|  |
| --- |
|  |
| U-SIEM |
| Руководство Администратора |

**АННОТАЦИЯ**

Настоящий документ представляет собой руководство администратора системы сбора, анализа и управления событиями в компьютерных сетях и информационных системах (далее U-SIEM).

Руководство описывает порядок действий при работе с системой по созданию, просмотру и редактированию основных средств анализа, визуализации и отчётности, предоставляемых системой.

Перед работой пользователя с U-SIEM рекомендуется внимательно ознакомиться с настоящим руководством**.**

**СОДЕРЖАНИЕ**

[СОКРАЩЕНИЯ И ТЕРМИНЫ 6](#_Toc153212101)

[АРХИТЕКТУРА СИСТЕМЫ 7](#_Toc153212102)

[1. Описание компонентов 7](#_Toc153212103)

[ИНСТАЛЛЯЦИЯ КОНСОЛИ 9](#_Toc153212104)

[ИНСТАЛЛЯЦИЯ АГЕНТОВ **Ошибка! Закладка не определена.**](#_Toc153212105)

[1. Установка **Ошибка! Закладка не определена.**](#_Toc153212106)

[2. Деинсталляция агента U-SIEM **Ошибка! Закладка не определена.**](#_Toc153212107)

[3. Дополнительные параметры и возможности агента **Ошибка! Закладка не определена.**](#_Toc153212108)

[КОНФИГУРИРОВАНИЕ СИСТЕМЫ 15](#_Toc153212109)

[1. Конфигурирование компонентов системы 15](#_Toc153212110)

[1.1. Агент 15](#_Toc153212111)

[1.2. Модуль сбора и обработки событий 16](#_Toc153212112)

[1.3. Модуль корреляции событий 19](#_Toc153212113)

[1.4. Модуль анализа и управления 21](#_Toc153212114)

[1.5. СУБД ClickHouse 24](#_Toc153212115)

[1.6. СУБД MariaDB 24](#_Toc153212116)

[2. Описание баз данных 24](#_Toc153212117)

[2.1. БД MariaDB 24](#_Toc153212118)

[2.2. БД ClickHouse 25](#_Toc153212119)

[3. Запуск/остановка компонентов 27](#_Toc153212120)

[4. Логирование в системе 28](#_Toc153212121)

[4.1. Логирование агентов 28](#_Toc153212122)

[4.2. Логирование Модуля сбора и обработки событий (Inforter) 29](#_Toc153212123)

[4.3. Логирование Модуля корреляции событий (InforterCE) 30](#_Toc153212124)

[4.4. Логирование Модуля управления и анализа (U-SIEMCore) 31](#_Toc153212125)

[4.5. Просмотр лог-файлов в консоли U-SIEM **Ошибка! Закладка не определена.**](#_Toc153212126)

[5. Требования к АРМ администратора/оператора 35](#_Toc153212127)

[5.1. Запуск консоли управления 36](#_Toc153212128)

[ОБНОВЛЕНИЕ КОМПОНЕНТОВ СИСТЕМЫ 37](#_Toc153212129)

[1. Обновление модуля сбора и обработки событий 37](#_Toc153212130)

[2. Обновление модуля корреляции событий 37](#_Toc153212131)

[3. Обновление модуля анализа и управления 38](#_Toc153212132)

[4. Обновление консоли U-SIEM 38](#_Toc153212133)

[5. Проверка работоспособности компонентов 38](#_Toc153212134)

[5.1. Модуль сбора и обработки событий 39](#_Toc153212135)

[5.2. БД Событий безопасности 39](#_Toc153212136)

[5.3. БД Служебных настроек 40](#_Toc153212137)

[5.4. Модуля управления и анализа 40](#_Toc153212138)

[5.5. Модуля корреляции событий 41](#_Toc153212139)

[5.6. Модуль ретрокорреляции событий 41](#_Toc153212140)

[УПРАВЛЕНИЕ РОЛЯМИ И ПРАВАМИ ДОСТУПА 43](#_Toc153212141)

[1. Создание роли 43](#_Toc153212142)

[2. Редактирование роли 44](#_Toc153212143)

[3. Фильтры 45](#_Toc153212144)

[4. Расширенные привилегии 46](#_Toc153212145)

[УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ 46](#_Toc153212146)

[1. Создание УЗ 47](#_Toc153212147)

[2. Внесение изменений в УЗ 48](#_Toc153212148)

[3. Мониторинг пользователей в системе 48](#_Toc153212149)

[НАСТРОЙКА ПАРОЛЬНОЙ ПОЛИТИКИ 49](#_Toc153212150)

[Приложение 1. Описание таблиц MariaDB 53](#_Toc153212151)

[1.1. SAV\_ALC\_CustomZones 53](#_Toc153212152)

[1.2. SAV\_ALC\_NetModel\_Asset 53](#_Toc153212153)

[1.3. SAV\_ALC\_NetModel\_Network 54](#_Toc153212154)

[1.4. SAV\_ALC\_NetModel\_Zone 54](#_Toc153212155)

[1.5. SAV\_ALC\_RVision\_Incidents 55](#_Toc153212156)

[1.6. actualresources 57](#_Toc153212157)

[1.7. config\_properties 58](#_Toc153212158)

[1.8. core\_properties 59](#_Toc153212159)

[1.9. roles 59](#_Toc153212160)

[1.10. roles\_access 60](#_Toc153212161)

[1.11. roles\_resources 60](#_Toc153212162)

[1.12. user\_auth\_attempts 61](#_Toc153212163)

[1.13. users 61](#_Toc153212164)

[1.14. usersPasswords 62](#_Toc153212165)

# СОКРАЩЕНИЯ И ТЕРМИНЫ

|  |  |
| --- | --- |
| Сокращение/ термин | Расшифровка/ описание |
| АК | Активный канал |
| АЛ | Активный лист |
| ИБ | Информационная безопасность |
| ЛКМ | Левая кнопка мыши |
| ОС | Операционная система |
| ПКМ | Правая кнопка мыши |
| ПМ | Пункт меню |
| УЗ | Учётная запись |
| Правила | Правила корреляции событий |

# АРХИТЕКТУРА СИСТЕМЫ

## Описание компонентов

Архитектура система U-SIEM представлена на рисунке ниже.

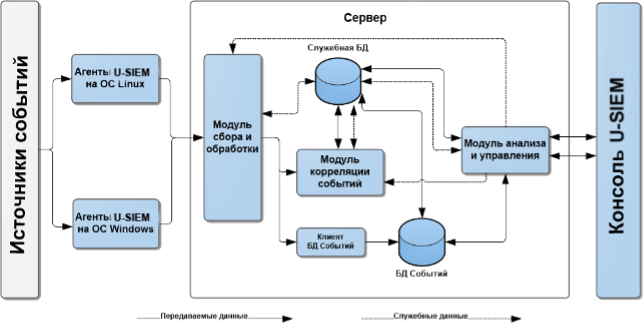


Рисунок 1. Архитектура U-SIEM

Описание компонентов системы U-SIEM представлено в таблице ниже.

