udv|group

UDV MultiProtect

Инструкция по установке

udv.group

support@udv.group

1. Требования для установки и работы UDV MultiProtect

Для корректной работы решения требуется сервер, работающий под управлением ОС Альт Сервер 10 актуальной версии и соответствующий следующим рекомендуемым требованиям:

- количество ядер процессора — 8;
- объем оперативной памяти (ОЗУ) — 32 ГБ;
- объем диска — 80 ГБ (SSD).

Перед началом установки выполните следующие действия:

1. Получите от заказчика ISO-образ установленной на сервер ОС для установки и обновления необходимых пакетов.
2. Получите от разработчиков архив с пакетами `mp.tar.gz`, актуальные справочники и дистрибутивы программы `nxlog` (при необходимости настройки отправки `syslog` на ОС Windows).
3. Проверьте сетевой доступ к серверу по протоколу `ssh`.

2. Установка

Чтобы установить UDV MultiProtect:

1. Откройте терминал ОС Альт Сервер и авторизуйтесь, используя учетную запись `root`.
2. Загрузите архив `mp.tar.gz` в домашнюю директорию пользователя.
3. Загрузите ISO-образ ОС Альт Сервер 10 в домашнюю директорию пользователя.
4. Распакуйте архив репозитория с пакетами:

   ```
   tar -xvzf mp.tar.gz -C /var/opt
   ```

5. Подключите репозитории системы Альт:

   ```
   mcedit /etc/apt/sources.list.d/altsp.list
   ```

6. Раскомментируйте следующие строки:

   ```
   rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux c10f/branch/x86_64 classic
    gostcrypto
   rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux c10f/branch/x86_64-i586
    classic
   rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux c10f/branch/noarch classic
   ```

7. Создайте конфигурационный файл репозитория:

   ```
   mcedit /etc/apt/sources.list.d/mp.list
   ```

8. Добавьте в созданный конфигурационный файл следующие строки:

   ```
   # Ours
   rpm file:/var/opt/mp/ours noarch classic
   rpm file:/var/opt/mp/ours x86_64 classic

   # Third
   rpm file:/var/opt/mp/third noarch classic
   rpm file:/var/opt/mp/third x86_64 classic
   ```

9. Обновите репозиторий и установите систему UDV MultiProtect:

   ```
   apt-get update && apt-get install udv-datapk udv-datapk-sensor -y
   ```

10. Отредактируйте ENV-файл компонента Management:

    ```
    mcedit /usr/share/udv/datapk/manager.env
    ```

    a. Измените значение переменной `HOST_IP` на адрес сервера, на котором выполняются все описанные выше действия.

11. Отредактируйте ENV-файл компонента Sensor:

    ```
    mcedit /usr/share/udv/datapk/sensor.env
    ```

    a. Измените значение переменной `LISTENING_INTERFACES` на наименования сетевых интерфейсов для прослушивания сетевого трафика.

12. Перезагрузите сервер:

```
systemctl reboot
```

- **Результат шага:** веб-интерфейс системы станет доступен для просмотра через браузер по протоколу `HTTPS`.

3. Настройка прослушивания сетевого трафика

> Прим.:
>
> Чтобы убедиться, что сетевой интерфейс работает и прослушивает трафик, воспользуйтесь командой `tcpdump -i <имя сетевого интерфейса>`.

Чтобы настроить прослушивание в системе UDV MultiProtect:

1. Откройте страницу Сенсоры.
2. Выберите сенсор в списке.
   - **Результат шага:** откроется панель настроек.
3. В блоке **Домашняя сеть** нажмите **Редактировать сеть**.
4. Нажмите **Добавить сеть**.
5. Укажите IP-адрес и маску подсети управляющего контура в качестве домашней подсети.

   > Прим.:
   >
   > Нажмите **Удалить сеть**, если добавленную ранее подсеть нужно исключить из списка.

6. Нажмите **Применить**.
7. Нажмите **Подтвердить**.
   - **Результат шага:** список активов обновится в соответствии с указанными сетями.

4. Настройка получеиния событий по syslog

В этом разделе:

4.1. Настройка syslog для ОС Linux

Чтобы настроить получение событий по `syslog` для систем семейства Linux:

1. Обеспечьте сетевой доступ от системы к серверу UDV MultiProtect по протоколам TCP/UDP (порт 514).

   > Прим.:
   >
   > Проверить наличие доступа можно с помощью команды `telnet <IP-адрес или имя сервера MultiProtect>:514`.

2. Создайте файл конфигурации `rsyslog`:

   ```
   mcedit /etc/rsyslog.d/multiprotect.conf
   ```

3. Добавьте в файл конфигурации следующую строку:

   ```
   *.* @@<IP-адрес или имя сервера MultiProtect>:514
   ```

4. Сохраните файл и перезапустите сервис:

   ```
   systemctl restart rsyslog
   ```

4.2. Настройка syslog для ОС Windows

Чтобы настроить получение событий по `syslog` для систем семейства Windows:

1. Скопируйте дистрибутив с файлом конфигурации `nxlog` в систему.
2. Установите `nxlog`, используя параметры по умолчанию.
3. Замените конфигурационный файл, расположенный по пути `C:\Program Files (<разрядность>)\nxlog\conf\nxlog.conf`, файлом из дистрибутива.
4. Замените в файле параметр `Host` (в разделе `Output out`) на IP-адрес сервера MultiProtect.
5. Перезапустите службу:

   ```
   sc restart nxlog
   ```

5. Настройка источника событий в системе UDV MultiProtect

> Прим.:
>
> Перед настройкой источника событий создайте актив системы, с которой будут поступать события. Это можно сделать на вкладке **Активы**.

Чтобы настроить источник событий:

1. Откройте страницу **Администрирование** → **Источники**.
2. Нажмите **Создать источник**.
3. Укажите наименование источника.
4. В качестве объекта защиты выберите созданный ранее актив.
5. Выберите протокол `Syslog`.
6. Нажмите **Создать**.

6. Настройка интеграции с UDV Orchestrator

Чтобы настроить интеграцию:

1. Откройте файл конфигурации менеджера инцидентов:

   ```
   mcedit /usr/lib/python3/site-packages/incident_manager/config.py
   ```

2. Укажите корректные значения для следующих параметров:

   - `auth_host: str = 'https://<IP-адрес и порт или имя сервера авторизации Keycloak>’`
   - `request_host: str = 'https://<IP-адрес и порт или имя сервиса state-machine>/statemachine'`

3. Укажите корректные данные для авторизации в параметре `auth_params`.
4. Проверьте, что в функции `request_url` указана актуальная версия API.