УДК 004.056.5(043.2)

Б. В. Черновол

СИСТЕМА АВТОМАТИЗОВАНОГО КЕРУВАННЯ БЕЗПЕКОЮ ЗАСТОСУНКІВ У ХМАРНОМУ СЕРЕДОВИЩІ

Вінницький національний технічний університет

Анотація. *Ця робота є першою частиною багатоаспектного дослідження, спрямованого на створення системи автоматизованого керування безпекою застосунків у хмарному середовищі. У фокусі цієї частини знаходиться розробка та впровадження підсистеми моніторингу застосунків в хмарних середовищах. В анотації розглядаються основні завдання, методи та потенційні вигоди цієї підсистеми для забезпечення безпеки та надійності хмарних застосунків. Впровадження такої підсистеми вказує на важливий крок у покращенні управління та безпеці хмарними застосунками у сучасному інформаційному середовищі.*

Ключові слова: *Хмарне середовище, моніторинг застосунків, безпека застосунків в хмарному середовищі*

Abstract. *This work represents the first part of a multifaceted study aimed at developing an automated application security management system in a cloud environment. This section focuses on the design and implementation of an application monitoring subsystem within cloud environments. The abstract discusses the core objectives, methods, and potential benefits of this subsystem in ensuring the security and reliability of cloud applications. The introduction of such a subsystem marks a significant step toward enhancing the management and security of cloud applications in the modern information environment..*

Keywords: *Cloud environment, application monitoring, application security in the cloud.*

Вступ

Хмарні обчислення набули великого значення в інформаційному суспільстві, надаючи компаніям і користувачам можливість легко та ефективно використовувати обчислювальні ресурси та послуги через Інтернет. Зараз хмарні середовища стали основними для розгортання та експлуатації різних застосунків, від корпоративних інформаційних систем до мобільних додатків. Проте, разом із цим збільшується і складність забезпечення безпеки цих застосунків у хмарних середовищах.

У даному дослідженні поставлено за мету розглянути ключові аспекти безпеки застосунків в хмарному середовищі та розробити автоматизовану підсистему для керування цією безпекою. Ця робота є першою частиною комплексного дослідження та акцентується на розробці підсистеми моніторингу застосунків. Ми розглянемо ключові виклики та ризики, пов'язані з хмарними технологіями зокрема AWS (Amazon Web Service), і представимо методи та підходи для вирішення цих проблем. Впровадження такої підсистеми є важливим кроком у покращенні надійності та безпеки хмарних застосунків, що стає дедалі важливішим у сучасному інформаційному середовищі.

Результати дослідження

Головною задачею дослідження є розробка та впровадження підсистеми моніторингу застосунків у хмарних середовищах з метою підвищення безпеки та надійності цих застосунків.

Для досягнення головної задачі дослідження було розроблено архітектуру та реалізовано підсистему моніторингу застосунків в хмарному середовищі. Ця підсистема дозволила відстежувати активність та стан застосунків у реальному часі та виявляти потенційні загрози та аномалії. Тестування та аналіз результатів підтвердили позитивний вплив цієї підсистеми на безпеку та надійність хмарних застосунків.

Щоб створити автоматизовану підсистему моніторингу, яка зможе виявляти та реагувати на збої процесу або служби за допомогою команди запуску AWS System Manager., наша розробка буде слідувати архітектурі, яка включає плагін procstat для моніторингу показників процесів використовуючи ці можливості автоматизації AWS. На рисунку 1 наведено архітектуру підсистеми моніторингу розроблену з використанням хмарного середовища AWS.

Спочатку маємо віртуальний сервер EC2 із встановленим агентом Amazon CloudWatch, який відправляє метричні дані до сервісу Amazon CloudWatch.

Для моніторингу показників продуктивності процесу ми використовуємо плагін "procstat". Він відстежує вказані метрики, доки процес активний.

