Тенанты в KUMA (Multitenancy)

Термины

- **Multitenancy** — "множественное владение", использование общих ресурсов разными пользователями изолировано друг от друга.
- **Tenant (тенант)** — ограницация / филиал организации (в рамках KUMA).
- **General tenant** — основной тенант (Main), который имеет доступ ко всем данным и настройкам своих филиалов, может осуществлять централизованное управление филиалами.

> Права на создание нового и редактирование существующего тенанта — только у пользователя с ролью General admin.

> Для редактирования ресурсов в определенном тенанте, помимо прав администратора тенанта добавьте еще права аналитика к УЗ

> Отключить Main тенант нельзя (можно переименовать), так как некоторые разделы в KUMA доступны только ему, например, Audit события KUMA складваются только в нем.

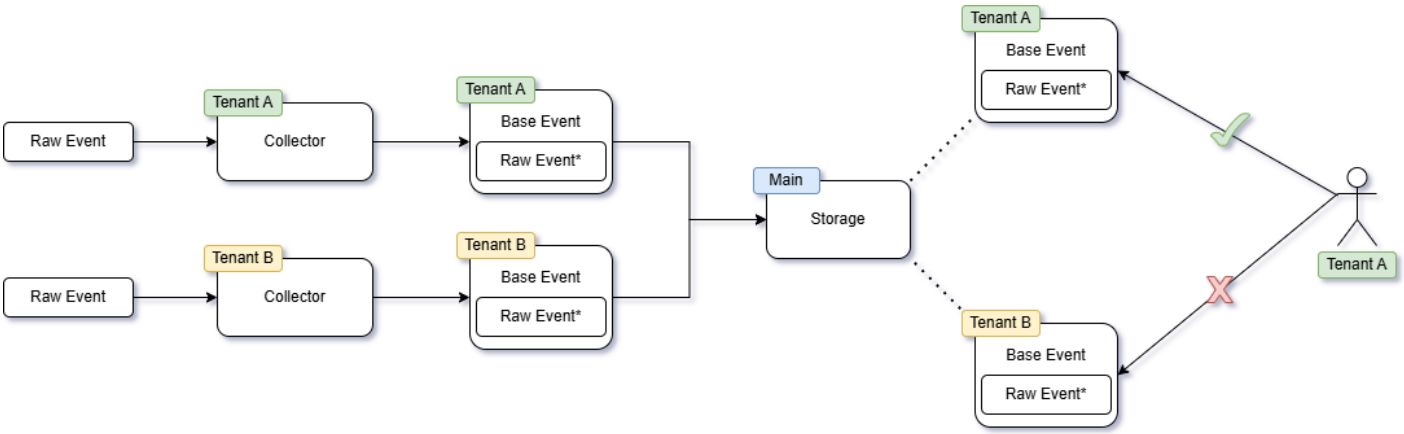
Принцип работы

KUMA Core (ядро SIEM) — это web консоль и компонент управления всеми микросервисами KUMA. В каждой инсталляции один сервер Core. Все остальные микросервисы можно распределять по инфраструктуре, как удобно, даже без разделения по тенантам.

Разделение по тенантам позволяет разграничить доступ пользователей KUMA по событиям (как базовым так и корреляционным), контенту (правила парсинга, корреляции и т.д.). Тенант может назначаться Коллектору или Коррелятору, а Хранилищу можно назначить Тенант (если это архитектурно тербуется), когда оно отдельное со своими дисками и

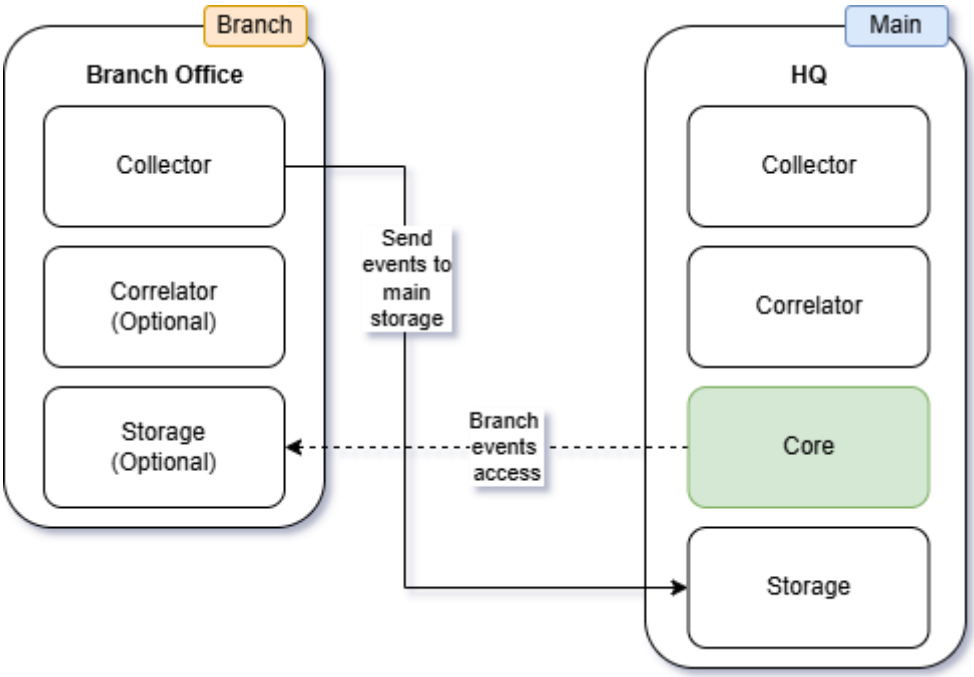
мощностями.