Таблица 1. Компоненты U-SIEM

|  |  |  |  |
| --- | --- | --- | --- |
| № | Компонент | Описание | Поддерживаемые ОС/СУБД |
|  | Агент | Предназначены сбора (активный/пассивный), нормализации и обогащения событий безопасности с целевых систем | RedHat/CentOS 8.x  Astra Linux Special Edition 1.7.  Microsoft Windows Server 2019. |
|  | Модуль сбора и обработки событий (Inforter) | Предназначен для:   * приёма и обработки входящего потока данных с агентов; * кэширования событий безопасности; * обработки (нормализацию и категоризацию данных) с последующим преобразованием и подготовке к записи в формате БД событий безопасности (в том числе событий с кириллицей); * отправки событий безопасности в БД событий безопасности; * отправки событий безопасности на корреляцию. | RedOS 7  RedHat/CentOS 8.x;  Astra Linux Special Edition 1.7;  AstraLinux 2.12.45;  Debian 10. |
|  | Модуль корреляции событий (InforterCE) | Предназначен для аналитической обработки событий безопасности в режиме реального времени. | RedOS 7  RedHat/CentOS 8.x/9.x;  Astra Linux Special Edition 1.7;  AstraLinux 2.12.45;  Debian 10. |
|  | Модуль анализа и управления (U-SIEMCore) | Предназначен для   * управление запросами пользователей к БД со стороны Консоли управления; * взаимодействие и мониторинг работы компонентов U-SIEM. | RedOS 7  RedHat/CentOS 8.x/9.x;  Astra Linux Special Edition 1.7;  AstraLinux 2.12.45;  Debian 10. |
|  | Консоль U-SIEM | Консоль управление U-SIEM, обеспечивает управление компонентами и настройками Системы, выполняет функции визуализаций, анализа и отчётности результатов пользовательских запросов к Системе. | Microsoft Windows 10 |
|  | Клиент ClickHouse | Предназначен для взаимодействия с колоночной БД Событий безопасности. | RedHat/CentOS 8.x/9.x;  Astra Linux Special Edition 1.7;  AstraLinux 2.12.45;  Debian 10. |
|  | БД Событий безопасности | Предназначена для хранения данных о событиях безопасности и инцидентах | ClickHouse client version 22.2.2, server version 22.2.2 revision 54455; |
|  | БД Служебных настроек | Предназначена для хранения данных служебных настроек. | Jatoba;  PostgreSQL из состава Astra Linux Special Edition 1.7;  Postgres Pro Enterprise;  Maria DB 10.3.28-MariaDB MariaDB Serve |

# ИНСТАЛЛЯЦИЯ КОНСОЛИ

Консоль U-SIEM предназначен для управления компонентами и настройками Системы, выполняет функции визуализаций, анализа и отчётности результатов пользовательских запросов к Системе.

Для инсталляции консоли на рабочее место пользователя системы необходимо воспользоваться инсталлятором. Для этого следует запустить файл «setup.exe»

Откроется следующее окно (см.Рисунок 2) с установкой компонентов необходимых для функционирования консоли.

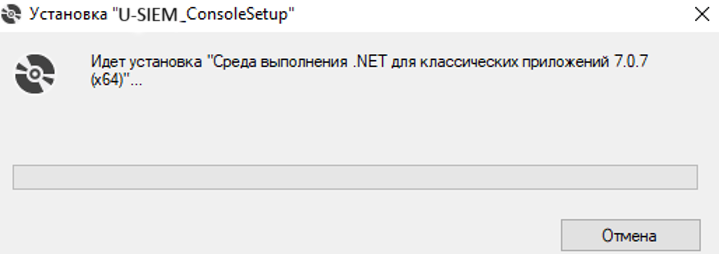


Рисунок 2. Установка компонентов .net

После чего откроется диалоговое окно с мастером установки консоли U-SIEM в нем необходимо нажать кнопку «Далее» (см. Рисунок 3).

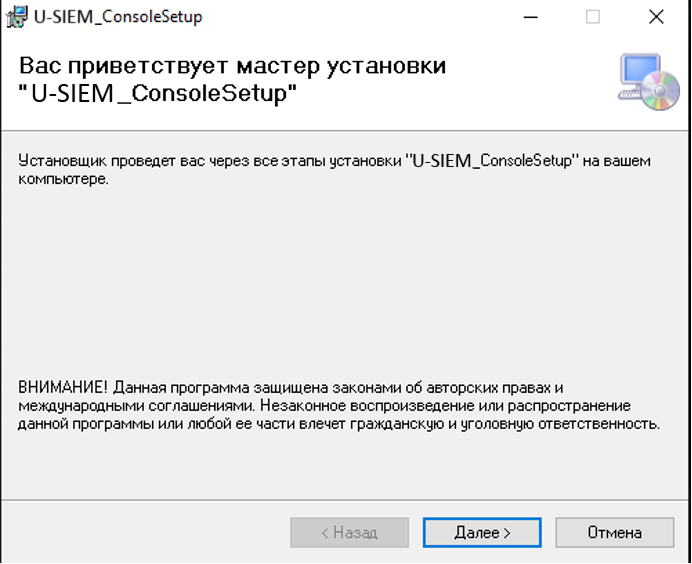


Рисунок 3. Мастер установки

После чего необходимо выбрать каталог, в котором будет располагаться консоль. При необходимости можно выбрать пользователей рабочей станции, которым необходимо установить консоль (см. Рисунок 4).

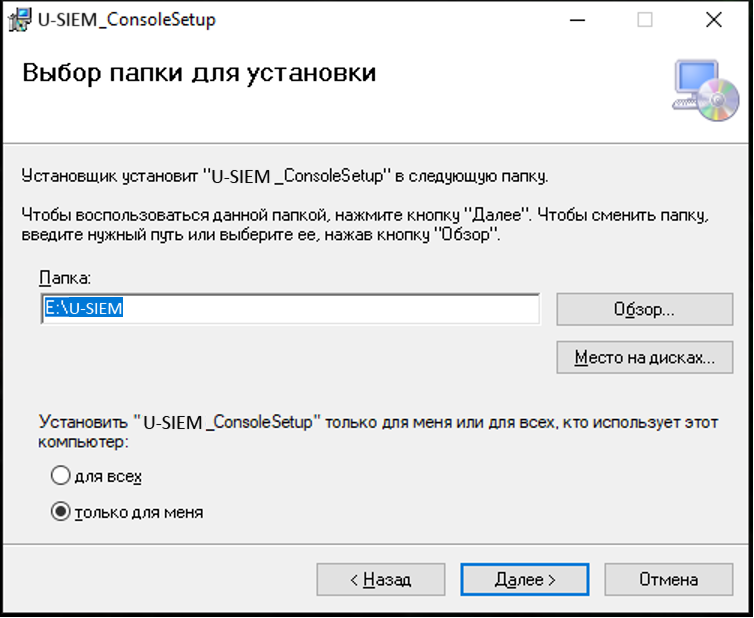


Рисунок 4. Указание каталога

Далее необходимо подтвердить установку консоли, для этого следует нажать на кнопку «Далее» (см. Рисунок 5).

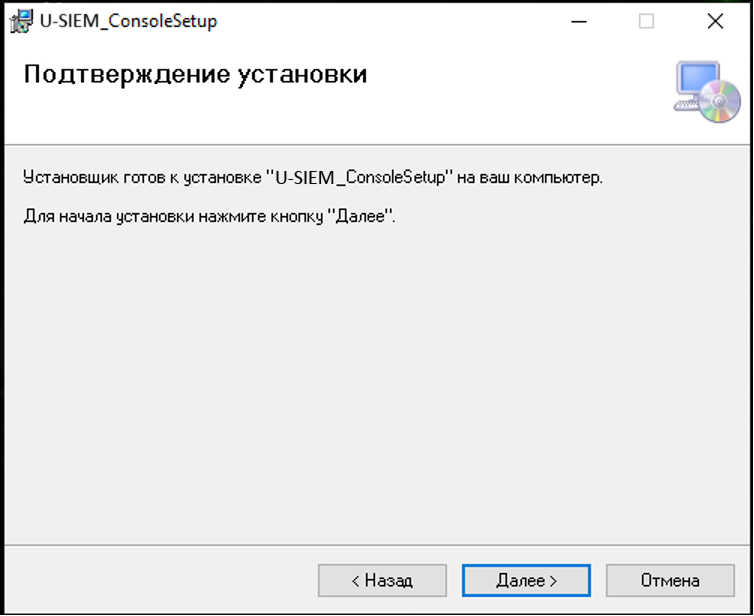


Рисунок 5. Подтверждение установки

Процесс установки может занять некоторое время. При необходимости процесс установки можно прервать, для этого следует нажать на кнопку «Отмена» (см.Рисунок 6).

