LABYRINTH

KONTROLA DOSTĘPU OPARTA NA ROLACH (RBAC)

Labyrinth Deception Platform, 2023

https://labyrinth.tech
info@labyrinth.tech
Labyrinth Development

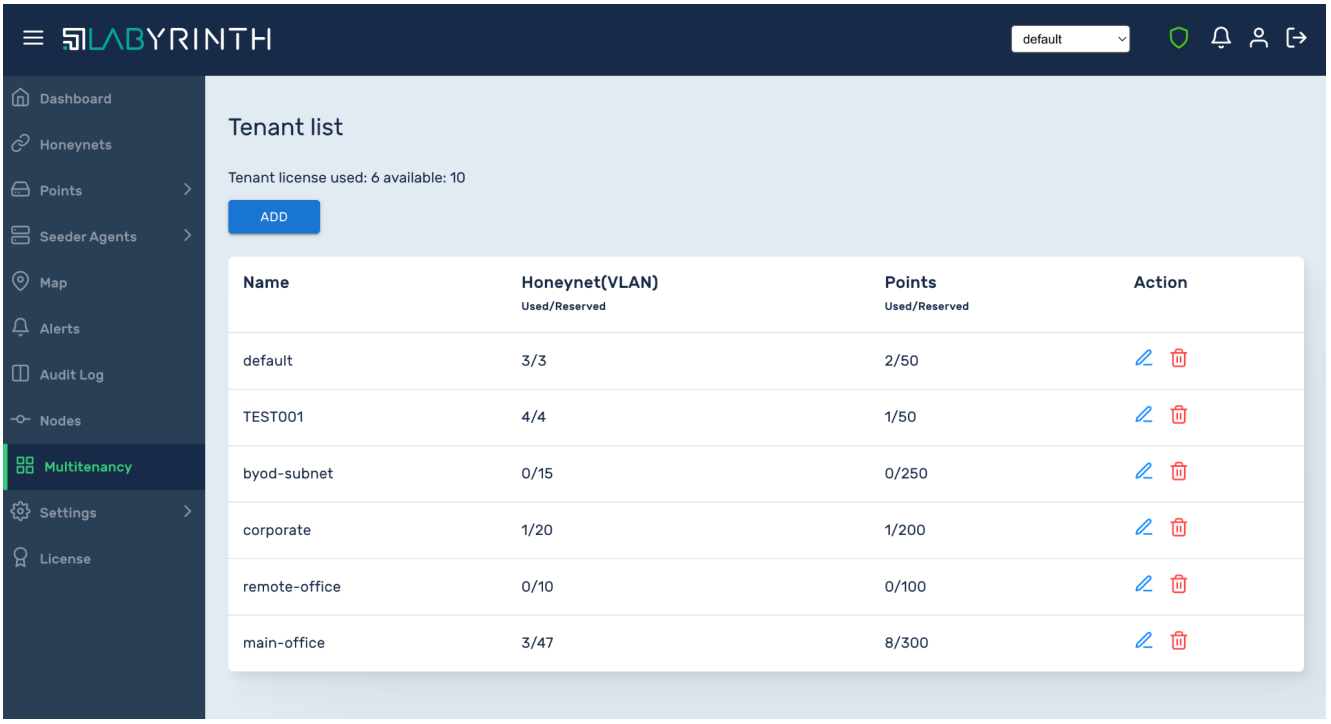
1. MULTITENANCY

Mówiąc najprościej, multitenancy (model wielu najemców) to zdolność różnych użytkowników lub firm do korzystania z odizolowanych od siebie zasobów w ramach tej samej usługi (jednej instalacji lub wdrożenia).

Dzisiejsza architektura modelu wielu najemców jest zatem jednym z najbardziej wydajnych modeli dostarczania usług IT i podstawowym sposobem oszczędzania zasobów obliczeniowych i pamięci dyskowej. Pojedyncza instancja aplikacji, działająca na pojedynczej infrastrukturze serwerowej, ale dostępna dla wielu użytkowników i firm jednocześnie, pozwala zminimalizować koszty świadczenia usług IT i zmaksymalizować ich jakość.

Podział na najemców w ramach platformy Labyrinth składa się z następujących elementów:

1. **„Domyślny" najemca**, którego użytkownicy mają dostęp do wszystkich najemców (superużytkowników). Rola użytkownika określa prawa dostępu;
2. Inni najemcy mają swoich własnych użytkowników z zakresem ograniczonym tylko do ich własnych najemców.



Tzw. „zerowy" najemca to Organizacja/Oddział/Dział, którego zadaniem jest świadczenie usług na rzecz innych Organizacji Klienta.

