?????????? ?? ?????????? ?????????? Central Node ? ?? ?????????? EDR ???????

??????????????:

- **?? ?? ??? ?? ??????? ?? ???? ????? ? ????.**
- **???????? ????????? ?? ???? ???? ????, ??? ????????? ?? ?????????? EDR ????? ?? ???????.**

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

?????? ???????????????? ? ????????????? ?? ?????? ?????????? ?????? ?????????. ???? ?????? ?????????? ?? ?????????, ??? ??????? ????????????? ?????????? ?????????? ????????? ?? ?????? ? ??????? ????????????? ????? ???????.

?????????? ?? ???? ?????????? EDR ????

В KATA база Elasticsearch располагается по этому пути

```
/data/storage/volumes/elasticsearch-1/
```

В KATA 4.X база Elasticsearch располагается по этому пути

```
/data/var/lib/kaspersky/storage /swarm/elasticsearch-1/
```

? ???? ??????? ?????????? ???????? ?????????? ??????? ????????? ? ???? Central Node

?????????? CIFS ????????? ??? ?????????? ?????????? Central Node

1. В KATA «из коробки» доступно монтирование общих ресурсов CIFS (только их). Примонтируйте общий ресурс.

```
mount.cifs <папка на стороннем сервере> <директория монтирования> <-o опции>


* вместо mount.cifs можно написать mount -t cifs.


Пример:
mount.cifs //10.10.10.1/backup /kata-backup
mount -t cifs //10.10.10.1/backup /kata-backup
где //10.10.10.1/backup – расшаренная папка, которую необходимо примонтировать.
```

   Примечание:
   Для работы CIFS/SMB необходимы порты:
   - TCP 445;
   - UDP 137;
   - UDP 138;
   - DP 139

   Для предоставления удалённого доступа используется TCP 445.
   Для разрешения имен NetBios используются порты UDP 137, 138 и TCP 139, без них будет работать только обращение по IP адресу.
2. После подключения папки, ее можно будет использовать для сохранения резервных копий CN и TAA

```
/kata-backup – директория смонтирована в корень.
Для проверки - можете выпонить df -h, и /kata-backup будет отображена в общем списке директорий.
```

??????????? NFS ????????? ??? ?????????? ??????????? Central Node ????? DKPG

1. Скачайте пакеты для поддержки NFS по ссылке:

```
https://box.kaspersky.com/f/bde4814949ff493ab876/?dl=1
Пароль от хранилища можно запросить у команды pre-sale инженеров Anti-APT
```

   Распакуйте и перенесите их в домашнюю директорию пользователя Admin

2. Установите пакеты вручную через dpkg в следующем порядке, чтобы добавить поддержку NFS:

```
Команды:
```

```
dpkg -i /home/admin/libtirpc-common_1.2.5-1_all.deb
dpkg -i /home/admin/libtirpc3_1.2.5-1_amd64.deb
dpkg -i /home/admin/keyutils_1.6-6ubuntu1_amd64.deb
dpkg -i /home/admin/libnfsidmap2_0.25-5.1ubuntu1_amd64.deb
dpkg -i /home/admin/rpcbind_1.2.5-8_amd64.deb
dpkg -i /home/admin/nfs-common_1.3.4-2.5ubuntu3.5_amd64.deb
```

3. Примонтируйте сетевой NFS каталог

```
Команда:

mount -t nfs 10.10.10.1:/mnt/nfs/backup /kata-backup
где 10.10.10.1 – сервер, на котором подключен каталог /mnt/nfs/backup
/kata-backup – каталог на CN куда монтируется шара.
```

4. Опционально: Автоматическое подключение каталога после перезагрузки CN

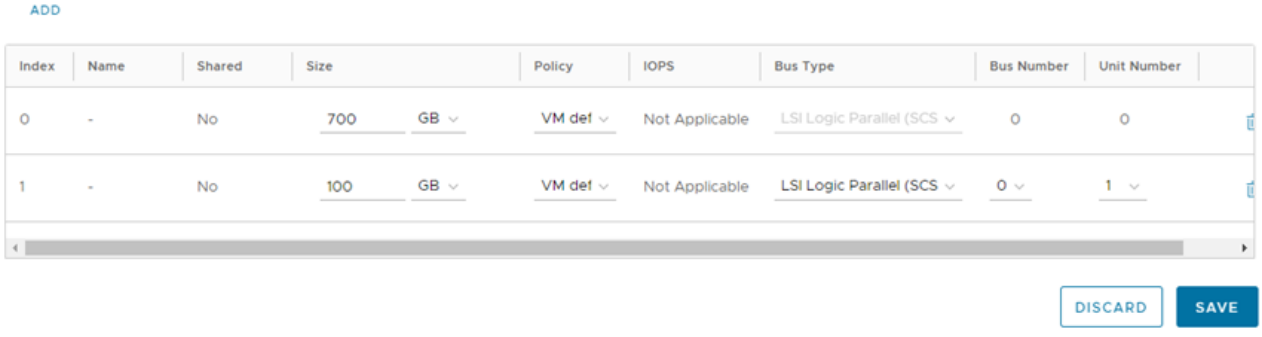
```
Открыть файл fstab:
vi /etc/fstab

Добавить строку:
10.10.10.1:/mnt/nfs/backup        /kata-backup    nfs     auto    0 0

где 10.10.10.1– адрес сервера NFS; /kata-backup – каталог, куда будет примонтирована
шара.
```

??????????? ??????????????? ????? ??? ?????????? ??????????? Central Node ? ??????????? ??????????

1. На платформе виртуализации добавьте диск.
   Перейдите в свойства ВМ, раздел диски. Добавьте диск необходимого объема.



2. Проверьте отображение подключенного диска.

```
sudo fdisk -l или lsblk
```

Отобразятся все диски и разделы.
Наш подклченный диск называется sdb, либо sdc, в зависимости от количества дисков/разделов.

3. Необходимо создать новый раздел.

```
fdisk /dev/sdb
где /dev/sdb - имя нового раздела.
```

Далее необходимо последовательно ввести указанные ключи:

```
n - создать новый раздел;
p - создать новый основной раздел;
Выбрать номер раздела, его первый и последний секторы (по умолчанию Enter);
w - сохранить новый раздел на диск.
```

```
root@1.srv.node1.node.dyn.kata:/home/admin# fdisk /dev/sdb

Welcome to fdisk (util-linux 2.34).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0xbe3c2481.

Command (m for help): n
Partition type
   p   primary (0 primary, 0 extended, 4 free)
   e   extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-209715199, default 2048):
Last sector, +/-sectors or +/-size{K,M,G,T,P} (2048-209715199, default 209715199):

Created a new partition 1 of type 'Linux' and of size 100 GiB.

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

root@1.srv.node1.node.dyn.kata:/home/admin# _
```

4. Определите файловую систему

```
df -hT
```

Отобразится список дисков и их файловые системы. В нашем случае это **ext4**

5. Отформатируйте подключенный диск

```
sudo mkfs.ext4 /dev/sdb
```

```
root@1.srv.node1.node.dyn.kata:/home/admin# mkfs.ext4 /dev/sdb
mke2fs 1.45.5 (07-Jan-2020)
Found a dos partition table in /dev/sdb
Proceed anyway? (y,N) y
Creating filesystem with 26214400 4k blocks and 6553600 inodes
Filesystem UUID: 1b8150a9-6737-4a01-91bd-a5e4f3bfecb4
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624, 11239424, 20480000, 23887872

Allocating group tables: done
Writing inode tables: done
Creating journal (131072 blocks): done
Writing superblocks and filesystem accounting information: done
```

6. Создайте папки в которые будет монтироваться подключенный диск для РК

```
Создайте каталог в директории /mnt:

sudo mkdir /mnt/kata-backup


Измените права доступа к каталогу (опционально).

Только root и только чтение и запись:

sudo chmod -R 660 /mnt/kata-backup


Примонтируйте диск:

sudo mount /dev/sdb /mnt/kata-backup


Опционально:

Для монтирования диска автоматически при загрузке системы, необходимо отредактировать

файл /etc/fstab.

Откройте любым текстовым редактором, например nano:


sudo nano /etc/fstab


В самый конец файла вставьте строку:


/dev/sdb /mnt/kata-backup ext4 defaults 0 0


Сохраните, выйдите.

Проверьте подключенный диск командой


df -hT
```

```
root@1.srv.node1.node.dyn.kata:/home/admin# mkdir /mnt/kata-bakup
root@1.srv.node1.node.dyn.kata:/home/admin# chmod -R 660 /mnt/kata-bakup/
root@1.srv.node1.node.dyn.kata:/home/admin# mount /d
data/ dev/
root@1.srv.node1.node.dyn.kata:/home/admin# mount /dev/sdb /mnt/kata-bakup/
root@1.srv.node1.node.dyn.kata:/home/admin# df -hT | grep /dev
udev           devtmpfs   32G     0   32G   0% /dev
/dev/sda2      ext4      137G   26G  105G  20% /
tmpfs          tmpfs      32G     0   32G   0% /dev/shm
/dev/sda3      ext4      550G  251M  522G   1% /data
/dev/sdb       ext4       98G   61M   93G   1% /mnt/kata-bakup
root@1.srv.node1.node.dyn.kata:/home/admin#
```

На этом этап подключения диска завершен.

????????? ??????????? ?????????? EDR ??????? ? Central Node

1. Остановите сервисы Docker.

   ```
   Выполните команды по очереди:
   systemctl stop docker
   systemctl disable docker.service
   systemctl disable docker.socket
   ```

   Примечание:
   Важно понимать, что процесс архивирования может занять некоторое время, поскольку оно зависит от размера телеметрии.
   Перед созданием архива убедитесь, что у вас достаточно места на сетевом ресурсе. Его можно приблизительно определить, проверив текущий размер телеметрии, например:

   ```
   du -hsx /data/var/lib/kaspersky/storage/swarm/elasticsearch-1/*

   Пример вывода:

   670 МБ    /data/var/lib/kaspersky/storage/swarm/elasticsearch-1/data
   6,5 МБ /data/var/lib/kaspersky/storage/swarm/elasticsearch-1/logs
   ```

   Основным ресурсоемким каталогом здесь будет /data/var/lib/kaspersky/storage/swarm/elasticsearch-1/ data.
2. Создайте бекап телеметрии ТАА.

   ```
   Выполните команду:
   tar -czf - /data/storage/volumes/elasticsearch-1/ > /mnt/kata-
   backup/elastic_5_1.tar.gz
   ```

   Процесс архивации может занять продолжительное время.

Примечание:
Данный архив БД телеметрии TAA можно использовать как РК долговременного хранения.

3. Запустите сервисы Docker после РК.

```
Выполните команды по очереди:
systemctl enable docker.socket
systemctl enable docker.service
systemctl start docker

Затем проверьте работу docker:
systemctl status docker
```

?????????????? ?????????? EDR ??????? ? Central Node

1. Остановите сервисы Docker

```
Выполните команды по очереди:
systemctl stop docker
systemctl disable docker.service
systemctl disable docker.socket
```

2. Удалите **содержимое elasticsearch** из CN (или переместите в tmp)

```
Выполните команду:
rm -rf /data/storage/volumes/elasticsearch-1/*
или
mv /data/storage/volumes/elasticsearch-1/* tmp/bkp/
```

3. Распакуйте архив с РК телеметрии TAA.

```
Выполните команду:
tar -xzf /mnt/kata-backup/elastic_5_1.tar.gz -C /data/storage/volumes/elasticsearch-1/
```

4. Запустите сервисы Docker после восстановления РК БД Телеметрии TAA.

```
Выполните команды по очереди:
systemctl start docker
systemctl enable docker.service
systemctl enable docker.socket
```

```
Затем проверьте работу docker:
systemctl status docker
```

ВАЖНО!
Elasticsearch должен найти и собрать/проиндексировать всю «новую» для него телеметрию. Необходимо подождать 15 минут на каждый 5ГБ БД Телеметрии, но индексация может завершиться быстрее.

5. Проверка работы запущенных контейнеров.

```
docker service ls | grep '0/1'
```

Здесь вы не должны увидеть никаких контейнеров, кроме тех, у которых в конце имени контейнера есть _configurator.

6. Войдите в веб-интерфейс и проверьте через ThreatHunting, события, которые мы восстановили в CN.

????????? ??????????? Central Node

Версии восстанавливаемой и установленной на сервер приложений должны совпадать. Если версии приложений не совпадают, при запуске восстановления приложения отобразится сообщение об ошибке и процесс восстановления будет прерван.

Создание резервной копии приложения в режиме Technical Support Mode.
Чтобы создать резервную копию KATA, выполните следующую команду в режиме Technical Support Mode сервера:

```
sudo kata-run.sh kata-backup-restore backup -b <path> -c -d <number of stored files> -e -q -a -s -n -l <filepath>
```

Где

Обязательный параметр	Параметр	Описание
Да	`-b <path>`	Создать файл с резервной копией приложения по указанному пути, где `<path>` – абсолютный или относительный путь к директории, в которой создается файл с резервной копией приложения.
Нет	`-c`	Очистить директорию перед сохранением файла с резервной копией приложения.
Нет	`-d <number of stored files>`	Указать максимальное количество файлов с резервной копией приложения, хранимых в директории, где `<number>` – количество файлов.
Нет	`-e`	Сохранить файлы в Хранилище.

Обязательный параметр	Параметр	Описание
Нет	`-q`	Сохранить файлы на карантине.
Нет	`-a`	Сохранить файлы, ожидающие повторной проверки (rescan).
Нет	`-s`	Сохранить артефакты Sandbox.
Нет	`-n`	Сохранить параметры Central Node или PCN.
Нет	`-l <filepath>`	Сохранить результат выполнения команды в файл, где `<filepath>` – имя файла журнала событий, включая абсолютный или относительный путь к файлу.

Пример:

```
sudo kata-run.sh kata-backup-restore backup -b <path> -c -d <number of stored files> -e -q -a -s -n -l <filepath>
```

????????????? ?? ?? Central Node

Чтобы восстановить KATA из резервной копии, выполните следующую команду в режиме Technical Support Mode сервера:

```
sudo kata-run.sh kata-backup-restore restore -r <path> -l <filepath>
```

Где

Обязательный параметр	Параметр	Описание
Да	`-r <path>`	Восстановить данные из файла резервной копии, где `<path>` – полный путь к файлу резервной копии.
Нет	`-l <filepath>`	Сохранить результат выполнения команды в файл, где `<filepath>` – имя файла журнала событий, включая абсолютный или относительный путь к файлу.

Резервная копия параметров сервера не содержит PCAP-файлы записанного зеркалированного сетевого трафика. Вы можете сохранить и восстановить PCAP-файлы самостоятельно, выполнив копирование из директории /data/volumes/dumps подключенного хранилища. После восстановления данных вам необходимо подключить внешнее хранилище.

Revision #25
Created 17 July 2025 12:48:25 by Administrator

Updated 6 February 2026 10:55:04 by Кирилл