всіх рівнів організації GCP (наприклад, обмеження створення облікових записів служби, обмеження розташування ресурсів тощо).
- Використання Менеджер розгортання Google Cloud розгортати нові середовища стандартним способом.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Неправильні конфігурації: прихована, але запобіжна загроза для хмарних даних: https://surl.li/tcjaec
Неправильна конфігурація хмари - серйозний ризик для безпеки хмари: https://surl.li/sqpjpb

Виявлення та зменшення недостатнього управління IAM та ключами в хмарних сервісах

Недостатньо IAM може статися в сценарії, коли у нас є велика кількість ідентифікаційних даних користувачів (наприклад, у корпоративній організації), але ми не можемо належним чином керувати цими ідентифікаційними даними. Або ми можемо використовувати криптографію для захисту конфіденційних даних, але не дотримуватися найкращих практик ротації ключів, і в результаті збільшуємо ймовірність витоку даних неавторизованими особами.

Деякі поширені наслідки недостатнього управління IAM та ключами:

- Невиконання принцип найменш привілейованих, що призводить до надання надмірної кількості дозволів.
- Не налаштування засобів контролю доступу - наприклад, надання несанкціонованого доступу до конфіденційних даних (таких як особиста інформація, дані кредитних карток, дані про охорону здоров'я тощо), що призводить до розкриття облікових даних.
- Недотримання політики щодо паролів (наприклад, дозвіл на короткі паролі, відсутність обов'язкової зміни паролів, дозвіл на повторне використання паролів тощо), що призводить до атак методом перебору паролів.
- Шифрування даних зі збереженням того самого криптографічного ключа без його ротації, що потенційно може призвести до порушення конфіденційності даних.
- Незастосування дотримання правил використання багатофакторної автентифікації (MFA), що може призвести до несанкціонованого доступу до ресурсів і даних.
- Вбудовування облікових даних або криптографічних ключів у код і скрипти, що може призвести до розкриття облікових даних.
- Не налаштовування журналів аудиту, що призводить до недостатньої видимості того, які ідентифікатори мають доступ до яких ресурсів.

Деякі найкращі практики для виявлення та зменшення недостатнього IAM у хмарних середовищах:

- Керуйте всім життєвим циклом ідентифікації для ваших співробітників та будь-яких субпідрядників, які мають доступ до ваших систем і даних - це має включати набір персоналу, надання облікових записів, керування доступом до ресурсів і, нарешті, скасування надання облікових записів, коли співробітник або субпідрядник звільнився з організації або більше не потребує доступу до систем даних.
- Використовуйте централізоване сховище для ідентифікаційних даних, де ви надаєте та видаляєте облікові записи, також встановлюєте політики паролів.
- Використовуйте федерацію, щоб дозволити доступ з локальних середовищ до хмарних середовищ і ресурсів, а також між системами IAM зовнішніх партнерів або клієнтів і вашими хмарними середовищами.

- Блокувати використання слабких та застарілих протоколів автентифікації (таких як Менеджер локальної мережі з новими технологіями (NTLM) та відкритий текст Легкий протокол доступу до каталогів (LDAP)).
- Забезпечте дотримання політики щодо паролів (наприклад, встановивши мінімальну довжину пароля, мінімальний та максимальний вік пароля, історію паролів, складні паролі, налаштування блокування та скасування облікового запису тощо).
- Забезпечити використання багатосторонньої аварійної допомоги (MFA).
- Перевіряти дії користувачів та співвідносити їхню діяльність за допомогою Інформація про безпеку та управління подіями (CIEM) система, яка дозволить вам виявляти аномальну поведінку (наприклад, вхід користувачів до системи після робочого часу, спроби користувачів отримати доступ до ресурсів вперше тощо).
- Переглядайте дії користувачів під час входу в систему. Якщо користувач не використовував свій обліковий запис протягом кількох тижнів, можливо, настав час заблокувати або деактивувати обліковий запис через неактивність, що також є частиною найменші привілеї принцип.
- Впроваджуйте управління ідентифікацією - чи мають потрібні користувачі потрібні ролі у потрібний час?
- Перегляньте права доступу користувачів, знайдіть облікові записи зі стандартними або розширеними дозволами, які не потрібні, та налаштуйте права облікових записів.
- Дотримуйтесь принципу найменші привілеї під час надання дозволів на доступ до ресурсів.
- Дотримуйтесь концепції розподіл обов'язків щоб уникнути наявності у окремих користувачів прав на виконання конфіденційних дій (наприклад, користувача з правами як на генерування ключів шифрування, так і на їх використання).
- Використовуйте безпечне централізоване сховище для створення, зберігання, отримання та ротації ключів шифрування.
- Використовуйте службу керування секретами для створення, зберігання, отримання та ротації таємниць, паролів, ключів API та ключів доступу всередині коду для доступу до ресурсів, зберігаючи при цьому таємниці захищеними та зашифрованими.
- Шифруйте всю конфіденційну інформацію (наприклад, особисті дані, номери кредитних карток, дані про здоров’я тощо).

Загальні сервіси AWS для допомоги у виявленні та усуненні недоліків у управлінні IAM та ключами

Деякі поширені сервіси AWS, які можна використовувати для зменшення недостатнього управління IAM та ключами:

- Використання AWS IAM налаштувати, хто може автентифікувати та отримувати доступ до ваших програм, ресурсів і даних, а також запровадити політики паролів.

- Використання Аналізатор доступу AWS IAM щоб виявити користувачів, які тривалий час не користувалися своїми обліковими записами.
- Використання Служба каталогів AWS налаштувати, хто може автентифікувати та отримувати доступ до вашої спадщини (на основі Аутентифікація Kerberos) серверів і програм, а також для забезпечення дотримання політик паролів.
- Забезпечте використання багатофакторної автентифікації (MFA), щоб уникнути успішного використання облікових даних користувачів для доступу до ваших програм і систем.
- Використання AWS KMS генерувати, зберігати та ротувати ключі шифрування.
- Використання Менеджер таємниць AWS для створення, зберігання та ротації таємниць (наприклад, облікових даних, ключів доступу, паролів тощо).
- Використання AWS CloudTrail для виявлення активності API, такої як невдалі спроби входу.

Загальні служби Azure для виявлення та усунення недоліків у сфері IAM та управлінні ключами.

Деякі поширені служби Azure, які можна використовувати для зменшення недостатнього управління IAM та ключами:

- Використання Azure AD налаштувати, хто може автентифікувати та отримувати доступ до ваших програм, ресурсів і даних, а також запровадити політики паролів.
- Використання Служби доменів Azure AD налаштувати, хто може автентифікувати та отримувати доступ до ваших застарілих серверів, програм, ресурсів і даних (на базі Kerberos), а також використовувати це для забезпечення дотримання політик паролів.
- Забезпечте використання багатофакторної автентифікації (MFA), щоб уникнути успішного використання облікових даних користувачів для доступу до ваших програм і систем.
- Використання Умовний доступ Azure AD застосовувати різні методи доступу та автентифікації, коли користувачі підключаються з корпоративної мережі, а не з невідомої IP-адреси.
- Використання Керування привілейованими ідентифікаторами Azure (ПІМ), щоб обмежити дозволи користувачів на доступ до ваших ресурсів Azure.
- Використання Сховище ключів Azure для створення, зберігання та ротації ключів шифрування та таємниць (наприклад, облікових даних, ключів доступу, паролів тощо).
- Увімкнути Журнали аудиту Azure AD і використовувати Аналітика журналів Azure для виявлення таких дій, як невдалі спроби входу.
- Використання Захист інформації Azure для виявлення подій збоїв автентифікації.

- Використання Azure Guardian зіставляти журнали з кількох джерел журналів для виявлення невдалих спроб входу.
- Використання Скринька клієнта Azure виявляти спроби входу Майкрософт інженери підтримки.

Загальні послуги GCP для сприяння виявленню та усуненню недоліків у сфері управління ідентифікацією та доступністю (IAM) та ключами.

Деякі поширені сервіси GCP, які можна використовувати для зменшення недостатнього управління ідентифікацією та доступом:

- Використання Google Cloud IAM налаштувати, хто може автентифікувати та отримувати доступ до ваших програм, ресурсів і даних, а також запровадити політики паролів.
- Використовуйте Керований сервіс Google для Майкрософт Active Directory налаштувати, хто може автентифікувати та отримувати доступ до ваших застарілих (на базі Kerberos) серверів і програм, ресурсів і даних, а також використовувати це для забезпечення дотримання політик паролів.
- Забезпечте використання багатофакторної автентифікації (MFA), щоб уникнути успішного, але несанкціонованого використання облікових даних користувачів для доступу до ваших програм і систем.
- Використання Google Cloud KMS генерувати, зберігати та ротувати ключі шифрування.
- Використання Менеджер таємниць Google для створення, зберігання та ротації таємниць (наприклад, облікових даних, ключів доступу, паролів тощо).
- Використання Ведення журналу в хмарі Google для виявлення таких дій, як невдалі спроби входу.
- Використання Центр керування безпекою хмари Google зіставляти журнали з кількох джерел журналів для виявлення невдалих спроб входу.
- Використання Прозорість доступу Google і Схвалення доступу для виявлення спроб входу інженерів служби підтримки Google.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Чи захищені ваші хмарні середовища від атак на основі ідентифікації?: https://surl.lu/oamybz

Виявлення та зменшення крадіжки облікових записів у хмарних сервісах

Викрадення облікового запису трапляється, коли обліковий запис (що належить людині або системному/ програмному/сервісному обліковому запису) скомпрометовано, і неавторизована особа отримує доступ до використання ресурсів і даних від імені (зазвичай з високими привілеями) скомпрометованого облікового запису.

Деякі поширені наслідки крадіжки облікового запису:

- Несанкціонований доступ до ресурсів.
- Витік та розкриття даних.
- Видалення даних.
- Компрометація системи.
- Крадіжка особистих даних.
- Зараження програмою-вимагачем або шкідливим кодом.
- Блокування облікового запису.
- Відмова в послугах.
- Відмова від гаманця (можливі величезні витрати на хмарні ресурси через неправильне використання ресурсів, таке як майнінг біткойнів).
- Пошкодження веб-сайту.

Деякі поширені методи крадіжки облікового запису такі:

- Фішингові атаки проти облікового запису системного адміністратора, що дозволяє зловмиснику отримати доступ до баз даних з даними клієнтів.
- Ключі доступу для привілейованого облікового запису, що зберігалися у загальнодоступному корзині S3, і в результаті хакери могли використовувати ключі доступу для розгортання кількох дорогих віртуальних машин для майнінгу біткойнів.
- Слабкі паролі адміністратора, що дозволяють зловмисникам отримати контроль над правами адміністратора та змінити дозволи, щоб надати публічний доступ до резервних копій, що містять фінансову інформацію клієнтів.

Деякі найкращі методи виявлення та запобігання крадіжці облікового запису:

- Забезпечте використання надійних паролів (наприклад, встановивши мінімальну довжину пароля, мінімальний та максимальний вік пароля, історію паролів, складні паролі, налаштування блокування та скасування облікового запису тощо).
- Забезпечити використання багатосторонньої аварійної допомоги (MFA).
- Перевіряти дії користувачів та співвідносити їхню активність за допомогою SIEM-системи, яка дозволить виявляти аномальну поведінку (наприклад, вхід користувачів після робочого часу, спроби користувачів отримати доступ до ресурсів вперше тощо).
- Дотримуйтесь принципу найменші привілеї під час надання дозволів на доступ до ресурсів.
- Дотримуйтесь концепції розподіл обов'язків щоб уникнути того, щоб один користувач мав право виконувати конфіденційні дії (наприклад, користувач з дозволами як на генерування ключів шифрування, так і на їх використання).
- Інвестуйте в обізнаність співробітників, щоб усі вони могли виявляти спроби фішингу, уникати відкриття електронних листів з невідомих джерел,

уникати запуску невідомих виконуваних файлів та уникати підключення знімних носіїв з невідомих джерел.

- Інвестуйте в планування забезпечення безперервності бізнесу, щоб підготуватися до відновлення після компрометації системи (наприклад, перебудови систем, відновлення даних із резервних копій, зміни облікових даних тощо).

Загальні сервіси AWS для допомоги у виявленні та усуненні наслідків викрадення облікових записів

Деякі поширені сервіси AWS для захисту від крадіжки облікових записів наведені нижче:

- Використання AWS IAM налаштувати, хто може автентифікувати та отримувати доступ до ваших програм, ресурсів і даних, а також запровадити політики паролів.
- Використання Аналізатор доступу AWS IAM щоб виявити користувачів, які тривалий час не користувалися своїми обліковими записами.
- Використання Служба каталогів AWS налаштувати, хто може автентифікувати та отримувати доступ до ваших застарілих серверів і програм (на базі Kerberos), а також застосовувати політики паролів.
- Забезпечте використання багатофакторної автентифікації (MFA), щоб уникнути успішного використання облікових даних користувачів для доступу до ваших програм і систем.
- Використання Amazon Guard Duty для виявлення компрометації облікового запису.
- Використання AWS CloudTrail для виявлення активності API, такої як невдалі спроби входу.
- Використання Резервне копіювання AWS щоб відновити ваше хмарне середовище після викрадання облікового запису.

Загальні служби Azure для виявлення та усунення наслідків викрадення облікового запису

Деякі поширені служби Azure для захисту від крадіжки облікового запису наведено нижче.

- Використання Azure AD налаштувати, хто може автентифікувати та отримувати доступ до ваших програм, ресурсів і даних, а також запровадити політики паролів.
- Використання Служби доменів Azure AD налаштувати, хто може автентифікувати та отримувати доступ до ваших застарілих (на базі Kerberos) серверів і програм, ресурсів і даних, а також використовувати це для забезпечення дотримання політик паролів.
- Забезпечте використання багатофакторної автентифікації (MFA), щоб уникнути успішного використання облікових даних користувачів для доступу до ваших програм і систем.

- Використання Умовний доступ Azure AD щоб забезпечити різні рівні доступу та різні методи автентифікації, коли користувачі підключаються з корпоративної мережі, а не з невідомої IP-адреси.
- Використання Azure PIM щоб обмежити дозволи користувачів на доступ до ваших ресурсів Azure.
- Увімкніть журнали аудиту Azure AD та використовуйте Azure Log Analytics для виявлення таких дій, як невдалі спроби входу.
- Використання Захист інформації Azure для виявлення подій збоїв автентифікації.
- Використання Azure Guardian зі ставляти журнали з кількох джерел журналів для виявлення невдалих спроб входу.
- Використання Резервне копіювання Azure щоб відновити ваше хмарне середовище після викрадання облікового запису.

Загальні сервіси GCP для виявлення та пом'якшення наслідків викрадення облікового запису

Деякі сервіси GCP, які можуть захистити від крадіжки облікового запису:

- Використання Google Cloud IAM налаштувати, хто може автентифікувати та отримувати доступ до ваших програм, ресурсів і даних, а також запровадити політики паролів.
- Використовуйте Керований сервіс Google для Microsoft Active Directory, щоб налаштувати, хто може автентифікувати та отримувати доступ до ваших застарілих серверів і програм (на базі Kerberos), ресурсів і даних, а також використовувати це для забезпечення дотримання політик паролів.
- Забезпечте використання багатофакторної автентифікації (MFA), щоб уникнути успішного використання облікових даних користувачів для доступу до ваших програм і систем
- Використання Ведення журналу в хмарі Google для виявлення таких дій, як невдалі спроби входу
- Використання Центр керування безпекою хмари Google зіставляти журнали з кількох джерел журналів для виявлення невдалих спроб входу.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Що таке хмарний джекінг? Як захистити свої дані, що зберігаються в хмарі: https://surl.lt/yxzrhe

Виявлення та зменшення внутрішніх загроз у хмарних сервісах

Внутрішня загроза це концепція, де уповноважений працівник (тобто*інсайдер*) виконує дію (зловмисно або випадково), яку не повинен був робити. Деякі поширені наслідки внутрішніх загроз такі:

- Втрата даних
- Витік даних
- Простої системи
- Втрата репутації компанії

- Грошові втрати внаслідок судових позовів

Деякі поширені приклади внутрішніх загроз наведені нижче:

- Адміністратор натискає на фішинговий електронний лист з невідомого джерела, в результаті чого файловий сервер заражається програмою-вимагачем, і всі файли шифруються.
- Працівник, який має право доступу до бухгалтерської системи, залишає свій ноутбук без нагляду, а неавторизована особа заволодіває його ноутбуком і краде дані клієнтів.
- Субпідрядник, який має доступ до баз даних з адресами електронної пошти клієнтів, експортує дані клієнтів та продає їх у даркнеті.

Деякі найкращі практики виявлення та зменшення внутрішніх загроз у хмарних середовищах наведено нижче:

- Інвестуйте в перевірку біографічних даних, перш ніж наймати працівників або субпідрядників.
- Забезпечте використання надійних паролів (наприклад, встановивши мінімальну довжину пароля, мінімальний та максимальний вік пароля, історію паролів, складні паролі, налаштування блокування та скасування облікового запису тощо).
- Перевіряти дії користувачів та співвідносити їхню активність за допомогою SIEM-системи, яка дозволить виявляти аномальну поведінку (наприклад, вхід користувачів після робочого часу, спроби користувачів отримати доступ до ресурсів вперше тощо).
- Дотримуйтесь принципу *найменші привілеї* під час надання дозволів на доступ до ресурсів.
- Дотримуйтесь концепції *розподіл обов'язків* щоб уникнути того, щоб окремі користувачі мали привілеї виконувати конфіденційні дії (наприклад, користувач з дозволами як на створення ключів шифрування, так і на їх використання).
- Забезпечте використання багатофакторної автентифікації (MFA), щоб мінімізувати ризик отримання зловмисниками контролю над обліковим записом внутрішнього співробітника без його відома, щоб отримати доступ до внутрішніх систем і даних.
- Інвестуйте в обізнаність співробітників, щоб усі вони могли виявляти спроби фішингу, уникати відкриття електронних листів з невідомих джерел, уникати запуску невідомих виконуваних файлів та уникати підключення знімних носіїв з невідомих джерел.
- Інвестуйте в планування забезпечення безперервності бізнесу, щоб підготуватися до відновлення після компрометації системи (наприклад, перебудови систем, відновлення даних із резервних копій, зміни облікових даних тощо).

- Шифруйте конфіденційні дані клієнтів і переконайтеся, що доступ до ключів шифрування обмежений лише уповноваженим персоналом, з аудитами всього процесу шифрування/ дешифрування ключів.
- Зберігайте резервні копії поза межами офісу та перевіряйте весь доступ до резервних копій.

Загальні сервіси AWS для допомоги у виявленні та усуненні внутрішніх загроз

Деякі сервіси AWS, які можуть захистити від внутрішніх загроз:

- Використання Amazon Guard Duty для виявлення аномальної поведінки у ваших облікових записах.
- Використання AWS CloudTrail для виявлення активності API, такої як доступ авторизованих користувачів до системи після робочого часу або виконання надмірної кількості дій, таких як завантаження кількох файлів, великі дії вибору з баз даних тощо.
- Використання AWS KMS шифрувати ваші дані та контролювати, хто має доступ до ключів шифрування.
- Використання Менеджер таємниць AWS зберігати таємниці (наприклад, облікові дані, ключі доступу, паролі тощо) та контролювати, хто має доступ до цих таємниць.
- Після виявлення компрометації облікового запису обов'язково замініть облікові дані, секретні дані та ключі шифрування належним чином.

Загальні служби Azure для сприяння виявленню та усуненню внутрішніх загроз

Деякі служби Azure, які можуть захистити від внутрішніх загроз:

- Використання Умовний доступ Azure AD застосовувати різні методи доступу та автентифікації, коли користувачі підключаються з корпоративної мережі, а не з невідомої IP-адреси.
- Використання Azure PIM щоб обмежити дозволи користувачів на доступ до ваших ресурсів Azure.
- Увімкнути Azure AD журнали аудиту та використовувати Azure Log Analytics для виявлення таких дій, як невдалі спроби входу.
- Використання Azure Guardian зіставляти журнали з кількох джерел журналів для виявлення таких дій, як доступ авторизованих користувачів до системи після робочого часу або виконання надмірних дій, таких як завантаження кількох файлів, великі дії вибору з баз даних тощо.
- Використання Сховище ключів Azure шифрувати ваші дані та контролювати, хто має доступ до ключів шифрування.
- Використання Сховище ключів Azure зберігати таємниці (наприклад, облікові дані, ключі доступу, паролі тощо) та контролювати, хто має доступ до цих таємниць.
- Після виявлення компрометації облікового запису замініть облікові дані, секретні дані та ключі шифрування належним чином.

Загальні послуги GCP для сприяння виявленню та усуненню внутрішніх загроз

Деякі сервіси GCP, які можуть захистити від внутрішніх загроз:

- Використання Ведення журналу в хмарі Google для виявлення таких дій, як невдалі спроби входу.
- Використання Центр керування безпекою хмари Google зіставляти журнали з кількох джерел журналів для виявлення невдалих спроб входу.
- Використання Хмарна система керування ключами GCP шифрувати ваші дані та контролювати, хто має доступ до ключів шифрування.
- Використання Менеджер таємниць Google зберігати таємниці (наприклад, облікові дані, ключі доступу, паролі тощо) та контролювати, хто має до них доступ.
- Після виявлення компрометації облікового запису замініть облікові дані, секретні дані та ключі шифрування належним чином.

Для отримання додаткової інформації зверніться до наступних ресурсів:
П'ять порад щодо захисту хмарних ресурсів від внутрішніх загроз: https://surl.li/xvyyne
Що таке внутрішня загроза?: https://surl.li/pinoxi

Виявлення та зменшення ризиків небезпечних API у хмарних сервісах

У сучасному світі всі сучасні розробки базуються на Інтерфейси прикладного програмування(API) для зв'язку між компонентами системи, здебільшого на основі веб-сервісів (використовуючи Простий протокол доступу до об'єктів(МИЛО)) або REST API. Той факт, що API публічно доступні, робить їх легкою мішенню для зловмисників, які намагаються отримати доступ до системи та завдати шкоди. Деякі поширені наслідки незахищених API такі:

- Витоки даних
- Витік даних
- Пошкодження цілісності даних
- Відмова в обслуговуванні

Деякі поширені приклади атак, що використовують незахищені API, наведені нижче:

- Через відсутність перевірки вхідних даних зловмисник може неправильно використовувати розкритий API та впроваджувати шкідливий код через API у серверну базу даних.
- Через відсутність перевірки вхідних даних зловмисник може виконати SQL-ін'єкцію через розкритий API та викрасти дані клієнтів з сайту роздрібної торгівлі.
- Через відсутність механізмів контролю доступу до програм, зловмисник може використовувати API для проникнення в хмарний сервіс, використовуючи обліковий запис з низькими привілеями.

- Зловмисник знайшов ключ API, що зберігається у репозиторії з відкритим вихідним кодом, і зміг виконати віддалені команди проти внутрішньої системи, використовуючи дозволи, які мав ключ API.

Деякі найкращі практики для виявлення та зменшення ризиків небезпечних API у хмарних середовищах:

- Використовуйте безпечний життєвий цикл розробки. Вбудуйте це як частину вашого процесу розробки - це включає такі елементи керування, як наведено нижче.
- Аутентифікація та авторизація. Забезпечити доступ до API.
- Перевірка вхідних даних. Перевірити та підтвердити, які рядки та/або дані можна вставляти в API.
- Атаки на рівні додатків Виявлення та зменшення наслідків таких атак, як атаки ін'єкцій, міжсайтовий скриптинг тощо.
- Проводьте перевірки коду для всіх ваших API.
- Шифрувати дані під час передачі за замовчуванням для всіх API.
- Підписуйте кожне повідомлення через API за допомогою криптографічного ключа, щоб уникнути підробки даних або зміни їх цілісності.
- Використовуйте брандмауер веб-застосунків(ВАФ) для захисту від відомих атак на рівні додатків.
- Використання розподілена відмова в обслуговуванні(DDoS-атак) служби захисту для захисту служби API від атак типу «відмова в обслуговуванні».
- Використовуйте XML-шлюз для захисту сервісу від атак на основі SOAP або REST API.
- Встановіть обмеження швидкості для API, щоб зменшити ймовірність автоматизованих атак.
- Обмежте тип методів HTTP до необхідного мінімуму (наприклад, GET без POST або DELETE).
- Перевіряти використання відкритих API та серверних систем для виявлення аномальної поведінки (наприклад, атак методом повного перебору або витоку даних).
- Виконайте перевірку схеми на стороні сервера, щоб переконатися, що через API можуть проходити лише добре відомі розміри полів, символи або регулярні вирази.

Загальні сервіси AWS для допомоги у виявленні та усуненні небезпечних API

Деякі сервіси AWS, які можуть забезпечити захист від незахищених API:

- Використання Шлюз Amazon API щоб дозволити вхідний доступ до API у вашому хмарному середовищі.
- Використання AWS WAF для виявлення та захисту від атак на рівні додатків.
- Використання AWS Shield для виявлення та захисту від DDoS-атак.

- Використання AWS IAM авторизувати доступ до API.
- Використання Amazon CloudWatch для виявлення піків у запитах API.
- Використання AWS CloudTrail щоб виявити, хто може здійснювати активність API через шлюз API.
- Використання Amazon Guard Duty для виявлення потенційної хакерської діяльності за допомогою ваших API.
- Використання Менеджер таємниць AWS для генерації, зберігання та ротації ключів API.

Загальні служби Azure для виявлення та усунення небезпечних API

Деякі служби Azure, які можуть забезпечити захист від незахищених API:

- Використання Керування API Azure щоб дозволити вхідний доступ до API у вашому хмарному середовищі.
- Використання Azure WAF для виявлення та захисту від атак на рівні додатків.
- Використання Захист від DDoS-атак у Azure для виявлення та захисту від DDoS-атак.
- Використання Azure Active Directory авторизувати доступ до API.
- Використання Монітор Azure для виявлення піків у запитах API.
- Використання Сховище ключів Azure для генерації, зберігання та ротації ключів API.
- Використання Azure Guardian співвідносити кілька джерел даних, щоб допомогти у виявленні потенційних атак на API.

Загальні сервіси GCP для допомоги у виявленні та усуненні загроз небезпечним API

Деякі сервіси GCP, які можуть забезпечити захист від незахищених API:

- Використання Шлюз API Google щоб дозволити вхідний доступ до API у вашому хмарному середовищі.
- Використання Google CloudArmor для виявлення та захисту як від атак на рівні додатків, так і від DDoS-атак.
- Використання Google Cloud IAM авторизувати доступ до API.
- Використання Журнали аудиту Google Cloud для моніторингу активності API Gateway.