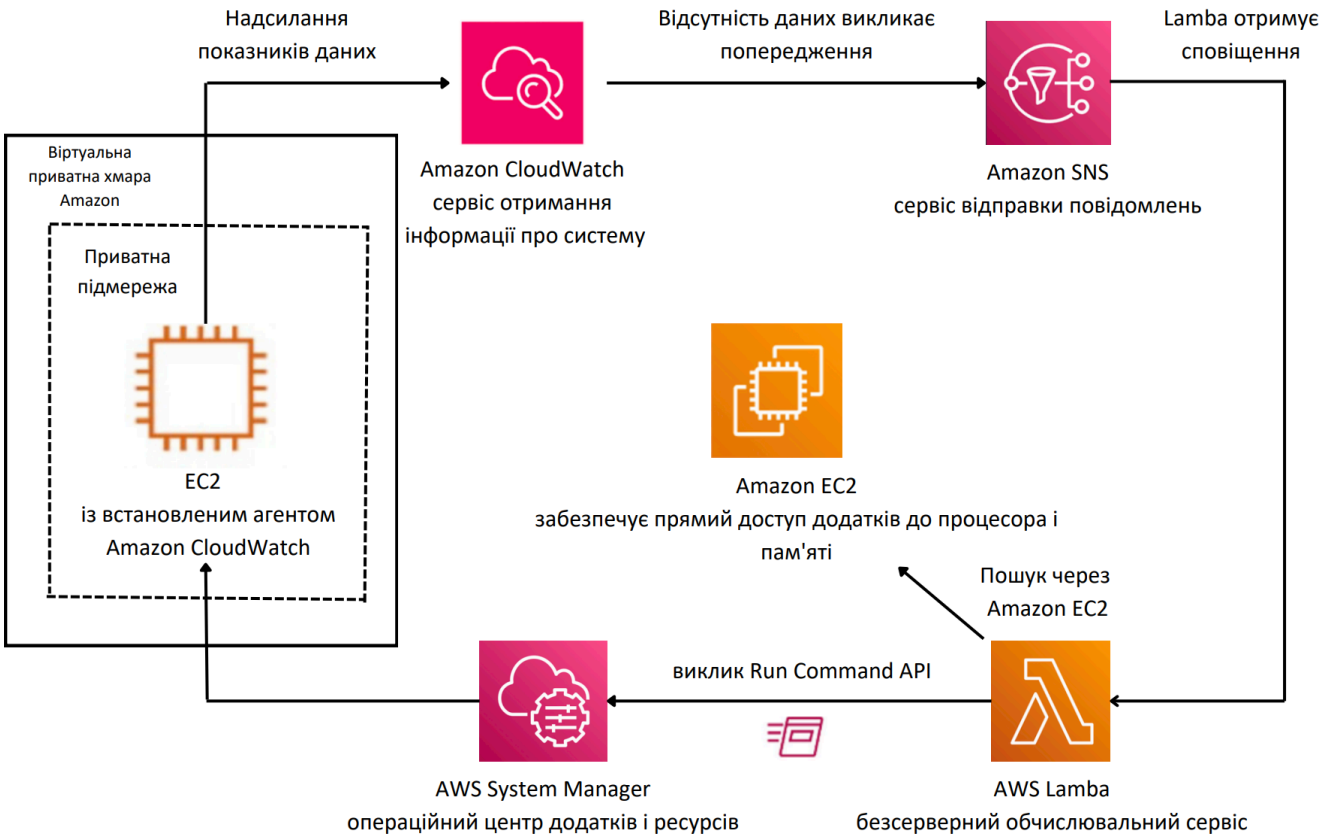

Рисунок 1 – Архітектура системи

Спочатку, встановимо політику порогу для певного метричного показника, де визначається, коли метрика вважатиметься "в порушенні порогу." Це дозволяє нам встановити, наприклад, відсутність даних або перевищення певного значення як критичні сценарії для спрацювання сповіщень.

Коли система CloudWatch визначає, що встановлений поріг порушується, це стає сигналом для генерації сповіщення в режимі "In alarm". Цей режим сповіщення створюється системою CloudWatch і автоматично активується, коли стан метричного показника відповідає заданому порогу або виникає інша визначена умова.

Це сповіщення, що знаходиться в режимі "In alarm", відправляється до визначеної теми Amazon Simple Notification Service (Amazon SNS). Тема Amazon SNS є спеціальною структурою, призначеною для обробки та розповсюдження повідомлень. Вона дозволяє групувати сповіщення та надсилати їх різним отримувачам, таким як електронна пошта, SMS, чи інші канали зв'язку. Amazon SNS є потужним інструментом для розповсюдження сповіщень на різні платформи та до різних споживачів.

Далі, після того як сповіщення в режимі "In alarm" відправлено до теми Amazon SNS, AWS Lambda включається в процес обробки цих сповіщень. Lambda функція є ключовим елементом у виконанні автоматичних дій, які ми бажаємо виконати при спрацюванні сповіщення.

Після запуску, AWS Lambda функція виконує заздалегідь налаштовані дії, визначені в коді функції. Однією з основних дій Lambda функції є витягнення необхідної інформації з отриманого сповіщення. Ця інформація може включати ім'я хоста або інші ідентифікатори, які були передані разом із сповіщенням.

