Тенанты в KUMA (Multitenancy)

Термины

- **Multitenancy** — "множественное владение", использование общих ресурсов разными пользователями изолировано друг от друга.
- **Tenant (тенант)** — ганизация / 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.

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

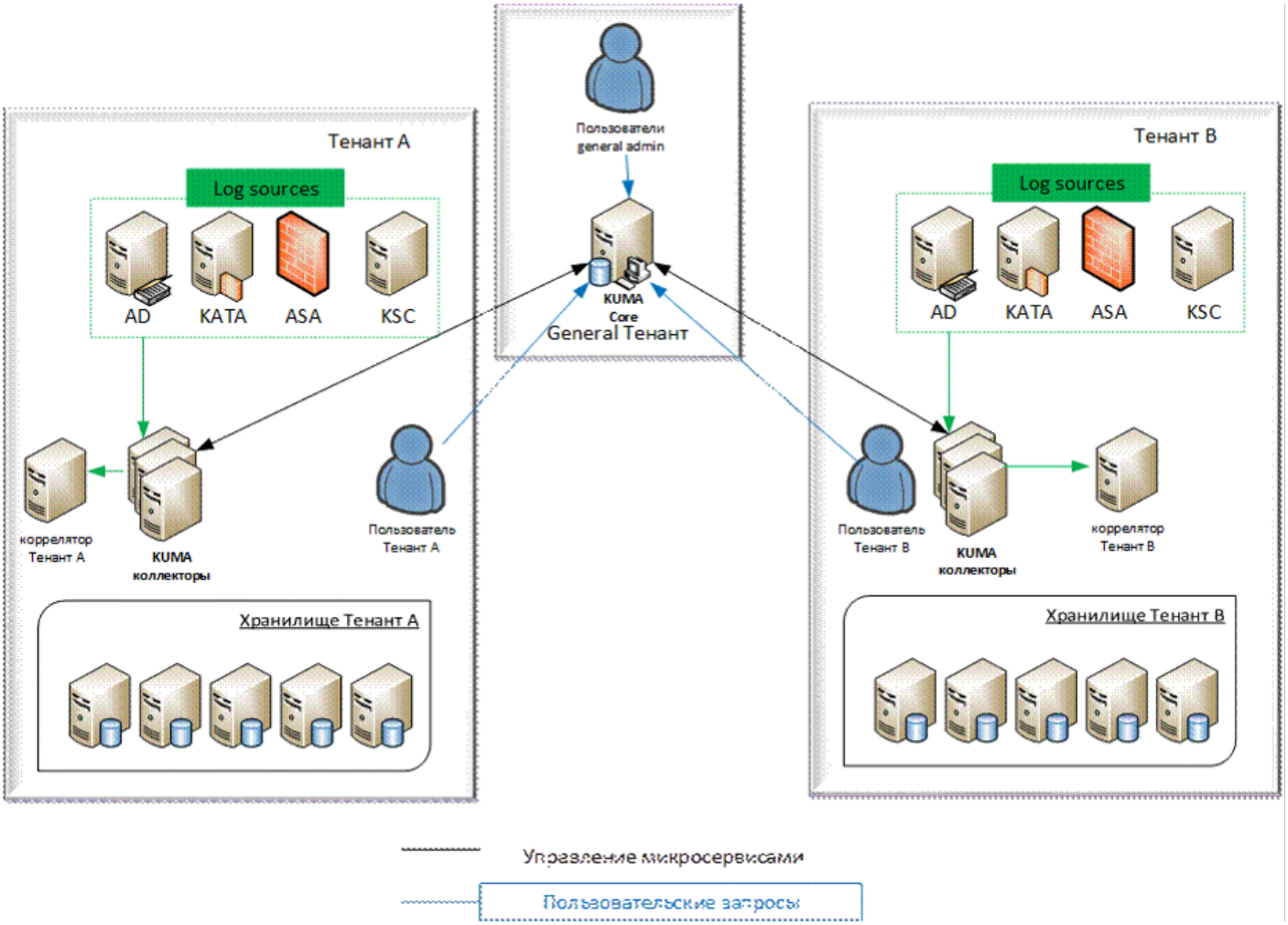
Принцип работы

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 удобней, даже без разделения по тенантам.

Разделение по тенантам позволяет регулировать доступ пользователей KUMA к тем или иным событиям, правилам корреляции и т.п. Например, может быть такая архитектура – тенанты, изолированные друг от друга на уровне событий и сетевого взаимодействия.

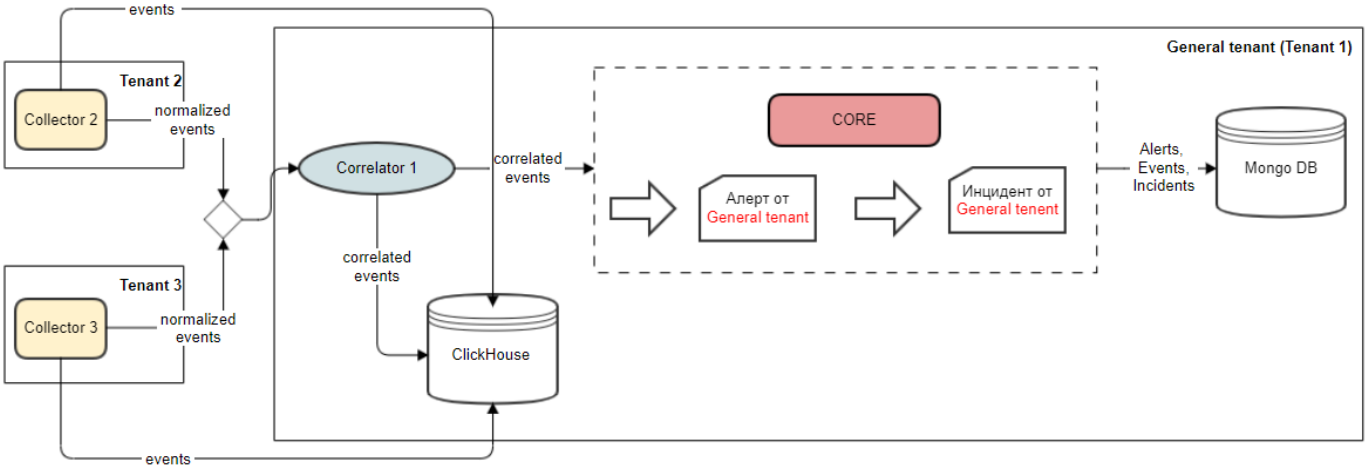
В этом случае в Core находятся только конфиги для всех микросервисов и алерты со всех тенантов. Пользователи подключаются к Core и отправляют поисковые запросы к хранилищам своих тенантов. Но при этом в Core летят не все события, а только результаты

поиска пользователей. Трафик в этом случае минимальный. Одна Core обеспечивает единую точку администрирования всей инфраструктуры KUMA.



Кросс-тенантный коррелятор

События разных тенантов могут быть собраны разными коллекторами, но направляться в один коррелятор, где уже будет обработка событий разных тенантов. Корреляционные события и алерты будут помечены тенантом коррелятора.



> Ресурсы, используемые в корреляторе, должны принадлежать тому же тенанту, что и сам коррелятор. Иначе при сохранении система будет выдавать ошибку. Исключение Shared тенант, ресурсы общего тенанта могут быть использованы в любом корреляторе.

Revision #3
Created 7 November 2023 08:49:01 by Boris Rzr
Updated 7 July 2024 09:02:26 by Koala