Для отримання додаткової інформації зверніться до наступних ресурсів:

Топ-10 безпеки API 2019 року: https://surl.li/grjokg

Виявлення та зменшення зловживань хмарними сервісами

Зловживання хмарними сервісами полягає у використанні масштабу ресурсів постачальника хмарних послуг та багатокористувацької архітектури для здійснення зловмисної діяльності.

Деякі поширені наслідки зловживання хмарними сервісами такі:

- Втрата доступності послуг через DDoS-атаки.

- Грошові втрати через використання хмарних ресурсів для майнінгу біткойнів без відома клієнта.

Деякі поширені приклади зловживання хмарними сервісами є наступними:

- Використання хмари для розгортання кількох серверів та проведення DDoS-атак
- Використання хмари для розгортання кількох дорогих серверів для майнінгу біткойнів
- Використання хмари для поширення спаму електронною поштою та фішингових атак
- Використання хмари для атак методом перебору паролів

Деякі найкращі практики виявлення та зменшення зловживань хмарними сервісами наведено нижче.

- Налаштуйте сповіщення про виставлення рахунків, щоб отримувати завчасні повідомлення про будь-яке збільшення споживання ресурсів.
- Дотримуйтесь концепції розподіл обов'язків щоб уникнути того, щоб окремі користувачі мали права на здійснення шкідливих дій (наприклад, користувач з правами як на розгортання дорогої віртуальної машини, так і на вхід до машини для поточного обслуговування).
- Використовуйте списки контролю доступу та встановлюйте правила мережі/брандмауера, щоб налаштувати, хто може отримувати доступ до ваших ресурсів (як для вхідного, так і для вихідного мережевого трафіку).
- Використовуйте IAM для контролю доступу до ваших хмарних середовищ.
- Змінюйте облікові дані, щоб уникнути неправомірного використання.
- Використовуйте журнали аудиту, щоб мати змогу контролювати доступ до ресурсів та виконані дії.
- Використовуйте служби захисту від DDoS-атак, щоб захистити своє хмарне середовище від атак типу «відмова в обслуговуванні».
- Використовуйте сервіси WAF для виявлення атак на рівні додатків та захисту від них.
- Інвестуйте в обізнаність співробітників щодо умов прийнятного використання постачальником хмарних послуг.

Загальні сервіси AWS для сприяння виявленню та усуненню зловживань хмарними сервісами

Деякі поширені сервіси AWS, які можуть захистити від зловживань хмарними сервісами:

- Використання Amazon CloudWatch налаштувати сповіщення про виставлення рахунків та отримувати сповіщення, коли перевищено певні порогові значення.
- Використання AWS IAM щоб налаштувати, хто може автентифікувати та отримувати доступ до ваших програм, ресурсів і даних.

- Використання Конфігурація AWS для виявлення змін конфігурації у вашому середовищі та хмарних ресурсах.
- Використання AWS WAF для виявлення та захисту від атак на рівні додатків.
- Використання AWS Shield для виявлення та захисту від DDoS-атак.
- Використання AWS CloudTrail для виявлення активності API (для користувачів, комп'ютерів, облікових записів служб тощо), яка може свідчити про нецільове використання ресурсів у вашому хмарному середовищі.
- Використання Amazon Guard Duty для виявлення будь-якої аномальної поведінки у ваших хмарних ресурсах (наприклад, майнінг біткойнів).
- Використання Елементи керування Amazon VPC (наприклад, мережеві ACL та групи безпеки) та мережевий брандмауер AWS для налаштування правил вхідного та вихідного доступу до мережі.
- Використання Менеджер патчів AWS Systems Manager автоматично розгортати патчі безпеки для серверів у вашому хмарному середовищі.

Загальні сервіси Azure для сприяння виявленню та усуненню зловживань хмарними сервісами

Деякі поширені сервіси Azure, які можуть захистити від зловживань хмарними сервісами:

- Використовуйте бюджети Azure для налаштування сповіщень про виставлення рахунків та отримання сповіщень, коли перевищено певні порогові значення.
- Використання Azure AD щоб налаштувати, хто може автентифікувати та отримувати доступ до ваших програм, ресурсів і даних.
- Використання Монітор Azure для виявлення дій (для користувачів, комп'ютерів, облікових записів служб тощо), які можуть свідчити про нецільове використання ресурсів у вашому хмарному середовищі.
- Використання Захисник Microsoft для хмари виявляти та надсилати сповіщення про можливе нецільове використання ресурсів у вашому хмарному середовищі.
- Використання Azure WAF для виявлення та захисту від атак на рівні додатків.
- Використання Захист від DDoS-атак у Azure для виявлення та захисту від DDoS-атак.
- Використання Групи підтримки Azure налаштувати правила вхідного та вихідного доступу до мережі.
- Використання Скринька клієнта Azure для виявлення спроб входу інженерів служби підтримки Microsoft.
- Використання Керування оновленнями Azure автоматично розгортати патчі безпеки для серверів у вашому хмарному середовищі.

Загальні сервіси GCP для сприяння виявленню та усуненню зловживань хмарними сервісами

Деякі поширені сервіси GCP, які можуть захистити від зловживань хмарними сервісами:

- Використовуйте бюджети GCP Billing для налаштування сповіщень про виставлення рахунків та отримання сповіщень про перевищення певних порогових значень.
- Використання Google Cloud IAM щоб налаштувати, хто може автентифікувати та отримувати доступ до ваших програм, ресурсів і даних.
- Використання Ведення журналу в хмарі Google для виявлення підозрілих дій, які можуть свідчити про нецільове використання ресурсів у вашому хмарному середовищі.
- Використання Google CloudArmor для виявлення та захисту як від атак прикладного рівня, так і від DDoS-атак.
- Використання Центр керування безпекою хмари Google співвідносити кілька джерел даних, щоб допомогти виявити нецільове використання ресурсів у вашому хмарному середовищі.
- Використовуйте правила брандмауера GCP VPC для налаштування правил вхідного та вихідного доступу до мережі.
- Використання Прозорість доступу Google і Схвалення доступу для виявлення спроб входу інженерів служби підтримки Google.
- Використання Керування патчами ОС Google автоматично розгортати патчі безпеки для серверів у вашому хмарному середовищі.

Для отримання додаткової інформації зверніться до наступних ресурсів: *Зловживання хмарними сервісами для приховування інформації*: https://surl.li/smgdce

3.2.Забезпечення відповідності та регулювання

Стандарти гарантують, що ми дотримуємося найкращих практик так само, як і більшість організацій у всьому світі в різних галузях, таких як інформаційна безпека, конфіденційність та захист даних, охорона здоров'я, фінанси тощо.

Відповідність вимогам у хмарних сервісах - це акт дотримання нормативних вимог та галузевих стандартів. Дотримання законів, нормативних актів та стандартів дозволяє організаціям вести свій бізнес безпечно, гарантуючи захист даних клієнтів.

У цьому розділі ми розглянемо такі питання:

- Відповідність вимогам та модель спільної відповідальності.
- Вступ до дотримання нормативних вимог та найкращих галузевих практик.
- Міжнародна організація зі стандартизації (ICO) стандарти, пов'язана з хмарними обчисленнями.
- Системні та організаційні елементи керування (**SOC**).

- Альянс хмарної безпеки (CSA (Компанія з питань соціального забезпечення)) Безпека, довіра, гарантії та ризик (ЗІРКА) програма.
- Стандарт безпеки даних індустрії платіжних карток (PCI DSS).
- Загальний регламент про захист даних (GDPR).
- Закон про перенесення та підзвітність медичного страхування (HIPAA)

Технічні вимоги

Для цього розділу читач повинен мати ґрунтовне розуміння концепцій інформаційної безпеки, таких як стандарти, програми відповідності, захист даних тощо.

Відповідність вимогам та модель спільної відповідальності

Згідно з моделлю спільної відповідальності, постачальник хмарних послуг у інфраструктурі як послуга/платформа як послуга (IaaS/PaaS) відповідає за фізичні аспекти хмари (від фізичних центрів обробки даних, апаратного забезпечення, сховищ даних, мережевого обладнання, хост-серверів до віртуалізації).

Програмне забезпечення як послуга(SaaS) постачальники також відповідають за рівні додатків (гостьові операційна система(ОС), керовані бази даних, кероване сховище, рівень додатків тощо). Як клієнти, ми очікуємо, що наші хмарні постачальники відповідатимуть нормативним вимогам (таким як захист інформації про кредитні картки згідно зі стандартом PCI DSS, захист особисту інформацію(Особиста інформація) у GDPR та інше) та працювати відповідно до найвищих стандартів безпеки (таких як ISO27001, SOC та інші).

Коли ми, як організації, обслуговуємо клієнтів, нам необхідно дотримуватися нормативних актів (під час роботи з фінансовими, медичними чи персональними даними), незалежно від того, чи будуємо ми нашу інфраструктуру вище IaaS/PaaS, чи обслуговуємо клієнтів як постачальники SaaS. Коли ми обслуговуємо клієнтів як постачальники SaaS, наші клієнти очікують, що ми працюватимемо відповідно до найвищих стандартів безпеки, і ми повинні довести нашим клієнтам, що наші засоби контролю безпеки є ефективними.

Щоб довести відповідність постачальника хмарних послуг найкращим практикам безпеки, вони проходять оцінювання сторонніми оцінювачами - нейтральними постачальниками безпеки.

Вступ до дотримання нормативних вимог та найкращих галузевих практик

Закони та нормативні акти є обов'язковими для будь-якої організації, яка веде бізнес, зберігає та обробляє конфіденційні дані (такі як особиста інформація, інформація про кредитні картки, медична інформація тощо) та обслуговує клієнтів як у приватному, так і в публічному середовищі, і хмарне середовище не є винятком.

Стандарти необов'язково розглядаються як найкраща практика та в багатьох випадках забезпечують важелі впливу організації на ведення бізнесу, наприклад, дотримання стандартів ISO. 27001 показує клієнтам та діловим партнерам, що організація досягла певного рівня зрілості в управління інформаційною безпекою(ІЗМ).

Найкращий спосіб керувати відповідністю вимогам у хмарних сервісах як автоматизованим та безперервним процесом - це постійно переглядати все хмарне середовище, представляти інформацію, інформаційні панелі та звіти, а також виправляти налаштування та ресурси, які перебувають у невідповідному стані.

Як забезпечити відповідність вимогам в AWS

Веб-сервіси Amazon (AWS) пропонує своїм клієнтам послугу під назвою Конфігурація AWS що дозволяє клієнтам постійно перевіряти стан відповідності всієї своєї організації AWS нормативним вимогам та найкращим галузевим практикам. Щоб переглянути актуальний перелік звітів про відповідність, яким відповідає AWS, ви можете скористатися Артефакт AWS.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Артефакт AWS: https://surl.li/sgupmf
Конфігурація AWS: https://surl.li/uddaqr

Як підтримувати відповідність вимогам в Azure

Azure пропонує своїм клієнтам послугу під назвою Захисник Microsoft для хмари що дозволяє їм постійно перевіряти стан відповідності всього клієнта Azure нормативним вимогам та найкращим галузевим практикам. Через Azure клієнти можуть переглядати актуальний перелік звітів про відповідність, яким Azure відповідає, як зазначено в Центр безпеки Azure.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Центр безпеки Azure -покращення відповідності нормативним вимогам: https://surl.li/ywuruj
Центр безпеки Azure: https://surl.lu/apgwze

Як забезпечити відповідність вимогам GCP

Хмарна платформа Google (GCP) пропонує своїм клієнтам послугу під назвою Центр команд безпеки Google, що дозволяє клієнтам постійно перевіряти стан відповідності всієї своєї організації GCP нормативним вимогам та найкращим галузевим практикам.

GCP також надає своїм клієнтам можливість переглядати актуальний перелік звітів про відповідність, яким відповідає GCP, як зазначено в Менеджер звітів Google про відповідність вимогам.

Міжнародна організація зі стандартизації (ICO) стандарти, пов'язана з хмарними обчисленнями

ISO - це неурядова міжнародна організація, яка публікує документи та підвищує обізнаність про стандарти з різних тем, а в контексті цієї посібника - про стандарти, пов’язані з інформаційною безпекою та хмарними сервісами.

Стандарт ISO/IEC 27001

ISO/Міжнародна електротехнічна комісія (IEK) 27000 Стандарт є найпоширенішим стандартом для ISM. Хоча він не є специфічним для хмари, він вважається найфундаментальнішим стандартом для постачальники хмарних послуг (Постачальники послуг зв'язку (CSP)), і це закладає міцну основу для будь-якого постачальника хмарних послуг, від гіпермасштабного хмарного постачальника до невеликого SaaS-провайдера.

ISO2700 поділяється на такі розділи:

- ISO/IEC27000:2018 надає огляд Системи ISM(СУІБ).
- ISO/IEC27001:2013 є стандартом для ISM.
- ISO/IEC27002:2013 визначає найкращі практики для ISM.

ISO27001складається з таких доменів:

- Політики інформаційної безпеки
- Організація інформаційної безпеки
- Безпека людських ресурсів
- Управління активами
- Контроль доступу
- Криптографічний
- Фізична та екологічна безпека
- Безпека операцій
- Безпека зв'язку
- Придбання, розробка та обслуговування системи
- Відносини з постачальниками
- Управління інцидентами інформаційної безпеки
- Управління безперервністю бізнесу в галузі інформаційної безпеки
- Відповідність

Для отримання додаткової інформації зверніться до наступних ресурсів:
ISO/IEC 27001 Управління інформаційною безпекою: https://surl.li/vmwzou
AWS—ISO/IEC 27001:2013: https://surl.li/zxtkdu
Блакитний -ISO/IEC 27001:2013: https://surl.li/gxndfj
GCP -ISO/IEC 27001: https://surl.li/lncqle

Стандарт ISO 27017

ISO/IEC27017 це набір рекомендацій щодо контролю інформаційної безпеки, що застосовується до хмарних сервісів, на основі ISO/IEC270023 моменту появи ISO27017базується на ISO27002, більшість елементів керування однакові.

Будь-яка організація, яка надає хмарні послуги, повинна розглянути питання про дотримання стандарту ISO 27017

Стандарт ISO27017 додає такі елементи керування:

- Спільні ролі та обов'язки в середовищі хмарних обчислень
- Видалення активів клієнтів хмарних сервісів
- Розділення у віртуальних обчислювальних середовищах
- Віртуальна машина (ВМ) загартування
- Операційна безпека адміністратора
- Моніторинг хмарних сервісів
- Узгодження управління безпекою для віртуальних та фізичних мереж

Для отримання додаткової інформації зверніться до наступних ресурсів:
ISO/IEC 27017:2015: https://surl.li/hjmaxg
AWS - Відповідність стандарту ISO/IEC 27017:2015: https://surli.cc/qggmad
Блакитний -ISO/IEC 27017:2015: https://surl.li/efvpkw
Належна клінічна практика (GCP) -ISO/IEC 27017: https://surl.lu/shzpzc

Стандарт ISO 27018

ISO/IEC27018це набір рекомендацій щодо впровадження заходів захисту персональних даних (PII) для хмарних сервісів, заснований на ISO/IEC27002 як ISO27018базується на ISO27002, більшість елементів керування однакові.

Будь-яка організація, яка надає хмарні послуги та зберігає або обробляє персональні дані, повинна розглянути питання про дотримання вимог ISO.27018стандарт ISO27018додає такі елементи керування:

Права клієнтів:

- Можливість доступу до своїх даних.
- Можливість видалення своїх даних.
- Знати мету обробки своїх даних.

Зобов'язання постачальника послуг (SP):

- Обробка запитів на розкриття даних від клієнтів
- Документування всіх запитів на розкриття даних
- Аудит усіх спроб доступу до даних клієнтів
- Повідомляти клієнтів про субпідрядників, які мають доступ до персональних даних клієнтів.
- Повідомляти клієнтів про витоки даних, пов'язані з їхніми персональними даними. Документувати всі політики та процедури, що стосуються персональних даних клієнтів.
- Шифрувати всі персональні дані клієнтів, що зберігаються (включаючи резервні копії).
- Процедури видалення даних
- Повідомляти клієнтів про країни, де зберігаються та обробляються їхні дані

Для отримання додаткової інформації зверніться до наступних ресурсів:
ISO/IEC 27018:2019: https://surl.li/ahptqv
AWS - Відповідність стандарту ISO/IEC 27018:2019: https://surl.lt/kbmsza
Блакитний - ISO/IEC 27018:2019: https://surl.li/bbdsnq
GCP -ISO/IEC 27018: https://surl.li/lkblxj

Системні та організаційні елементи керування (SOC)

SOC - це система звітності, яка дозволяє постачальникам хмарних послуг повідомляти про ефективність своєї програми управління ризиками кібербезпеки сертифіковані державні бухгалтери(CPA) та широке коло зацікавлених сторін - серед інших, клієнтів.

Будь-яка організація, яка надає хмарні послуги, повинна розглянути можливість дотримання стандарту SOC. SOC складається з таких типів звітів:

СОК 1-Фінансовий звіт:

- SOC 1 Тип 1—Атестація контролю для CSP на певний момент часу
- SOC 1 Тип 2—Атестація контролю для CSP та його ефективності протягом щонайменше 6-місячного періоду
- СОК 2—Звіт про засоби контролю, що стосуються безпеки, доступності, цілісності та конфіденційності або приватності
- SOC 2 Тип 1—Опис систем постачальників хмарних послуг та придатність дизайну засобів контролю
- SOC 2 Тип 2—Опис систем постачальників хмарних послуг, придатність структури засобів контролю та їх ефективність

  💻 *Примітка!* З точки зору клієнта, SOC 2 Тип 2 є найбільш релевантним звітом, оскільки він відображає фактичну ефективність заходів безпеки постачальника хмарних послуг.
- СОК 3—Звіт керівництва, що містить гарантію щодо контролю постачальника хмарних послуг, що стосується безпеки, доступності, цілісності та конфіденційності або приватності.

  💻 *Примітка!* Звіти SOC 3 є звітами високого рівня, і тому вони публічно доступні клієнтам.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Системні та організаційні засоби контролю AWS (SOC): https://surl.li/sjktgy
Azure -Системні та організаційні елементи керування (SOC) 1 Тип 2: https://surl.li/nschhh
GCP—SOC 2: https://surl.li/bpdeuq

Альянс хмарної безпеки (CSA (Компанія з питань соціального забезпечення)) Безпека, довіра, гарантії та ризик (ЗІРКА) програма

Що таке програма CSA STAR? CSA - це організація, яка публікує документи, передовий досвід та підвищує обізнаність щодо хмарної безпеки.

Будь-яка організація, яка надає хмарні послуги, повинна розглянути можливість дотримання вимог програми CSA STAR. CSA створила два документи, пов'язані з хмарною безпекою, а саме:

- *Матриця керування хмарою(CCM)* - Система контролю кібербезпеки для хмарних обчислень
- *Анкета ініціативи з оцінювання консенсусу(CAIQ)* - Набір галузево прийнятих засобів контролю безпеки для послуг IaaS/PaaS/SaaS

CSA створила програму під назвою STAR, яка є відкритим реєстром постачальників хмарних послуг, що публічно діляться своїми засобами контролю безпеки для різних моделей обслуговування та дозволяють клієнтам завантажувати та перевіряти відповідність постачальника найкращим галузевим практикам.

ЗІРКА Рівень 1

STAR Level 1 - це анкета самооцінки, за допомогою якої постачальники хмарних послуг прозоро діляться своїми засобами контролю безпеки.

Клієнтам слід використовувати анкету самооцінки як гарну відправну точку для середовищ з низьким рівнем ризику, оскільки анкету не перевіряв на ефективність заходів контролю незалежний сторонній аудитор.

ЗІРКА Рівень 2

STAR Level 2 пропонує хмарних постачальників, які вже відповідають стандартам ISO27001, звіти SOC 2 та інші можливості перевірки своїх засобів безпеки стороннім аудитором, а також додають клієнту рівень комфорту в анкеті самооцінки постачальника хмарних послуг, оцінюючи фактичну ефективність засобів контролю, заявлених постачальником хмарних послуг. Клієнтам слід використовувати відповідність STAR рівня 2 для середовищ із середнім та високим рівнем ризику, а також для підвищення гарантій безпеки та конфіденційності хмарних послуг.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Зірка CSA: https://surli.cc/jjmwup
AWS та Альянс хмарної безпеки (CSA): https://surl.li/kbkogw
Сертифікація Azure -Cloud Security Alliance (CSA) STAR: https://surl.li/goclui
GCP та Альянс хмарної безпеки (CSA): https://surl.li/gcsrrw

Стандарт безпеки даних індустрії платіжних карток (PCI DSS)

Що таке PCI DSS? PCI DSS -це стандарт інформаційної безпеки для зберігання, передачі та обробки інформації про кредитні картки, створений MasterCard, American Express, Visa, JCB International та Discover Financial Services.

Будь-яка організація, що зберігає або обробляє інформацію про кредитні картки, повинна дотримуватися стандарту PCI DSS. Стандарт PCI має такі вимоги:

- Використовуйте брандмауер для захисту середовища PCI

- Встановіть політики паролів
- Захистіть збережені дані кредитної картки
- Шифруйте дані кредитної картки під час транзиту
- Використовуйте антивірусне програмне забезпечення
- Здійснювати управління виправленнями
- Обмежте доступ до даних кредитної картки
- Призначте унікальний ідентифікатор кожній особі з доступом до даних кредитної картки
- Обмежте фізичний доступ до даних кредитних карток
- Ведення журналів
- Проводити оцінки вразливостей та тести на проникнення
- Проводити оцінку ризиків та документувати процес

Будь-який постачальник послуг або організація, яка зберігає, передає або обробляє інформацію про кредитні картки, повинна дотримуватися стандарту PCI DSS. Як найкраща практика, дотримуйтесь документації вашого постачальника хмарних послуг щодо того, які сервіси та засоби контролю використовувати для відповідності стандарту PCI та забезпечення безпеки інформації про кредитні картки.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Стандарти безпеки PCI: https://surl.lu/vtjeez
Доповнення до інформації: Керівні принципи хмарних обчислень PCI SSC: https://surl.li/lqhwpb
Azure -Зіставлення елементів керування зразком плану PCI-DSS версії 3.2.1: https://surl.li/qbzjsw

Загальний регламент про захист даних (GDPR)

Що таке GDPR? GDPR - це європейський регламент про захист даних, спрямований на захист персональних даних Європейський Союз (ЄС) громадяни.

Будь-яка організація, яка зберігає або обробляє інформацію про громадян ЄС, повинна дотримуватися GDPR. Він визначає персональні дані як будь-яку інформацію, що стосується ідентифікованої або ідентифікованої фізичної особи. GDPR застосовується до будь-якої організації, яка обробляє або збирає персональні дані громадян ЄС, як у центрах обробки даних у Європі, так і до/з-за меж Європи.

Ось основні розділи GDPR, що стосуються технічних заходів, які можуть бути пов'язані з хмарними сервісами:

- Розділ 2 - Принципи
- Розділ 3 - Права суб'єкта даних
- Розділ 4 - Контролер та процесор

- Розділ 5 - Передача персональних даних третім країнам або міжнародним організаціям
- Розділ 9 - Положення, що стосуються конкретних ситуацій обробки

Деякі методи захисту персональних даних:

- Шифруйте всі персональні дані під час передачі (використовуйте Безпека транспортного рівня(TLS) 1.2) або у стані спокою (використовуйте Розширений стандарт шифрування(AEC) 256 алгоритм).
- Переконайтеся, що постачальник хмарних послуг пропонує вам можливість контролювати ключі шифрування (ключі, керовані клієнтом).
- Забезпечити використання багатофакторна автентифікація (МЗС) для будь-якого користувача, який має доступ до персональних даних.
- Дотримуйтесь принципу потрібно знати.
- Переконайтеся, що персональні дані громадян ЄС зберігаються в центрах обробки даних у межах ЄС або в центрах обробки даних країн, які отримують належний рівень захисту даних від ЄС.
- Переконайтеся, що ви підписали угода про обробку даних з вашим хмарним постачальником.
- Переконайтеся, що постачальник хмарних послуг провів аудит безпеки стороннім аудитором, перш ніж обробляти персональні дані.
- Збирайте лише мінімально необхідний обсяг персональних даних.
- Переконайтеся, що ви можете знайти персональні дані та видалити їх, виконавши запит клієнта.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Загальний регламент про захист даних: https://surl.li/xlcfza
Azure -Короткий зміст Загального регламенту про захист даних: https://surl.li/ehzjsb
Azure -Типові положення Європейського Союзу: https://surl.li/nxfyfy
Google Cloud та Загальний регламент про захист даних (GDPR): https://surl.li/tlbexo
GCP -Типові договірні положення ЄС: https://surl.li/dardzt

Закон про перенесення та підзвітність медичного страхування (HIPAA)

Що таке HIPAA? HIPAA - це закон Сполучених Штатів для організацій, що займаються електронними транзакціями в галузі охорони здоров'я та особистою інформацією (PII) у галузях охорони здоров'я та медичного страхування.

Ось основні правила безпеки HIPAA:

- Адміністративні гарантії
- Фізичні засоби безпеки
- Технічні заходи безпеки
- Організаційні, політики та процедури, а також вимоги до документації

- Основи аналізу ризиків та управління ризиками

Деякі найкращі практики для впровадження:

- Шифруйте всю медичну інформацію під час передачі (за допомогою TLS 1.2) або в стані спокою (за допомогою алгоритму AES 256).
- Увімкнути журнал аудиту для будь-якої інформації, пов’язаної з даними охорони здоров’я.
- Автентифікувати та авторизувати будь-який запит на доступ до медичних даних.
- Дотримуйтесь принцип найменших привілеїв(ПОЛП) під час доступу до даних охорони здоров’я.
- Проводити тестування на проникнення для систем, що містять дані охорони здоров'я.
- Підтримуйте всі системи в актуальному стані (забезпечте керування виправленнями).
- Увімкніть резервне копіювання для будь-якої системи, яка містить дані охорони здоров’я.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Керівництво щодо HIPAA та хмарних обчислень: https://surl.li/uhogdd
Архітектура для безпеки та відповідності HIPAA на Amazon Web Services: https://surl.li/iosvpg
Блакитний -HIPAA: https://surl.li/bucyrx
GCP—HIPAA: https://surl.li/vguxey

3.3 Взаємодія з постачальниками хмарних послуг

У традиційному центрі обробки даних ми контролюємо все - від фізичних до логічних засобів безпеки. Щоб отримати гарантію роботи з хмарними постачальниками, існує кілька варіантів, таких як:

Проведіть оцінку ризиків перед взаємодією з постачальником хмарних послуг - одним із гарних варіантів перегляд звітів SOC2 Type 2 (які засоби контролю встановив постачальник хмарних послуг і наскільки вони ефективні).

