**Система управління ідентифікацією та доступом для корпоративного середовища (IAMPro)**

Мета: створити систему, яка забезпечить безпечний доступ до ресурсів організації, з урахуванням гнучкості, масштабованості та інтеграції зі сторонніми сервісами.

|  |  |  |
| --- | --- | --- |
| **Роль** | **Опис** | **Обов'язки та привілеї** |
| Адміністратор системи (System Administrator) | Освітлення та підтримка всієї системи IAMPro. | * Управління всіма аспектами системи. * Створення, редагування та видалення користувачів. * Налаштування прав доступу. |
| Керівник відділу (Department Head) | Керівник окремого підрозділу, який управляє доступом для своєї команди. | * Управління доступом до ресурсів для підлеглих. * Редагування політик доступу для команди. * Нагляд за активністю в межах відділу. |
| Користувач (User) | Стандартний користувач, який має доступ до певних ресурсів. | * Доступ до ресурсів, дозволених на основі ролі. * Зміна власних налаштувань безпеки (паролі, MFA). |
| Аудитор (Auditor) | Особа, відповідальна за перевірку та аудит використання системи, забезпечення її відповідності стандартам безпеки.   |  | | --- | |  | | * Перегляд логів та звітів. * Аналіз активності користувачів. * Перевірка налаштувань безпеки та політик доступу. |
| Менеджер безпеки (Security Manager) | Керівник, відповідальний за безпеку системи, моніторинг загроз та реагування на інциденти. | * Налаштування політик безпеки та моніторинг загроз. * Розслідування інцидентів безпеки та ініціювання заходів реагування. |

**High-Level Design (HLD) для IAMPro**

Опис апаратних та програмних інтерфейсів:

**Апаратне забезпечення (Hardware):**

Сервери та інфраструктура: Система буде розгорнута на хмарних платформах або фізичних серверах, залежно від вимог до безпеки та продуктивності. Система повинна бути масштабованою для підтримки великої кількості користувачів та інтеграцій.

**Клієнтські пристрої:**

Користувачі можуть доступати систему через різноманітні пристрої, включаючи десктопи, ноутбуки, мобільні телефони, використовуючи браузери або мобільні додатки.

**Програмне забезпечення (Software):**

Базова платформа: Система буде побудована на сучасних технологіях, таких як Java, Python або .NET, для серверної логіки, а також на базі хмарних платформ (AWS, Azure, Google Cloud).

**Системи управління базами даних**:

Для зберігання даних користувачів, політик доступу та аудиту буде використовуватися реляційна база даних (наприклад, PostgreSQL або MySQL) або NoSQL для масштабованості.

**Інтерфейси інтеграції:**

Для інтеграції з іншими системами (наприклад, ERP, CRM, хмарні сервіси) будуть використовуватися стандарти протоколів SAML, OAuth, OpenID Connect.

**Опис інтерфейсів користувача:**

**Веб-інтерфейс**:

**Інтерфейс адміністрування**: Панель для адміністраторів системи, де можна управляти користувачами, політиками доступу та настройками безпеки. Доступний лише для адміністраторів та менеджерів безпеки.

**Інтерфейс керівника відділу**: Панель для керівників відділів, де вони можуть налаштовувати доступ для своїх співробітників, переглядати звіти та аудити.

**Інтерфейс користувача:** Зручний інтерфейс для співробітників, де вони можуть змінювати свої налаштування безпеки, переглядати доступні ресурси та реєструватися на елективні курси або інші ресурси.

**Мобільний додаток:** Мобільний додаток для доступу до системи на мобільних пристроях, з можливістю підтвердження аутентифікації за допомогою биометрії або OTP (одноразовий пароль).

**Опис робочого процесу користувача:**

**Процес аутентифікації:**

Користувач входить в систему, вводячи логін та пароль.

Якщо включена багатофакторна аутентифікація (MFA), система відправляє код на мобільний пристрій або електронну пошту.

Після успішної аутентифікації користувач отримує доступ до ресурсів згідно з політиками доступу, визначеними адміністратором або керівником відділу.

**Процес управління доступом:**

Адміністратор або керівник відділу надає або відкликає доступ до певних ресурсів для користувачів.

Для кожного ресурсу визначається політика доступу (наприклад, лише читання, редагування або адміністрування).

Логування всіх змін у політиках доступу для забезпечення аудиту.

**Специфікації продуктивності:**

**Швидкість відповіді:** Система повинна забезпечити швидкий доступ до ресурсів, час відгуку для користувачів не повинен перевищувати 2 секунд для критичних операцій.

**Масштабованість**: Система повинна підтримувати одночасне підключення до 1000 користувачів у реальному часі з можливістю масштабування для підтримки більших навантажень.

**Безпека**: Система повинна забезпечувати шифрування даних на всіх етапах (в відправці та зберіганні), підтримку багатофакторної аутентифікації та відповідність стандартам безпеки (наприклад, GDPR).

**Архітектура системи:**

Мікросервісна архітектура: Для забезпечення гнучкості та масштабованості система буде побудована на мікросервісах, що дозволить окремо розгортати компоненти для аутентифікації, управління користувачами, управління доступом і аудиту.

**Інтеграційний шар**: Для взаємодії з іншими корпоративними системами (ERP, CRM) використовуватиметься спеціальний інтерфейс API, що забезпечує безпечну передачу даних між системами.

**Високий рівень доступності (HA):** Система повинна працювати в режимі високої доступності, використовуючи кластеризацію серверів та автоматичне відновлення у разі збоїв.