Ниже схематично представлен путь событий в единое Хранилище (Тенант Main), где пользователь Тенанта А может видеть только свои события (Тенанта А):



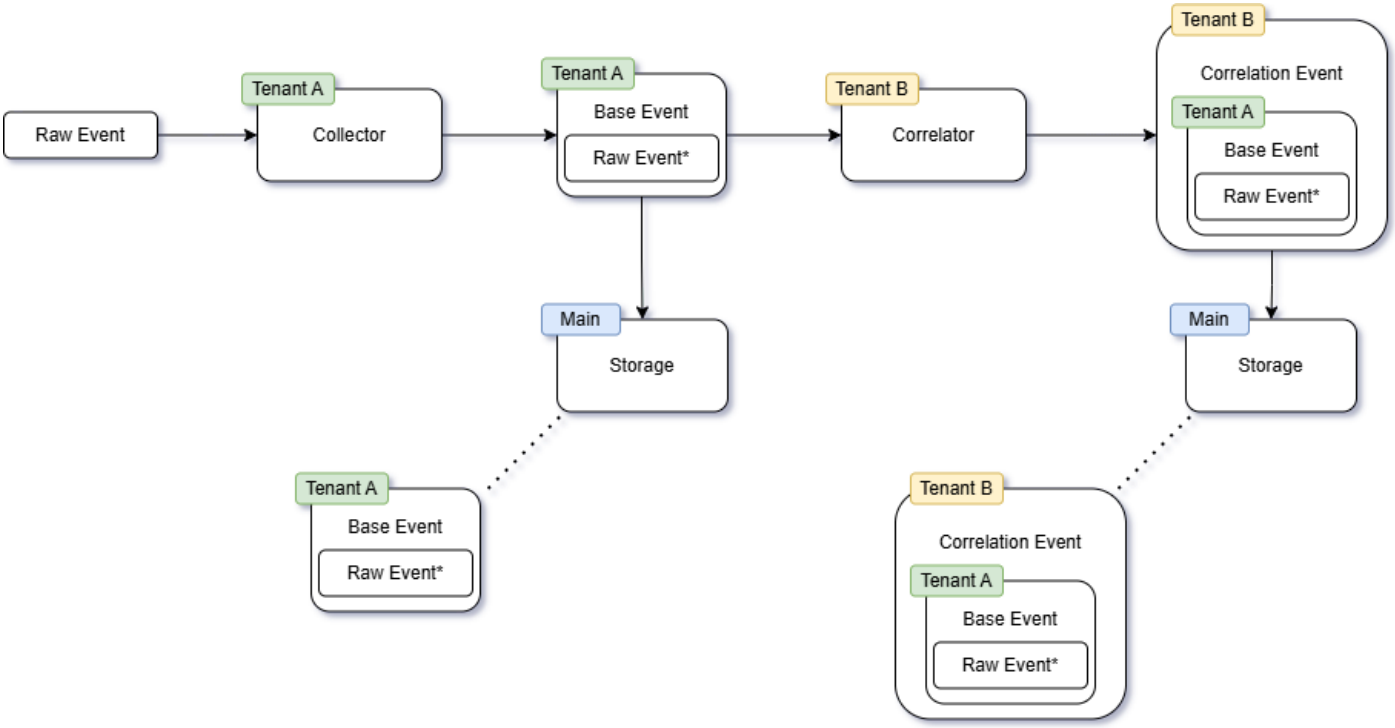
В случае использования нескольких Тенантов в Core находятся только конфигурации для всех микросервисов и алерты со всех тенантов. Пользователи подключаются к Core и отправляют поисковые запросы к хранилищам своих тенантов. Но при этом в Core летят не все события, а только результаты поиска пользователей. Трафик в этом случае минимальный. Одна Core обеспечивает единую точку администрирования всей инфраструктуры KUMA.

Отдельные Коррелятор и/или Хранилище имеет смысл если не хочется значительно нагружать каналы связи между Головным офисом и Филиалом, либо архитектурные / организационные требования.



Кросс-тенантный коррелятор

События разных тенантов могут быть собраны коЛЛекторами, но направляться в один коРРелятор, в этом случае корреляционные события и алерты будут помечены тенантом коррелятора. Ниже представлен пример отправки события от коллектора в Тенанте А в коррелятор Тенант В:



> Ресурсы, используемые в коррелляторе, должны принадлежать тому же тенанту , что и сам коррелятор (т.е. правила корреляции из Тенанта А могут прилинковаться к коррелятору Тенанта А). Исключение Shared тенант, ресурсы общего тенанта могут быть использованы в любом коррелляторе.

Revision #5
Created 7 November 2023 08:49:01 by Boris Rzr
Updated 16 January 2025 08:25:57 by Boris Rzr