Мати хороший контракт, який чітко визначає зобов'язання постачальника хмарних послуг (наприклад, Угода про рівень обслуговування(Угода про рівень обслуговування) для обробки інцидентів безпеки та угода про рівень обслуговування (SLA) для повідомлення нас як клієнтів).

У цьому параграфі ми розглянемо такі теми:

- Вибір постачальника хмарних послуг
- Хмарний провайдер
- Поради щодо укладання договорів з постачальниками хмарних послуг
- Проведення тестування на проникнення в хмарних середовищах

Технічні вимоги

Для цього розділу читачеві необхідно мати фундаментальне розуміння таких концепцій, як моделі хмарних сервісів, бізнес-вимоги, оцінка постачальників та тестування на проникнення.

Вибір постачальника хмарних послуг

Перш ніж вибрати постачальника хмарних послуг, нам потрібно запитати себе: Чого ми намагаємося досягти, переходячи до хмари чи використовуючи хмару?

Перш ніж почати співпрацю з постачальником хмарних послуг, нам потрібно зробити кілька кроків:

- Визначити наші бізнес-цілі, яких постачальник хмарних послуг допоможе нам досягти.
- Ознайомимося з потенційним постачальником хмарних послуг та спробуємо зрозуміти його рівень зрілості.
- Підписати контракт із постачальником хмарних послуг, який захистить нас як клієнтів.
- Провести оцінку хмарного середовища, щоб переконатися в ефективності його заходів безпеки.

На наступній діаграмі (Рис.3.1) показано кроки, необхідні для вибору постачальника хмарних послуг:

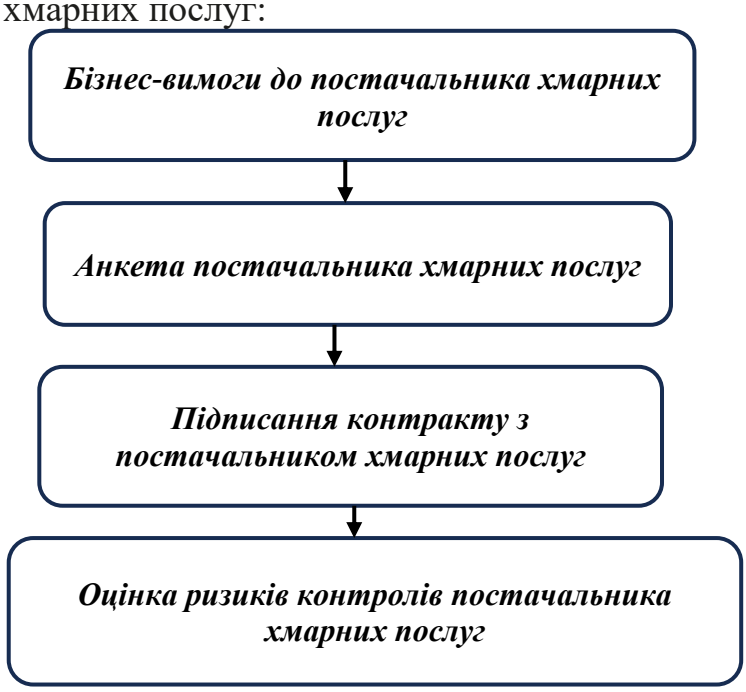

Рисунок 3.1 - Вибір постачальника хмарних послуг

Яка модель хмарного сервісу найкраще підходить для наших потреб?

Це перше питання, яке нам потрібно собі поставити. Якщо ми все ще робимо перші кроки в хмарі, маємо застарілі системи, які хочемо перенести в хмару, і не маємо залежностей від апаратного забезпечення певних постачальників (таких

як IBM AIX, Oracle SPARC тощо), тоді Інфраструктура як послуга(Інфраструктура як послуга (IAA)) є найбільш підходящою моделлю.

Доки наші локальні сервери базуються на архітектурі x86 і їх можна віртуалізувати, ми повинні мати можливість мігрувати або перебудовувати наші системи на основі будь-якого з основних постачальників IaaS.

Одна з тем, яку нам слід розглянути -це наша здатність підключатися до хмарного постачальника в гібридній моделі та розширювати наш локальний центр обробки даних - які гібридні хмарні можливості потенційних хмарних постачальників?

Можливо, ми вже обрали хмарного провайдера, але тепер у нас є бізнес-або технічна вимога працювати певним сервісом (наприклад, Інтернет речей(Інтернет речей), машинне навчання та аналітика даних), що вважається вищим, і воно існує в іншого хмарного постачальника. У цьому випадку нам потрібно розглянути багатохмарну архітектуру та переглянути багатохмарні можливості обох хмарних постачальників.

Ми повинні пам'ятати, що згідно з моделлю спільної відповідальності, ми несемо відповідальність за всю підтримку операційної системи, таку як керування виправленнями, оновлення програмного забезпечення, резервне копіювання, посилення безпеки та доступність.

Якщо ми плануємо створювати нові додатки на основі безсерверної (або функціонально-послугової) архітектури, або якщо ми надаємо перевагу використанню керованих сервісів (таких як сервіси баз даних, машинне навчання та аналітика даних), тоді Платформа як послуга (PaaS) має бути нашою бажаною моделлю обслуговування.

Якщо ми обираємо модель PaaS, нам потрібно врахувати, як ми плануємо підключити нашу розробку (або Безперервна інтеграція/Безперервна доставка (ДІ/КД)) інфраструктуру до хмарного середовища та як ми плануємо підключати наші програми (незалежно від того, чи розташовані вони локально, чи в нашому середовищі IaaS) до послуг PaaS.

Можливо, найпростіша модель обслуговування для організацій, які бажають використовувати хмарні сервіси або замінити застарілу локальну систему, таку як Управління взаємовідносинами з клієнтами (CRM), Планування ресурсів підприємства(ERP) та обмін повідомленнями, з повністю керованим сервісом, варто обрати модель SaaS.

Під час вибору зрілого постачальника SaaS (як пояснено далі в цьому розділі, з відповідей, які ми отримали від постачальника послуг на анкету, згадану в Що таке хмарний провайдер? розділ), ми маємо переваги використання послуги без тягаря постійного обслуговування, додавання засобів контролю безпеки, турботи про доступність тощо.

Якщо ми все ж таки вирішимо використовувати модель SaaS, нам потрібно розуміти, що не всі постачальники SaaS пропонують нам однаковий рівень безпеки. Не всі постачальники SaaS дотримуються найкращих практик безпеки, таких як багатокористувацька оренда (повне розділення між клієнтами послуги), захист від атак на основі інфраструктури або додатків, звіти аудиту та сертифікати безпеки.

Конфіденційність даних та суверенітет даних

Перш ніж вибрати постачальника послуг публічної хмари (з будь-якої з моделей обслуговування), нам потрібно проконсультуватися з нашим співробітником із захисту даних, нашим юридичним відділом або експертом з питань конфіденційності даних, щоб перевірити, які закони та правила вимагаються нашою організацією щодо нашої галузі, нашої країни та даних, які ми плануємо зберігати або обробляти в хмарі.

Оскільки дані, що зберігаються в хмарі, можуть (потенційно) бути репліковані по всьому світу, нам потрібно зрозуміти, чи існують закони, які вимагають від нас зберігати наші дані локально в певній країні.

Незалежно від того, чи обслуговуємо ми клієнтів у певній країні чи в кількох місцях (або, можливо, усьому світі), нам потрібно знати, чи має постачальник хмарних послуг центр обробки даних у певних країнах.

Існують сценарії, коли у нас є вимоги щодо регулювання (наприклад, Індустрія платіжних карток(PCI-інтерфейс) та Fed RAMP), і нам потрібно створити ціле хмарне середовище, яке відповідатиме таким нормам - у цьому випадку нам потрібно перевірити, чи має постачальник хмарних послуг середовища, що відповідають цим нормам, у певних регіонах.

Одним із гарних прикладів є AWS Gov Cloud та Azure для уряду США, які є спеціалізованими хмарними середовищами лише для урядових установ. Іншим прикладом є AWS China та Microsoft Azure у Китаї, які є повністю окремими хмарними середовищами для зберігання та обробки даних у Китаї.

Для моделей IaaS та PaaS це не повинно бути проблемою, оскільки більшість сервісів IaaS або навіть PaaS є регіональними - після вибору цільового регіону наші дані не залишать його (якщо ми не оберемо глобальний сервіс або не вирішимо реплікувати дані між регіонами, щоб наблизитися до наших клієнтів).

Одним із альтернативних способів гарантувати, що наші дані не будуть скопійовані за межі певного регіону, є шифрування наших даних, оскільки ключі шифрування є регіональними ресурсами, що гарантує, що наші дані не будуть репліковані або доступні за межами певного регіону.

Для SaaS-сервісів немає однозначної відповіді на питання, чи можемо ми зберегти суверенітет даних. Деякі SaaS-провайдери реплікують наші дані в різних регіонах, щоб забезпечити кращу доступність сервісів, або ж вони можуть зберігати наші резервні копії в іншому регіоні, щоб краще захистити наші дані. Найкращим рішенням для IaaS та PaaS-сервісів є ознайомлення з документацією постачальника.

Для SaaS-сервісів, окрім ознайомлення з документацією постачальника, наполегливо рекомендується проконсультуватися з постачальником SaaS та поставити конкретні запитання щодо конфіденційності або суверенітету даних, перш ніж підписувати контракт з постачальниками SaaS.

Аудит та моніторинг

Моніторинг та аудит ваших хмарних середовищ Аудит має вирішальне значення для захисту хмарних середовищ, отримання інформації про те, що відбувається у вашому хмарному середовищі, а також як частина реагування на інциденти та криміналістики, якщо хмарне середовище було порушено.

Досвідчені постачальники хмарних послуг пропонують вам документовані API для отримання журналів аудиту активності до вашого Інформація про безпеку та управління подіями(CIEM) системи для подальшого аналізу того, хто входив у сервіс і які дії були вжиті (як успіхи, так і невдачі).

Іншим типом журналу є журнал служб (наприклад, сховища об'єктів, балансувальників навантаження та керованих баз даних).

Більшість розвинених постачальників хмарних послуг пропонують нам документовані API для отримання цих журналів.

Іншим типом журналу аудиту є журнал хоста (наприклад, Операційна система(ОС), журнали безпеки та програм). Шукайте хмарного провайдера, який пропонує вам спосіб отримання журналів хоста та їх зберігання в централізованій службі реєстрації, яка надає доступ до API. Це дозволить нам підключитися до API та отримати журнали до наших SIEM-систем для подальшого аналізу.

З точки зору інфраструктури, шукайте хмарних постачальників, які пропонують вам документовані API для отримання даних про продуктивність і дозволяють передбачати проблеми з продуктивністю, перш ніж ви отримаєте скарги від своїх клієнтів.

З точки зору застосунку, шукайте хмарних постачальників, які пропонують вам документовані API для отримання аналітики застосунку, журналів помилок та статистики про кількість невдалих дій у системі, що дозволяє вам вносити дані в Управління продуктивністю застосунків(АПМ) інструмент.

З фінансової точки зору, зверніться до постачальників хмарних послуг, які пропонують вам документовані API для отримання платіжної інформації, що дозволяє вам вносити дані до інструментів управління витратами, генерувати сповіщення про виставлення рахунків тощо.

Важливо враховувати вартість журналів. Деякі сервіси пропонують безкоштовний рівень зберігання (наприклад, протягом 30 днів), і якщо ми хочемо зберігати журнали протягом тривалого періоду часу (наприклад, через вимоги нормативних актів), нам потрібно враховувати вартість.

Ще один важливий момент, який слід врахувати, - це зберігання журналів. Постачальники хмарних послуг (такі як SaaS-провайдери) можуть зберігати журнали протягом 60–90 днів. Якщо нам потрібно зберігати журнали протягом тривалішого періоду, нам потрібен спосіб витягувати ці журнали та копіювати їх до зовнішнього сховища журналів.

Автентифікація

Перш ніж використовувати хмарний сервіс, ми повинні врахувати, як ми збираємося автентифікувати наших внутрішніх користувачів або зовнішніх клієнтів.

Оцінюючи хмарний сервіс, нам потрібно перевірити, які механізми автентифікації доступні. Деякі постачальники хмарних послуг пропонують нам внутрішні можливості автентифікації та авторизації, які вбудовані як частина хмарного рішення.

Як найкраща практика, нам слід уникати використання хмарних сервісів, які не підтримують стандартні механізми автентифікації, такі як Azure. Active Directory (AD) або будь-який із відомих протоколів на основі SAML чи OAuth 2.0, що дозволяє нам об’єднати нашу існуючу службу каталогів із хмарною службою без необхідності створювати нові облікові записи для наших кінцевих користувачів.

Для зовнішніх клієнтів обирайте рішення, що підтримують протокол OpenID Connect, який дозволяє вашим клієнтам проходити автентифікацію за допомогою їхніх особистих облікових записів Facebook, Apple, LinkedIn, Twitter та інших постачальників ідентифікації.

Хмарний провайдер

Що таке анкета постачальника хмарних послуг? Щоб оцінити постачальника хмарних послуг, перед початком співпраці дуже часто надсилають йому анкету з усіма темами, які, на думку вашої команди, потрібно поставити, щоб ознайомитися з ним.

Зрілі постачальники хмарних послуг, найімовірніше, поділилися інформацією про свої засоби контролю відповідності та безпеки.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Анкета ініціативи з оцінювання консенсусу GCP CSA (CAIQ): https://surli.cc/vsdqya

Розглядаючи потенційного постачальника хмарних послуг, враховуйте модель спільної відповідальності. Відповіді постачальника хмарних послуг дозволять нам чітко зрозуміти, які обов'язки постачальника хмарних послуг (за захист наших даних) порівняно з нашими обов'язками (і можливостями) як клієнтів щодо захисту наших даних.

Запитання є частиною процесу оцінки ризиків і можуть походити з різних областей.

Я відкритий для пропозицій, можливо, нам варто поставити іншим постачальникам хмарних послуг такі питання:

Пов'язані з хмарною інфраструктурою:

- Яка модель хмарних послуг (IaaS, PaaS та SaaS)?
- Як називається постачальник хмарної інфраструктури?
- Де розташовані центри обробки даних постачальника хмарних послуг?

Пов'язані з архітектурою:

- Чи пропонує постачальник хмарних послуг повне розділення між клієнтами (обчислення, сховище, база даних та мережа) для кількох орендарів?
- Чи пропонує постачальник хмарних послуг розділення між виробничим середовищем та середовищем розробки або тестування (обчислення, сховище, база даних та мережа)?

Пов'язані з мережею:

- Чи пропонує постачальник хмарних послуг послуги типу «сайт-сайт» (або «точка-сайт»)?
- Віртуальна приватна мережа(VPN) підключення з локальної мережі (або з будь-якого місця в Інтернеті) до хмарного середовища?
- Чи пропонує постачальник хмарних послуг виділене мережеве з'єднання (наприклад, AWS Direct Connect, Azure ExpressRoute та Google Cloud Interconnect) з локальної мережі до хмарного середовища?

Пов'язані з даними:

- Чи має постачальник хмарних послуг офіційну політику конфіденційності?
- Чи має постачальник хмарних послуг штатного працівника? Спеціаліст із захисту даних(ДЗО)?
- Чи відповідає постачальник послуг хмарної інфраструктури законам і нормативним актам про конфіденційність даних (таким як Загальний регламент про захист даних(GDPR) у Європі та Закон Каліфорнії про конфіденційність споживачів (CCPA) у Каліфорнії)?
- Чи пропонує постачальник хмарних послуг вбудований механізм класифікації даних (таких як особиста інформація, інформація про кредитні картки або дані про охорону здоров'я)?
- Чи пропонує постачальник хмарних послуг документацію щодо розгортання та захисту середовищ PCI (наприклад, зберігання, зберігання або обробка інформації про кредитні картки)?
- Чи пропонує постачальник хмарних послуг документацію щодо розгортання та захисту середовищ, що містять персональну інформацію (наприклад, інформацію громадян Європи, як це визначено в GDPR)?
- Чи пропонує постачальник хмарних послуг документацію щодо розгортання та захисту середовищ, що містять медичну інформацію (наприклад, медичну інформацію США, як визначено в Закон про перенесення та підзвітність медичного страхування(HIPAA)?

Аутентифікація та авторизація:

- Чи підтримує постачальник хмарних послуг стандартні протоколи автентифікації та авторизації для підключення до хмари з локального середовища або будь-якого зовнішнього середовища (такі протоколи, як SAML та OAuth 2.0)?

- Чи підтримує постачальник хмарних послуг протоколи автентифікації (такі як OpenID Connect) для автентифікації зовнішніх ідентифікаційних даних (таких як Facebook, Apple, LinkedIn та Twitter)?
- Чи підтримує хмарний провайдерКонтроль доступу на основі ролей(RBAC)?
- Чи дозволяє постачальник хмарних послуг керувати дозволами на доступ до хмарних ресурсів на основі Постачальника ідентифікаційних даних (Постачальник ідентифікаційних даних) групи (наприклад, групи Azure AD) та зіставляти групи з ролями?
- Чи підтримує хмарний провайдер багатофакторну автентифікацію (МЗС)?
- Чи містить хмара паролі за замовчуванням? Якщо так, чи можемо ми вимкнути або замінити всі паролі за замовчуванням?
- Чи містить хмара облікові записи за замовчуванням (такі як адміністратор та root)? Якщо так, чи можемо ми вимкнути або видалити ці облікові записи?

Керування сеансами:

- Чи підтримує хмарний провайдер автоматичне завершення сеансу після 15 хвилин бездіяльності?
- Чи генерує постачальник хмарних послуг випадкові та обмежені в часі ідентифікатори сеансів для кожної особи, автентифікованої в сервісі?
- Чи забезпечує постачальник хмарних послуг відключення сеансу в кінці кожного сеансу?
- Чи забезпечує постачальник хмарних послуг окремий сеанс для кожної автентифікованої особи?

Шифрування під час передачі:

- Чи забезпечує постачальник хмарних послуг шифрування в стані спокою за допомогою захищених протоколів (таких як TLS 1.2 або вище) для кожної з підтримуваних служб?
- Якщо постачальник хмарних послуг надає доступ до HTTPS-сервісів в Інтернеті, чи всі сервіси (або URL-адреси) отримують оцінку A+ у тесті SSL Labs (https://www.ssllabs.com/ssltest)?

Шифрування в стані спокою:

- Чи пропонує постачальник хмарних послуг шифрування для баз даних у стані спокою?
- Чи пропонує постачальник хмарних послуг шифрування для сховища об'єктів у стані спокою?
- Чи пропонує постачальник хмарних послуг шифрування в стані спокою для протоколів обміну файлами (таких як Передача файлів по мережі(NFS) або Звичайна передача файлів через Інтернет(CIFS)/Блок повідомлень сервера (Малий та середній бізнес))?
- Чи пропонує постачальник хмарних послуг механізм ротації ключів для кожного з підтримуваних механізмів шифрування в стані спокою?

- Чи підтримує постачальник хмарних послуг ключі, керовані клієнтом, для кожного з підтримуваних механізмів шифрування в стані спокою?

Реагування на інциденти:

- Чи має постачальник хмарних послуг вбудовані механізми для виявлення інцидентів безпеки на своїй інфраструктурі або інфраструктурі, що обслуговує його клієнтів?
- Чи має постачальник хмарних послуг задокументований процес реагування на інциденти?
- Чи має постачальник хмарних послуг спеціалізовану команду реагування на інциденти?
- Яка угода про рівень обслуговування постачальника хмарних послуг щодо обробки інцидентів безпеки?
- Яка угода про рівень обслуговування постачальника хмарних послуг щодо обробки критичних вразливостей?

Тестування на проникнення та оцінка безпеки:

- Чи проводив постачальник хмарних послуг оцінку безпеки зовнішнім аудитором протягом останніх 12 місяців?
- Якщо постачальник хмарних послуг проводив оцінки безпеки в минулому, чи всі вразливості були виправлені?
- Чи проводив постачальник хмарних послуг тестування на проникнення зовнішнім аудитором протягом останніх 12 місяців?
- Якщо постачальник хмарних послуг проводив тестування на проникнення в минулому, чи всі вразливості були виправлені?
- Чи дозволить хмарний провайдер своїм клієнтам планувати тестування на проникнення?

Безпечний життєвий цикл розробки:

- Чи проводить постачальник хмарних послуг постійне навчання для своїх співробітників (та сторонніх постачальників) щодо безпечної розробки?
- Чи дотримується постачальник хмарних послуг відомої методології життєвого циклу безпечної розробки (наприклад, життєвого циклу безпеки Microsoft, платформи безпечної розробки програмного забезпечення NIST або якоїсь іншої методології)?
- Чи впроваджує постачальник хмарних послуг Статичне тестування безпеки додатків (SAST) як частину свого безпечного життєвого циклу розробки?
- Чи впроваджує постачальник хмарних послуг Динамічне тестування безпеки застосунків (ДАСТ) як частину свого безпечного життєвого циклу розробки?
- Чи впроваджує постачальник хмарних послуг Інтерактивне тестування безпеки застосунків (ІАСТ) як частину свого безпечного життєвого циклу розробки?

- Чи впроваджує постачальник хмарних послуг аналіз складу програмного забезпечення (СКА) як частину свого безпечного життєвого циклу розробки?
- Як постачальник хмарних послуг зберігає таємниці (такі як ключі API, привілейовані облікові дані та ключі SSH) у своїй інфраструктурі та коді?
- Які засоби контролю безпеки впровадив постачальник хмарних послуг для обробки завантаження файлів?

Аудит та моніторинг:

- Чи веде постачальник хмарних послуг журнал аудиту кожної спроби входу до своїх сервісів (як успішних, так і невдалих)?
- Чи веде постачальник хмарних послуг журнал аудиту дій, виконаних над його сервісами (як успіхів, так і невдач)?
- Які записи зберігає постачальник хмарних послуг у рамках процесу реєстрації?
- Чи веде постачальник хмарних послуг облік дій, виконаних його власними системними адміністраторами (включаючи сторонніх постачальників), які мають доступ до інфраструктури та даних клієнтів?

Безперервність бізнесу:

- Чи надає постачальник хмарних послуг інформацію про перебої в обслуговуванні та історичну інформацію про минулі перебої?
- Чи має постачальник хмарних послуг задокументовані процеси забезпечення безперервності бізнесу та відновлення після аварій?
- Що таке хмарний постачальник Цільовий час відновлення (РТО)?
- Що таке постачальник хмарних послуг Мета точки відновлення (РПО)?
- Чи має постачальник хмарних послуг задокументовані процеси управління змінами?
- Чи має постачальник хмарних послуг задокументовані процеси резервного копіювання?

Пов'язані з дотриманням вимог:

- Який стандарт ISO, пов'язаний з хмарою та хмарною безпекою, застосовується постачальником хмарних послуг за останні 12 місяців?
- Чи опублікував постачальник хмарних послуг угоду про сумісність послуг (CSA)? Безпека, довіра, гарантії та ризик (ЗІРКА) звіт?
- Чи публікував постачальник хмарних послуг звіт SOC 2 протягом останніх 12 місяців?
- Чи має постачальник хмарних послуг задокументовану політику інформаційної безпеки?
- Чи має постачальник хмарних послуг спеціалізовану Головний спеціаліст з інформаційної безпеки (CISO (Інформаційна служба))/Директор зі стратегії (CSO)?

- Які логічні засоби контролю впроваджує постачальник хмарних послуг для захисту своєї інфраструктури?
- Які логічні засоби контролю пропонує хмарний провайдер для захисту даних клієнтів?
- Які логічні засоби контролю були застосовані до співробітників хмарних постачальників, які мають доступ до інфраструктури та даних клієнтів (наприклад, захист від шкідливого програмного забезпечення, контроль пристроїв, повне шифрування диска, багатофакторна автентифікація та VPN-клієнт)?
- Які фізичні засоби контролю впроваджує постачальник хмарних послуг для захисту своїх центрів обробки даних?
- Чи проводить постачальник хмарних послуг постійну оцінку вразливостей?
- Чи здійснює постачальник хмарних послуг постійне управління виправленнями?
- Чи відповідає інфраструктура постачальника хмарних послуг (обчислення, сховище та мережа) відомим стандартам посилення захисту (таким як бенчмарки CIS, NIST тощо)?
- Чи проводить постачальник хмарних послуг постійне навчання для своїх співробітників (та сторонніх постачальників) щодо інформаційної безпеки та конфіденційності даних?

CSA Матриця хмарних елементів керування (CCM) - це система контролю кібербезпеки для хмарних обчислень.

Для отримання додаткової інформації зверніться до наступних ресурсів:
https://cloudsecurityalliance.org/research/cloud-controlsmatrix/
Що, чому та як у відповідях на анкети безпеки:
https://learn.g2.com/security-questionnaire
7 критеріїв оцінки хмарних сервісів, які допоможуть вам вибрати правильного постачальника хмарних послуг:
https://www.threatstack.com/blog/7-cloud-service-evaluationcriteria-to-help-you-choose-the-right-cloud-service-provider
8 критеріїв, які допоможуть вам вибрати правильного постачальника хмарних послуг:
https://www.cloudindustryforum.org/content/8-criteria-ensureyou-select-right-cloud-service-provider

Поради щодо укладання договорів з постачальниками хмарних послуг

Гарний контракт захищає вашу організацію під час взаємодії з постачальниками хмарних послуг, оскільки ви не маєте фізичного контролю над своїми даними. Ви не завжди маєте можливість впливати на контракти з постачальниками хмарних послуг.

Щоб користуватися послугами IaaS, вам потрібен лише номер кредитної картки. Як невелика організація, ви отримаєте такий самий контракт, як і всі інші

клієнти, і після того, як ви погодитеся з умовами контракту, ви не зможете вносити жодних змін.

Якщо ви можете взяти на себе зобов'язання щодо значного споживання хмарних сервісів, ви можете зв'язатися зі своїм постачальником IaaS та підписати угоду, таку як AWS. Програма знижок для підприємств (ЕДП) або угод Azure EA, щоб мати змогу домовлятися про умови ціноутворення.

Щоб користуватися SaaS-сервісами, ви підписуєте контракт з обраним вами SaaS-провайдером, де маєте можливість впливати на умови контракту - набагато більше, ніж просто питання ціноутворення.

В цій темі ми розглянемо поширені питання, які слід обговорювати та включати до контрактів з постачальниками хмарних послуг:

Умови виходу:

- Які є можливості для розірвання договору у клієнтів?
- Чи є якісь штрафи з боку клієнтів за розірвання договору?

