Континент версия 4

> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Настройки Континента

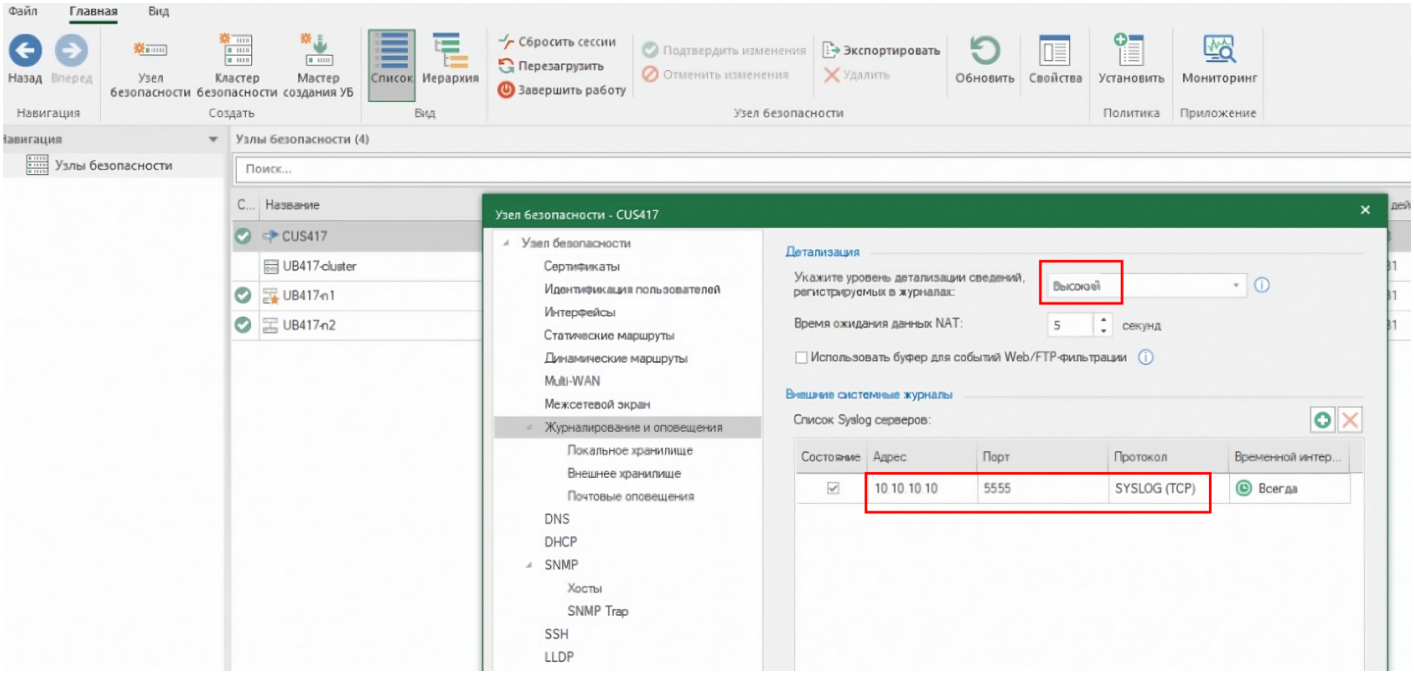
Откройте Менеджер конфигурации Континента.

В настройках узла безопасности раскройте пункт **Журналирование и оповещение**, затем нажмите ⊕ и пропишете IP адрес и порт коллектора KUMA, рекомендуется использовать протокол TCP.

Уровени детализации журнала в Континенте (Рекомендуемый уровень детализации **Высокий**):

Уровень детализации журнала	**Уровень важности события**
Отладочный	Отладка (DEBUG)
Минимальный	Информация (INFO)
Низкий	Ошибка (ERR)
Средний	Критическая ошибка (CRIT)
Высокий	Тревога (ALERT)
Предустановленный	Предупреждение (Warning)

Пример настройки ниже:



Нажмите **Применить** и **ОК**.

Настройка KUMA

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий Usergate.

1. На шаге **Транспорт** укажите тип и порт в соответствии с настройками на стороне Континента.

2. На шаге **Парсинг** событий выберите нормализатор **[2024-05-03] Unix AuditD (REGEX)** из папки нормализоторов Community-Pack.

3. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:

- **Хранилище**. Для отправки обработанных событий в хранилище.
- **Коррелятор**. Для отправки обработанных событий в коррелятор.

Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

4. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

5. Скопируйте появившуюся команду для установки коллектора KUMA.

Полезные ссылки

Справка по Континенту версия 4 - **тут**

Статья в HABR по интеграции Континента и KUMA -

https://habr.com/ru/companies/tssolution/articles/792078/

Revision #3
Created 8 May 2024 07:24:38 by Boris Rzr
Updated 29 January 2025 07:43:29 by Koala