2. KONTROLA DOSTĘPU OPARTA NA ROLACH (RBAC)

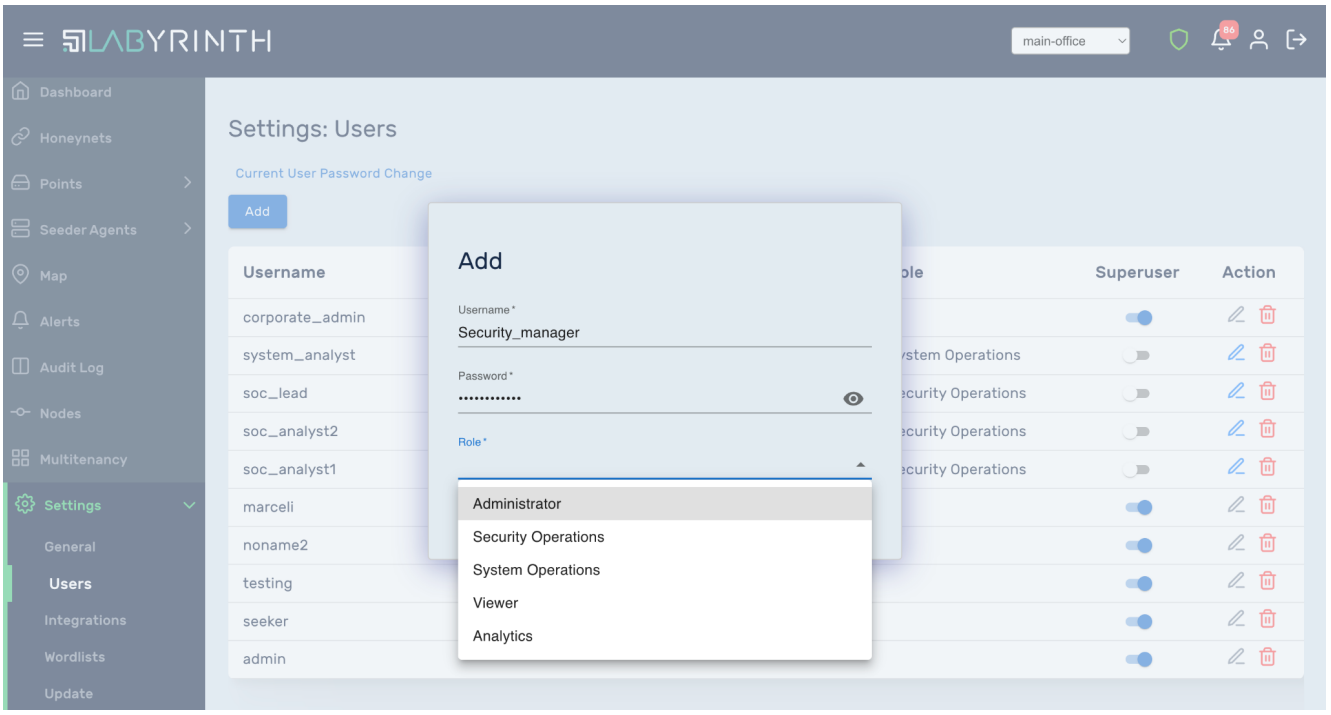
Istotą podejścia RBAC (Role-based access control) jest tworzenie ról odzwierciedlających role biznesowe w firmie i przypisywanie ich użytkownikom. Na podstawie tych ról sprawdzana jest zdolność użytkownika do wykonania określonej akcji.

2.1. Role

Rola jest szablonem uprawnień i dostępów w systemie definiowanym podczas tworzenia użytkownika. Później może być zmieniona przez Superużytkownika lub użytkownika tego najemcy z rolą Administratora.

Istnieje pięć możliwych ról dla użytkowników najemcy dla nowo utworzonego użytkownika:

1. **Administrator** to rola z pełnymi uprawnieniami w ramach najemcy. Użytkownik z tą rolą może tworzyć innych użytkowników w ramach najemcy, w tym użytkowników z rolą Administratora.
2. **Operacje systemowe** to rola, która ma dostęp do komponentów systemu w celu konfiguracji. Dane dotyczące incydentów bezpieczeństwa nie są dostępne.
3. **Operacje bezpieczeństwa** to rola przeznaczona do obsługi incydentów bezpieczeństwa. Rola ma dostęp do danych o wykrytych atakach (Alerts) oraz zarządzania Honeynet, Point i Seeder, ale nie ma dostępu do ustawień systemowych w ramach najemcy.
4. **Widz** to rola podobna do roli Administratora, ale w trybie do odczytu.
5. **Analityka** to rola, która ma dostęp tylko do danych o incydentach bezpieczeństwa.



2.2. Grupy użytkowników

Grupy użytkowników definiują zestaw uprawnień dostępu do jednego lub wielu najemców oraz odpowiadające im uprawnienia.

W systemie występują dwie grupy użytkowników:

1. Superużytkownicy;
2. Zwykli użytkownicy najemcy.

Superużytkownik posiada najwyższe uprawnienia w systemie, wykozystywane do:

- przełączania do dowolnego najemcy;
- zarządzania sekcją menu Multitenancy;
- aktualizacji systemu;
- globalnych ustawień systemu;
- tworzenia nowych Superużytkowników.

Zwykli użytkownicy najemcy funkcjonują tylko w obrębie swojego najemcy na podstawie przypisanej im roli. Mają dostęp wyłącznie do danych swojego najemcy.