Розташування даних:

- Чи вказано в договорі точне місцезнаходження даних (тобто країну)?
- Чи містить контракт угода про обробку даних для встановлення місця розташування даних клієнтів та того, чи можна обробляти дані за межами певної країни?
- Чи вказано в договорі, як постачальник хмарних послуг захищатиме дані клієнтів?

Видалення даних:

- Чи зобов'язаний постачальник хмарних послуг видаляти дані клієнтів під час розірвання договору?
- Які стандарти видалення даних використовує постачальник хмарних послуг під час розірвання договору зі своїми клієнтами?
- Як довго постачальник хмарних послуг зберігатиме дані клієнтів після розірвання договору?

Експорт даних:

- Чи існує зобов'язання з боку постачальника хмарних послуг повертати дані клієнтів після розірвання договору?
- Які опції пропонує хмарний провайдер своїм клієнтам для експорту резервних копій своїх даних після розірвання договору?

Реагування на інциденти:

- Чи вказано в договорі, які зобов'язання постачальника хмарних послуг щодо обробки інцидентів безпеки систем, що зберігають або обробляють дані клієнтів?

- Яка угода про рівень обслуговування постачальника хмарних послуг щодо виправлення вразливостей безпеки в системах, які зберігають або обробляють дані клієнтів?
- Яка угода про рівень обслуговування постачальника хмарних послуг щодо повідомлення своїх клієнтів про інциденти безпеки, що впливають на системи, що зберігають або обробляють дані клієнтів?
- Чи уточнює контракт, які зобов'язання мають сторонні постачальники хмарного провайдера щодо систем, що зберігають або обробляють дані клієнтів?
- Чи містить контракт інформацію про обізнаність у сфері безпеки, конфіденційність та безпечну розробку для співробітників постачальника хмарних послуг та сторонніх постачальників?

Для отримання додаткової інформації зверніться до наступних ресурсів:
Угоди та поправки до Azure EA: https://surl.lu/bmmbog

Проведення тестування на проникнення в хмарних середовищах

Один із способів підвищити нашу впевненість у постачальнику хмарних послуг - це провести тест на проникнення, щоб виміряти ефективність їхніх засобів контролю безпеки.

У моделі SaaS тест на проникнення дозволяє нам оцінити, як постачальник SaaS захищає наші дані. У моделі IaaS тест на проникнення дозволяє нам оцінити ефективність впроваджених нами засобів контролю безпеки. У середовищах IaaS ми відповідаємо за рівень ОС та мережеве середовище навколо віртуальних машин або контейнерів.

У середовищах PaaS, зокрема в безсерверних (або Функція як послуга(FaaS)), ми не відповідаємо за нижній рівень ОС; однак, оскільки ми імпортуємо наш код, ми відповідаємо за дотримання безпечного життєвого циклу розробки.

У SaaS-середовищі ми відповідаємо лише за введення даних та контроль доступу до сервісу.

Якщо ми надаємо сервіс в Інтернеті або використовуємо SaaS-сервіс, нам потрібно оцінити такі теми, як:

- Чи дозволяє сервіс лише мінімальну кількість портів/протоколів для загальнодоступного Інтернету?
- Чи застосовує служба належні засоби контролю автентифікації, щоб забезпечити доступ до неї лише автентифікованим особам?
- Чи забезпечує служба належний контроль авторизації, щоб переконатися, що автентифіковані особи мають мінімальний обсяг доступу, необхідний для виконання своїх завдань?
- Чи виконує служба належну перевірку вхідних даних, щоб переконатися, що всі дані, введені в систему, очищені, а система захищена від атак ін'єкцій, міжсайтового скриптингу та будь-яких інших атак, що виникають внаслідок неправильної перевірки вхідних даних?

- Чи виконує сервіс вилучення даних перед вставкою у серверну базу даних - даних, які потенційно можуть повернутися до кінцевого клієнта та вплинути на нього?
- Чи веде сервіс журнал аудиту будь-яких спроб доступу та запитів, виконаних кінцевим клієнтом?

Тест на проникнення разом з оцінкою вразливостей дозволяє нам виміряти засоби контролю безпеки сервісів; однак, ми завжди повинні пам'ятати, що хмарні середовища відрізняються від локальних.

За своєю суттю, хмарні середовища є публічними та спільними для багатьох клієнтів.

Ми повинні дотримуватися умов використання постачальника хмарних послуг. Якщо ми не використовуємо SaaS-сервіс від одного з постачальників гіпермасштабної хмари, є ймовірність, що SaaS-сервіс розгортається над одним із постачальників гіпермасштабної IaaS, тобто ми повинні дотримуватися всього ланцюжка поставок - умов використання як постачальників IaaS нижчого рівня, так і SaaS вищого рівня.

Зрілі хмарні провайдери будують свої сервіси за повністю багатоорендарною моделлю, що означає, що кожен клієнт матиме власну виділену інфраструктуру (наприклад, сервери, базу даних, сховище та розділення мережі).

Не так рідко можна зустріти SaaS-провайдера, який пропонує нам свої послуги, одночасно обмінюючись ресурсами між клієнтами (наприклад, спільним використанням віртуальних серверів та баз даних).

У сценаріях, коли постачальник SaaS не використовує сучасну хмарну архітектуру (тобто багатокористувацьку оренду), атака зловмисника на одного клієнта збільшить ймовірність того, що наша організація по Guardian дає під час роботи з тим самим постачальником SaaS.

Більшість постачальників IaaS дозволять вам запускати інструменти безпеки на віртуальних серверах у вашому середовищі IaaS, сканувати порти або тестувати прикладний рівень (наприклад, атаки з використанням ін'єкцій) на віртуальних серверах у вашому середовищі IaaS.

Постачальники SaaS дозволять вам проводити тести безпеки у вашому середовищі, за умови, що SaaS спочатку було створено в багатокористувацькому середовищі.

Цілком ймовірно, що жоден постачальник хмарних послуг не дозволить вам виконувати атаки типу «відмова в обслуговуванні» на хмарну інфраструктуру або будь-які спроби порушення чи впливу на середовища чи ресурси інших клієнтів.

Для отримання додаткової інформації зверніться до наступних ресурсів:
AWS –*Тестування на проникнення*: https://surl.li/zlmlka
Google –*Найчастіші запитання щодо хмарної безпеки*: https://surli.cc/zrgkhe

Підсумки Розділу 3

У Розділі 3 зосереджено увагу на дотриманні загальних правил та стандартів у процесі використання хмарних сервісів. Для кожного з розглянутих нормативів і стандартів подано ключові положення та найкращі практики як для постачальників хмарних послуг, так і для клієнтів/організацій, що споживають відповідні сервіси.

Володіння знаннями щодо чинних стандартів дозволяє формувати чіткі вимоги до хмарних постачальників, а також визначати, які саме механізми безпеки необхідно впроваджувати з урахуванням законодавчих та галузевих обмежень. Вказано на практичне значення звітів SOC 2 Type 2 та Матриці контролю хмарних сервісів CSA як основних джерел інформації для оцінювання відповідності. Анкетування постачальників визначено як один із дієвих інструментів виявлення рівня надійності та зрілості їхніх практик.

Проаналізовано вивчення методів вимірювання ефективності хмарних середовищ. У цьому контексті розглянуто як можливості тестування на проникнення для IaaS-рішень, що розгортаються та адмініструються клієнтами, так і аспекти дотримання політик безпеки у випадку використання SaaS-пропозицій.

Засвоєння матеріалу цього розділу дозволяє клієнтам отримати впевненість у використанні хмарних сервісів, що зберігають або обробляють дані поза межами власних центрів обробки даних.

Контрольні питання до Розділу 3.

1. Що таке відповідність вимогам у хмарних сервісах?
2. Як модель спільної відповідальності розподіляє обов’язки між CSP та клієнтом?
3. Хто відповідає за фізичну інфраструктуру в IaaS/PaaS-моделі?
4. Хто відповідає за рівень застосунків у SaaS?
5. Чому важливе використання сторонніх аудиторів для перевірки CSP?
6. Який сервіс AWS дозволяє постійно перевіряти відповідність налаштувань безпеки стандартам?
7. Який інструмент Azure забезпечує постійний моніторинг відповідності?
8. Як GCP Security Command Center допомагає підтримувати відповідність?
9. Де клієнт може переглянути офіційні звіти про відповідність постачальника хмари?
10. Чому важливий безперервний аудит конфігурацій у хмарі?
11. Що таке ISO/IEC 27001 і для чого він застосовується?
12. Які основні домени охоплює ISO 27001?
13. Чим ISO 27017 відрізняється від ISO 27001?
14. Які додаткові заходи безпеки вводить ISO 27017 для хмарних середовищ?
15. Що регламентує ISO 27018 і на кого він орієнтований?
16. Які права користувачів передбачає ISO 27018?
17. Що таке звіт SOC і для чого він використовується?

18.Чим відрізняється SOC 1 від SOC 2?
19.Яка різниця між SOC 2 Type 1 і SOC 2 Type 2?
20.Чому SOC 2 Type 2 є найбільш важливим для клієнтів?
21.Чим звіт SOC 3 відрізняється від SOC 2?
22.Що таке програма CSA STAR?
23.Яка різниця між STAR Level 1 і STAR Level 2?
24.Які документи CSA лежать в основі оцінки безпеки хмарних сервісів?
25.Що таке PCI DSS і які основні вимоги він висуває до безпеки карткових даних?
26.Назвіть три технічні вимоги PCI DSS для захисту даних кредитних карток.
27.Що таке GDPR і кого він стосується?
28.Які основні принципи GDPR впливають на хмарні сервіси?
29.Які технічні заходи слід застосовувати для захисту персональних даних відповідно до GDPR?
30.Що таке «угода про обробку даних» і чому вона важлива для хмарних сервісів?
31.Яка основна мета проведення тесту на проникнення у хмарних середовищах?
32. У чому полягає різниця між тестом на проникнення в моделях SaaS, IaaS та PaaS?
33. За які рівні безпеки відповідає користувач у середовищі IaaS?
34.Хто відповідає за безпечний життєвий цикл розробки у моделі PaaS?
35.Яку відповідальність несе користувач у SaaS-середовищі?
36.Назви принаймні три аспекти, які потрібно оцінити під час перевірки SaaS-сервісу, доступного через Інтернет.
37.Чому важливо перевіряти автентифікацію та авторизацію в хмарних сервісах?
38.Які загрози може спричинити відсутність належної перевірки вхідних даних?
39.Яку роль відіграє журнал аудиту у забезпеченні безпеки хмарного сервісу?
40.Чим хмарні середовища принципово відрізняються від локальних середовищ з точки зору безпеки?
41.Що означає поняття «багатоорендарна модель» у контексті хмарних сервісів?
42.Які ризики виникають, якщо постачальник SaaS не використовує багатоорендарну архітектуру?
43.Чому важливо дотримуватися умов використання постачальників IaaS та SaaS?
44.Які види тестів безпеки зазвичай дозволяють постачальники IaaS і SaaS?
45.Чому постачальники хмарних послуг забороняють атаки типу «відмова в обслуговуванні» (DoS)?

РОЗДІЛ 4. РОЗШИРЕНЕ ВИКОРИСТАННЯ ХМАРНИХ СЕРВІСІВ

Після завершення цієї частини ви матимете ґрунтовне розуміння передових методів використання хмарних сервісів.

Ця частина посібника складається з наступних параграфів:

- *4.1. Управління гібридними хмарами*
- *4.2. Керування багатохмарними середовищами*
- *4.3. Безпека у великомасштабних середовищах*

4.1. Управління гібридними хмари

Гібридна хмара - це поєднання локального центру обробки даних або приватної хмари та середовища публічної хмари.

Гібридна хмара вважається продовженням нашого локального центру обробки даних і, як така, допомагає нам мінімізувати зусилля, необхідні для контролю, обслуговування та захисту нашої інфраструктури та послуг у всьому гібридному рішенні.

Ми не лише розширюємо інфраструктуру нашого локального центру обробки даних до хмари, але й розширюємо межі нашої безпеки до хмари, тому ми хочемо мати централізований спосіб контролю операцій безпеки в гібридній архітектурі.

У цьому розділі ми розглянемо такі теми:

- Стратегія гібридної хмари.
- Керування ідентифікаторами в гібридних хмарних середовищах.
- Мережева архітектура для гібридних хмарних середовищ.
- Сервіси зберігання даних для гібридних хмарних середовищ.
- Обчислювальні сервіси для гібридних хмарних середовищ.
- Захист гібридних хмарних середовищ.

Технічні вимоги

Для цього розділу вам потрібно буде мати ґрунтовне розуміння таких концепцій, як управління ідентифікацією, мережа, сховище даних, обчислення та способи забезпечення безпеки хмарних середовищ.

Стратегія гібридної хмари

Перш ніж використовувати гібридну хмарну архітектуру, нам потрібно запитати себе, чого ми намагаємося досягти за допомогою гібридного хмарного рішення?

Хмарні рішення для гібридних середовищ мають такі переваги:

- Інтеграція локальних ресурсів із хмарними ресурсами
- Вбудована інтеграція з хмарними сервісами
- Практично необмежена ємність (обчислювальна та сховище) для зберігання журналів та виконання кореляцій між подіями
- Практично необмежений обсяг сховища для зберігання даних (для резервного копіювання, дотримання нормативних вимог, аварійного відновлення тощо)
- Підтримка федеративного керування ідентифікаторами (дозволяє одній ідентифікаційній особі отримувати доступ до ресурсів у гібридних середовищах)

Розрив хмар

Ідея хмарного розгортання полягає в тому, щоб дозволити програмам, що працюють локально, розгортатися в хмарі, коли виникає потреба в додаткових ресурсах - як запланованих, так і незапланованих.

Деякі приклади розриву хмар наведені нижче:

- Великий попит на хмарні ресурси протягом короткого періоду з вихідних Чорної п'ятниці до Кіберпонеділка
- Кампанія, під час якої телефонна компанія виводить на ринок новий продукт
- Великі пакетні обробки, такі як генетичні дослідження

Резервне копіювання та відновлення після аварій

Хмара - це чудове рішення для резервного копіювання та/або аварійного відновлення ваших локальних середовищ. Вона (майже) не має обмежень для зберігання довгострокових резервних копій і дуже добре підходить для побудови цілих середовищ протягом кількох хвилин, щоб забезпечити аварійне відновлення.

Архів та зберігання даних

Регулювання може вимагати від нас архівування журналів та їх зберігання протягом тривалого періоду (років).

Хмара пропонує нам дешеве рішення для архівування рівнів зберігання.

Розподілена обробка даних

Якщо є потреба в обробці величезних обсягів даних (наприклад, Apache Hadoop), високопродуктивні обчислення (наприклад, прогнозування погоди) або машинне навчання (наприклад, аналіз відео), хмара може бути ідеальним рішенням.

Щоразу, коли у нас немає необхідних ресурсів у нашому локальному центрі обробки даних, ми можемо розгорнути кластери в хмарі, виконати процес аналізу даних і, після завершення процесу, видалити всі непотрібні ресурси, щоб заощадити гроші.

Модернізація застосунків

Щоб уникнути обмежень локальної та застарілої інфраструктури, хмара дозволяє нам перепроектувати наші програми та перейти на сучасні архітектури, такі як мікросервіси, або навіть стати безсерверними.

Деякі робочі навантаження можна перенести в хмару (наприклад, сучасні розробки), тоді як інші робочі навантаження повинні залишатися локально (через правила, які змушують нас зберігати дані локально) - таке змішане середовище створює гібридну архітектуру.

Хмарна стратегія допомагає організаціям вирішити, що робити зі своїми існуючими програмами та системами:

- Вихід на пенсію. Визначте, які програми більше не потрібні.
- Зберегти. Визначте, які програми потрібні, але міграція до хмари буде занадто складною і має залишатися локально.
- Замінити. Вирішіть, які програми можна замінити керованими послугами або SaaS-рішеннями.
- Перехостинг. Визначте, які програми можна підняти та змістити з мінімальними зусиллями для хмари
- Переплатформування. Визначте, які програми потребують мінімальних змін для перенесення в хмару (наприклад, оновлення ОС).
- Рефакторинг. Визначте, яка програма потребує значних змін для перенесення в хмару (наприклад, перехід від монолітної до мікросервісної архітектури).
- Переосмислити. Визначте, які програми потрібно перебудувати з нуля, щоб скористатися перевагами хмари (такими як еластичність, багаторегіональність тощо).

Для отримання додаткової інформації зверніться до наступних ресурсів:
Стратегія міграції бази даних AWS: https://surl.lu/qleycr
Гібридна хмара: Забезпечення ротації до нового:
https://surl.li/glvvcn

Керування ідентифікаторами в гібридних хмарних середовищах

Одним із перших рішень перед використанням гібридної хмари є управління ідентифікацією. Організації хотіли зберегти свого існуючого постачальника ідентифікаційних даних, мати єдину ідентифікаційну особу для кожного зі своїх кінцевих користувачів (зберігаючи при цьому існуючі облікові дані) та все ще мати можливість доступу до ресурсів у хмарі.

Керування ідентифікацією в гібридних хмарних середовищах можна розділити на такі області:

- Реплікація каталогів Розширення локального каталогу в хмару з односторонньою реплікацією або синхронізацією між ними.

- Федеративна автентифікація Локальний компонент здійснює автентифікацію користувача в хмарі за допомогою SAML, OIDC або іншого протоколу.

Деякі переваги використання централізованого управління ідентифікацією наведені нижче.

- Єдине місце для надання або скасування надання ідентифікаторів.
- Повторне використання надійних облікових даних та можливостей автентифікації.
- Централізація аудитів доступу.
- Уникайте підтримки кожного механізму хмарної ідентифікації.

Як керувати ідентифікацією в гібридних середовищах AWS

Локальні середовища можуть мати різні типи постачальників ідентифікаційних даних - від Active Directory (AD) (для програм на базі Windows) до каталогів ідентифікаційних даних на базі LDAP (здебільшого для програм на базі Linux). Організація також може розглянути Мова розмітки тверджень безпеки(SAML)-автентифікація для хмарних сервісів.

Amazon підтримує такі рішення для керування ідентифікацією для гібридних середовищ:

- *AWS IAM зі службами федерації AD(ADFS).* Надає вам можливість використовувати службу каталогів AWS IAM на основі SAML для керування вашими локальними ідентифікаторами (з локальної служби AD).
- *Керований Microsoft AD від AWS.* Повністю керована служба Active Directory дозволяє керувати ідентифікаторами користувачів з локальної служби Active Directory або локального постачальника LDAP (зазвичай для програм на базі Linux).
- *Роз'єм.* ADпроксі-сервіс, який дозволяє керувати сервісами AWS, такими як Amazon WorkSpaces, Amazon EC2 та іншими, за допомогою локальної Active Directory.
- *Єдиний вхід AWS.* Це дозволяє централізовано створювати ідентифікаційні дані в організаціях AWS або переносити ідентифікаційні дані з Microsoft AD чи інших постачальників ідентифікаційних даних (таких як Okta, OneLogin тощо).

Для отримання додаткової інформації зверніться до наступних ресурсів:
Що таке служба каталогів AWS?: https://surli.cc/lfgxqe
Поширені запитання щодо єдиного входу в AWS: https://surl.li/inrxpf

Як керувати ідентифікаторами в гібридних середовищах Azure

Azure підтримує такі рішення для керування ідентифікацією для гібридних середовищ:

- Azure AD Автентифікація на основі SAML. Під час синхронізації з локальною AD (за допомогою Azure AD Connect) ви можете мати єдину ідентифікаційну особу з доступом (відповідно до потреб бізнесу) як до локальних ресурсів, так і до хмарних ресурсів (таких як ресурси Azure та будь-який хмарний сервіс на основі SAML).
- Служби доменів Azure AD Роль, яка дозволяє інтеграцію застарілих протоколів, таких як Kerberos (для програм на базі Windows) або LDAP (для програм на базі Linux).

Для отримання додаткової інформації зверніться до наступних ресурсів:
Інтеграції Azure Active Directory з протоколами автентифікації та синхронізації: https://surl.li/pbmdrc
в Azure Active Directory?: https://surl.li/hgejlf

Як керувати ідентифікацією в гібридних середовищах GCP

Google підтримує такі рішення для керування ідентифікацією для гібридних середовищ:

- *Google Cloud Identity зі службами федерації AD(AD FS).* Надає вам можливість використовувати служби каталогів на основі SAML для керування локальними ідентифікаторами (з локальної служби AD) або LDAP (для програм на базі Linux).
- *Керований сервіс Google для Microsoft AD.* Повністю керована AD, яка дозволяє керувати ідентифікаторами користувачів з локальної AD.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Розгортання служб федерації Active Directory: https://surl.li/zsahrc

Найкращі практики керування ідентифікаторами в гібридних середовищах

Оскільки управління ідентифікацією дотримується тих самих концепцій у різних сценаріях гібридної хмари, рекомендується дотримуватися цих рекомендацій:

- Завжди передавайте інформацію для автентифікації через захищені протоколи - від TLS для автентифікації на основі SAML, через Kerberos всередині міжсайтових VPN-тунелів (через IPsec) до LDAP через SSL (LDAPS).
- Увімкнути Багатофакторна автентифікація (МЗС) для будь-якого облікового запису з правами доступу до хмарного середовища.
- Коли ви надаєте доступ до ресурсів, завжди дотримуйтесь концепції найменші привілеї.
- Увімкніть аудит усіх подій входу (як успішних, так і невдалих) та надсилайте журнали до бажаної вами системи SIEM.

- Створіть правила у вашій системі SIEM, щоб сповіщати вас про аномальну поведінку (наприклад, вхід root або адміністратора, кілька невдалих входів тощо).
- Використовуйте спеціалізовані послуги, такі як Amazon Guard Duty, Захисник Microsoft для хмари, Центр команд безпеки Google, та багато іншого для виявлення атак на основі ідентифікації.
- Коли це можливо, використовуйте Управління ідентифікацією(ІДМ) системи для забезпечення, скасування забезпечення та керування доступом (дозволами) в усьому вашому гібридному середовищі.

Мережева архітектура для гібридних хмарних середовищ

Другий важливий момент, який слід враховувати під час побудови гібридної архітектури, - це те, як підключитися з локального середовища до хмари.

Рекомендований спосіб підключення до хмарних середовищ, розглядаючи хмару як розширення локального центру обробки даних, полягає у використанні безпечного та постійного мережевого з'єднання - або VPN типу «сайт-сайт», або виділеного з'єднання.

Захищене та постійне з'єднання дозволить вам встановити контроль доступу (правила брандмауера 4-го рівня) між локальними та хмарними сегментами, а також зберегти доступ до ресурсів у хмарі (або дозволити доступ із хмарних ресурсів до локального середовища) відповідно до потреб бізнесу. Нижче наведено деякі рішення, які ви можете обрати залежно від конкретної ситуації, з якою ви маєте справу:

Вам слід обрати VPN-рішення в таких ситуаціях:

- Вам потрібен швидкий час розгортання.
- Ви можете проходити тунель IPsec через Інтернет.
- У вас немає вимог до пропускної здатності.
- Ви шукаєте недороге рішення.

Вам слід обрати з'єднання (Пряме підключення AWS(DX), Azure ExpressRoute, З'єднання Google Cloud) у таких ситуаціях:

- У вас є вимоги до пропускної здатності (вам потрібне рішення з фіксованою пропускною здатністю).
- Ви б хотіли мати Угоди про рівень обслуговування(Угоди про рівень обслуговування (SLA)) щодо підключення до мережі.
- Ви хочете мати приватне з'єднання між вашим локальним середовищем та хмарним середовищем.

Як підключити локальне середовище до AWS

Amazon пропонує такі послуги для забезпечення гібридного підключення:

- Керована VPN-мережа типу «сайт-сайт» від AWSПовністю керований VPN-сервіс, який забезпечує підключення від шлюзу клієнта (клієнтська сторона VPN) через тунель IPsec.

- AWS VPN CloudHub Модель «хаб і спиці», яка використовує VPN-мережі під керуванням AWS для підключення Amazon VPC до кількох центрів обробки даних клієнтів, кожен з яких має власні тунелі IPsec.
- Транзитний шлюз AWS та VPN: Служба, яка дозволяє підключення до однієї мережі (хабу) через VPN-тунель між локальним середовищем та кількома VPC в одному регіоні.
- AWS DX Виділене з'єднання з локального середовища до одного або кількох віртуальних ПК в тому ж регіоні з попередньо визначеною пропускною здатністю мережі.
- AWS DX та транзитний шлюз AWS Виділене з'єднання з локального середовища до одного або кількох віртуальних ПК у максимум трьох регіонах із заздалегідь визначеною пропускною здатністю мережі.

Нижче наведено деякі найкращі практики, які слід пам'ятати:

- Завжди думайте про Безкласова міждоменна маршрутизація(CIDR) перед налаштуванням сегментів мережі в хмарі, щоб уникнути конфліктів IP-адрес між локальним середовищем і хмарою.
- Використання мережеві ACL, групи безпеки, та таблиці маршрутів налаштувати правила мережевого доступу між локальним середовищем та ресурсами всередині ваших віртуальних віртуальних ПК.
- Для резервування плануйте резервне підключення - з кількох VPN-підключень або резервних з'єднань - використовуючи різних мережевих провайдерів або комбінацію з'єднань та VPN-підключення.
- Використовуйте подвійне VPN-з'єднання типу «сайт-сайт» разом із транзитним шлюзом AWS для забезпечення резервування з'єднань між вашим локальним середовищем і хмарою.
- Використовуйте кілька DX-з'єднання зі шлюзом DX, щоб забезпечити резервування з'єднань між вашим локальним середовищем і хмарою.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Гібридне мережеве підключення: https://surl.li/kpgswv
Транзитний шлюз AWS та VPN: https://surl.li/hucnlm
AWS Direct Connect та AWS Transit Gateway: https://surl.li/womntj
AWS VPN CloudHub: https://surl.li/mfmuvr

Як підключити локальне середовище до Azure

Azure пропонує такі послуги для забезпечення гібридного підключення:

- Шлюз Azure VPN Повністю керований VPN-сервіс, який забезпечує підключення локального середовища до хмари через тунелі IPsec.
- Azure ExpressRoute Виділене підключення з локального середовища до однієї або кількох віртуальних мереж Azure у заздалегідь визначеній пропускній здатності мережі.

- Підключення до мережі Hub and Spoke Модель «хаб і спиці», яка використовує шлюз Azure VPN для підключення локального середовища до кількох віртуальних мереж за допомогою одного тунелю IPsec.

