

# KEDR Expert on-premise: ?????? ?????????????????? ?? ?????????????????? ? ?????????????????? ??????????????????

Версия продукта: KEDR Expert on-premise 8.0

Актуальный список ограничений: [support.kaspersky.ru/kedr-expert-on-premise/8.0/303912](https://support.kaspersky.ru/kedr-expert-on-premise/8.0/303912)

## 1. Проверка основных компонентов KUMA (вне Kubernetes кластера):

```
systemctl status kuma-collector-<id>.service  
systemctl status kuma-correlator-<id>.service  
systemctl status kuma-storage-<id>.service
```

ID компонента можно скопировать из консоли OSMP (Ресурсы и сервисы - Активные сервисы)

Ресурсы и сервисы / Сервисы

### Сервисы

+ Добавить ▾ | Развернуть | Обновить параметры | Перезапустить

| <input type="checkbox"/> | Статус ▾ | Тип ▾     | Сервис ▾             | Версия ▾ |
|--------------------------|----------|-----------|----------------------|----------|
| <input type="checkbox"/> | ● Вкл    | Коллектор | [OOTB] Kaspersky EDR | 4.3.0.95 |
| <input type="checkbox"/> | ● Вкл    | Коллектор | [OOTB] Kasp          |          |
| <input type="checkbox"/> | ● Вкл    | Коллектор | [OOTB] Kasp          |          |

- Копировать идентификатор
- Скачать журнал
- Скачать дамп

Работа с логами через системное журналирование:

```
journalctl -xe
journalctl -xe | grep "<component-name-with-id>"
journalctl -u "<component-name-with-id>" -e
```

Работа с логами коллекторов, корреляторов и хранилищ:

```
less /opt/kaspersky/kuma/collector/<collector_id>/log/collector
less /opt/kaspersky/kuma/correlator/<correlator_id>/log/correlator
less /opt/kaspersky/kuma/storage/<storage_id>/log/storage
tail -n 100 /opt/Kaspersky/kuma/storage/<storage_id>/log/storage
systemctl list-units | grep kuma-<name service>
```

Проверить открыт ли удаленный порт:

```
telnet <host-ip> <port>
nc -uzv <host-ip> <port>
nmap <host-ip> -p <port>
```

Проверить открытые порты:

```
firewall-cmd --list-ports
```

Открыть порт на firewall:

```
firewall-cmd --add-port=7210/tcp --permanent
firewall-cmd --reload
```

Проверка входящих подключений через tcpdump:

```
tcpdump -i any port 5144 -A
```

## 2. Полезные команды для работы с Kubernetes

### Для Kubernetes k0s Cluster

| Task              | Command                               |
|-------------------|---------------------------------------|
| View cluster info | k0s kubectl cluster-info              |
| View nodes        | k0s kubectl get nodes                 |
| View node details | k0s kubectl describe node <node-name> |
| Check k0s status  | k0s status                            |

### Для Kubernetes k0s Pods

| Task          | Command                 |
|---------------|-------------------------|
| List all pods | k0s kubectl get pods -A |

|                                    |   |
|------------------------------------|---|
| List all pods changes in real-time | k0s kubectl get pods -A --watch                           |
| List pods in a namespace           | k0s kubectl get pods -n <namespace>                       |
| Pod details                        | k0s kubectl describe pod <pod-name> -n <namespace>        |
| Delete pod                         | k0s kubectl delete pod <pod-name> -n <namespace>          |
| Exec into a pod                    | k0s kubectl exec -it <pod-name> -n <namespace> -- /bin/sh |

## Для Kubernetes k0s Namespace

| Task                           | Command                             |
|--------------------------------|-------------------------------------|
| List namespaces                | k0s kubectl get namespaces -A       |
| Get all resources in namespace | k0s kubectl get all -n <namespace>  |
| Delete namespace               | k0s kubectl delete namespace <name> |

## Для Kubernetes k0s Secrets & ConfigMaps

| Task                         | Command  |
|------------------------------|--|
| List all secrets             | k0s kubectl get secrets -A                                   |
| List secrets in a namespace  | k0s kubectl get secret -n <namespace>                        |
| View secret (base64 encoded) | k0s kubectl get secret <name> -n <namespace> -o yaml         |
| Decode secret                | k0s kubectl get secret -o jsonpath="{.data.}" -n <namespace> |
| List configmaps              | k0s kubectl get configmap                                    |
| View configmap               | k0s kubectl describe configmap <name>                        |

## Для Kubernetes k0s Logs

| Task                             | Command   |
|----------------------------------|---|
| View logs of a pod               | k0s kubectl logs <pod-name> -n <namespace>              |
| Get logs of a pod in a real time | k0s kubectl logs -f <pod-name> -n <namespace>           |
| Save a specific log to the file  | k0s kubectl logs -f <pod-name> -n <namespace> > log.txt |
| Stream logs                      | k0s kubectl logs -f <pod-name> -n <namespace>           |
| View logs of previous run        | k0s kubectl logs --previous <pod-name> -n <namespace>   |

## Для Kubernetes k0s Deployments & Services

| Task                            | Command                                       |
|---------------------------------|---|
| List all deployments            | k0s kubectl get deployments -A                |
| List deployments in a namespace | k0s kubectl get deployments -n <namespace>    |
| List services                   | k0s kubectl get svc                           |
| View deployment status          | k0s kubectl rollout status deployment/<name>  |
| Restart deployment              | k0s kubectl rollout restart deployment <name> |

## Для Kubernetes k0s PVC

| Task                      | Command  |
|---------------------------|--|
| List all PV               | K0s kubectl get pvc -A                             |
| List PVCs in a namespace  | k0s kubectl get pvc -n <namespace>                 |
| PVC details               | k0s kubectl describe pvc <pvc-name> -n <namespace> |
| Edit a PVC in a namespace | k0s kubectl edit pvc -n <namespace>                |
| List all PV               | K0s kubectl get pv -A                              |
| List PVCs in a namespace  | k0s kubectl get pv -n <namespace>                  |
| PVC details               | k0s kubectl describe pv <pvc-name> -n <namespace>  |

## 3. Получение диагностической информации о KEDR (XDR) компонентах

Утилита KDT позволяет получать диагностическую информацию о компонентах KEDR (XDR), устранять неполадки самостоятельно или с помощью службы технической поддержки

Kaspersky.

1) После установки вы можете выполнить следующую команду, чтобы просмотреть список всех установленных компонентов:

```
./kdt state
```

2) Отобразится список установленных компонентов. Правильно установленные компоненты имеют статус "Succeeded". Если установка компонента завершилась неудачно, этот компонент имеет статус "Failed".

3) Чтобы просмотреть полный журнал установки некорректно установленного компонента, выполните следующую команду:

```
./kdt state -l <имя_компонента>
```

4) Чтобы получить диагностическую информацию о компонентах и веб-плагирах управления на хосте администратора, где расположена утилита KDT, выполните следующую команду и укажите необходимый флаг:

```
./kdt logs get <флаг>
```

a. Где <флаги> - это параметры команды, которая позволяет настроить результат ведения журнала.

b. Вы можете указать следующие параметры ведения журнала:

- Период регистрации, например, все журналы за последние 12 часов:

```
./kdt logs get --to-archive --last=12h
```

- Вы можете получить диагностическую информацию за период от 2 минут до 7 дней. Если период регистрации не указан, вы получите его за максимальное время.
- Путь к целевому файлу и каталог для сохранения диагностической информации:

```
./kdt logs get -D ./path_to_folder/ --last=12h
```

5) Чтобы просмотреть доступные флаги, выполните одну из следующих команд:

```
./kdt logs get -h  
./kdt logs get --help
```

6) Логи также можно загрузить непосредственно из pod'ов. Для этого выполните команды (не забудьте изменить namespace):

```
k0s kubectl get pods -A  
k0s kubectl get pods -n irp
```

```
k0s kubectl logs interpreter-58c5856f7c-hfd87 -n irp
```

Где имя **interpreter-58c5856f7c-hfd87** должно быть изменено на уникальное имя вашего pod'a

---

Revision #1

Created 21 April 2026 05:12:41 by Кирилл

Updated 21 April 2026 10:32:29 by Кирилл