?????????? ???????? ?????? ? ????????? KSC

> Инструкция актуально для всех версий KEDR 8.x
> Дата исправления: 12.11.2026

???????

- OSMP EDR строился как единая консоль управления, тесно интегрированная с EPP. Связь с серверами KSC - это канал получения данных об активах и выполнения части действий реагирования, а не «опция для удобства».
- **Вариант A - подключить существующий KSC как подчиненный.**
- **Вариант B - не подчинять KSC вовсе.**

1. ????? OSMP EDR ????? ? ????????? KSC

В on-prem развертывании предполагается, что серверы KSC, управляющие защитой на хостах, встроены в единую иерархию под сервером KSC из состава OSMP. Иерархия даёт:

- **шлюзовые соединения** к подчиненным серверам любого уровня вложенности - без повторной аутентификации и явного указания параметров подключения, включая серверы в **DMZ**, без исключений на сетевой инфраструктуре;
- **наследование прав** с группы администрирования корневого сервера, из которой растёт ветвь;
- **централизованные EPP-сценарии**: развертывание защиты и обновлений (включая EDR-агенты), групповые политики по всей иерархии, выборки устройств, групповые задачи, распространение инсталляционных пакетов;
- **связь серверов KSC и их активов с тенантами платформы** - по этому каналу Asset Manager наполняет карточки активов данными KSC.

Поэтому вопрос «подчинять или нет» - это вопрос об объёме доступных сценариев, а не только о топологии.

2. ??????? A: ????????? KSC ? ???????????? ????????

Общая идея: существующие серверы KSC регистрируются как подчиненные, но права пользователей OSMP на эту ветвь урезаются. Управление EPP в полном объёме остаётся в штатной веб- или MMC-консоли KSC - во всех конфигурациях ниже.

A1: ????? ??????? ??????

Обычным пользователям консоли OSMP не назначаются на сервере KSC из состава OSMP никакие права и роли, кроме права подключения и базового чтения. Без этого права вход в консоль невозможен.

Цена простоты: данные всех подчиненных серверов доступны на чтение.

A2: ?????? ?????? ????? KSC

1. На сервере KSC в составе OSMP создать **группу администрирования**, логически соответствующую существующему корневому (или отдельно стоящему) серверу KSC.
2. В настройках этой группы **разорвать наследование прав**.
3. **Зарегистрировать** существующий сервер KSC как подчиненный в этой группе.
4. Повторить для каждого корневого или отдельно стоящего сервера. Если права пользователям OSMP на них не нужны - все можно разместить в одной группе администрирования.

Результат: пользователи OSMP не получают доступ к интерфейсу управления этими серверами и их вложенными подчиненными серверами. Существующие администраторы KSC продолжают работать в своих консолях без ограничений.

A3: ???????? ????? ? ???????????? ?????? ????

На базе A2 главный администратор OSMP выдаёт ограниченному кругу пользователей выбранные права на группу администрирования, к которой подключены существующие серверы. Операции на этих серверах и их вложенных подчиненных смогут выполнять только эти пользователи.

Ограничение, которое стоит принять заранее: права на подчиненные серверы при подключении через консоль OSMP наследуются от прав на группу администрирования, в

которой они зарегистрированы. Если в одной группе несколько подчиненных серверов, включая вложенных, права на них будут **одинаковыми**. Разделить права на серверы глубже первого уровня вложенности в этой модели нельзя.

A4: ????? ????? ??????????? ?????????????

Миграция данных корневого сервера на сервер KSC из состава OSMP с переподключением устройств даёт независимое управление правами на серверы, ранее бывшие непосредственно подчиненными старому корню.

- миграция данных трудоёмка и требует планирования, особенно при множестве подчиненных серверов;
- переподключение устройств в общем случае **не бесшовно**: может потребовать задач смены сервера или повторного развертывания защиты;
- часть сценариев KSC в развертывании OSMP может быть недоступна - например, патч-менеджмент стороннего ПО и ОС Windows. Состав доступного сверяйте по документации релиза.

3. ??????? B: ?? ????????? KSC ?????

Этот вариант официально не входит в техническую поддержку

??? ????????

Область	Проявление
EPP-действия реагирования	Не работают действия, реализуемые не через Agent-server протокол: перемещение хоста в указанную группу администрирования KSC, принудительное обновление баз
Карточка актива	Практически нет данных: установленные компоненты KES, найденные уязвимости ПО, актуальность антивирусных баз
Видимость парка	Хосты без корректно установленного и подключенного EDR-агента в консоли OSMP не видны
Единая политика	Нельзя задать общие базовые параметры защиты для всех endpoints единой политикой

????? ??????? B ????????

- ограниченный **пилот** с узким скоупом: только Detection & Response на явно определённом сегменте;
- регламент **категорически** запрещает изменение контура EPP, и заказчик готов принять перечень ограничений;
- EPP-контур живёт автономно, а SOC согласен собирать контекст по активу в консоли KSC.

??? ??????????????

1. **Разделение труда в инциденте:** SOC инициирует EPP-действие заявкой, IT выполняет его в консоли KSC. Согласовать SLA на такие заявки.
2. **Регулярная сверка покрытия:** сравнивать список хостов в KSC со списком активов в OSMP, чтобы выявлять «слепые зоны» без EDR-агента.
3. **Контекст актива - из KSC:** регламентом предусмотреть выгрузку или ссылку на данные KSC в карточке инцидента.
4. **Критерии перехода к варианту А** определить заранее - например, появление потребности в EPP-действиях или полной инвентаризации.

Revision #3
Created 12 November 2026 08:05:30 by Кирилл
Updated 12 November 2026 12:03:20 by Кирилл