Компанія Продажа

Займається продажем та доставкою товарів. Має додаток інтернет магазину. Інтегровані сервіси такі як оплата онлайн та замовлення доставки різними службами.

Цілі інтеграції у хмарне сховище:

Швидка масштабованість

Безперебійна робота сервісів

Захист даних

Шляхом інтеграції можна досягнути постійного зросту продажів, відповідати нормам захисту даних, використовуючи резервне копіювання та шифрування. Зменшення витрат на масштабування процесів та витрати відділу підримки ІТ ресурсів. Збільшення обсягу трафіку та прийому замовлень з різних регіонів.

Компанія використовує декілька додатків таких як бази даних , різні таблиці, створення замовлень, сам магазин, оплата покупок.

Для інтеграції найбільше підійде гібридний метод, так як компанія вже має наявну інфраструктуру. Буде найбільш вигідним та практичним використання як хмарних рішень так локальних об’єднуючи та синхронізуючи роботу.

Дані передаються у форматі особистих даних такі як ім’я, прізвище, також дані про оплату - трансакційні дані, а також дані ідентичності для доступу до додатку.

Azure Logic Apps дозволяє автоматизувати робочі процеси та інтегрувати різні додатки та сервіси без необхідності написання коду. Azure API Management дозволяє централізовано керувати API, забезпечуючи безпеку, моніторинг та аналітику.

Основні політики для інтеграції.

Політика управління доступом до даних : Встановити чіткі правила щодо доступу до даних, щоб забезпечити, що тільки авторизовані користувачі мають доступ до конфіденційної інформації. Політика збереження та видалення даних : Встановити правила щодо збереження та видалення даних для забезпечення їхньої цілісності та відповідності нормативним вимогам.

Тестування як обов’язкова норма має бути автоматизоване та мати неохідний графік виконання тестів. Також потрібно впровадити повний цикл перевірки роботи сервісів як на рівні коду так і на рівні мережі та доступу до данних. Обов’язково включити перевірку аутентифікації та авторизації. Найважливішими формами тестування будуть інтеграція: потрібно впевнитися, що додаток та сервіси працюють належним чином та взаємодіють. Другий важливим фактором буде безпека: перевірка ідентичності, зберігання даних та доступ тільки авторизованим користувачам і тільки у межах їх дозволу.

### **Стратегія перевірки вхідних даних для реєстрації користувача**

1. **Перевірка типу даних**:
   1. **Ім'я користувача**: Перевірити, що введене значення є рядком (string).
   2. **Електронна пошта**: Перевірити, що введене значення є рядком (string).
   3. **Пароль**: Перевірити, що введене значення є рядком (string).
   4. **Вік**: Перевірити, що введене значення є цілим числом (integer).
2. **Перевірка формату**:
   1. **Ім'я користувача**: Перевірити, що ім'я користувача містить лише допустимі символи (букви, цифри, підкреслення) та має довжину від 3 до 20 символів.
   2. **Електронна пошта**: Перевірити, що електронна пошта відповідає стандартному формату електронної пошти
   3. **Пароль**: Перевірити, що пароль містить принаймні одну велику літеру, одну малу літеру, одну цифру та один спеціальний символ, а також має довжину від 8 до 20 символів.
   4. **Вік**: Перевірити, що вік знаходиться в допустимому діапазоні (наприклад, від 18 до 100 років).

### **Додаткові перевірки:**

* **Узгодженість**: Перевірити, що введені дані узгоджуються між собою (наприклад, підтвердження пароля повинно збігатися з основним паролем).
* **Унікальність**: Перевірити, що ім'я користувача та електронна пошта є унікальними та не використовуються іншими користувачами.