Нижче наведено деякі найкращі практики, які варто врахувати:

- Завжди думайте про CIDR перед налаштуванням сегментів мережі в хмарі, щоб уникнути конфліктів IP-адрес між локальним середовищем і хмарою.
- Використання Групи мережевої безпеки(НСГ) для налаштування правил доступу до мережі між локальним середовищем та ресурсами у ваших віртуальних мережах.
- Для резервування плануйте резервне підключення - з кількох VPN-підключень або резервного ExpressRoute з використанням різних мережевих провайдерів, або комбінації ExpressRoute та VPN-підключення.
- Використовуйте кілька VPN-підключень типу «сайт-сайт» для резервування підключень між локальним середовищем і хмарою.
- Налаштуйте кілька підключень з вашого локального середовища (через мережу вашого постачальника послуг) до каналу Azure ExpressRoute для забезпечення резервування підключень між вашим локальним середовищем і хмарою.

Для отримання додаткової інформації зверніться до наступного ресурсу:
Підключення локальної мережі до Azure: https://surl.li/auuvso

Як підключити локальне середовище до GCP

GCP пропонує такі послуги для забезпечення гібридного підключення:

- *Хмарний VPN від Google*. Повністю керований VPN-сервіс, який забезпечує підключення локального середовища до хмари через тунель IPsec.
- *З'єднання Google Cloud.* Виділене з'єднання з локального середовища до одного або кількох віртуальних ПК у заздалегідь визначеній пропускній здатності мережі.

Нижче наведено деякі найкращі практики, які варто врахувати:

- Завжди думайте про CIDR перед налаштуванням сегментів мережі в хмарі, щоб уникнути конфліктів IP-адрес між локальним середовищем і хмарою.
- Використання правила брандмауера налаштувати правила мережевого доступу між локальним середовищем та ресурсами всередині ваших віртуальних віртуальних ПК.
- Для резервування плануйте резервне підключення - від кількох VPN-підключень або резервного хмарного з'єднання з використанням різних мережевих провайдерів, або комбінацію хмарного з'єднання та VPN-підключення.
- Використовуйте Висока доступність(ХА) VPN для резервування з'єднань між вашим локальним середовищем та хмарою.

- Використання Виділений інтерконект для резервування з’єднань між вашим локальним середовищем та хмарою.

Для отримання додаткової інформації зверніться до наступного ресурсу: *Гібридні та мультихмарні мережеві топології*: https://surl.li/fznmbg

Сервіси зберігання даних для гібридних хмарних середовищ

Тепер, коли ми визначилися з управлінням ідентифікацією та топологією мережі, наступне, що нам потрібно розглянути, це як використовувати гібридні хмари для передачі та зберігання даних.

Розглядаючи можливість підключення гібридного сховища, враховуйте наступне:

- Пропускна здатність/затримка/час передачі.
- Використання публічного та приватного підключення.
- Переміщення файлів проти синхронізації файлів.
- Вимоги до шифрування (під час передачі та в стані спокою).
- Контроль доступу для гібридного рішення.
- Підтримувані протоколи (NFS, CIFS та інші).

Як підключитися до служб зберігання даних через гібридні середовища AWS

Amazon пропонує такі послуги для передачі даних у хмару в гібридній архітектурі:

- *Шлюз сховища AWS.* Віртуальний пристрій для встановлення локальних середовищ, який дозволяє доступ з локальних середовищ до служби сховища об'єктів (Amazon S3/Glacier), сховища файлів (Amazon FSx для Windows), блокове сховище (Amazon EBS) та служба резервного копіювання (Резервне копіювання AWS)
- *Синхронізація даних AWS.* Служба передачі даних між локальним середовищем та сховищем об'єктів (Amazon S3), сховище файлів NFS (Amazon EFS) та сховище файлів SMB (Amazon FSx для Windows)
- *Сімейство передачі AWS.* Служба передачі файлів між локальним середовищем та сховищем об'єктів (Amazon S3) або сховище файлів NFS (Amazon EFS), вище протоколів SFTP, FTPS та FTP

Нижче наведено деякі найкращі практики, які варто врахувати:

- Використання Шлюз сховища AWS коли вам потрібне постійне з’єднання між локальним середовищем та вашими сервісами зберігання даних AWS.
- Використання Синхронізація даних AWS коли вам потрібно скопіювати файли до/з хмари.
- Використання Сімейство передачі AWS коли ви хочете скопіювати файли в хмару через протоколи SFTP або FTPS.
- Завжди вибирайте захищені протоколи (такі як TLS, SFTP або FTPS) під час передачі файлів у хмару.

- Завжди налаштовуйте дозволи IAM для хмарних ресурсів відповідно до потреб вашого бізнесу.
- Увімкнути аудит будь-якого доступу до хмарних ресурсів.
- Шифруйте дані в стані спокою, коли вони зберігаються в хмарі.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Найчастіші запитання щодо шлюзу сховища AWS: https://surli.cc/krqsfh
Як працює AWS DataSync: https://surl.li/alsgik

Як підключитися до служб зберігання даних через гібридні середовища Azure

Azure пропонує такі сервіси для передачі даних у хмару в гібридній архітектурі:

- *Шлюз Azure Data Box.* Пристрій для встановлення локальних середовищ, який дозволяє копіювати дані з локального середовища до сховища Azure за допомогою протоколу NFS або SMB.
- *Фабрика даних Azure.* Вилучення-Перетворення-Завантаження (ETL) рішення для копіювання файлів до таких служб, як Azure Storage, Azure SQL, Azure HDInsight тощо.
- *Синхронізація файлів Azure.* Служба копіювання даних, яка інсталюється як агент на комп'ютерах Windows і дозволяє копіювати файли через протокол SMB або NFS до сховища Azure.

Нижче наведено деякі найкращі практики, які варто врахувати:

- Використання Шлюз Azure Data Box коли вам потрібен довгостроковий архів ваших даних або для передачі великих обсягів даних.
- Використання Фабрика даних Azure коли вам потрібно створити процес переміщення даних до/з хмари до таких сервісів, як Azure Storage, Azure SQL, Azure Data Lake Storage тощо.
- Використання Синхронізація файлів Azure коли вам потрібно скопіювати (або синхронізувати) файли до сховища Azure.
- Завжди вибирайте захищені протоколи (наприклад, TLS) під час передачі файлів у хмару.
- Завжди налаштовуйте дозволи для хмарних ресурсів відповідно до потреб вашого бізнесу.
- Увімкнути аудит будь-якого доступу до хмарних ресурсів.
- Шифруйте дані в стані спокою, коли вони зберігаються в хмарі.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Варіанти використання для Azure Data Box Gateway: https://surl.lu/pojmfv
Що таке Фабрика даних Azure?: https://surl.li/zxuqmd
Що таке синхронізація файлів Azure?: https://surli.cc/lprcde

Як підключитися до служб зберігання даних через гібридні середовища GCP

GCP пропонує послугу передачі локальних даних - програмний сервіс, який дозволяє передавати великі обсяги даних з локального середовища до Google Cloud Storage.

Нижче наведено деякі найкращі практики, які варто врахувати:

- Завжди вибирайте захищені протоколи (наприклад, TLS) під час передачі файлів у хмару.
- Завжди налаштовуйте дозволи на хмарні ресурси відповідно до потреб вашого бізнесу.
- Увімкнути аудит будь-якого доступу до хмарних ресурсів.
- Шифрування дані в стані спокою коли воно зберігається в хмарі.

Для отримання додаткової інформації зверніться до наступного ресурсу:
Огляд служби передачі локальних даних: https://surl.lu/vabmsc

Обчислювальні сервіси для гібридних хмарних середовищ

Гібридна хмарна архітектура не обмежується лише підключенням локальних середовищ до хмари для споживання ресурсів. Вона також може використовуватися в сценаріях, коли організація хоче зберігати свої дані локально (через регуляторні обмеження або затримку мережі), водночас користуючись перевагами хмарних можливостей і, можливо, колись у майбутньому, мати можливість переносити дані та ресурси до хмари.

Використання обчислювальних сервісів у гібридних середовищах AWS

Amazon пропонує такі послуги в топології локального розгортання:

- *Аванпости AWS.* Повністю керований сервіс, що містить той самий тип обчислювальних, сховищних, баз даних та мережевих можливостей, що й локально у формі фізичної стійки.
- *Amazon ECS Anywhere.* Дає вам можливість розгортати Amazon ECS локально (ті ж можливості та API, що й у хмарній версії)
- *Amazon EKS Anywhere.* Дає вам можливість розгортати Сервіс Amazon Kubernetes(EKC) локально (ті ж можливості, що й у хмарній версії)

Нижче наведено деякі найкращі практики, які варто врахувати:

- Підключіть локальний сервіс (AWS Outposts, ECS Anywhere або EKS Anywhere) до регіону AWS, розташованого поблизу вашого фізичного місцезнаходження.
- Переконайтеся, що між вашим локальним центром обробки даних (де ви локально розгорнули попередні служби) та регіоном AWS є мережеве з’єднання.

- Використання Аванпости AWS коли ви хочете розгорнути локально сервіси AWS (EC2, EBS, RDS тощо), щоб ваші дані не залишали ваш центр обробки даних (або вашу країну).
- Використання ВПК, групи безпеки, та Локальний шлюз (LGW) щоб обмежити доступ між ресурсами вашого локального центру обробки даних та ресурсами, розгорнутими в AWS Outposts.
- Використання зашифровані протоколи (наприклад, TLS) між вашим локальним центром обробки даних та сервісами AWS, які ви розгорнули локально (AWS Outposts, ECS Anywhere та EKS Anywhere).
- Шифрування дані в стані спокою для ресурсів, розгорнутих всередині AWS Outposts (так само, як і в хмарі).
- Використання Amazon ECS Anywhere розгортати середовища розробки або невеликі виробничі середовища ECS локально на основі ваших можливостей та API ECS, а потім перенести їх у хмару, щоб отримати повний доступ до сервісу Amazon ECS.
- Використання Amazon EKS Будь-де для розгортання середовищ розробки або невеликих виробничих середовищ Kubernetes локально на основі ваших можливостей EKS, а потім для швидкого перенесення в хмару, щоб мати повний доступ до сервісу Amazon EKS.
- Використовуйте мінімальний Дозволи IAM для всіх ресурсів AWS, розгорнутих локально (так само, як і в хмарі).
- Використання AWS CloudTrail для моніторингу активності всіх ресурсів AWS, розгорнутих локально (так само, як і в хмарі).

Для отримання додаткової інформації зверніться до наступних ресурсів:
Найчастіші запитання щодо Amazon ECS Anywhere: https://surli.cc/ebsicb
Найчастіші запитання щодо Amazon EKS Anywhere: https://surl.li/bqenou

Використання обчислювальних служб у гібридних середовищах Azure

Azure пропонує такі послуги в локальній топології розгортання:

- *Центр стека Azure.* Повністю керований сервіс, що містить той самий тип обчислювальних, сховищних, баз даних та мережевих можливостей, що й локально розгорнуті у формі фізичної стійки.
- *Лазурна дуга.* Сервіс, який дозволяє уніфіковано керувати вашими ресурсами - як в Azure, так і локально (налаштування політики Azure та керування віртуальними машинами, кластерами Kubernetes і базами даних з однієї консолі).

Нижче наведено деякі найкращі практики, які варто врахувати:

- Використання Центр стека Azure коли ви хочете розгорнути локально служби Azure (віртуальну машину, керовані диски Azure, сховище BLOB-об’єктів Azure тощо), щоб ваші дані не залишали ваш центр обробки даних (або вашу країну).

- Використовуйте вбудовані мережеві ACL Azure Stack Hub, щоб обмежити доступ між ресурсами вашого локального центру обробки даних та ресурсами, розгорнутими всередині Azure Stack Hub.
- Шифруйте всі дані під час передачі за допомогою Протокол TLS під час передачі трафіку між Azure Stack Hub та вашим локальним центром обробки даних.
- Підключення Центр стека Azuredo Azure AD або AD FS, щоб налаштувати мінімальний контроль доступу до ресурсів у Azure Stack Hub на основі ролей.
- Використання Захисник Microsoft для кінцевих точок щоб захистити віртуальні машини, розгорнуті в Azure Stack Hub, і переконатися, що ви оновлюєте антивірус.

Використовуйте Azure Arc для таких сценаріїв:

- Управління активами для всіх ваших ресурсів (віртуальних машин, Kubernetes та баз даних)
- Централізоване налаштування керування доступом на основі ролей як для ресурсів Azure, так і для локальних ресурсів
- Централізоване налаштування політик за допомогою Політика Azure, як на віртуальних машинах, так і на кластерах Kubernetes
- Оновлення патчів безпеки на серверах, як в Azure, так і локально
- Захист ваших серверів за допомогою Захисник Microsoft для хмари, як в Azure, так і локально
- Підключення всіх ваших серверів до Служба Azure Sentinel SIEM, як в Azure, так і локально
- Моніторинг ваших серверів за допомогою Монітор Azure, як в Azure, так і локально
- Захист кластерів Kubernetes за допомогою Захисник Microsoft для контейнерів, як в Azure, так і локально

Для отримання додаткової інформації зверніться до наступних ресурсів:

Що таке Azure Stack Hub?: https://surl.lt/psxihs
Огляд Azure Arc: https://surl.li/ueylkg

Використання обчислювальних сервісів у гібридних середовищах GCP

GCP пропонує послугу під назвою Кластери Антосу що дозволяє керувати та розгортати кластери Kubernetes у хмарі та локально (на основі платформи віртуалізації або bare metal).

Нижче наведено деякі найкращі практики, які варто врахувати:

- Використовуйте кластери Anthos, якщо хочете запускати кластер GKE локально, використовуючи ті самі можливості, версію та API, що й повністю керований GKE у хмарі.
- Використовуйте приватний сервер репозиторію пакетів, щоб забезпечити безпеку ваших пакетів і ніколи не залишати ваш локальний центр обробки

даних. Переконайтеся, що всі пакети використовують найновіші бібліотеки та бінарні файли.

- Використовуйте Інтерфейс зберігання контейнерів (Місце злочину) драйвер для підключення локального кластера Kubernetes до сховища.
- Використання Google Cloud IAM надати кластеру Kubernetes мінімальні дозволи на доступ до ресурсів.
- Якщо ви використовуєте RHEL або CentOS, обов'язково встановіть використання SELinux.

Для отримання додаткової інформації зверніться до наступного ресурсу: *Кластери Антосу*: https://surli.cc/wgorxz

Захист гібридних хмарних середовищ

Коли йдеться про захист гібридних хмарних середовищ, ми шукаємо рішення, які можуть централізовано керувати всім вашим середовищем (як локальним, так і хмарним).

Як захистити гібридні середовища AWS. AWS пропонує такі послуги для управління безпекою в гібридних середовищах:

- *Системний менеджер AWS*. Це дозволяє керувати віртуальними машинами з точки зору відповідності, управління виправленнями та посилення захисту (центральне розташування для запуску скриптів у гібридних середовищах).
- *Менеджер таємниць AWS.* Централізоване та захищене місце для керування секретами (обліковними даними, ключами API тощо) у гібридних середовищах.
- *Відновлення після аварій AWS Elastic*. Забезпечує безпечну реплікацію даних для аварійного відновлення між локальними середовищами та хмарою.
- *Агент Amazon CloudWatch.* Дозволяє збирати журнали ОС з віртуальних машин у гібридних середовищах.

Нижче наведено деякі найкращі практики, які варто врахувати:

- Розгортання Агент системного менеджера AWS як на хмарних екземплярах EC2, так і на локальних серверах (Windows або Linux).
- Використання Системний менеджер AWS щоб встановити базовий рівень виправлень та отримувати сповіщення про віртуальні машини, на яких відсутні виправлення безпеки (згодом ви можете надсилати виправлення безпеки за допомогою Systems Manager).
- Використання Агент системного менеджера AWS щоб передавати журнали аудиту з ваших локальних віртуальних машин до WS CloudTrail. Після того, як усі журнали будуть збережені в CloudTrail, ви можете використовувати AWS GuardDuty, щоб отримувати сповіщення про можливе порушення у вашому гібридному середовищі.
- Використання AWS IAM надати мінімальні дозволи, щоб дозволити вашим локальним віртуальним машинам взаємодіяти з сервісами AWS.

- Шифруйте весь трафік між вашими локальними агентами Systems Manager та службою AWS Systems Manager за допомогою TLS.
- Використання Менеджер систем AWS Менеджер змін щоб перевірити зміни конфігурації на всіх ваших віртуальних машинах (як у хмарі, так і локально).
- Використання Менеджер таємниць AWS генерувати, скасовувати, зберігати та отримувати конфіденційну інформацію (наприклад, облікові дані бази даних, ключі API тощо) замість зберігання таємниць, жорстко закодованих у ваших віртуальних машинах.
- Використання CloudTrail для аудиту активності API AWS Secrets Manager (наприклад, хто генерує таємниці, хто отримує доступ до таємниць тощо).
- Використання Відновлення після аварій AWS Elastic створити рішення для аварійного відновлення ваших локальних віртуальних машин шляхом реплікації цілих віртуальних машин у хмару.
- Розгортання Агент Amazon CloudWatch як на хмарних екземплярах EC2, так і на локальних серверах (Windows або Linux).
- Використання Журнали Amazon CloudWatch як центральне сховище журналів, де можна створювати сповіщення про такі дії, як невдалі входи, події, пов'язані з безпекою, з журналів подій безпеки ОС тощо.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Налаштування AWS Systems Manager для гібридних середовищ: https://surl.li/hxnjpz
Функції менеджера таємниць AWS: https://surl.li/vqfbbo
Відновлення після аварій AWS Elastic: https://surl.li/gnhvsp
Встановлення агента CloudWatch на локальних серверах: https://surl.li/tnyvud
Що таке журнали Amazon CloudWatch?: https://surli.cc/mjdysz

Як захистити гібридні середовища Azure

Azure пропонує такі послуги для керування безпекою в гібридних середовищах:

- *Захисник Microsoft для хмари.* Сервіс для захисту серверів і клієнтів (Windows та Linux) і баз даних SQL. Це також централізований сервіс для управління безпекою в хмарі та локально.
- *Azure Guardian Хмарний сервіс SIEM.*

Нижче наведено деякі найкращі практики, які варто врахувати:

- Розгортання Лазурна дуга і увімкнути Захисник Microsoft на всіх ваших віртуальних машинах, що знаходяться локально та в хмарі.
- Розгорніть Аналіз журналів агент на ваших локальних серверах, щоб дозволити отримання інформації безпеки всередині Консоль Microsoft Defender для хмари.
- Розгорніть Microsoft Defender для SQL у ваших локальних базах даних SQL.

- Використовуйте вбудовану оцінку вразливостей, яка постачається з Microsoft Defender for Cloud, щоб виявляти вразливості у вашому локальному середовищі та хмарі.
- Використовуйте Microsoft Defender для SQL, щоб сканувати всі ваші бази даних SQL на наявність вразливостей - як локально, так і в хмарі.
- Використовуйте кластери Microsoft Defender for Containers для захисту всіх кластерів Kubernetes - як локальних, так і хмарних.
- Підключіть Microsoft Defender for Containers до Azure Sentinel, щоб мати змогу співвідносити інциденти безпеки та реагування на сповіщення безпеки - як локально, так і в хмарі.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Що таке Microsoft Defender для хмари?: https://surl.li/okyyvb
Що таке Azure Sentinel?: https://surl.li/bdtzwz

Як захистити гібридні середовища GCP

GCP пропонує такі послуги для управління безпекою в гібридних середовищах:

- *Кінцеві точки Google Cloud*. Сервіс для захисту, моніторингу, аналізу та встановлення квот для API - як у хмарі, так і локально
- *Приватний доступ до Google*. Забезпечує приватний доступ до API та служб Google з локальних середовищ

Під час використання кінцевих точок Google Cloud пам’ятайте про наступне:

- Шифруйте трафік за допомогою SSL за допомогою Розширюваний проксі-сервер служби(Емоційне сприйняття (ЕСП)) для збереження конфіденційності конфіденційної інформації (як-от облікові дані, ідентифікаційна інформація тощо).
- Використовуйте ESP для перевірки запитів на автентифікацію до сервера API (наприклад, автентифікація Firebase, Auth0, автентифікація токенів Google ID тощо).
- Якщо ви використовуєте ключі API, обмежте доступ до цих ключів API за допомогою API керування послугами.
- Використовуйте Google Cloud IAM для обмеження доступу до API.

Коли вам потрібно отримати доступ до API або служб Google з локальних середовищ, пам’ятайте про наступне:

- Підключіться до свого VPC за допомогою Cloud VPN або Cloud Interconnect.
- Перенаправити трафік черезprivate.googleapis.com для API, які не підтримують елементи керування послугою VPC.
- Перенаправити трафік через restricted.googleapis.com для API, що підтримують елементи керування послугою VPC.

- Використовуйте правила брандмауера, щоб дозволити доступ з локального середовища до вашого VPC.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Документація хмарних кінцевих точок: https://surl.li/tpiahg
Налаштування приватного доступу до Google для локальних хостів: https://surl.li/cmlhzg

4.2. Керування багатохмарними середовищами

Багатохмарність полягає у використанні кількох хмар або постачальників хмарних послуг для налаштування спільного середовища, інфраструктури або навіть рівня додатків.

Організації, які роблять перші кроки у використанні хмарних сервісів, розглядають мультихмарний підхід як рішення для захисту себе від прив'язка до постачальника сценарій - сценарій, коли вся наша інфраструктура або програми залежать від екосистеми одного постачальника хмарних послуг.

Одне з питань, яке ставлять собі організації, полягає в тому, що нам робити, якщо постачальник хмарних послуг припинить свою діяльність? Як нам перенести наші активи до іншого постачальника хмарних послуг? Теоретично, багатохмарний підхід може вирішити ризик прив'язки до постачальника; однак організації повинні усвідомлювати складнощі, пов'язані з багатохмарними середовищами.

Безперервність бізнесу є ще однією важливою проблемою. Багатохмарна архітектура дозволяє нам розгортати робочі навантаження на кількох хмарних постачальниках, що зменшує вплив на бізнес, який може статися з одним хмарним постачальником (наприклад, збій у роботі служби автентифікації, який блокує нам роботу з сервісами, розгорнутими в хмарі).

Постачальник налаштований як резервний для іншого хмарного постачальника. Ці архітектури, засновані на контейнерах, забезпечують переносимість між хмарними постачальниками, одночасно зменшуючи залежність від конкретної хмарної екосистеми (від Віртуальні машини (Віртуальні машини), сервіси зберігання даних, керовані бази даних тощо). Мультихмарність дозволяє нам мати переваги екосистеми кожного хмарного постачальника, включаючи найновіші версії Kubernetes, найбільш масштабовану базу даних NoSQL та найновіші процесори GPU.

У цьому параграфі ми розглянемо такі теми:

- Мультихмарна стратегія.
- Керування ідентифікаторами в багатохмарних середовищах.
- Мережева архітектура для багатохмарних середовищ.
- Безпека даних у багатохмарних середовищах.
- Управління витратами в багатохмарних середовищах.
- Управління станом безпеки хмари (CSPM).

- Управління правами доступу до хмарної інфраструктури (CIEM).
- Керування виправленнями та конфігураціями в багатохмарних середовищах.
- Моніторинг та аудит багатохмарних середовищ.

Технічні вимоги

Для цього розділу вам потрібно мати ґрунтовне розуміння таких концепцій, як управління ідентифікацією, мережа, обчислення та як захистити хмарні середовища.

Багатохмарна стратегія

Перш ніж використовувати багатохмарну архітектуру, нам потрібно запитати себе, чого ми намагаємося досягти за допомогою багатохмарної стратегії? Деякі з найпоширеніших варіантів використання багатохмарної стратегії обговорюються в наступних розділах.

Свобода вибору постачальника хмарних послуг

Більшість хмарних постачальників пропонують нам однакові фундаментальні послуги (такі як обчислення, сховище та бази даних). Свобода вибору хмарного постачальника дозволяє нам вирішувати для кожного робочого навантаження, де ми хочемо розгорнути наші ресурси (віртуальні машини, контейнери, базу даних тощо), у випадку, якщо один із хмарних постачальників змінить свої Угода про рівень обслуговування (Угода про рівень обслуговування) або модель ціноутворення.

Свобода вибору послуг

Ця свобода означає, що якщо один із постачальників хмарних послуг пропонує певну послугу, яка недоступна в інших постачальників хмарних послуг, наприклад, аналітику даних для великих наборів даних, або пропозицію Functionas-a-Service, яка підтримує певну мову розробки, що не підтримується іншими постачальниками хмарних послуг, ви можете вільно обрати багатохмарну стратегію.

Знижена вартість

У більшості випадків розподіл робочих навантажень між кількома хмарними постачальниками збільшить вартість через витрати на вихідний трафік через Інтернет та між хмарними постачальниками, а також знання, необхідні для навчання персоналу роботі з кількома хмарними постачальниками.

Існують сценарії, коли ви можете використовувати одну й ту саму послугу від кількох хмарних постачальників, тоді як вартість використання послуги дешевша у одного з хмарних постачальників у регіоні, близькому до ваших клієнтів.

Організаціям необхідно враховувати, що розподіл робочих навантажень між кількома постачальниками хмарних послуг вплине на знижки на основі обсягу,

де вони можуть не досягти економії від масштабу. У контексті цього розділу організація повинна враховувати, які можливості вона повинна створити у всіх постачальників хмарних послуг.

Суверенітет даних

Хоча більшість великих постачальників хмарних послуг мають центри обробки даних у центральних районах США та Європи, існують випадки, коли місцеві закони чи нормативні акти вимагають від вашої організації зберігати дані клієнтів локально в певній країні. Можуть бути сценарії, коли певний постачальник хмарних послуг не має місцевої присутності в одному з регіонів вашого клієнта, що робить багатохмарний підхід відповідним рішенням.

Резервне копіювання та відновлення після аварій

Зберігання даних у кількох місцях, у кількох хмарних постачальників, зменшить ризик втрати даних вашою організацією або подолання проблем з доступністю послуг хмарних постачальників у певному регіоні, або навіть подолання глобальних проблем з доступністю послуг.

Підвищення надійності

Навіть попри те, що більшість великих постачальників хмарних послуг пропонують Розподілена відмова в обслуговуванні (DDoS-атак) служб захисту, можуть виникнути сценарії, коли один із постачальників хмарних послуг наразі сам перебуває під DDoS-атакою, постачальники хмарних послуг можуть поGuardian дати від перебоїв у наданні послуг, інтернет-провайдери можуть зіткнутися із затримкою, або робочі навантаження можуть вийти з ладу з різних причин.

Щоб підвищити надійність, розглянемо такі теми, як:

- Реплікація даних між хмарними провайдерами, що впливає на вартість (надмірне сховище, вартість передачі даних тощо).
- Сценарії перемикання на резервний рахунок - де ви керуєте своїми DNS-записами та оновлюєте їх у разі перемикання на резервний рахунок між провайдерами?
- Автоматизація - які інструменти чи сервіси ви використовуватимете для резервного перемикання між постачальниками?
- Знання - чи має ваш IT-персонал або розробник достатньо знань, щоб перемикатися між хмарними провайдерами?