Зі зібраною інформацією, AWS Lambda функція використовує API Amazon EC2 для пошуку ідентифікатора відповідного екземпляра EC2, який потрібно змінити або керувати. Цей ідентифікатор є ключовим елементом для подальшого виконання дій на конкретному екземплярі EC2.

Цей етап дозволяє нам точно ідентифікувати, який сервер потребує дій та визначити його місцезнаходження в хмарному середовищі AWS, що є критичним для подальшого управління та реагування на незвичайні ситуації.

Отриманий ідентифікатор екземпляра EC2, який був ідентифікований за допомогою AWS Lambda, є критичним елементом у виконанні подальших дій на сервері. Цей ідентифікатор використовується для взаємодії з API AWS Systems Manager, що є інструментом для керування та підтримки інфраструктури в хмарному середовищі.

За допомогою цього ідентифікатора AWS Systems Manager може встановити зв'язок із конкретним екземпляром EC2 та ініціювати виконання певної команди оболонки на цьому екземплярі.

Наприклад, ця команда може бути спрямована на перезапуск певної служби або відновлення роботи системи в цілому.

Цей етап дозволяє системі ефективно реагувати на виявлені проблеми або незвичайні ситуації, запускаючи автоматичні дії на конкретних серверах, що допомагає відновити нормальну роботу системи без значного втручання людини. Такий підхід сприяє автоматизації та покращенню управління ресурсами в хмарному середовищі AWS.

З використанням цього підходу створюється високоякісна система, яка дозволяє автоматично моніторити та реагувати на незвичайні ситуації в хмарному середовищі. Основною метою цієї системи є забезпечення ефективного управління ресурсами та надання швидкої реакції на будь-які проблеми, які можуть виникнути у процесі роботи застосунків у хмарному середовищі.

Система автоматично моніторить стан різних показників та метрик, і коли виявляється будь-яке порушення чи незвичайна ситуація, вона відразу ж ініціює відповідні дії для вирішення проблеми. Це може включати в себе автоматичний перезапуск певних служб або екземплярів, відновлення нормальної роботи системи, або надсилання сповіщень та повідомлень адміністраторам.

Завдяки цій системі ресурси ефективно розподіляються та використовуються, а випадки збоїв чи простоювань мінімізуються. Цей підхід допомагає забезпечити надійну та безперебійну роботу хмарних застосунків та забезпечити високу доступність послуг у хмарному середовищі.

Висновки

Запровадження системи автоматизованого моніторингу та управління безпекою та ресурсами в хмарному середовищі AWS є кроком вперед у забезпеченні надійності та безпеки хмарних застосунків. Ця система надає можливість автоматично виявляти незвичайні ситуації, швидко реагувати на них та вживати відповідних заходів для їх вирішення. Механізми моніторингу та сповіщення CloudWatch, Amazon SNS і AWS Lambda дозволяють не тільки виявляти проблеми, але і автоматично ініціювати відповідні дії для їх розв'язання. Цей підхід спрощує процес управління та зменшує вплив випадків простоювань та збоїв на роботу застосунків. Завдяки цій системі, ресурси ефективно розподіляються та використовуються, що допомагає підвищити надійність та безпеку хмарних застосунків. Вона дозволяє забезпечити високу доступність послуг у хмарному середовищі та покращити загальну ефективність управління ресурсами. Впровадження такої системи вимагає правильного налаштування та підтримки. Із правильним підходом, ця система може стати надійним інструментом для забезпечення безпеки та надійності хмарних застосунків.

.

.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Prashant Lakhera. AWS for System Administrators, 2021. 388 c.
2. Dario Lucas Goldfarb, Thiago Morais. AWS Certified Security Study Guide, 2021. 496 c.
3. Detecting and remediating process issues on EC2 instances using Amazon CloudWatch and AWS Systems Manager. URL : https://aws.amazon.com/ru/blogs/mt/detecting-remediating-process-issues-on-ec2-instances-using-amazon-cloudwatch-aws-systems-manager/ (дата звернення: 17.10.2023) .

Черновол Борис Віталійович — студент групи 1БС-22м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: boryacernovol@gmail.com.*

Borys Vitaliyovych Chernovol — Department of Information Techologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, email : boryacernovol@gmail.com.

Шелепало Галина Василівна — к. фіз.-мат. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна.

Shelepalo Halyna V. — PhD (Eng), Associated Professor of Data Protection Department in Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine..