Программное обеспечение «BI.ZONE EDR»

Дистрибутивы

Установка производилась на:

1. ОС Альт Сервер 10 (alt-server-10.2-x86_64.iso)
   md5sum: 28827cc95d0dc18c1fb7ecccf0ddcac8
2. ОС Альт Рабочая станция 10 (alt-workstation-10.2-x86_64.iso)
   md5sum: 5ad8a1e6472950d2bbf63d9981d043b5
3. ОС Альт Рабочая станция K 10 (alt-kworkstation-10.2-x86_64.iso)
   md5sum: 1758b0876c975c166e50ef6176a7873a
4. ОС Альт Образование 10 (alt-education-10.2-x86_64.iso)
   md5sum: b010a82239cb4567f91095b9afd3521b

Установка

Выполнение команд для установки BI.ZONE EDR выполняется от пользователя root (https://www.altlinux.org/Su):
$ su -
#

Действия на сервере:
Для установки BI.ZONE EDR Сервер выполнить команду:
 # rpm -Uvh bz_sensors_server-amd64-v1.35.2.rpm

Для установки BI.ZONE EDR Trigger-worker выполнить команду:
 # rpm -Uvh bz_sensors_trigger_worker-amd64-v1.35.2.rpm

Для установки BI.ZONE EDR Warden выполнить команду:
 # rpm -Uvh bz_warden- v1.1.0.rpm

Для установки BI.ZONE EDR IRP выполнить команду:
 # rpm -Uvh portal-allerts_0.2.el7.x86_64.rpm

Действия на релее:
Для установки BI.ZONE EDR Relay выполнить команду:
 # rpm -Uvh bz_sensors_relay-amd64-v1.35.2.rpm

Действия на агентах:
Для установки BI.ZONE EDR Агента выполнить команду:
 # rpm -Uvh bz_sensors_agent-amd64-v2.20.0-x64.rpm

Настройка

Действия на сервере:
Настройка конфигов:
1.Для настройки конфига сервера необходимо зайти в конфигурационный файл /opt/BI.Zone/BZ_Sensors/Server/config.toml. Выполнить правки согласно документации.
2. Для настройки конфига Warden необходимо зайти в конфигурационный файл /opt/BI.Zone/Warden/config.yaml. Выполнить правки согласно документации.
3. Для настройки конфига Trigger-worker необходимо зайти в конфигурационный файл /opt/BI.Zone/BZ_Sensors/TriggerWorker/config.yml. Выполнить правки согласно документации.

Действия на релее:
Настройка конфига:
1.Для настройки конфига релея необходимо зайти в конфигурационный файл /opt/BI.Zone/BZ_Sensors/Relay/config.toml. Выполнить правки согласно документации.

Действия на агентах:
Остановка агента:
 # systemctl stop bzsenagent

Настройка конфига:
 # /opt/BI.Zone/Sensors/Agent/bzsenagent config -a xxx.xxx.xxx.xxx:9992 -s xxx.xxx.xxx.xxx:9991 -t 10s -p 15s -l debug (где xxx.xxx.xxx.xxx - ip адрес сервера, где установлен bzserver)

Запуск
Все команды выполняются от пользователя root (https://www.altlinux.org/Su):
$ su -
#

Действия на сервере:
Запуск Warden:
 # systemctl start bzwarden

Миграция базы данных:
 # bzmigrator migrate-up

Запуск Сервера:
 # systemctl start bzserver

Запуск Trigger-worker:
 # systemctl start bztrigger-worker

Действия на релее:
Запуск релея:
 # systemctl start bzrelay

Действия на агентах:
Запуск агента:
 # systemctl start bzsenagent

Главное окно сервера