Можливість перемикати свої робочі навантаження до іншого хмарного постачальника (за умови, що ви вже створили ціле виробниче середовище на іншому хмарному постачальнику та синхронізували дані) дозволить вам зменшити ризик недоступності ваших сервісів.

Управління ідентифікацією

Мультихмарна стратегія повинна враховувати управління ідентифікацією. Кожен постачальник хмарних послуг має власну Управління ідентифікацією та доступом(Ідентифікація та доступність) рішення, яке створює труднощі та

можливості для централізованого життєвого циклу ідентифікації (впровадження, управління доступом та виведення з експлуатації) та управління обліковими даними.

Вищезазначені проблеми посилюють мотивацію до централізації на одному Ідентифікація та доступність рішення, яке має бути інтегроване з кожним постачальником хмарних послуг.

Безпека даних

Мультихмарна стратегія повинна враховувати проблеми безпеки даних. Типові приклади безпеки даних у мультихмарному середовищі наведені нижче:

- Збереження місця розташування даних під час роботи з кількома хмарними постачальниками.
- Реплікація даних між хмарними постачальниками та в межах одного хмарного постачальника в кількох регіонах.
- Контроль доступу до ваших даних через кількох хмарних провайдерів.
- Шифрування та керування ключами через кількох хмарних провайдерів.
- Аудит доступу до даних за допомогою децентралізованих аудиторських рішень.
- Неправильні конфігурації під час роботи з кількома постачальниками хмарних послуг, кожен з яких має власні сервіси та можливості.

Управління активами

Мультихмарна стратегія ускладнює управління активами для будь-якої організації. Організація повинна мати прозорість або централізовану інвентаризацію всього свого хмарного середовища в режимі реального часу - які активи вона має, де розташовані їхні активи (який хмарний постачальник та який обліковий запис), хто володіє її активами та хто має доступ до її активів.

Розрив у навичках

Мультихмарна стратегія повинна враховувати той факт, що робота з кількома хмарними постачальниками вимагає практичного досвіду в архітектурі, розробці та експлуатації, а також роботи з кількома хмарними рішеннями. Організація повинна інвестувати в навчання співробітників як постійний процес, щоб надати співробітникам необхідні знання для обслуговування кількох хмарних платформ. Важливою темою для інвестування є автоматизація, масштабування впливу співробітників та зменшення операційного навантаження.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Мультихмарність та як створити мультихмарну стратегію: https://surl.li/ffgwng

Керування ідентифікаторами в багатохмарних середовищах

Одним із перших рішень, яке слід вирішити перед використанням багатохмарної стратегії, є керування ідентифікацією. Організації хотіли б зберегти свого існуючого постачальника ідентифікації (IdP), мати єдину ідентифікацію для кожного зі своїх кінцевих користувачів (зберігаючи при цьому існуючі облікові дані) та все ще мати можливість доступу до ресурсів у хмарі. Якщо організація вже використовує Office 365 для керування поштовими скриньками та співпраці, розгляньте можливість використання Azure Active Directory (ААД) та його централізовану службу управління ідентифікацією.

Azure AD вважається найбільш використовуваним постачальником ідентифікаційних даних. Він підтримує об'єднання ідентифікаційних даних з більшістю основних хмарних провайдерів та здатний інтегруватися з більшістю Програмне забезпечення як послуга (SaaS) рішення. Інші популярні постачальники послуг керування ідентифікацією, які не розглядаються в цьому посібнику - це Okta, Ping Identity та OneLogin, які надають вам універсальну службу каталогів для керування користувачами, групами та пристроями, забезпечення дотримання Багатофакторна автентифікація (МЗС), а також єдиний вхід для кількох хмарних провайдерів і SaaS-додатків.

Як керувати ідентифікацією в AWS у багатохмарних середовищах

AWS надає такі послуги для керування ідентифікацією в багатохмарних середовищах:

- *Єдиний вхід AWS (Єдиний вхід)* - сервіс, що дозволяє єдиний вхід в організаціях AWS або підключення до ідентифікаційних даних у зовнішніх хмарних сервісах ідентифікації на основі протоколу SAML, таких як Azure AD або Google G Suite.
- *Amazon Cognito* - сервіс, який дозволяє єдиний вхід для веб- або мобільних застосунків, водночас дозволяючи клієнтам підключатися за допомогою зовнішніх постачальників ідентифікаційних даних, таких як Apple, Facebook або Google, або автентифікації на основі SAML, як-от Azure AD.

Найкращі практики такі:

- Використання Єдиний вхід AWS як Постачальник ідентифікаційних даних для об’єднання та керування доступом до хмарних програм (таких як Salesforce, Box та Office 365). AWS SSO також може забезпечити об’єднаний доступ, приймаючи вхідний SAML для таких сервісів, як Okta.
- Використання Amazon Cognito керувати доступом до веб- або мобільних застосунків, орієнтованих на клієнтів, за допомогою зовнішніх постачальників ідентифікаційних даних, таких як Azure AD, Apple, Facebook або Google.
- Використання AWS CloudTrail реєструвати всі виклики API AWS SSO.
- Використання AWS CloudTrail реєструвати всі виклики Amazon Cognito API.
- Використання Amazon Guard Dutyгенерувати події безпеки (на основі AWS CloudTrail) про підозрілу активність (наприклад, спробу грубої сили з

використанням зовнішньої ідентифікаційної особи) та надсилати сповіщення, використовуючи як Простий сервіс сповіщень AWS (Соціальні мережі), до таких служб, як SMS, мобільні, електронні сповіщення, або запускати функцію Lambda для виконання певних дій (наприклад, блокування доступу до мережі за допомогою групи безпеки).

- Використання TLS 1.2 під час надсилання викликів API до Amazon Cognito.
- Під час роботи з AWS SSO, якщо вам потрібно налаштувати детальний доступ до ресурсів на основі зовнішніх атрибутів ідентифікації (таких як назва та розташування), використовуйте Контроль доступу на основі атрибутів(ABAC) разом із політикою IAM (наприклад, умовами в політиці IAM).
- Під час роботи з AWS SSO із зовнішнім постачальником ідентифікаційних даних або AWS SSO як постачальником ідентифікаційних даних, який підтримує МЗС, забезпечте використання багатофакторної автентифікації (MFA) у налаштуваннях зовнішнього постачальника ідентифікаційних даних, щоб забезпечити надійну автентифікацію.
- Під час роботи з Amazon Cognitoщоб дозволити доступ до веб- або мобільних програм, забезпечте використання багатофакторної автентифікації (MFA) для пулу користувачів, щоб забезпечити надійну автентифікацію.
- Використання Amazon CloudWatch або будь-які інші інструменти SIEM чи аналітики для моніторингу пулів користувачів Amazon Cognito та спрацьовування тривоги при перевищенні певного порогу (наприклад, велика кількість невдалих спроб входу до федерації від зовнішнього постачальника ідентифікаційних даних).
- Використання Amazon Cognito функції захисту від скомпрометованих облікових даних, які виявляють, чи були скомпрометовані облікові дані користувача, і блокують спроби доступу з боку цього користувача.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Автоматизація федерації SAML 2.0 для середовищ AWS з кількома обліковими записами, що використовують Azure AD: https://surl.li/bzxisl
Додавання постачальників ідентифікації SAML до пулу користувачів: https://surl.lu/paaiwc
Додавання багатофакторної автентифікації (MFA) до пулу користувачів: https://surli.cc/qepjyg

Як керувати ідентифікаторами в Azure в багатохмарних середовищах

Azure надає такі послуги для керування ідентифікацією в багатохмарних середовищах:

- *Azure AD* - постачальник ідентифікаційних даних Azure, який дозволяє доступ до ресурсів Azure або SaaS-додатків за допомогою зовнішніх постачальників ідентифікаційних даних на основі SAML, таких як AWS SSO або Google Identity.

- *Azure AD B2C* - постачальник ідентифікаційних даних Azure, який дозволяє доступ до клієнтських програм або SaaS-сервісів, що не належать Microsoft, використовуючи зовнішні ідентифікатори, такі як Gmail та Facebook.

Найкращі практики такі:

- Використовуйте Azure AD у поєднанні з Єдиний вхід AWS, щоб забезпечити централізоване керування ідентифікаторами для ресурсів Azure та AWS.
- Використовуйте Azure AD у поєднанні з Google Identity або Google IAM, щоб забезпечити централізоване керування ідентифікаторами для ресурсів Azure та GCP.
- Використовуйте Azure AD B2C, щоб надати доступ до клієнтських програм або сторонніх SaaS-сервісів.
- Використовуйте умовний доступ для примусового використання багатофакторної автентифікації (MFA) під час підключення за допомогою зовнішніх постачальників ідентифікаційних даних.
- Під час використання Єдиний вхід AWS як постачальник ідентифікаторів, інтегрований з Azure AD, налаштовує Azure Керування привілейованими ідентифікаторами (ПІМ) для налаштування своєчасного доступу до порталу Azure та ресурсів Azure.
- Використання Захисник Microsoft для хмарних програм для моніторингу захищених сервісів (використовуючи комбіновану ідентифікацію).
- Використання Захисник Microsoft для хмарних програм щоб захистити ваше об'єднане середовище від ризикованих користувачів або витоку даних.
- Використовуйте TLS 1.2 під час надсилання викликів API до Azure AD B2C.
- Під час використання Azure AD B2C для автентифікації вебзастосунків створюйте окремі середовища - розділені між розробкою, тестуванням та виробництвом.
- Перевіряти кожну веб-програму, що використовує Azure AD B2C, за допомогою подій журналу аудиту, що зберігаються в Azure Monitor, і надсилати журнали до служби SIEM (наприклад, Azure Sentinel).

Для отримання додаткової інформації зверніться до наступних ресурсів:
Багатохмарна безпека та ідентифікація за допомогою Azure та Amazon Web Services (AWS): https://surli.cc/bvqocw
Рекомендації та найкращі практики для Azure Active Directory B2C: https://surl.li/lahjpk

Як керувати ідентифікацією в GCP у багатохмарних середовищах

Google надає Cloud IAM як послугу, що дозволяє інтеграцію з іншими постачальниками ідентифікаційних даних, такими як AWS або Azure AD.

Найкращі практики такі:

- Під час інтеграції Google Cloud із зовнішніми постачальниками ідентифікаційних даних (такими як AWS або Azure AD) використовуйте

короткочасні токени доступу Google, такі як Служба токенів безпеки AWS видати себе за обліковий запис служби.

- Під час інтеграції Google Cloud з Azure AD обов'язково забезпечте використання багатофакторної автентифікації (MFA) в Azure AD.
- Під час інтеграції між Google Cloud та Azure AD синхронізуйте групи з Azure AD, а не керуйте групами в Google Cloud.
- Уникайте автоматичного налаштування ідентифікаційних даних користувачів із обліковими записами споживачів, щоб уникнути створення дублікатів облікових записів.

Під час підключення ідентифікаторів Google до Azure AD ідентифікатори користувачів стають гостьовими обліковими записами в Azure AD. Як найкраща практика, виконайте такі дії:

- Надайте доступ гостьовим користувачам до Google Cloud у межах виділеного організаційного підрозділу.
- Застосуйте політику, щоб обмежити максимальну тривалість сеансу для гостьових користувачів до 8 годин.
- Встановіть метод повторної автентифікації на використання пароля, щоб змусити користувача повторно автентифікуватися за допомогою своїх облікових даних Azure AD.

Мережева архітектура для багатохмарних середовищ

Другий важливий момент, який слід враховувати під час побудови багатохмарної архітектури - це налаштування мережевого з'єднання між різними хмарними постачальниками, а також між локальним програмним забезпеченням та хмарними постачальниками.

Рекомендований спосіб підключення до хмарних середовищ - це безпечне та постійне мережеве з'єднання за допомогою виділеного з'єднання (наприклад, Пряме підключення AWS або Azure ExpressRoute) для підключення з локальної мережі до хмари або за допомогою мережі «сайт-сайт» Віртуальна приватна мережа(VPN) (або з локальної мережі до хмари, або між постачальниками хмарних послуг).

Захищене та постійне з'єднання дозволить встановити контроль доступу (правила брандмауера 4-го рівня) між хмарними постачальниками та хмарними сегментами, а також забезпечити доступ до ресурсів у хмарі (або дозволити доступ до хмарних ресурсів) відповідно до потреб бізнесу.

Розглядаючи архітектуру мережі (Рис.4.1), необхідно враховувати наступне:

- Які ресурси слід зберігати в таємниці (наприклад, передача даних та зв'язок між службами на сервері)?
- Які ресурси можуть бути публічними (наприклад, публічні виклики API, фронтенд-сервіси та кінцеві точки VPN)?

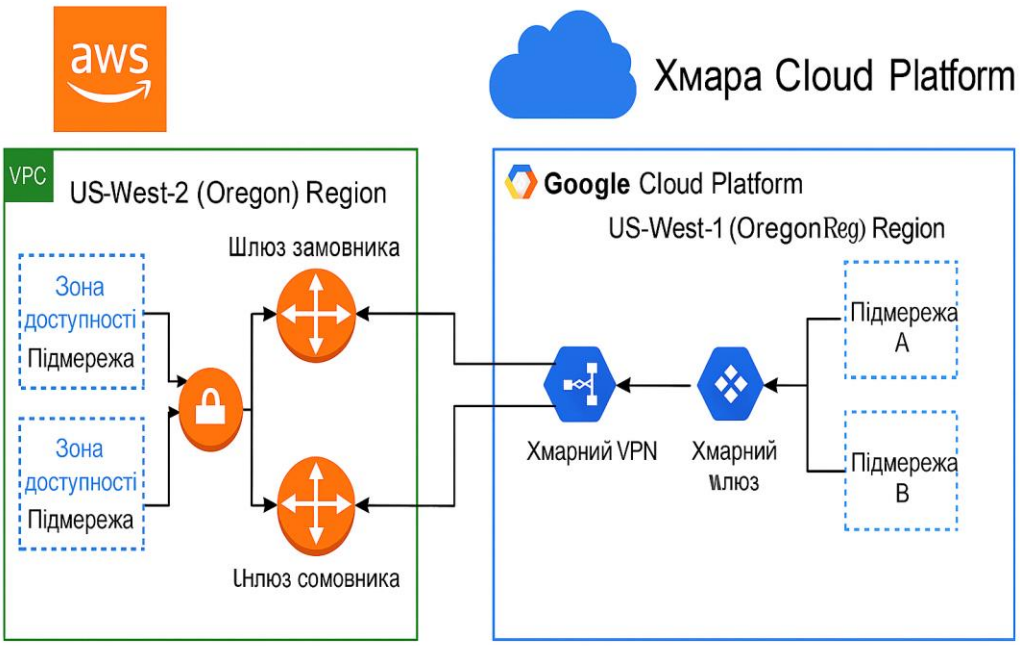

Рисунок 4.2 - Мережеве з'єднання від GCP до AWS

Як створити мережеве з'єднання між AWS та GCP

Щоб створити VPN-тунель IPsec між AWS та GCP, дотримуйтесь цих загальних рекомендацій:

- Створіть спеціалізовану AWS Віртуальна приватна хмара(ВПК) з новою підмережею для VPN-тунелю.
- Створіть виділений GCP VPC з новою підмережею для VPN-тунелю.
- Якщо резервування мережі не потрібне, створіть з'єднання між AWS віртуальний приватний шлюз(використовуючи VPN під керуванням AWS) та Google Cloud VPN.
- Якщо потрібне резервування мережі, створіть з'єднання між AWS транзитний шлюзі Google Висока доступність(XA) VPN.

Найкращі практики такі:

- Завжди думайте про Безкласова міждоменна маршрутизація(CIDR) перед налаштуванням сегментів мережі в хмарі, щоб уникнути конфлікту IP-адрес між постачальниками хмарних послуг.
- На стороні AWS використовуйте мережу Списки контролю доступу(ACL) та групи безпеки для захисту ресурсів у вашому AWS VPC.
- На стороні GCP використовуйте правила брандмауера для захисту ресурсів усередині вашої GCP VPC.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Підключення AWS та GCP VPC за допомогою тунелю IPSec VPN з BGP: https://surli.cc/cttxaa

Багатохмарна архітектура з використанням VPN між GCP та AWS: https://surl.li/lcknhj

Як створити мережеве з'єднання між AWS та Azure

Щоб створити VPN-тунель IPsec між AWS та Azure, дотримуйтесь цих загальних рекомендацій:

- Створіть виділений AWS VPC з новою підмережею для VPN-тунелю.
- Створіть виділену віртуальну мережу Azure з новою підмережею для VPN-тунелю.
- Створіть з'єднання між віртуальним приватним шлюзом AWS (за допомогою VPN, керованого AWS) та шлюзом Azure VPN.

🗐 *Важливе зауваження!* Для резервування мережі створіть два VPN-тунелі.

Найкращі практики такі:

- Завжди думайте про CIDR перед налаштуванням сегментів мережі в хмарі, щоб уникнути конфлікту IP-адрес між постачальниками хмарних послуг.
- На стороні AWS використовуйте мережеві ACL та групи безпеки для захисту ресурсів усередині вашої AWS VPC.
- На стороні Azure використовуйте групи безпеки мережі для захисту ресурсів у вашій віртуальній мережі Azure.

Для отримання додаткової інформації зверніться до наступного ресурсу:
Як створити VPN між Azure та AWS, використовуючи лише керовані рішення: https://surli.cc/hkmaco

Як створити мережеве з'єднання між Azure та GCP

Щоб створити тунель IPsec VPN між Azure та GCP, дотримуйтесь цих загальних інструкцій:

- Створіть виділену віртуальну мережу Azure з новою підмережею для VPN-тунелю.
- Створіть виділений GCP VPC з новою підмережею для VPN-тунелю.
- Якщо резервування мережі не потрібне, створіть з'єднання між Azure VPN Gateway та Google Cloud VPN.
- Якщо потрібне резервування мережі, створіть з'єднання між Azure VPN Gateway та Google HA VPN.

🗐 *Важливе зауваження!* Для резервування мережі створіть два VPN-тунелі.

Найкращі практики такі:

- Завжди думайте про CIDR перед налаштуванням сегментів мережі в хмарі, щоб уникнути конфлікту IP-адрес між постачальниками хмарних послуг.

- На стороні Azure використовуйте групи безпеки мережі для захисту ресурсів у вашій віртуальній мережі Azure.
- На стороні GCP використовуйте правила брандмауера для захисту ресурсів усередині вашої GCP VPC.

Для отримання додаткової інформації зверніться до наступного ресурсу: *Створення VPN-з'єднання типу «сайт-сайт» між GCP та Azure за допомогою приватного доступу Google*: https://surl.lu/rzqxwx

Безпека даних у багатохмарних середовищах

Безпека даних у хмарі стосується захисту даних під час їх передачі мережею, у стані спокою та під час використання.

Шифрування під час передачі

Щоб захистити своє хмарне середовище, переконайтеся, що всі дані передаються через захищені протоколи. Деякі альтернативи захищеним протоколам наведено нижче.

- Забезпечте використання TLS 1.2 для доступу до ресурсів у всьому вашому багатохмарному середовищі.
- Налаштуйте VPN-тунелі IPsec між вашими локальними та хмарними середовищами, а також між хмарними постачальниками.

Шифрування в стані спокою

Усі основні постачальники хмарних послуг мають власні Послуги з управління ключами (KMSes), для керування ключами, секретами, обліковими даними тощо. Хоча вбудовані служби керування ключами (KMS) можуть зберігати, керувати, отримувати та обертати ключі та таємниці, вони інтегровані у власну екосистему хмарного провайдера. Вибираючи рішення для обробки шифрування в стані спокою, зверніть увагу на такі можливості:

- Можливість шифрування даних у стані спокою через кількох хмарних провайдерів - кожен хмарний провайдер має власну KMS. Якщо вам потрібно спільно використовувати ключі шифрування між кількома хмарними провайдерами, вам потрібно розгорнути стороннє рішення для досягнення цієї мети.
- Здатність обробляти масштаб вашого хмарного середовища (генерувати тисячі ключів від кількох хмарних постачальників).

  Важливе зауваження! Розглянемо Модуль апаратної безпеки(HSM), коли вам потрібно дотримуватися норм (таких як PCI DDS), оскільки пристрої HSM стійкі до несанкціонованого доступу та захищені від несанкціонованого доступу.
- Можливість створювати, зберігати, отримувати та ротувати як ключі, так і таємниці з кількох хмарних сервісів.

- Можливість налаштування контролю доступу на основі ролей - хто може генерувати ключі/таємниці для якого хмарного облікового запису або хмарного постачальника.
- Можливість створення повного журналу аудиту для рішення KMS для подальшого розслідування.

Використовується шифрування

Концепція шифрування, що використовується, полягає в тому, щоб мати змогу захистити дані під час роботи в пам'яті на ВМ або контейнер. Найвідомішою концепцією шифрування, що використовується, є конфіденційні обчислення Поширені альтернативи конфіденційним обчисленням такі:

- AWS Nitro Enclaves
- Конфіденційні обчислення Azure
- Конфіденційні обчислення Google

Для захисту даних у багатохмарних середовищах, у поєднанні з централізованими рішеннями для забезпечення ресурсів, прагніть розгортати віртуальні машини або контейнери, які підтримують одне з вищезгаданих рішень для конфіденційних обчислень.

Управління витратами в багатохмарних середовищах

Хоча управління витратами може здаватися не безпосередньо пов'язаним з безпекою, він має наслідки для багатохмарного середовища.

Управління витратами є частиною забезпечення видимості всього вашого багатохмарного середовища з точки зору витрат. Усі основні постачальники хмарних послуг мають власні вбудовані служби управління витратами, які забезпечують необхідну видимість ваших хмарних облікових записів, підписок або проектів.

Коли організації переходять від одного постачальника хмарних послуг (у багатьох випадках з кількома обліковими записами в одного постачальника хмарних послуг для різних середовищ або бізнес-потреб) до багатохмарної системи, вони починають усвідомлювати, що їм бракує необхідної прозорості щодо вартості хмарних послуг.

Деякі з проблем, які часто виникають у організацій, такі:

- Вартість передачі даних (також відома як вихідні дані).
- Витрачаються надлишкові ресурси (такі як кілька систем журналювання, служби резервного копіювання та рішення для захисту від шкідливого програмного забезпечення).

Можливі ризики відсутності прозорості витрат полягають у наступному:

- Високі платежі від кількох постачальників хмарних послуг, без знання того, які ресурси були використані та чи потрібні нам ці ресурси.

- Виявлення аномальних витрат, таких як стягнення плати в неочікуваних регіонах, неочікувані послуги або аномальні обсяги, які можуть бути ознаками компрометації, особливо під час роботи в багатохмарному середовищі.
- Потенційний сценарій відмови у гаманці, коли хакер отримує доступ до одного з наших хмарних облікових записів, споживаючи дорогі обчислювальні ресурси для майнінгу біткойнів. Без належної видимості або механізму сповіщення, до того часу, як ми дізнаємося, що хтось використовує наші ресурси, нам доведеться заплатити тисячі доларів постачальникам хмарних послуг.

Найкращі практики такі:

- Розгорніть рішення для управління витратами, яке підтримує кількох постачальників хмарних послуг.
- Позначте всі ресурси у всіх ваших хмарних облікових записах, у всіх ваших хмарних постачальників.
- Створюйте сповіщення про виставлення рахунків для кожного з ваших хмарних облікових записів, коли перевищено певний поріг (наприклад, коли загальне щомісячне споживання облікового запису тестового середовища перевищує 500 доларів США або коли загальне щомісячне споживання облікового запису виробничого середовища перевищує 1500 доларів США).
- Налаштуйте бюджет для кожного з ваших хмарних облікових записів. Після налаштування бюджету згенеруйте автоматичне сповіщення про бюджет, коли буде перевищено певний поріг бюджету (наприклад, 75%).
- Розгорніть можливості автоматизації для видалення невикористовуваних ресурсів (таких як віртуальні машини, контейнери та керовані бази даних). Автоматизація дозволить вам розгортати середовища розробки або тестування, коли потрібні ресурси.

Перегляньте звіти про рекомендації щодо витрат і дотримуйтесь рекомендацій, таких як:

- Зменшення розміру віртуальної машини до меншого типу (з меншим процесором або пам'яттю). Вимкнення недостатньо задіяних віртуальних машин.
- Змініть варіанти придбання віртуальних машин з оплати за запитом (або оплати за використання) на резервований екземпляр (зарахування на 1 або 3 роки вперед) або навіть точковий (або попередньо придбаний), залежно від очікуваного часу виконання віртуальної машини.
- Перейдіть на дешевше блокове сховище (обсяги дисків) відповідно до фактичного використання (завантаження дискового простору).
- Перенесіть об’єкти зі служб сховища об’єктів на дешевший рівень (з гарячого або сховища в режимі реального часу на холодне або майже в режимі реального часу, або навіть на холодне чи архівне сховище).
- Видаліть непотрібні резервні копії або знімки.

Управління станом безпеки хмари (CSPM)

У рамках забезпечення прозорості у ваших багатохмарних середовищах, протягом останніх кількох років з'явилася нова концепція.

Є численні пропозиції від багатьох сторонніх постачальників CSPM постачальників, але фундаментальна ідея всіх рішень CSPM полягає у видимості неправильних конфігурацій - ключова тема під час роботи в багатохмарному середовищі та керування кількома хмарними обліковими записами.

Вибираючи рішення CSPM, зверніть увагу на такі можливості:

- Підтримка кількох хмарних провайдерів.
- Видимість неправильних конфігурацій (таких як відкритий порт та загальнодоступне сховище об'єктів).
- Видимість IAM (наприклад, ключі API, розташовані в загальнодоступному сховищі об'єктів, ключі доступу або паролі, які не змінювалися протягом останніх 90 днів, дозволи користувачів та облікові записи, для яких відсутня багатофакторна автентифікація).
- Видимість усіх ваших хмарних ресурсів у багатохмарному середовищі.
- Можливість оцінювати ризики в усьому вашому багатохмарному середовищі.
- Здатність визначати пріоритети зменшення ризиків - ваші співробітники повинні знати, які ризики потрібно негайно враховувати.
- Контекстна видимість - загальнодоступний веб-сервер потрібно виправити спочатку, тоді як сервери, що знаходяться в приватній підмережі, захищеній суворим контролем доступу до мережі, можна виправити пізніше.
- Можливість автоматичного виправлення неправильних конфігурацій.
- Отримайте аналітику векторів атак - зрозумійте, як потенційний зловмисник може скористатися неправильною конфігурацією для порушення безпеки вашого хмарного середовища.
- Видимість уразливих компонентів (таких як відсутні патчі безпеки на віртуальній машині або стара бібліотека з відкритим кодом всередині контейнера).
- Отримайте інформацію про заходи щодо пом’якшення наслідків - ваші співробітники повинні знати, які дії вжити для усунення неправильної конфігурації або потенційного ризику.
- Перевірте відповідність усього вашого багатохмарного середовища відомим стандартам безпеки (таким як ISO 27001) та нормативним актам (таким як Загальний регламент про захист даних(GDPR) та Закон про перенесення та підзвітність медичного страхування(HIPAA)).
- Безперервний моніторинг усього вашого багатохмарного середовища - виявлення загроз і неправильної конфігурації має бути безперервним процесом.
- Інтеграція з SIEM-системами для подальшого розслідування.

- Інтеграція із системою квитків для надсилання завдань, щоб ваші співробітники могли обробляти сповіщення від рішення CSPM.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Управління станом безпеки хмари (CSPM): https://surl.li/yastaa

Управління правами доступу до хмарної інфраструктури (CIEM)

Новою концепцією, розробленою за останні кілька років, є CIEM. Деякі постачальники пропонують комбіноване рішення CSPM та CIEM в одному продукті, що враховує стратегію багатохмарних партнерів.

Рішення CIEM дозволяють нам контролювати та керувати ідентифікаторами (як людей, так і машин) та правами доступу в багатохмарному середовищі з центральної консолі, застосовуючи принцип найменших привілеїв доступу до нашої хмарної інфраструктури.

Вибираючи рішення CIEM, зверніть увагу на такі можливості:

- Підтримка кількох хмарних провайдерів.
- Інвентаризація існуючих прав.
- Виявлення та усунення неправильних конфігурацій IAM.
- Можливість контролювати доступ до ресурсів, служб та адміністративних облікових записів
- Виявлення ризиків, пов'язаних з помилками конфігурації.
- Визначення тіньових облікових записів адміністраторів у багатохмарному середовищі
- Пропозиції щодо корекції політики.
- Автоматична генерація політик доступу відповідно до фактичних потреб ідентифікації.
- Виявлення надмірних дозволів на доступ до ідентифікаційних даних.
- Виявлення дозволів на доступ для зовнішніх користувачів та користувачів різних облікових записів.

Керування виправленнями та конфігураціями в багатохмарних середовищах

Однією з проблем у багатохмарних середовищах є централізоване керування оновленнями програмного забезпечення та змінами конфігурації.

Вибираючи рішення для керування виправленнями, зверніть увагу на такі можливості:

- Можливість централізовано керувати розгортанням патчів з одного місця
- Підтримка розгортання патчів безпеки на платформах Windows та Linux
- Підтримка інвентаризації активів
- Підтримка відкату патчів у разі проблемного патчу безпеки
- Підтримка розгортання патчів безпеки через захищені протоколи (такі як тунель TLS між центральним сервером патчів та віддаленою віртуальною машиною)

- Можливість розгортання патчів безпеки на групі серверів (наприклад, у різних середовищах та з різним циклом патчів, щоб уникнути порушення доступності у разі кластеризації серверів)
- Можливість розгортання патчів безпеки сторонніх розробників (таких як патчі для самостійно керованих серверів баз даних, веб-серверів та клієнтських інструментів)
- Можливість налаштування мінімальних облікових даних для доступу до віддалених віртуальних машин у всьому вашому багатохмарному середовищі для розгортання виправлень
- Можливість налаштувати вікно обслуговування для розгортання патчів (щоб уникнути розгортання патчів у робочий час)
- Можливість генерувати звіти про відповідність вимогам (наприклад, який відсоток ваших серверів вже розгорнуто з патчем, а які сервери все ще не мають патчу)
- Можливість інтеграції рішення для керування виправленнямитіз системою квитків, щоб ваші співробітники могли дбати про вразливі віртуальні машини

Ще одним питанням, яку необхідно розглянути під час роботи з командами розробників, є турбота про бібліотеки з відкритим кодом, також відомі як Аналіз складу програмного забезпечення(СКА).

Вибираючи рішення SCA, зверніть увагу на такі можливості:

- Можливість централізовано керувати всім вашим багатохмарним середовищем з центрального місця
- Можливість інтеграції з кількома репозиторіями вихідного коду
- Можливість інтеграції з кількома реєстрами контейнерів у багатохмарних середовищах
- Можливість пошуку застарілих репозиторіїв бібліотек з відкритим кодом
- Здатність виявляти як вразливу, так і застарілу бібліотеку з відкритим кодом, а також усі її залежності
- Можливість налаштування мінімальних облікових даних для доступу до віддаленого вихідного коду або реєстрів контейнерів
- Можливість інтеграції рішення SCA з Безперервна інтеграція/Безперервна доставка (ДІ/КД) процеси (у середовищах з кількома хмарами та кількома обліковими записами поширеною є наявність кількох конвеєрів CI/CD)
- Можливість генерувати звіти, що дозволяють вам бачити, які вразливі компоненти існують у ваших середовищах розробки або виробництва
- Можливість перервати процес збірки, якщо ви використовуєте вразливі компоненти
- Можливість встановити рівень серйозності вразливості, дозволений у ваших середовищах, перед перериванням процесу збірки (наприклад, не дозволяти завершення процесу збірки, якщо в одній з бібліотек або залежностей з відкритим кодом існують критичні вразливості)

- Можливість інтеграції рішення SCA із системою кешування, щоб ваші співробітники могли дбати про вразливі компоненти в рамках процесу збірки

Управління конфігурацією та змінами також є важливими темами, які слід враховувати в багатохмарних середовищах.

Вибираючи рішення для управління конфігурацією та змінами, зверніть увагу на такі можливості:

- Можливість централізовано керувати всім вашим багатохмарним середовищем
- Можливість налаштування мінімальних облікових даних для доступу до ресурсів у кількох хмарних постачальників та кількох хмарних облікових записах
- Здатність виявляти відповідність загальновідомим стандартам, таким як Центр інтернет-безпеки(СНД) еталон інститут стандартів і технологій(НІСТ)
- Здатність виявляти зміну конфігурації в багатохмарному середовищі
- Можливість автоматизувати зміну конфігурації в кількох хмарних облікових записах
- Можливість інтеграції рішення для керування конфігурацією або змінами із системою оформлення заявок, щоб ваші співробітники могли самостійно керувати змінами
- Можливість інтеграції із системою SIEM для генерування сповіщень про виявлення зміни конфігурації в одній із ваших систем

Моніторинг та аудит багатохмарних середовищ

Моніторинг є важливою частиною багатохмарної видимості. Він може мати кілька рівнів, таких як:

- Використання ресурсів (ведення журналу продуктивності).
- Моніторинг запущених програм на наявність помилок (ведення журналу програм).
- Аудит безпеки та ведення журналу для виявлення інцидентів безпеки.

Вибираючи рішення для моніторингу безпеки для багатохмарних середовищ, зверніть увагу на такі можливості:

- Можливість підключення до кількох хмарних постачальників, використовуючи власні API хмарних постачальників.
- Можливість підключення до віддалених API за допомогою захищених протоколів (таких як TLS 1.2).
- Вбудовані роз'єми для кількох хмарних рішень як поширених Інфраструктур, як послуги Інфраструктура, як послуги (IAA)/Платформа, як послуга(PaaS) та (SaaS).

- Можливість отримувати канали від служб виявлення загроз, таких як Amazon Guard Duty, Захисник Microsoft для хмари, та Центр команд безпеки Google.
- Можливість отримувати канали від сторонніх рішень для управління вразливостями.
- Можливість отримувати дані від рішень для управління конфігурацією для виявлення неправильної конфігурації або відхилення від стандартів.
- Здатність виявляти аномальну поведінку користувачів (наприклад, користувач намагається отримати доступ до ресурсу вперше або поза звичайним робочим часом) та подати сповіщення.
- Можливість зберігати всі журнали зашифрованими в стані спокою.
- Можливість налаштування керування доступом до рішення для моніторингу на основі ролей для різних співробітників у різних ролях (таких як IT-персонал, аналітики безпеки та аудитори) та в різних місцях вашої організації (наприклад, не всім командам потрібен доступ для перегляду інформації про все ваше хмарне середовище).
- Можливість отримувати дані моніторингу в режимі реального часу та безперервно з усього вашого багатохмарного середовища.
- Можливість створювати правила кореляції між різними джерелами журналів (такими як журнали аудиту, рішення для виявлення кінцевих точок та журнали потоків мережевого трафіку).
- Можливість виконання автоматизованих дій з виправлення помилок (таких як закриття відкритого порту та вимкнення скомпрометованого облікового запису).
- Можливість створювати сповіщення на основі журналів та надсилати їх до центральної SIEM-системи.
- Можливість інтеграції із системою продажу заявок, щоб ваші співробітники могли вирішувати виявлені інциденти безпеки.

4.3. Безпека у великомасштабних середовищах

Попередньо ми розглядали керування обліковим записом на основі одного хмарного постачальника, при цьому всі ресурси знаходяться в одному місці. У цьому параграфі ми розглянемо масштабні хмарні середовища - такі, що мають кілька облікових записів для різних відділів або різних бізнес-потреб, часто в кількох регіонах світу.

Деякі питання, які організації часто ставлять собі:

- Як забезпечити управління кількома обліковими записами?
- Як отримати уявлення про все моє хмарне середовище?
- Як керувати середовищем з кількома регіонами?
- Які можливості автоматизації я маю?

У цьому параграфі ми розглянемо такі теми:

- Управління управлінням та політикою у великих масштабах

- Автоматизація з використанням інфраструктури як коду
- Безпека у великомасштабних хмарних середовищах

Технічні вимоги

Для цього розділу вам потрібно мати ґрунтовне розуміння таких понять, як зони посадки, правила, захисні огорожі, інфраструктура як код(IAЦ), а також концепції, пов'язані з безпекою, такі як управління виправленнями, управління конфігурацією, а також управління відповідністю вимогам і вразливостями.

Управління управлінням та політикою у великих масштабах

Коли організації починають впроваджувати хмарні сервіси, наполегливо рекомендується планувати та враховувати управління хмарою (розгортання активів, безпека даних, управління ризиками тощо), ще до того, як вони зіткнуться з необхідністю керувати кількома хмарними середовищами та кількома обліковими записами.

Відсутність планування ускладнює виправлення конфігурації, виконаної ad hoc, оскільки відсутність однорідності призводить до неоднорідності активів, які потребують захисту, відсутності повторюваності, надмірності, великої поверхні атаки та самостійно нав'язаних обмежень через технічний борг, від якого важко позбутися (наприклад, перекриття блоків CIDR).

Деяка важлива термінологія, пов'язана з управлінням, така:

- *Зони посадки.* Це попередньо налаштовані середовища, що надаються за допомогою коду (політики, рекомендації, інструкції та централізовано керовані служби), як пояснено в наступному розділі.
- *Політики відповідності.* Це конкретні правила для оцінки або забезпечення дотримання конфігурації ресурсів відповідно до найкращих практик або нормативних вимог (наприклад, будь-яке новостворене сховище об'єктів має бути зашифроване в стані спокою за допомогою ключа, керованого клієнтом).
- *Огородження.* Автоматизований спосіб виявлення або забезпечення бажаної конфігурації (наприклад, переконатися, що жодного публічного корзини S3 не налаштовано, або зашифрувати базу даних у стані спокою під час її створення), перш ніж зміни потраплять у виробниче середовище (що дозволяє співробітникам виконувати свою роботу з мінімальними обмеженнями, що на них накладаються).

Зони посадки пропонують такі переваги:

Поширений тип базового плану спільних або попередньо налаштованих облікових записів:

- Мережа. Заповнювач для мережевих служб (таких як VPN-шлюз).
- Управління ідентифікацією та доступом. Заповнювач для таких служб, як служби каталогів або IAM, політики паролів тощо.
- Управління та моніторинг. Заповнювач для таких служб, як централізоване керування журналами, моніторинг та сповіщення тощо.

- Попередньо налаштовані базові показники облікових записів. Прикладом є торговельний автомат з автоматичною інтеграцією, а також інші спільні служби (відповідність, засоби контролю безпеки, мережа, моніторинг тощо).
- Конфігурація централізованого виставлення рахунків
- Налаштування квот облікового запису (наприклад, скільки віртуальних машин можуть створювати користувачі в певному обліковому записі)
- Тегування. Забезпечити використання тегів (заборонити створення нетегованих ресурсів)

Управління в AWS

У цьому розділі ми розглянемо сервіси AWS, які дозволяють здійснювати управління у великих масштабах. На наступній діаграмі зображено ієрархію кількох облікових записів AWS:

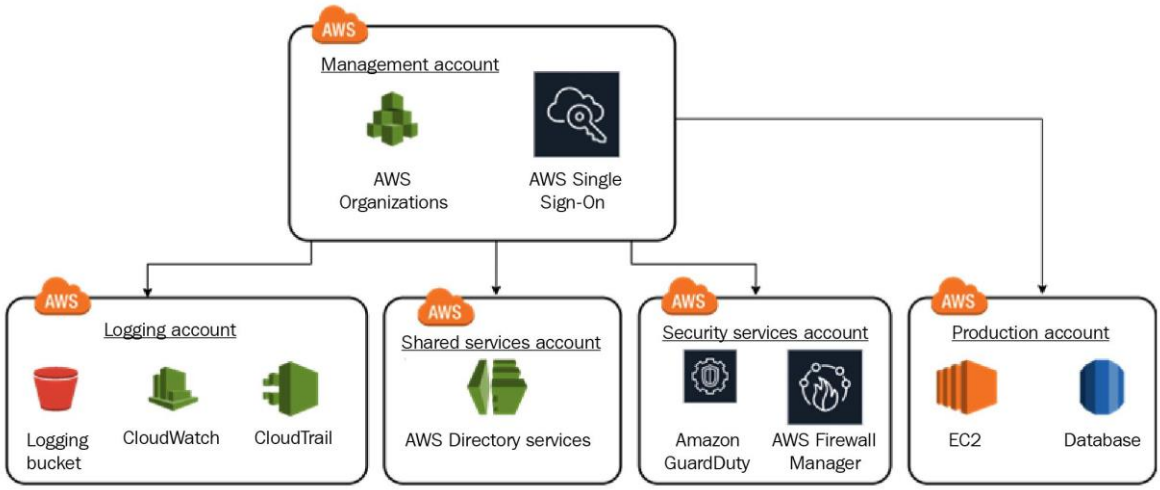

Рисунок 4.3 - Ієрархія кількох облікових записів AWS

На попередній діаграмі (Рис.4.3) показано концепцію посадкової зони AWS.

Зона посадки AWS

AWS Landing Zone - це один із сервісів AWS, який дозволяє організаціям легко створювати кілька облікових записів як частина організацій AWS безпечним та стандартним способом.

Під час створення цільових зон AWS налаштовуються такі сервіси:

- *AWS CloudTrail*. Цей сервіс створює журнал аудиту або дії API для кожного щойно створеного облікового запису AWS. Усі журнали зберігаються в центральному корзині S3 в обліковому записі архіву журналів.
- *Конфігурація AWS.* Цей сервіс містить файли журналів конфігурації для кожного щойно створеного облікового запису AWS та сервісів AWS у цьому обліковому записі. Усі журнали зберігаються в центральному корзині S3 в обліковому записі архіву журналів.

- *Правила конфігурації AWS.* Ця служба надає правила для моніторингу шифрування сховища (EBS, S3 та RDS), політики паролів IAM, налаштувань MFA root-акаунта, публічних S3-бакетів та незахищених груп безпеки (наприклад, дозвіл на доступ SSH з будь-якого джерела).
- *AWS IAM*. Цей сервіс використовується для встановлення політики паролів IAM для всієї організації, SSO тощо.
- *Amazon VPC.* Ця служба використовується для видалення VPC за замовчуванням у всіх регіонах, налаштування мережевого пірингу з VPC спільних служб тощо.
- *Сповіщення про цільову зону AWS*. Ця служба надає сповіщення про такі елементи, як вхід до облікового запису root, невдалі входи до консолі та помилки автентифікації API в обліковому записі.
- *Amazon Guard Duty.* Цей сервіс є центральним місцем для пошуку результатів (загроз) безпеки Guard Duty для всієї організації.

Для отримання додаткової інформації зверніться до наступного ресурсу:
Зона посадки AWS: https://surli.cc/jfpjqh

Диспетчерська вежа AWS

AWS Control Tower - це сервіс, який дозволяє організаціям створювати кілька облікових записів, дотримуючись найкращих практик AWS.

Деякі з найкращих практик, яких слід дотримуватися:

- Встановіть надійний пароль для користувача root облікового запису AWS та увімкніть багатофакторну автентифікацію (MFA).
- Виберіть регіон, який буде вашим домашнім регіоном для розгортання налаштувань цільової зони та зберігання S3-бакетів для аудиту та конфігурацій.
- Налаштуйте ключі AWS KMS для шифрування та розшифрування ресурсів у вашій організації AWS.
- Використовуйте каталог послуг AWS, щоб налаштувати, які ресурси (такі як образи віртуальних машин, сервери, програмне забезпечення та бази даних) можуть розгортатися користувачами у вашій організації AWS.
- Виберіть політики контролю послуг, щоб забезпечити їх дотримання та встановлювати спеціальні обмеження у вашій організації AWS.
- Налаштуйте AWS SSO для забезпечення використання багатофакторної автентифікації (MFA) та дозвольте користувачам використовувати єдиний логін для збору ресурсів у вашій організації AWS.
- Використовуйте AWS Security Hub для збору сповіщень про відповідність вимогам та безпеку в одній консолі.
- Налаштуйте політики життєвого циклу S3 для перенесення рідше використовуваних даних сховища об’єктів на рівень архіву.
- Використовуйте AWS WAF для захисту всієї вашої організації AWS від атак на рівні додатків.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Найчастіші запитання щодо AWS Control Tower: https://surl.li/fxcknn
Найкращі практики для адміністраторів AWS Control Tower: https://surl.lu/kxmocp

Організації AWS

AWS Organizations надає клієнтам централізований спосіб налаштування облікових записів AWS відповідно до різних бізнес-потреб (таких як IT-послуги, маркетинг, HR тощо), централізованої конфігурації (за допомогою AWS Config), механізмів безпеки (таких як CloudTrail та GuardDuty) та спільного використання ресурсів (консолідоване виставлення рахунків).

Для отримання додаткової інформації зверніться до наступного ресурсу:
Найчастіші запитання організацій AWS: https://surl.li/pxdwuy

Політики контролю послуг AWS (SCP)

Політики контролю доступу (SCP) - це організаційні політики, які дозволяють клієнтам керувати максимальними доступними дозволами для всіх облікових записів в організації. Ці політики дозволяють вам керувати root-акаунтами AWS.

Нижче наведено деякі приклади політик контролю послуг:

- Заборонити створення ресурсів у регіонах за межами Європи (через GDPR).
- Вимагати багатофакторна автентифікація (МЗС) для виконання дії API (наприклад, зупинки або завершення роботи екземпляра EC2).
- Заблокувати доступ до сервісу для облікового запису root (наприклад, заблокувати всі дії, пов’язані з сервісом EC2, за допомогою облікових даних облікового запису root).
- Забороняє користувачам вимикати CloudWatch та вносити зміни до конфігурації CloudWatch.
- Заборонити користувачам вимикати конфігурацію AWS або вносити зміни до її правил.
- Заборонити користувачам вимикати AWS Guard Duty або вносити зміни до його конфігурації.
- Дозволити створення певних типів екземплярів EC2 (для економії коштів).
- Вимагайте теги під час створення нових ресурсів.
- Заборонити користувачам видаляти журнали потоку VPC.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Політики контролю послуг AWS (SCP): https://surl.li/jcvvsm
Приклади політик контролю послуг: https://surli.cc/tavoku
Як використовувати політики контролю послуг для встановлення обмежень дозволів для різних облікових записів у вашій організації AWS: https://surl.lu/qikpjk

Менеджер доступу до ресурсів AWS

AWS Resource Access Manager дозволяє клієнтам спільно використовувати ресурси між обліковими записами AWS, замість того, щоб створювати їх у кожному обліковому записі AWS.

Нижче наведено кілька прикладів послуг, які можна використовувати спільно між обліковими записами:

- Amazon EC2
- Конструктор образів EC2
- Мережевий брандмауер AWS
- Менеджер ліцензій AWS
- AWS VPC
- Менеджер систем AWS, менеджер інцидентів
- Amazon Аврора

Для отримання додаткової інформації зверніться до наступного ресурсу:
Найчастіші запитання щодо менеджера доступу до ресурсів AWS: https://surl.lu/fkkvak
Спільні ресурси AWS: https://surl.li/mxxmlz
Безпека в AWS Resource Access Manager: https://surl.li/jgoazx

Управління в Azure

У цьому розділі ми розглянемо сервіси Azure, які дозволяють масштабне управління.

Наведена нижче діаграма (Рис.4.4) показує ієрархію кількох підписок Azure.

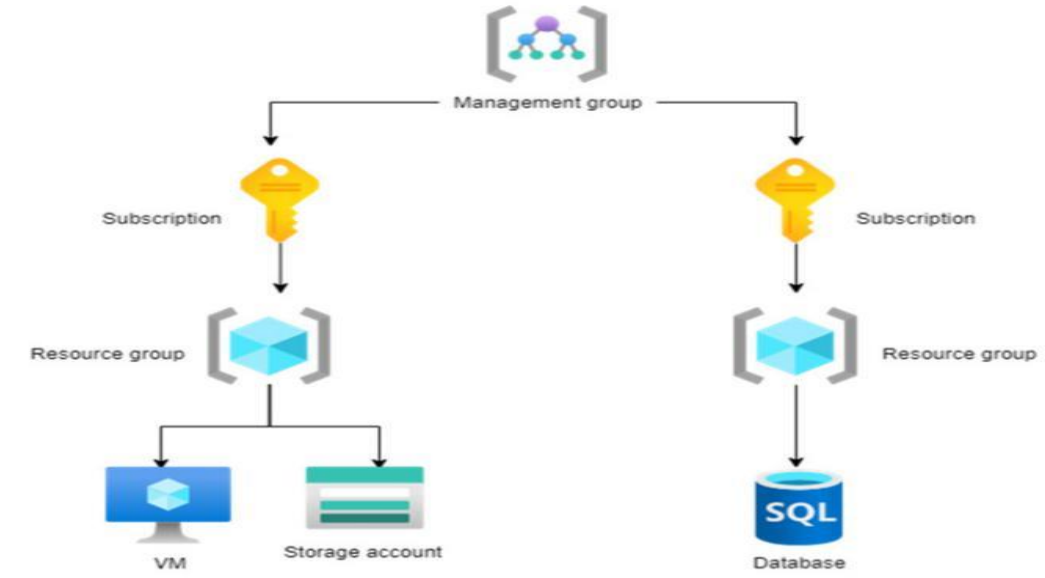

Рисунок 4.4 - Ієрархія кількох підписок Azure

Azure зони посадки

Цільові зони Azure дозволяють організаціям легко створювати кілька підписок як частину клієнта Azure безпечним та стандартним способом.

Під час створення цільових зон Azure налаштовуються такі служби:

Ідентичність:

- Azure Active Directory: Встановлює політику паролів для всієї організації, багатофакторної автентифікації тощо.
- Azure PIM Контролює доступ до ресурсів всередині Azure AD та в Azure, а також забезпечує використання багатофакторної автентифікації (MFA).

Безпека:

- Сховище ключів Azure Шифрує/розшифровує дані, таємниці, паролі тощо Захисник Microsoft для хмари Відповідність вимогам та виявлення загроз

Нетворкінг:

- *DDoS-атак у Azure.* Сервіс, що забезпечує захист від DDoS- атак Azure DNS: Керована служба DNS
- *Брандмауер Azure.* Забезпечує керований брандмауер 7-го рівня, IDS/IPS та фільтрацію URL-адрес.

Моніторинг:

- *Монітор Azure.* Центральне сховище журналів.
- *Справність служби Azure.* Надає сповіщення про служби Azure (по всьому світу), які можуть впливати на служби клієнтів.
- *Консультант Azure Надає.* сповіщення на основі найкращих практик (надійність, безпека, продуктивність, вартість та операційна досконалість).

Вартість:

- *Управління витратами Azure.* Налаштовує бюджети та сповіщення про бюджет

Для отримання додаткової інформації зверніться до наступних ресурсів:
Що таке зона посадки Azure?: https://surl.lu/epkmva
6 найкращих порад щодо налаштування нового середовища Microsoft Azure: https://surl.lu/fasqoa

Групи керування Azure

Групи керування Azure - це логічний спосіб групування кількох підписок Azure, які мають схоже використання (наприклад, усі виробничі підписки, усі підписки розробників тощо). Після групування цих підписок можна застосувати умови керування до груп керування.

Типовим прикладом такої політики є обмеження створення ресурсів певним регіоном Azure (заборона створення ресурсів за межами ЄС через GDPR).

Деякі з найкращих практик, яких слід дотримуватися:

- Використання контроль доступу на основі ролей (RBAC) для контролю доступу користувачів до підписок у групі керування відповідно до бізнес-вимог та принципу найменших привілеїв.
- Використовуйте Azure Policy для централізованого застосування налаштувань до всіх підписок у групі керування.
- Налаштуйте нову групу керування (за допомогою політики Azure) та встановіть її як групу керування за замовчуванням, щоб уникнути сценаріїв, коли щойно створені підписки призначаються кореневій групі керування.
- Вимагати авторизації для створення нової групи керування (змінити поведінку за замовчуванням, коли всім користувачам дозволено створювати нові групи керування).
- Використовуйте журнал активності Azure для аудиту груп керування.

Для отримання додаткової інформації зверніться до наступного ресурсу:
Що таке групи керування Azure?: https://surl.lt/nkxajl
Як захистити ієрархію ресурсів: https://surli.cc/qoghnu

Політика Azure

Політики Azure - це типи політик, які дозволяють клієнтам керувати максимальною кількістю доступних дозволів для всіх підписок у клієнті (або в групі керування).

Нижче наведено деякі приклади політик контролю послуг:

- Заборонити створення ресурсів у регіонах за межами Європи (через GDPR).
- Забезпечити використання багатофакторної автентифікації (MFA) для всіх облікових записів із правами власника на підписки.
- Увімкнути моніторинг у Microsoft Defender для хмари.
- Розгорніть Microsoft Defender для серверів SQL.
- Застосовуйте шифрування сховища BLOB-об'єктів за допомогою ключа, керованого клієнтом, під час створення сховища BLOB-об'єктів.
- Забезпечити SSL-з’єднання для серверів MySQL.
- Потрібно мінімальне використання TLS 1.2 на Azure SQL.
- Блокуйте доступ віртуальних машин до Інтернету за допомогою RDP або SSH.
- Забезпечити термін дії сховищ ключів.