**Функціональні вимоги**

1. Аутентифікація користувачів: Підтримка багатофакторної аутентифікації (MFA).

2. Авторизація: Надання доступу до ресурсів на основі ролей (RBAC).

3. Керування ролями: Створення, редагування та видалення ролей із чітко визначеними правами доступу.

4. Інтеграція з зовнішніми сервісами: Сумісність із хмарними сервісами (AWS, Azure, Google Workspace тощо).

5. Керування сесіями: Можливість моніторингу та примусового завершення активних сесій користувачів.

6. Моніторинг доступу: Відображення історії входів і виходів із системи.

7. Управління обліковими записами: Автоматизація створення, оновлення та видалення облікових записів.

8. Єдиний вхід (SSO): Надання доступу до різних систем організації через одну аутентифікацію.

9. Динамічне оновлення прав доступу: Миттєве застосування змін до прав користувачів без переривання роботи.

10. Інтеграція з системами захисту: Взаємодія із засобами управління інформаційною безпекою (SIEM) для обміну даними.

**Нефункціональні вимоги**

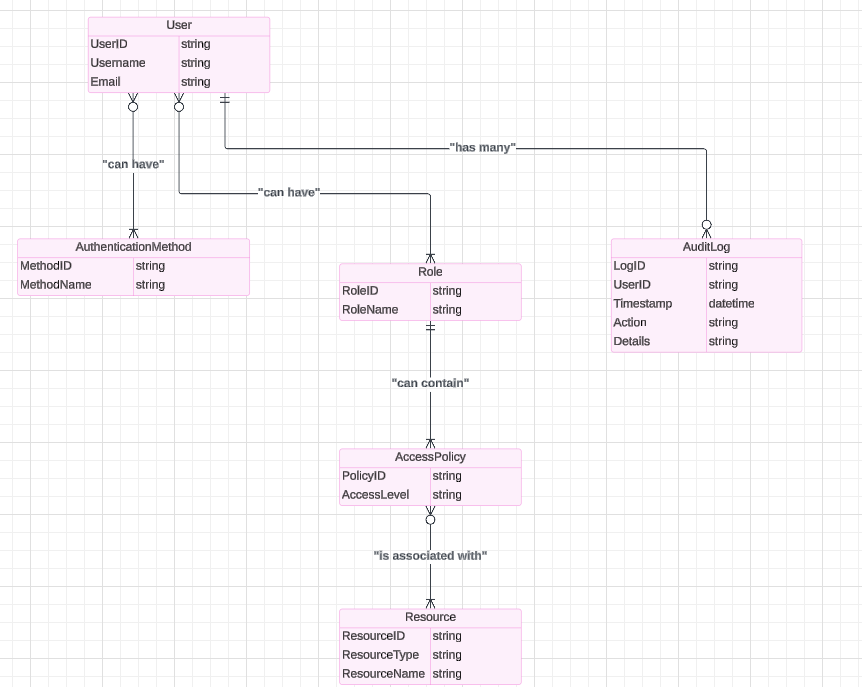
Масштабованість: Система повинна підтримувати одночасний доступ великої кількості користувачів.

Висока доступність: Забезпечення безперервної роботи з мінімальним часом простою.

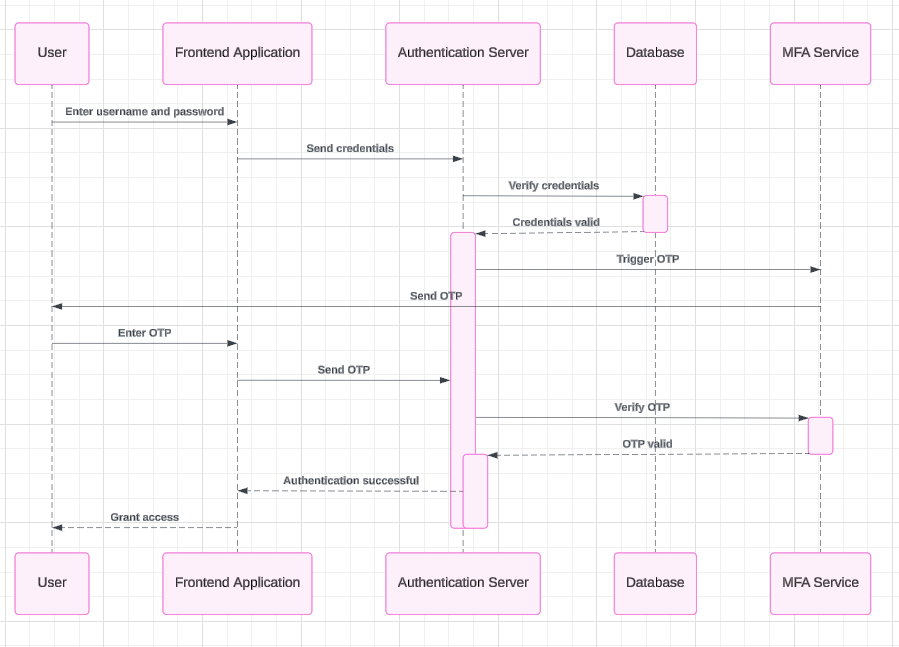
Безпека: Захист від атак, таких як SQL-ін'єкції, XSS, і brute-force.

Продуктивність: Час відповіді системи на запити не повинен перевищувати 2 секунд.

Юзабіліті: Інтуїтивно зрозумілий інтерфейс для адміністраторів і кінцевих користувачів.

**ER-diagram**

**Sequence diagram**

****