Для отримання додаткової інформації зверніться до наступного ресурсу:
Що таке політика Azure?: https://surli.cc/pqyvqi
Вбудовані визначення політик Azure Policy: https://surl.lu/ahgkax

Управління в Google Cloud

Менеджер ресурсів Google. Керування масштабними середовищами на базі Google Cloud означає управління кількома проектами GCP в одній організації Google.

Google Resource Manager дозволяє клієнтам централізовано створювати та керувати кількома проектами GCP. У деяких випадках проекти групуються за бізнес-потребами в логічну групу, яка називається папками (папка для всіх виробничих проектів GCP, папка для всіх проектів GCP у розробці тощо).

За допомогою Google Resource Manager ви можете застосовувати політики IAM до всієї вашої організації Google (ви можете вказати, який користувач може виконувати які дії - хто може розгортати віртуальні машини, хто може створювати хмарне сховище тощо).

Деякі з найкращих практик, яких слід дотримуватися:

- План Визначте ієрархію Google Cloud відповідно до потреб вашого бізнесу або організації (відділи, команди та проекти GCP).
- Підключіть облікові записи вашої організації до Cloud Identity (наприклад, Google Workspaces).
- Забезпечити використання тегів і міток під час створення проєкту GCP (для цілей виставлення рахунків та для визначення того, який ресурс або проєкт належить до середовища виробництва, розробки або тестування).
- Уникайте створення міток, назва або опис яких містять конфіденційну інформацію.
- Встановіть правила іменування проектів (що дозволить вам визначити, який проект належить до середовища виробництва, розробки чи тестування).
- Створюйте проекти автоматизованим способом (за допомогою Google Deployment Manager або HashiCorp Terraform).
- Встановлюйте квоти та обмеження на рівні проекту (уникаючи сценаріїв, коли один адміністратор може розгорнути велику кількість дорогих віртуальних машин в одному проекті).
- Використовуйте Службу політики організацій Google для централізованого застосування налаштувань у всій вашій організації Google.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Документація менеджера ресурсів: https://surl.li/eotwax
Розгортані схеми безпеки та зони посадки: https://surl.li/zyrpsw
Керування хмарними ресурсами: https://surl.li/dkdtuc

Служба політики організації Google

Служба політики організації дозволяє налаштовувати обмеження щодо використання ресурсів

У вашій організації Google та визначати обмеження для дотримання вимог вашими співробітниками.

Нижче наведено деякі приклади політик організації:

- Заборонити створення ресурсів за межами Європи (через GDPR).
- Хмарний SQL Обмеження доступу до публічних IP-адрес в екземплярах Cloud SQL.
- Хмарне сховище: Google Cloud Platform - режим детального ведення журналу аудиту.
- Хмарне сховище Забезпечити рівномірний доступ на рівні контейнера.
- Обчислювальний сервіс Compute Engine контейнерів Забезпечити використання екранованих віртуальних машин.
- Обчислювальний сервіс Compute Engine контейнерів Обмеження неконфіденційних обчислень.
- Обчислювальний сервіс Compute Engine контейнерів Визначення дозволених зовнішніх IP-адрес для екземплярів віртуальних машин.
- Обчислювальний сервіс Compute Engine контейнерів Вимкнути доступ до послідовного порту віртуальної машини.
- Управління ідентифікацією та доступом Вимкнути створення облікового запису служби.

Автоматизація з використанням інфраструктури як коду

Автоматизація за допомогою IaC. Керування великими хмарними середовищами вимагає зміни мислення. Ручне розгортання схильне до людських помилок, відхилень від стандартів конфігурації та важко підтримувати в довгостроковій перспективі, оскільки воно не масштабується. Ідея IaC полягає в переході від ручного до автоматизованого способу розгортання або внесення змін до ресурсів у хмарному середовищі за допомогою коду.

Інфраструктура та комунікація (IaC) допомагає поєднати кілька організацій у межах одного постачальника хмарних послуг або навіть кількох постачальників хмарних послуг.

Існує два способи використання IaC:

- Декларативний. Визначте бажаний стан (наприклад, сховище об'єктів має бути зашифроване в стані спокою).
- Імператив. Визначте, як інфраструктуру потрібно змінити відповідно до ваших вимог (наприклад, упорядковані кроки для створення конфігурації мережі, а потім обчислювальних ресурсів у ній).

Нижче наведено переваги використання IaC:

- Зменшення витрат. Люди можуть зосередитися на завданнях, відмінних від забезпечення ресурсами чи їх зміни.

Швидке розгортання Автоматизація завжди швидше за ручну роботу.

Зменшення ризику Після тестування розгортання всі майбутні розгортання досягатимуть однакових результатів - без людських помилок.

- *Стабільні та масштабовані середовища.* Після тестування розгортання можна легко розгортати нові середовища будь-якого розміру (просто змініть масштаб у файлах конфігурації).
- *Документація.* Оскільки кожне налаштування або зміна записуються всередині коду, ви маєте повний контроль над тим, які конфігурації були реалізовані. Ви можете зберігати всі конфігурації в центральному репозиторії вихідного коду та відстежувати зміни конфігурації або виявлення відхилень за попередньо налаштованими політиками.
- *Неправильні конфігурації безпеки.* Ви можете перевірити наявність невідповідностей перед налаштуванням.

AWS CloudFormation

AWS Cloud Formation - це сервіс Amazon IaC. Cloud Formation дозволяє розгортати та оновлювати обчислювальні, баз даних, сховища, мережеві та багато інших ресурсів AWS стандартним способом.

Деякі з найкращих практик AWS Cloud Formation наведено нижче:

- Використовуйте AWS IAM для контролю доступу до розгортання або оновлення ресурсів.
- Уникайте вбудовування облікових даних у код AWS Cloud Formation - використовуйте AWS Secrets Manager для зберігання облікових даних і таємниць.
- Використовуйте AWS CloudTrail для аудиту активності API Cloud Formation.
- Використовуйте правило AWS Config для перевірки відповідності попередньо визначеній політиці щодо ресурсів, що зберігаються в реєстрі Cloud Formation.
- Використовуйте AWS Cloud Formation Guard для перевірки шаблонів Cloud Formation на відповідність наборам правил (наприклад, усі томи EBS мають бути зашифровані в стані спокою).
- Використовуйте статичний аналіз коду для перевірки коду Cloud Formation на наявність вразливостей безпеки.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Найкращі практики безпеки для AWS Cloud Formation: https://surl.li/ppfszl

Шаблони Azure Resource Manager (ARM)

Шаблони ARM - це рішення Azure IaC, яке дозволяє створювати або оновлювати ресурси Azure.

Деякі з найкращих практик, яких слід дотримуватися:

- Використання Azure RBAC розгортати або оновлювати ресурси.

- Уникайте вбудовування облікових даних у шаблони Azure ARM - використовуйте Azure Key Vault для зберігання облікових даних і таємниць.
- Використання безпечний рядок для всіх паролів та таємниць.
- Використання захищені налаштування щоб переконатися, що ваші таємниці зашифровані, коли вони передаються як параметри до віртуальних машин.
- Використовуйте статичний аналіз коду для перевірки коду вашого ARM-шаблону на наявність вразливостей безпеки.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Що таке ARM-шаблони?: https://surl.lt/fqnwne
Посібник: Інтеграція Azure Key Vault у розгортання шаблону ARM: https://surl.li/niyegh

Менеджер розгортання Google Cloud

GCP Deployment Manager - це рішення Google Cloud IaC, яке дозволяє створювати або оновлювати ресурси GCP.

Деякі з найкращих практик, яких слід дотримуватися:
- Використання Хмарна IAM ролі для керування доступом до розгортання або оновлення ресурсів за допомогою Deployment Manager.
- Уникайте зберігання облікових даних у коді Deployment Manager.
- Використовуйте систему контролю версій, щоб дозволити резервні варіанти для забезпечення журналу аудиту змін коду.
- Використовуйте статичний аналіз коду для перевірки коду Deployment Manager на наявність вразливостей безпеки.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Початок роботи з менеджером розгортання: https://surl.li/nmyfut
Налаштування контролю доступу в конфігурації: https://surl.li/pvvtoa

Терраформ HashiCorp

Terraform вважається найпоширенішим рішенням для IaC. Він працює з різними хмарними провайдерами для розгортання та оновлення ресурсів. Terraform варто розглянути, оскільки він забезпечує стандартизований синтаксис для різних хмарних провайдерів. Це рішення з відкритим кодом з великою спільнотою, яке надає підтримку та має пряму інтеграцію з хмарними API.

Нижче наведено деякі з найкращих практик щодо Terraform:
- Увімкнути журналювання як для усунення несправностей, так і для журналів аудиту (перевірити, який користувач запускав скрипти та вносив зміни до певного середовища чи ресурсу).
- Під час збірки з сервера збірки нам знадобиться якісна система аудиту системи контролю версій, щоб дізнатися, хто реєстрував або об'єднував код.
- Завжди використовуйте захищені протоколи (наприклад, HTTPS/TLS 1.2).

- Зберігайте стан Terraform віддалено.
- Підготовка коду Terraform за допомогою сервера збірки.
- Зберігайте код Terraform у системі контролю версій.
- Уникайте зберігання облікових даних у коді; натомість використовуйте такі рішення, як Hashi Corp Vault, для зберігання всієї конфіденційної інформації (облікових даних, таємниць, паролів тощо).
- Використовуйте статичний аналіз коду для перевірки коду Terraform на наявність вразливостей безпеки.

Наступний код заблокує весь публічний доступ до S3:

```
ресурс "aws_s3_bucket" "mytestbucket2021" { контейнер
   = "моє тестове контейнер 2021"
}
ресурс "aws_s3_bucket_public_access_block" "mytestbucket2021" {
   контейнер = aws_s3_bucket.mytestbucket2021.id
   блокові_публічні_атаки        = правда
   block_public_policy = true
}
```

Для отримання додаткової інформації зверніться до наступного ресурсу: *Вступ до Terraform*: https://surl.li/ftcqjs

Безпека у великомасштабних хмарних середовищах

У попередніх розділах ми розглянули сервіси, які дозволяють нам захищати наші хмарні середовища - від керування виправленнями, керування конфігурацією, відповідності вимогам, керування вразливостями тощо.

Більшість сервісів, побудованих у хмарі, є регіональними (вони функціонують у межах одного регіону). Робота у великомасштабних хмарних середовищах вимагає від нас засобів контролю безпеки під час розподілу їх між кількома обліковими записами в кількох регіонах.

Управління безпекою у великих масштабах під час роботи з AWS

У цьому розділі ми розглянемо керовані сервіси, які можуть допомогти нам забезпечити засоби контролю безпеки у великих середовищах AWS (що містять кілька облікових записів у кількох регіонах).

Керування виправленнями

Щоб керувати виправленнями в середовищах AWS за допомогою хмарних інструментів, виконайте такі дії:

1. Використовуйте автоматизацію AWS Systems Manager.
2. Розгорніть патчі безпеки на основі тегів ресурсів або згрупуйте ресурси за допомогою груп ресурсів AWS на основі цільового облікового запису та регіону.

3. Створіть Роль виконання автоматизації системного менеджера AWS роль у кожному з цільових облікових записів, щоб мати змогу розгортати необхідні виправлення.
   💻 *Примітка!* AWS Systems Manager Automation не є багатохмарним рішенням - для задоволення цієї вимоги доступні сторонні інструменти, такі як Ansible, Salt та інші.

Для отримання додаткової інформації зверніться до наступних ресурсів: *Запуск автоматизації в кількох регіонах та облікових записах AWS*: https://surl.li/oypsus

Управління конфігурацією

Якщо ви бажаєте запускати керування конфігурацією в середовищах AWS, скористайтеся сервісом AWS Config.

Використовуйте агрегатор (ресурс AWS Config) для збору змін конфігурації ресурсів з кількох облікових записів AWS та кількох регіонів AWS - це дозволить вам керувати змінами конфігурації у великих масштабах.

Для кількох хмарних систем або кількох облікових записів AWS може знадобитися сторонній інструмент для інтеграції з реєстратором конфігурації AWS.

Для отримання додаткової інформації зверніться до наступних ресурсів: *Агрегація даних для кількох облікових записів та кількох регіонів*: https://surl.li/fgwhqn

Відповідність вимогам безпеки

Якщо ви бажаєте перевірити відповідність вимогам безпеки в середовищах AWS, скористайтеся сервісом Amazon Inspector. Amazon Inspector дозволяє сканувати екземпляри EC2, виявляти вразливості безпеки (через відсутність патчів безпеки), знаходити відповідність бенчмарку CIS (відомому стандарту безпеки) та неправильні конфігурації (наприклад, відкритий SSH-порт з Інтернету, також відомий як мережева доступність). Amazon Inspector дозволяє перевіряти відповідність вимогам безпеки через AWS Security Hub та інтеграцію зі сторонніми рішеннями CI/ CD.

Для отримання додаткової інформації зверніться до наступних ресурсів: *Автоматизуйте сканування безпеки для міжакаунтних робочих навантажень за допомогою Amazon Inspector та AWS Security Hub*: https://surli.cc/mxvngn

Управління загрозами

Для управління загрозами в середовищах AWS використовуйте Amazon GuardDuty.

Amazon GuardDuty дозволяє виявляти шкідливу активність на основі Amazon CloudTrail (журнал аудиту API), подій даних S3, журналів потоку VPC (мережа) та журналів DNS Route53.

Виберіть один зі своїх облікових записів AWS для адміністрування Amazon GuardDuty та підключіть облікові записи з усієї вашої організації AWS як учасників, що дозволить Amazon GuardDuty мати єдине уявлення про управління загрозами для всієї вашої організації AWS.

Рекомендується інтегрувати Amazon GuardDuty з AWS Security Hub або зі сторонніми інструментами для підтримки гібридних/багатохмарних середовищ.

Для отримання додаткової інформації зверніться до наступного ресурсу:
Керування кількома обліковими записами в Amazon GuardDuty: https://surli.cc/zzyufn

Керування безпекою у великих масштабах під час роботи з Azure

У цьому розділі ми розглянемо керовані служби, які можуть допомогти забезпечити засоби контролю безпеки у великих середовищах Azure (що містять кілька підписок у кількох регіонах).

Керування виправленнями

Для керування виправленнями в середовищах Azure використовуйте Azure Automation Update Management. Update Management дозволяє розгортати виправлення безпеки для машин у кількох підписках Azure, що належать одному клієнту Azure AD. Для багатохмарного рішення рекомендується звернутися до стороннього рішення для керування виправленнями.

Для отримання додаткової інформації зверніться до наступного ресурсу:
Огляд керування оновленнями: https://surl.li/tayapa

Відповідність вимогам безпеки

Якщо ви хочете запустити систему відповідності вимогам безпеки в середовищах Azure, використовуйте Microsoft Defender for Cloud.

Microsoft Defender for Cloud дозволяє збирати дані про безпеку та стан відповідності вимогам з віртуальних машин Azure за кількома підписками з однієї консолі.

Для отримання додаткової інформації зверніться до наступних ресурсів:
Міжклієнтське управління в Центрі безпеки: https://surli.cc/sfphmn
Увімкнення Центру безпеки для всіх підписок у групі керування: https://surl.li/llfwwh

Управління загрозами

Для керування загрозами в середовищах Azure використовуйте Microsoft Defender for Cloud.

Microsoft Defender for Cloud підтримує кілька служб, зокрема кінцеві точки, сховища, бази даних (такі як Azure SQL та керовані бази даних для MySQL) тощо.

Azure Defender дозволяє виявляти загрози (такі як шкідлива активність на віртуальній машині, багаторазове завантаження/вивантаження з облікового запису сховища, потенційні спроби порушення керованих баз даних тощо) з однієї консолі та в кількох підписках Azure.

Управління безпекою у великих масштабах під час роботи з Google Cloud

Google має централізований сервіс під назвою, який дозволяє вам досягати таких цілей у вашій організації Google (що містить кілька проектів GCP):

- *Відповідність.* Перевірити відповідність галузевим стандартам (таким як Центр інтернет-безпеки (СНД)) еталонні показники, Стандарт платіжної картки(PCI-DDS) та інше)
- *Управління вразливостями.* Виявлення відомих вразливостей вебзастосунків у сервісах Google App Engine, Compute Engine та GKE
- *Управління вразливістю контейнерів.* Виявлення підозрілих бінарних файлів та бібліотек у контейнерах

Для отримання додаткової інформації зверніться до наступного ресурсу: *Концептуальний огляд центру командування безпеки*: https://surl.li/tvqfcv

Підсумки Розділу 4

У Розділі 4 було розглянуто стратегії та підходи до побудови гібридних, багатохмарних і великомасштабних хмарних середовищ.

Насамперед увагу приділено архітектурам гібридних хмар, які поєднують локальні ресурси з можливостями хмарних провайдерів. Обґрунтовано важливість стратегії гібридної хмари як інструменту інтеграції локальних обчислювальних і систем збереження інформаії з хмарними сервісами. Проаналізовано механізми IAM від AWS, Azure та GCP, які забезпечують централізовану каталогову службу з уніфікованою ідентифікацією користувачів. Розглянуто методи інтеграції локального середовища з хмарою в гібридній архітектурі, сервіси зберігання даних для міграції інформації та обчислювальні сервіси, що дозволяють однаково керувати ресурсами як у локальній інфраструктурі, так і у хмарі. Також проаналізовано сервіси централізованого управління безпекою, які забезпечують контроль як локальних, так і хмарних середовищ.

Визначено значення багатохмарної стратегії для забезпечення гнучкості, відмовостійкості та оптимізації витрат. Оцінено можливості IAM для централізованого управління ідентифікаціями у таких середовищах. Досліджено методи взаємодії між різними хмарними платформами, зокрема VPN-тунелі типу site-to-site. Приділено увага механізмам забезпечення безпеки даних: шифрування під час передавання, шифрування в стані спокою та концепцію конфіденційних обчислень. Окремо досліджено підходи до управління

виправленнями, конфігураціями та моніторингом у багатохмарних інфраструктурах.

Заключна частина розділу присвячена великим хмарним середовищам, що охоплюють кілька облікових записів, підписок або проєктів. Проаналізовано підходи до розгортання організаційної структури, формування політик контролю та забезпечення дотримання вимог на рівні всієї організації. Розглянуто застосування методології Infrastructure as Code (IaC) для автоматизації процесів - від вбудованих інструментів AWS, Azure і GCP до універсальних рішень, зокрема Terraform. Також було вивчено сервіси безпеки, що дозволяють централізовано керувати виправленнями, забезпечувати відповідність вимогам і здійснювати управління загрозами у масштабних організаційних структурах.

Таким чином, матеріал розділу формує комплексне уявлення про підходи до побудови гібридних і багатохмарних архітектур, а також про особливості управління безпекою у великомасштабних хмарних середовищах. Здобуті знання надають організаціям практичні інструменти для ефективної інтеграції, контролю та безпечної експлуатації розподілених хмарних інфраструктур.

Контрольні питання до Розділу 4

1. Що таке внутрішня загроза у хмарному середовищі?
2. Наведіть приклад сценарію навмисної шкоди від співробітника.
3. Які ризики несе адміністративний доступ до резервних копій?
4. Чому важливо перевіряти біографічні дані працівників перед наймом?
5. Які вимоги варто встановити до паролів, щоб зменшити ризик зламу?
6. Яку роль відіграє SIEM-система у виявленні внутрішніх загроз?
7. Що означає принцип «найменших привілеїв» і як він знижує ризики?
8. Наведіть приклад концепції «розподілу обов’язків» у хмарній безпеці.
9. Чому багатофакторна автентифікація (MFA) є критичною для захисту облікових записів?
10. Як підвищення обізнаності співробітників допомагає виявляти фішингові атаки?
11. Які елементи має включати план забезпечення безперервності бізнесу (BCP) у разі внутрішньої загрози?
12. Як слід організувати процес шифрування конфіденційних даних клієнтів?
13. Чому доступ до ключів шифрування має бути суворо обмежений?
14. Які заходи потрібно вжити для захисту резервних копій поза межами офісу?
15. Які можливості AWS GuardDuty надає для виявлення внутрішніх загроз?
16. Для чого використовується AWS CloudTrail у контексті внутрішніх загроз?
17. Як AWS KMS допомагає у контролі доступу до даних?
18. Для чого використовується AWS Secrets Manager у захисті облікових даних?
19. Яку функцію виконує Conditional Access в Azure AD при захисті від внутрішніх загроз?

20. Як Azure PIM обмежує надмірні привілеї користувачів?
21. Яку роль відіграє Azure Log Analytics у виявленні підозрілої активності?
22. Що таке Azure Key Vault і як він сприяє безпеці даних?
23. Які інструменти GCP можна використовувати для виявлення невдалих спроб входу?
24. Як Google Cloud KMS захищає дані від внутрішніх загроз?
25. Які кроки потрібно зробити після виявлення компрометації облікового запису у GCP?

Правильні відповіді на контрольні запитання

Запитання	Відповідь
1. Внутрішні загрози	
Чому навіть при використанні MFA обліковий запис співробітника може бути скомпрометований, і як цього уникнути?	Можлива компрометація через фішинг токенів або крадіжку сесії; для запобігання потрібні поведінкові аналізатори доступу (UEBA), постійний моніторинг та сегментація доступу.
Який ризик виникає, якщо одна особа має права створення та використання ключів шифрування?	Можливість несанкціонованого шифрування або дешифрування даних без контролю, що порушує принцип розподілу обов'язків.
Як можна технічно обмежити доступ до резервних копій у хмарі для запобігання їх видаленню внутрішнім зловмисником?	Використання WORM-сховищ (Write Once Read Many), окремих облікових записів для резервного зберігання та політик IAM з deny-правами на видалення.
Чому недостатньо просто шифрувати дані, щоб виконати вимоги безпеки при внутрішніх загрозах?	Бо важливо також контролювати доступ до ключів, вести журнали операцій із ключами та забезпечувати ротацію ключів.
Як SIEM може виявити компрометацію облікового запису адміністратора?	Через кореляцію подій, наприклад, нетиповий час входу, підвищення привілеїв і зміну налаштувань безпеки у стислі терміни.
2. Небезпечні API	
Чому обмеження швидкості запитів до API (rate limiting) може запобігти і DoS-атакам, і витоку даних?	Воно зменшує можливість масового перебору запитів (brute-force) та запобігає перевантаженню API великою кількістю запитів.
Як криптографічне підписування API-повідомлень допомагає запобігти атакам типу "man-in-the-middle"?	Воно дозволяє перевірити автентичність і цілісність повідомлення, навіть якщо трафік перехоплено.
Чому навіть захищений HTTPS-з'єднанням API може бути вразливим до SQL-ін'єкцій?	HTTPS шифрує трафік, але не перевіряє коректність вхідних даних; відсутність валідації робить API вразливим на рівні застосунку.
Як WAF може виявити атаку, якщо вона використовує невідомий тип вразливості?	Через поведінкові алгоритми та аналіз аномалій у структурі запитів.

Запитання	Відповідь
Чому відкритий публічний API без автентифікації є критичною уразливістю навіть у тестовому середовищі?	Бо тестові середовища часто підключені до продакшн-систем або містять конфіденційні дані, і їх легко експлуатувати як плацдарм атаки.
3. Зловживання хмарними сервісами	
Як можна виявити майнінг криптовалют у хмарі без встановлення додаткового ПЗ на сервери?	Через моніторинг нетипово високого використання CPU/GPU та аналіз мережевого трафіку на відомі майнінг-пули.
Чому збільшення витрат у рахунках хмарного провайдера може бути ознакою зловживання?	Бо це може свідчити про несанкціоноване розгортання ресурсів для DDoS чи майнінгу.
Як використання VPC ACL та Security Groups може одночасно обмежувати і вхідний, і вихідний шкідливий трафік?	VPC ACL працюють на рівні підмереж, Security Groups -на рівні інстансу, що дозволяє фільтрувати обидва напрями.
Як можна запобігти використанню облікових даних адміністратора для запуску дорогих обчислювальних задач?	Використання IAM з обмеженням прав та окремих облікових записів для критичних операцій.
Чому навчання персоналу правилам прийнятного використання хмари має юридичне значення?	Бо фіксує зобов'язання працівника, що може бути використано в юридичних спорах при порушеннях.
4. Стандарти, відповідність та регулювання	
Чим відрізняється ISO 27001 від ISO 27017 у контексті хмарних сервісів?	ISO 27001 є загальним стандартом управління інформаційною безпекою, ISO 27017 додає спеціалізовані контролі для хмарних середовищ.
Чому SOC 2 Type 2 надає більше гарантій безпеки, ніж SOC 2 Type 1?	Бо SOC 2 Type 2 перевіряє ефективність контролів у дії протягом періоду (не менше 6 місяців), а не лише їх проєкт.
Яка ключова відмінність CSA STAR Level 2 від Level 1?	Level 2 включає сторонній аудит і перевірку ефективності контролів, а Level 1 -лише самооцінку.

Запитання	Відповідь
Чому PCI DSS вимагає ізоляції середовища для зберігання даних платіжних карток від іншої інфраструктури?	Щоб мінімізувати поверхню атаки та запобігти перетоку даних у незахищені сегменти мережі.
Як GDPR регламентує зберігання персональних даних громадян ЄС у хмарі поза межами ЄС?	Дозволяє лише у країнах з адекватним рівнем захисту або при наявності спеціальних договірних механізмів (SCC, BCR).

ПЕРЕЛІК ЛІТЕРАТУРНИХ ДЖЕРЕЛ.

1. Kozlovskyi, V., & Tkachuk, L. (2025). Innovative approaches to improving cybersecurity in cloud environments. *Cybersecurity: Education, Science, Technology, 1*(23), 45–58. Retrieved from https://surl.li/hfidzq

2. Thales Group. (2025). Cloud environment protection: Key challenges and priorities for 2025. *Softprom*. Retrieved from https://surl.li/enmnbn

3. Shortridge, K., & Safavi, A. (2023). *Security chaos engineering: Sustaining resilience in software and systems*. O'Reilly Media.

4. Cerra, A. (2022). *The cybersecurity playbook: How every leader and employee can contribute to a culture of security*. CRC Press.

5. Mohurle, S., & Patel, A. (2021). *Practical cloud security: A guide for secure design and deployment*. Packt Publishing.

НАВЧАЛЬНЕ ВИДАННЯ

Лахно Валерій Анатолійович
Мамченко Сергій Миколайович
Криворучко Олена Володимирівна

БЕЗПЕКА ІНФРАСТРУКТУРИ ХМАРНИХ ОБЧИСЛЕНЬ

НАВЧАЛЬНИЙ ПОСІБНИК