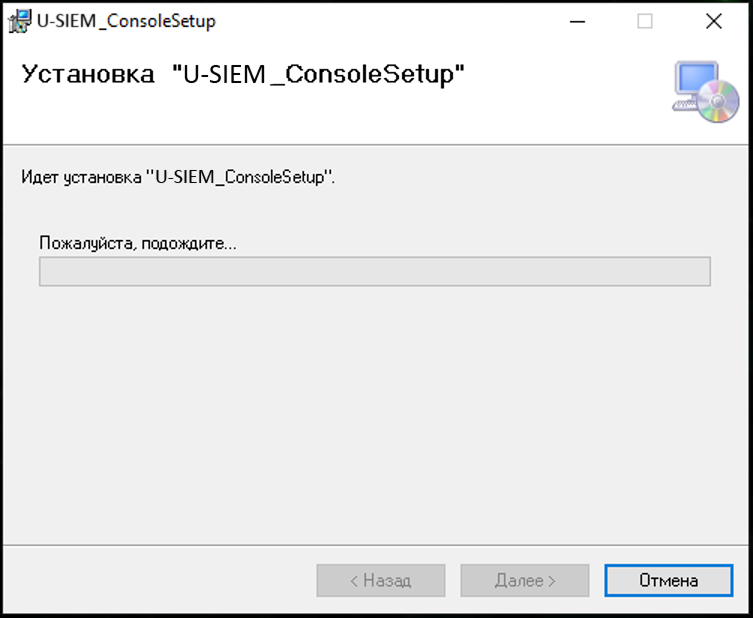


Рисунок 6. Установка консоли

После успешной установки консоли U-SIEM откроется диалоговое окно завершения установки (см.Рисунок 7). Для завершения процесса следует нажать на кнопку «Закрыть». Консоль U-SIEM успешно установилась на рабочее место и ярлык для работы с системой должен быть автоматически расположен на рабочем столе.

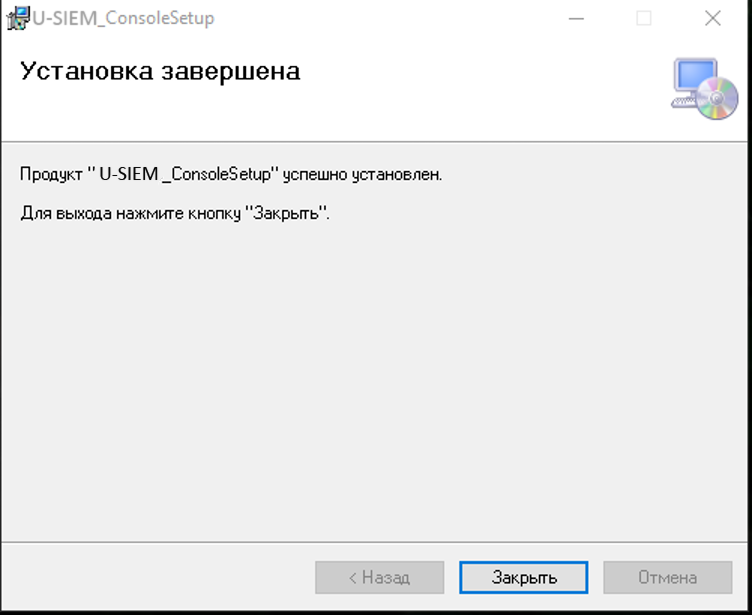


Рисунок 7. Завершение установки

# КОНФИГУРИРОВАНИЕ СИСТЕМЫ

## Конфигурирование компонентов системы

В каждом компоненте Системы есть собственные файлы конфигурации. Изменение параметров конфигураций должно осуществляться квалифицированным специалистом администрирования U-SIEM, т.к. может привести к неработоспособности отдельных компонентов или всей Системы в целом.

Перечень конфигурационных файлов (приводятся пути расположения компонентов по-умолчанию):

* для компонента «Агент» файл конфигурации расположен в /opt/agent с названием «config.xml»;
* для компонента «Inforter» файл конфигурации расположен в /opt/inforter с названием «config.xml»;
* для компонента «Inforter\_CE» файл конфигурации расположен в /opt/inforter\_ce с названием «config.xml»;
* для компонента «U-SIEMCore» файлы конфигурации и настройки параметров логирования расположены в /opt/U-SIEMCore/config с названием «appsettings.json» и «log4net.config»;
* конфигурационный файл СУБД ClickHouse расположен в /etc/clickhouse-server/ с названием «config.xml». Внесение изменений в этот файл не рекомендуется без участия вендора (U-SIEM) и может привести к неработоспособности компонента;
* конфигурационные файлы СУБД MyriaDB расположены в /etc/my.cnf.d/\*.\*. Внесение изменений в эти файлы не рекомендуется без участия вендора (U-SIEM) и может привести к неработоспособности компонента.

Примеры с описанием параметров конфигурации приведены ниже:

### **Агент**

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Рисунок 8. Пример конфигурационного файла Агента

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование** | **Описание** | **Примечание** |
| **Agent – общие параметры настройки** | | | |
| 1 | type | Тип агента |  |
| 2 | id | Порядковый номера агента |  |
| 3 | logging\_level | Уровень логирования |  |
| 4 | servicename | Имя процесса |  |
| 5 | servicedescription | Описание процесса |  |
| 6 | rawevent | Запись необработанных событий | true-включено  false-выключено |
| 7 | cachesize | Размер временного буфера | Значение в Мбайтах |
| **Sources – параметры настройки источников событий** | | | |
| 8 | sources count | Количество источников событий |  |
| 9 | configfile | Парсер агента |  |
| 10 | port | Порт |  |
| 11 | protocol | Протокол |  |
| **Destinations – параметры настройки адресов для отправки логов** | | | |
| 12 | destinations count | Количество адресов отправки |  |
| 13 | destination agentid | ID агента |  |
| 14 | type | Вид логов для передачи |  |
| 15 | host | Узел |  |
| 16 | port | Порт |  |
| 17 | protocol | Протокол |  |
| 18 | cefver | Версия CEF |  |

### **Модуль сбора и обработки событий**

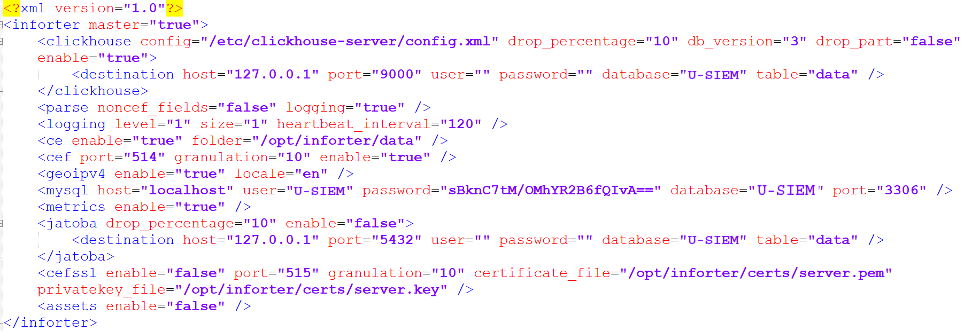


Рисунок 9. Пример конфигурационного файла Inforter

| **№** | **Наименование** | **Описание** | **Примечание** |
| --- | --- | --- | --- |
| **Inforter** | | | |
| 1 | master | Режим работы модуля сбора и обработки | true – стандартный режим с отправкой событий на корреляцию  false – контроль свободного места на шардах СУБД ClickHouse |
| **Clickhouse – настройки взаимодействия с базой данных**  Система U-SIEM может работать с СУБД Jatoba вместо СУБД ClickHouse | | | |
| 2 | config | Расположение конфигурационного файла |  |
| 3 | drop\_percentage | Порог удаления старых партиций в базе данных |  |
| 4 | db\_version | Версия СУБД ClickHouse |  |
| 5 | drop\_part | Способ отчистки базы данных | true – удаление партов в партициях  false – удаление партиций |
| 6 | enable | Использование СУБД ClickHouse | true-включено  false-выключено |
| **Clickhouse destination – Параметры расположения базы данных** | | | |
| 3 | host | Узел нахождения базы данных |  |
| 4 | port | Порт |  |
| 5 | user | Имя пользователя |  |
| 6 | password | Пароль |  |
| 7 | database | Наименование базы данных |  |
| 8 | table | Наименование таблицы |  |
| **parse** | | | |
| 9 | noncef\_fields | Включение парсинга событий не в формате CEF | true-включено (при включении данного параметра возрастает нагрузка на inforter)  false-выключено |
| 10 | logging | Логирование событий не CEF формата |  |
| **Logging – параметры настройки логирования** | | | |
| 11 | logging\_level | Уровень логирования |  |
| 12 | size | Размер одного лог файла | Значение в Мбайтах |
| 13 | heartbeat\_interval | Интервал сообщений о состоянии inforter’а | Значение в секундах |
| **CE– параметры настройки взаимодействия с модулем корреляции** | | | |
| 14 | enable | Перенаправление событий на модуль корреляции | true-включено  false-выключено |
| 15 | folder | Путь к папке с событиями модуля корреляции | Папка хранения файлов для модуля корреляции |
| **CEF – параметры настройки CEF файлов** | | | |
| 16 | port | Порт для приема CEF файлов |  |
| 17 | granulation | Грануляция принимаемых событий | Значение в секундах |
| 18 | enable | Приём данных в формате CEF | true-включено  false-выключено |
| **geoipv4 – параметры настройки геолокации** | | | |
| 19 | enable | Геолокация | true-включено  false-выключено |
| 20 | locale | Язык локализация | En-Английский Ru-Русский |
| **Mysql – параметры расположения базы данных Savrus** | | | |
| 21 | host | Узел |  |
| 22 | user | Имя пользователя |  |
| 23 | password | Пароль |  |
| 24 | database | Наименование базы данных |  |
| 25 | port | Порт |  |
| **Metrics – параметры настройки метрик inforter’а** | | | |
| 26 | enable | Служебные события inforter’а | true-включено  false-выключено |
| **Jatoba – настройка взаимодействия с СУБД Jatoba**  Система U-SIEM может работать с СУБД Jatoba вместо СУБД ClickHouse | | | |
| 27 | drop\_percentage | Порог удаления старых партиций в базе данных |  |
| 28 | enable | Использование СУБД Jatoba | true-включено  false-выключено |
| **Jatoba destination – Параметры расположения базы данных Jatoba** | | | |
| 29 | host | Узел |  |
| 30 | port | Порт |  |
| 31 | user | Имя пользователя |  |
| 32 | password | Пароль |  |
| 33 | database | Наименование базы данных |  |
| 34 | table | Таблица |  |
| **Cefssl** | | | |
| 35 | enable | Прием данных в формате CEF по протоколу SSL |  |
| 36 | port | Порт |  |
| 37 | granulation | Грануляция принимаемых событий | Значение в секундах |
| 38 | certificate\_file | Расположение файлов сертификата |  |
| 39 | privatekey\_file | Расположение файла ключа |  |
| **assets** | | | |
| 40 | enable | Использование ассетов | true-включено  false-выключено |

### **Модуль корреляции событий**



Рисунок 10. Пример конфигурационного файла InforterCE

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование** | **Описание** | **Примечание** |
| **Logging – параметры настройки уровня логирования** | | | |
| 1 | logging\_level | Уровень логирования |  |
| 2 | size | Размер одного лог файла | Размер в Мбайтах |
| 3 | heartbeat\_interval | Интервал сообщений о состоянии модуля корреляции | Значение в секундах |
| **ce – параметры настройки взаимодействия с модулем infortera’а** | | | |
| 4 | folder | Путь к папке с событиями модуля корреляции | Папка хранения файлов для модуля корреляции |
| 5 | rules\_matches | Предельное количество срабатываний одного правила в секунду | При превышении значения правило выключается |
| **Mysql – параметры расположения базы данных U-SIEM6** | | | |
| 6 | host | Узел |  |
| 7 | user | Имя пользователя |  |
| 8 | password | Пароль |  |
| 9 | database | Наименование базы данных |  |
| 10 | port | Порт |  |
| **Еmail – параметры настройки оповещений** | | | |
| 11 | email from | Отправитель оповещения |  |
| 12 | url | Адрес почтового сервиса |  |
| 13 | user | Имя пользователя |  |
| 14 | password | Пароль |  |
| 15 | encryption | Тип шифрования |  |
| U-SIEMCore – параметры расположения U-SIEMCore (модуля управления и анализа) | | | |
| 16 | folder | Расположение U-SIEMCore (модуля управления и анализа) |  |
| **U-SIEMCore folder – расположение модуля анализа и управления** | | | |
| **Metrics – параметры настройки метрик коррелятора** | | | |
| 17 | enable | Служебные события коррелятора | true-включено  false-выключено |
| **ssl – расположение ssl сертификатов** | | | |
| 18 | certificate\_file | Расположение файлов сертификата |  |
| 19 | privatekey\_file | Расположение файла ключа |  |
| **https** | | | |
| 20 | enable | Отображение In memory list в веб-браузере | true-включено  false-выключено |
| 21 | port | Порт | 8444 |

### **Модуль анализа и управления**

Настроечный файл модуля анализа и управления представлен ниже.



Рисунок 11. Пример конфигурационного файла SavrusCore

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование** | **Описание** | **Примечание** |
| 1 | **Logging –** настройка логирования в системных журналах операционной системы | | |
| 2 | **AllowedHosts –** Подключение производится со всех адресов по протоколу HTTP2 | | |
| **Config –** настройки SavrusCore | | | |
| 3 | log4NetConfigPath | Расположение конфигурационного файла библиотеки log4Net | Библиотека log4Net используется для логирования компонента savruscore |
| 4 | ch.host | Хост, на котором расположена СУБД ClickHouse | Если все компоненты расположены на одном сервере, то рекомендуемый параметр 127.0.0.1 |
| 5 | ch.port | Порт подключения СУБД ClickHouse |  |
| 14 | ch.db | Наименование базы данных СУБД ClickHouse |  |
| 15 | ch.table | Наименование таблицы с данными о событиях безопасности СУБД ClickHouse |  |
| 16 | ch.Timeout | Таймаут соединения с СУБД ClickHouse |  |
| 17 | ch.user | Пользователь СУБД ClickHouse |  |
| 18 | ch.pass | Пароль СУБД ClickHouse |  |
| 19 | mysql.host | хост, на котором расположена СУБД MariaDB | Если все компоненты расположены на одном сервере, то рекомендуемый параметр 127.0.0.1 |
| 20 | mysql.port | Порт подключения СУБД MariaDB |  |
| 21 | mysql.db | Наименование базы данных СУБД MariaDB |  |
| 22 | mysql.user | Пользователь СУБД MariaDB |  |
| 23 | mysql.pass | Пароль СУБД MariaDB |  |
| 24 | servicePort | Порт, по которому U-SIEMCore ожидает запросов от Консоли U-SIEM | Значение 7888 |
| 25 | countQueue | На данный момент не используются | |
| 26 | branchesPath |
| 27 | timeOffsetHour | Часовой пояс U-SIEMCore |  |
| 28 | tls | Версия используемого tls |  |
| 29 | device.vendor | Используются для идентификации служебных событий от конкретного U-SIEMCore в консоли U-SIEM | |
| 30 | device.product |

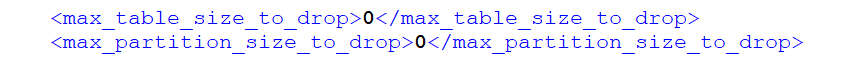
Настроечный файл библиотеки логирования log4net представлен ниже.

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

### **СУБД ClickHouse**

В конфигурационном файле ClickHouse необходимо раскомментировать строки: «max\_table\_size\_to\_drop», «max\_partition\_size\_to\_drop».



Внесение других изменений в конфигурационный файл не рекомендуется, т. к. может привести к неработоспособности системы.

### **СУБД MariaDB**

При установке компонентов (модуль сбора и обработки, модуля управления и анализа, ClickHouse) на одном сервере, внесение изменений в конфигурационный файл не рекомендуется, т. к. может привести к неработоспособности системы. При другом размещении компонентов необходимо обратится за консультацией к вендору.

## Описание баз данных

### **БД MariaDB**

В базе данных, реализованной на СУБД MariaDB, имеются таблицы, описанные в таблице ниже. Подробное описание таблиц представлено в Приложение 1. Описание таблиц MariaDB.

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование таблицы** | **Описание** | **Примечание** |
| 1. | SAV\_ALC\_CustomZones | Используется для хранения данных о геолокации |  |
| 2. | SAV\_ALC\_NetModel\_Asset | Используется для хранения данных о внутренней структуре организации |  |
| 3. | SAV\_ALC\_NetModel\_Network | Используется для хранения данных о внутренней структуре организации |  |
| 4. | SAV\_ALC\_NetModel\_Zone | Используется для хранения данных о внутренней структуре организации |  |
| 5. | SAV\_ALC\_RVision\_Incidents | Используется для хранения данных о инцидентах |  |
| 6. | SAV\_ALD\_<название> | Используется для хранения активных списков, создаваемых пользователями в системе U-SIEM |  |
| 7. | actualresources | Используется для хранения данных о ресурсах системы | Правила, активные листы, папки и т.д. |
| 8. | config\_properties | Используется для хранения параметров парольной политики |  |
| 9. | core\_properties | Используется для хранения служебных данных, характерных для всех пользователей сервиса. |  |
| 10. | roles | Используется для хранения данных о наименовании роли |  |
| 11. | roles\_access | Используется для хранения данных о правах ролей |  |
| 12. | roles\_resources | Используется для хранения данных о доступах ролей |  |
| 13. | user\_auth\_attempts | Используется для хранения данных о неудачных попытках входа пользователя в систему |  |
| 14. | users | Используется для хранения данных о пользователях |  |
| 15. | userspasswords | Используется для хранения данных о паролях пользователей |  |

### **БД ClickHouse**

В базе данных, реализованной на СУБД ClickHouse, имеются таблицы, описанные в таблице ниже.

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование таблицы** | **Описание** | **Примечание** |
| **Служебные таблицы** | | | |
| 1. | GeoLite2CityBlocksIPv4 | Используется для хранения данных о геолокации и сети. Используется для обогащения событий безопасности данными геолокации. |  |
| 2. | GeoLite2CityLocationsEN | Используется для хранения данных о геолокации на английском языке. |  |
| 3. | GeoLite2CityLocationsRU | Используется для хранения данных о геолокации на русском языке |  |
| 4. | ZonesIPv4 | Используется для хранения данных о территориальных зонах |  |
| 5 | mv\_deviceProduct | Материализованное представление, служащее для отрисовки данных в выпадающих списках |  |
| 6 | mv\_deviceVendor | Материализованное представление, служащее для отрисовки данных в выпадающих списках |  |
| 7. | mv\_destinstionUserName | Материализованное представление, использующееся в контекстном поиске |  |
| 8. | mv\_sourceUserName | Материализованное представление, использующееся в контекстном поиске |  |
| **Основные таблицы** | | | |
| 9. | data | Используется хранения информации о событиях безопасности |  |
| 10. | View\_data | Представление таблицы data |  |
| **Таблицы для визуализации** | | | |
| 11. | mv\_agent\_events | Материализованное представление, служащее для отрисовки данных |  |
| 12. | mv\_start\_Cache | Материализованное представление, служащее для отрисовки данных |  |
| 13. | mv\_start\_EPS\_Agent\_H | Материализованное представление, служащее для отрисовки данных |  |
| 14. | mv\_start\_EPS\_DB\_H | Материализованное представление, служащее для отрисовки данных |  |
| 15. | mv\_start\_RCname | Материализованное представление, служащее для отрисовки данных |  |
| 16. | mv\_start\_Rule\_name | Материализованное представление, служащее для отрисовки данных |  |
| 17. | mv\_start\_Rule\_Vendor | Материализованное представление, служащее для отрисовки данных |  |
| 18. | mv\_start\_activelists | Материализованное представление, служащее для отрисовки данных |  |
| 19. | mv\_start\_agent\_EPS | Материализованное представление, служащее для отрисовки данных |  |
| 20. | mv\_start\_database\_info | Материализованное представление, служащее для отрисовки данных |  |
| 21. | mv\_start\_destinationAddress | Материализованное представление, служащее для отрисовки данных |  |
| 22. | mv\_start\_destinationHostName | Материализованное представление, служащее для отрисовки данных |  |
| 23. | mv\_start\_destinationUserName | Материализованное представление, служащее для отрисовки данных |  |
| 24. | mv\_start\_deviceAddress | Материализованное представление, служащее для отрисовки данных |  |
| 25. | mv\_start\_deviceProduct | Материализованное представление, служащее для отрисовки данных |  |
| 26. | mv\_start\_deviceVendor | Материализованное представление, служащее для отрисовки данных |  |
| 27. | mv\_start\_main | Материализованное представление, служащее для отрисовки данных |  |
| 28. | mv\_start\_name | Материализованное представление, служащее для отрисовки данных |  |
| 29. | mv\_start\_resources | Материализованное представление, служащее для отрисовки данных |  |
| 30. | mv\_start\_severity | Материализованное представление, служащее для отрисовки данных |  |
| 31. | mv\_start\_sourceAddress | Материализованное представление, служащее для отрисовки данных |  |
| 32. | mv\_start\_sourceHostName | Материализованное представление, служащее для отрисовки данных |  |
| 33. | mv\_start\_sourceUserName | Материализованное представление, служащее для отрисовки данных |  |
| 34. | mv\_start\_type | Материализованное представление, служащее для отрисовки данных |  |

## Запуск/остановка компонентов

В случае неактивности одного из модулей, можно осуществить запуск компонентов в ручном режиме в указанной выше последовательности. Останов компонентов, при необходимости, должен осуществляться в обратном порядке.

Если при запуске компонентов один из них автоматически не запустился, перед его запуском в ручном режиме необходимо в обратной последовательности остановить работу следующих за ним компонентов.

Остановка компонентов осуществляется командами:

***systemctl stop <ИмяКомпонента>***

где <ИмяКомпонента> соответствует значениям соответствующих модулей в разделе «Проверка работоспособности компонентов».

Запуск компонентов осуществляется командами:

***Systemctl start <ИмяКомпонента>***

где <ИмяКомпонента> соответствует значениям соответствующих модулей в разделе «Проверка работоспособности компонентов».

Проверка статуса компонентов осуществляется командами:

***systemctl status <имя компонента>***

где <ИмяКомпонента> соответствует значениям соответствующих модулей в разделе «Проверка работоспособности компонентов».

В случае возникновения вопросов, обратитесь в службу поддержки вендора.

## Логирование в системе

Логирование в системе U-SIEM осуществляется на агентах, модуле сбора и обработки событий (Inforter), модуле корреляции событий (InforterCE), модуле управления и анализа (U-SIEMCore) и в консоли U-SIEM.

Каждый компонент системы осуществляет логирование локально в log-файлы. Компоненты Inforter, InforterCE и U-SIEMCore также направляют данные мониторинга в БД реализованную на СУБД ClickHouse. Для этого в конфигурационных файлах Inforter, InforterCE необходимо включить опцию метрики, а в U-SIEMCore в опциях device.vendor и device.product указать желаемое наименование. После этого в Консоли U-SIEM можно будет построить Активный канал (а также любой вид визуализации данных) по служебным событиям компонентов системы, для этого следует в условии АК в полях device.vendor и device.product необходимый компонент.

### **Логирование агентов**

**Настройка**

Настройка логирования агентов производится в конфигурационных файлах (config.xml). В параметре «logging\_level» необходимо указать желаемый уровень логирования.



Агент поддерживает 7 уровней логирования:

* 0 уровень логирования TRACE - логирование всех операций и выше;
* 1 уровень логирования DEBUG - логирование отладочной информации и выше;
* 2 уровень логирования INFO - логирование информационных сообщений и выше;
* 3 уровень логирования WARN - логирование предупреждений и выше;
* 4 уровень логирования ERROR - логирование ошибок и выше;
* 5 уровень логирования CRITICAL - логирование только критических ошибок;
* 6 уровень логирования NONE – выключено.

Уровень TRACE необходимо использовать только в режиме отладки и выявления ошибок. Не используйте его в штатном/продуктивном режиме работы системы.

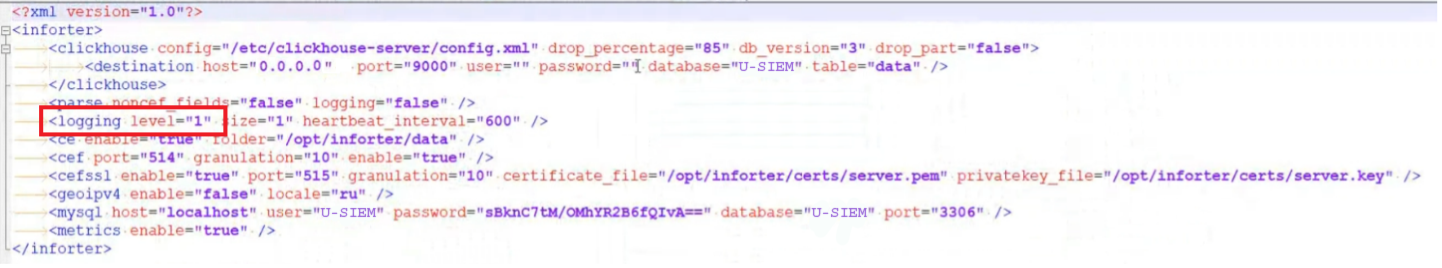
**Просмотр лог-файлов**

Лог-файлы агентов хранятся в папке: /opt/agent/logs

### **Логирование Модуля сбора и обработки событий (Inforter)**

**Настройка**

Настройка логирования inforter производится в конфигурационных файлах (config.xml). В параметре «logging\_level» необходимо указать желаемый уровень логирования.



Inforter поддерживает 7 уровней логирования:

* 0 уровень логирования TRACE - логирование всех операций и выше;
* 1 уровень логирования DEBUG - логирование отладочной информации и выше;
* 2 уровень логирования INFO - логирование информационных сообщений и выше;
* 3 уровень логирования WARN - логирование предупреждений и выше;
* 4 уровень логирования ERROR - логирование ошибок и выше;
* 5 уровень логирования CRITICAL - логирование только критических ошибок;
* 6 уровень логирования NONE – выключено.

Уровень TRACE необходимо использовать только в режиме отладки и выявления ошибок. Не используйте его в штатном/продуктивном режиме работы системы.

**Просмотр лог-файлов**

Лог-файлы inforter хранятся в папке:/opt/inforter/logs/

### **Логирование Модуля корреляции событий (InforterCE)**

**Настройка**

Настройка логирования InforterCE производится в конфигурационных файлах (config.xml). В параметре «logging\_level» необходимо указать желаемый уровень логирования.

InforterCE поддерживает 7 уровней логирования:

* 0 уровень логирования TRACE - логирование всех операций и выше;
* 1 уровень логирования DEBUG - логирование отладочной информации и выше;
* 2 уровень логирования INFO - логирование информационных сообщений и выше;
* 3 уровень логирования WARN - логирование предупреждений и выше;
* 4 уровень логирования ERROR - логирование ошибок и выше;
* 5 уровень логирования CRITICAL - логирование только критических ошибок;
* 6 уровень логирования NONE – выключено.

Уровень TRACE необходимо использовать только в режиме отладки и выявления ошибок. Не используйте его в штатном/продуктивном режиме работы системы.

**Просмотр лог-файлов**

Лог-файлы inforter хранятся в папке:/opt/inforter\_ce/logs/

### **Логирование Модуля управления и анализа (SavrusCore)**

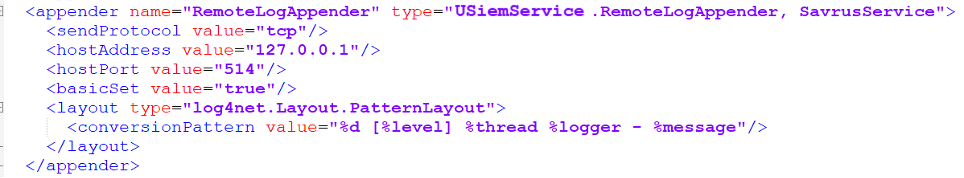
Логирование модуля управления и анализа построено на использовании библиотеки log4net. U-SIEMCore поддерживает следующие способы логирования:

* логирование в консоль отладки;
* логирование ошибок в файл /logs/errors.log;
* логирование потока выполнения приложения в файл /logs/U-SIEMmgrsvc.log;
* логирование событий приложения в систему U-SIEM.

**Настройка**

Настройки параметров логирования, уровней логирования и формата сообщений находятся в соответствующем разделе файла конфигурации /config/log4net.config.

За функционал логирования отвечает класс RemoteLogAppender, унаследованный от шаблонного библиотечного класса, класс LogObject, содержащий определение наборов событий и отвечающий за формирование раздела Extension строки сообщения в формате CEF.



В разделе конфигурации имеются настраиваемые параметры, отвечающие за выбор отправляемых событий и доставку сообщений:

* <sendProtocol value="tcp"/> – протокол передачи сообщений в систему U-SIEM, допускаются значения "udp" и "tcp";
* <hostAddress value="172.16.42.106"/> – IPv4 адрес приёмника сообщений;
* <hostPort value="514"/> – порт, на котором приёмник ожидает поток сообщений;
* <basicSet value="true"/> – выбор набора логируемых событий: типовой/расширенный, допускаются значения "true" и "false".

**Описание логируемых событий**

Модуль поддерживает два набора событий: типовой и расширенный.

**Типовой набор событий (name, deviceEventClassId)**

|  |  |
| --- | --- |
| **Наименование события** | **Код** |
| Начало работы (запуск) системы | 10001 |
| Окончание(остановка) работы системы | 10002 |
| Вход пользователя в систему | 10101 |
| Выход пользователя из системы | 10102 |
| Неуспешный вход в систему | 10103 |
| Создание учетной записи | 10201 |
| Удаление учетной записи | 10202 |
| Блокировка(отключение) учетной записи | 10203 |
| Разблокировка(включение) учетной записи | 10204 |
| Смена пароля учетной записи | 10205 |
| Создание группы(роли) пользователей | 10301 |
| Удаление группы(роли) пользователей | 10302 |
| Изменение прав группы(роли) пользователей | 10303 |
| Назначение\исключение прав пользователя на объект | 10304 |
| Исключение пользователя из состава группы(роли). | 10401 |
| Включение пользователя в состав группы(роли). | 10402 |
| Очистка журнала событий | 10501 |
| Изменение настроек аудита(включение\отключение, изменение уровня логирования) | 10502 |
| Изменение конфигурации системы(конфигурационных файлов, настроек СУБД, настроек ПО) | 10503 |
| Включение правил консолью | 10601 |
| Выключение правил консолью | 10602 |

**Расширенный набор событий (name, deviceEventClassId):**

|  |  |
| --- | --- |
| **Наименование события** | **Код** |
| Создание объекта. (при необходимости детального аудита) | 20301 |
| Удаление объекта. (при необходимости детального аудита) | 20302 |
| Изменение объекта. (при необходимости детального аудита) | 20303 |
| Чтение объекта. (при необходимости детального аудита) | 20304 |
| Копирование объекта. (при необходимости детального аудита) | 20305 |
| Установка прав доступа на объект. (при необходимости детального аудита) | 20306 |
| Изменение прав доступа на объект. (при необходимости детального аудита) | 20307 |
| Вход пользователя в подсистему. | 20201 |
| Выход пользователя из подсистемы. | 20202 |
| Отключение пользователя\сессии по тайм-ауту | 20203 |
| Неверное имя при входе в систему. | 20204 |
| Неверный пароль при входе в систему. | 20205 |
| Смена пароля пользователя Администратором системы. | 20206 |
| Запуск\восстановление подсистемы (компонент, сервисов, инстансов) | 20501 |
| Остановка\сбой подсистемы (компонент, сервисов, инстансов) | 20502 |
| События успешного\неуспешного контроля целостности файлов\объектов | 20503 |
| Неуспешная валидация данных | 20504 |
| Архивирование данных. (при необходимости детального аудита) | 20505 |
| Попытка удаления журналов аудита | 20506 |

**Просмотр лог-файлов**

Лог-файлы потока выполнения приложения находится по пути: /opt/savruscore/logs/U-SIEMmgrsvc.log, логирование ошибок ведётся в файле errors.log. Также имеется возможность посмотреть их в консоли U-SIEM.

Для просмотра логов компонента U-SIEMCore необходимо в консоли U-SIEM в разделе «Администрирование» выбрать вкладку «Лог»

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 12. Пример логов системы

### **Логирование консоли U-SIEM**

Логирование консоли U-SIEM построено на использовании библиотеки log4net. Консоль U-SIEM поддерживает следующие способы логирования:

* логирование ошибок в файл /logs/errors.log;
* логирование потока выполнения приложения в файл /logs/ U-SIEM.log.

Настройки параметров логирования, уровней логирования и формата сообщений находятся в файле конфигурации log4net.config. Логирование консоли осуществляется в локальный файл без отправки в БД.



Параметры ротации лог-файлов настраиваются в разделах:

* <maxSizeRollBackups value="10"/>
* <maximumFileSize value="5MB"/>

## Требования к АРМ администратора/оператора

Для работы Консоли U-SIEM необходимо рабочее место под управлением ОС семейства MS Windows и сетевым доступом к серверу управления U-SIEM TCP/7889 (по умолчанию), TCP/22 (для администрирования).

### **Запуск консоли управления**

Для входа в Консоль U-SIEM необходимо запустить ярлык «Savrus6» на рабочем столе.

При первом запуске Консоли U-SIEM необходимо осуществить настройку подключения к серверам/компонентам U-SIEM. В случае поставки U-SIEM в виде виртуальной машины используются значения полей, заявленные по умолчанию.

Для настройки подключения и запуска Консоли U-SIEM необходимо обеспечить заполнение следующих полей:

|  |  |  |
| --- | --- | --- |
| № | Название поля | Данные для наполнения |
|  | Адрес менеджера | IP Адрес или Имя сервера Модуля управления и анализа |
|  | Порт менеджера | Порт (по умолчанию TCP/7888) – для соединения и  взаимодействия с Модулем управления и анализа |
|  | Тип подключения | GRPC или GRPC-WEB. Рекомендуется использовать GRPC |
|  | TLS | 1.0 / 1.1 / 1.2 / 1.3. Рекомендуется использовать 1.2 |
|  | Имя пользователя | Имя пользователя/администратора  для авторизации (по умолчанию - admin) |
|  | Пароль | q1q1q1q1 |

# ОБНОВЛЕНИЕ КОМПОНЕНТОВ СИСТЕМЫ

В случае выпуска мажорных версий обновления системы – обновление осуществляется с помощью инсталлятора. В случае выпуска минорных версий обновлений системы – обновление обеспечивается отдельных компонентов системы согласно положениям ниже. Дополнительно необходимо учитывать рекомендуемые параметры конфигурации компонентов системы (см. раздел «Конфигурирование компонентов системы»).

## Обновление модуля сбора и обработки событий

Для обновления необходимо произвести следующие действия:

1. Скопировать в /opt папку «inforter\_<date>».
2. Переименовать старую папку «inforter», например в «inforter\_old».
3. Переименовать новую скопированную папку «inforter\_<date>» в «inforter».
4. Добавить права для запуска файла (пользователем с привилегиями root) /opt/inforter/chmod +x inforter.
5. При наличии памяти на сервере более 32 Gb для работы может быть активирована работа компонента встроенной геолокации, для этого в /opt/inforter/config.xml правится строчка:

<geoipv4 enable="false" locale="ru" /> в <geoipv4 enable="true" locale="ru" />

1. Проверить в файле «config.xml» уровень логирования. «logging\_level» должен быть выставлен в значение 1 или 2 (не 0 !!!).
2. После обновления компонента или параметров его необходимо перезагрузить (restart).

## Обновление модуля корреляции событий

Для обновления необходимо произвести следующие действия:

1. Скопировать в /opt папку «inforter\_ce\_<date>».
2. Переименовать старую папку «inforter\_ce», например в «inforter\_ce\_old».
3. Переименовать новую скопированную папку «inforter\_ce\_<date>» в «inforter\_ce».
4. Добавить права для запуска файла (пользователем с привилегиями root) /opt/inforter\_ce/chmod +x inforter\_ce.
5. Проверить в файле «config.xml» уровень логирования. «logging\_level» должен быть выставлен в значение 1 или 2 (не 0 !!!).
6. После обновления компонента или параметров его необходимо перезагрузить (restart).

## Обновление модуля анализа и управления

Для обновления необходимо произвести следующие действия:

* + 1. Скопировать в /opt папку «U-SIEMCore \_<date>».
    2. Переименовать старую папку «U-SIEMCore», например в «U-SIEMCore \_old».
    3. Переименовать новую скопированную папку «U-SIEMCore\_<date>» в «U-SIEMCore».
    4. Проверить выставлено ли в файле config/appsettings.json корректное значение параметра ch.table источника данных (по умолчанию data).
    5. После обновления компонента или параметров его необходимо перезагрузить (restart).

## Обновление консоли U-SIEM

Обновление ядра как правило требует установки соответствующего релиза консоли U-SIEM. Для обновления консоли необходимо загрузить и развернуть соответствующий релиз. Для доступности прежних стартовых дашбордов для каждого инстанса необходимо перенести файлы конфигурации стартовых дашбордов из предыдущего релиза.

## Проверка работоспособности компонентов

Система U-SIEM и её компоненты рассчитаны на беспрерывную работу. В случае плановый перезагрузки серверов, где располагаются компоненты, Система автоматически продолжит работу в штатном режиме. Для контроля работоспособности компонентов можно осуществить ряд контрольных процедур.

Все процедуры проводятся пользователем с правами root на уровне ОС (где установлены соответствующие компоненты). Для проведения контрольных и сервисных процедур необходима организация SSH соединения с компонентами Системы (RDP соединения для серверов под управлением ОС Windows, при наличии).

Проверка работоспособности Агентов осуществляется путём анализа лог-файлов, располагающихся в директориях установки агентов – agent\*.log. Кастомизация параметров Агентов осуществляется с помощью настроечных файлов в директориях установки агентов – agent.properties.

### **Модуль сбора и обработки событий**

Для проверки работоспособности Модуль сбора и обработки событий (Inforter) выполняется следующая команда:

systemctl status inforter

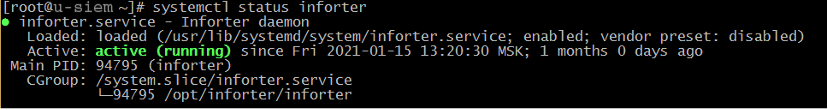


Рисунок 13. Проверка статуса работы Inforter

В случае корректной работы модуля должен быть возвращён результат «Started Inforter daemon»

Дополнительная информация о работе компонента может быть получена из логов – по умолчанию логирование обеспечивается в файлы в /opt/inforter/inforter.log.\*

### **БД Событий безопасности**

Для проверки работоспособности выполняется следующая команда:

systemctl status clickhouse-server.service

В случае корректной работы модуля должен быть возвращён результат active (exited), аналогично представленному на рисунке ниже:

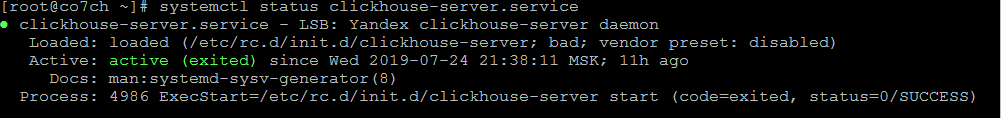


Рисунок 14.Проверка статуса работы ClickHouse

### **БД Служебных настроек**

Для проверки работоспособности выполняется следующая команда:

systemctl status mariadb.service или systemctl status mysqld.service

(в зависимости от того, какая БД была установлена и поддерживается ОС)

В случае корректной работы модуля должен быть возвращён результат active (running), аналогично представленному на рисунках ниже:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 15. Проверка статуса работы MariaDB

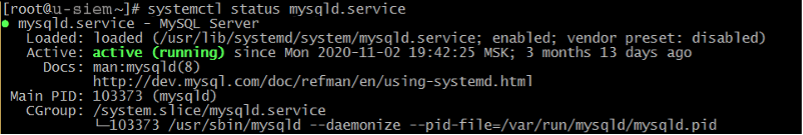


Рисунок 16. Проверка статуса работы MySQL

### **Модуля управления и анализа**

Для проверки работоспособности Модуля управления и анализа (компонента управления) выполняется следующая команда:

systemctl status U-SIEMCore

В случае корректной работы модуля должен быть возвращён результат active (running), аналогично представленному на рисунке ниже:

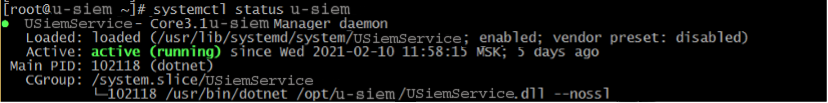


Рисунок 17. Проверка статуса работы U-SIEMCore

Дополнительная информация о работе компонента может быть получена из логов – по умолчанию логирование обеспечивается в файлы в /opt/ U-SIEMCore /logs/\*.\*

### **Модуля корреляции событий**

Для проверки работоспособности Модуль корреляционной обработки событий (Inforter\_ce) (в режиме реального времени) выполняется следующая команда:

systemctl status inforter\_ce

В случае корректной работы модуля должен быть возвращён результат Started Inforter CE daemon, аналогично представленному на рисунке ниже:

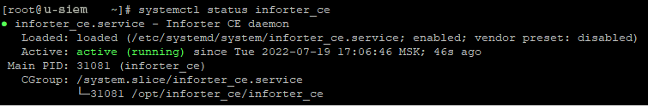


Рисунок 18. Проверка статуса работы InforterCE

Дополнительная информация о работе компонента может быть получена из логов – по умолчанию логирование обеспечивается в файлы в /opt/inforter\_ce/inforter\_ce.log.\*

### **Модуль ретрокорреляции событий**

Для проверки работоспособности Модуля ретрокорреляции событий, инициирование которого осуществляется через штатный планировщик задач ОС выполняется следующая команда:

Crontab -l

**Изображение выглядит как текст

Автоматически созданное описание**

Наличие соответствующих задач в планировщике и одноименных скриптов в каталогах – говорит о наличии настроенного Модуля ретрокорреляции событий.

Дополнительно можно анализировать работу соответствующих модулей и контролировать их состояние через Консоль. Ключевые поля, по которым можно искать события:

* deviceVendor = U-SIEM AND deviceProduct = Inforter – для контроля состояния компонента «Модуль сбора и обработки событий, а также состояния хранилища служебных настроек (служебные события);
* deviceVendor = U-SIEM AND deviceProduct = InforterCE – для контроля состояния компонента «Модуля корреляции» (служебные события);
* (type =2 OR type =4) AND agentType = correlation – для контроля результатов корреляционной обработки событий (в режиме реального времени и в режиме постобработки событий соответственно) (результирующие корреляционные события).

# АДМИНИСТРИРОВАНИЕ

## УПРАВЛЕНИЕ РОЛЯМИ И ПРАВАМИ ДОСТУПА

Система U-SIEM поддерживает ролевую модель доступа к ресурсам системы, для управления ролями в меню ресурсов на вкладке «Администрирование» предусмотрен раздел «Роли пользователей» (см. Рисунок *19*).

Изображение выглядит как Мультимедийное программное обеспечение, программное обеспечение, Графическое программное обеспечение, снимок экрана

Автоматически созданное описание

Рисунок 19. Окно управления ролями

### **Создание роли**

Для добавления новой роли в систему необходимо нажать ЛКМ на кнопку «Добавить роль»  Или кликнуть ПКМ на роль и в контекстном меню выбрать пункт «Добавить роль».

В открывшемся диалоговом окне следует ввести имя добавляемой роли (см. Рисунок 20) и нажать кнопку «Сохранить».

Изображение выглядит как текст, снимок экрана, Шрифт, дизайн

Автоматически созданное описание

Рисунок 20. Диалоговое окно "Имя роли"

После чего следует настроить права доступа к ресурсам для новой роли. Подробное описание ресурсов представлено в «Руководстве пользователя U-SIEM». Для предоставления прав по разным категориям необходимо нажать на выпадающий список. После чего появиться перечень доступных категорий (см. Рисунок 21).

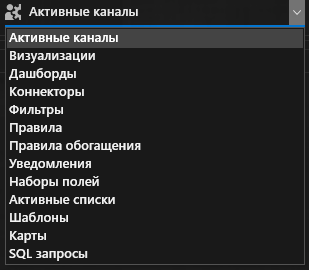


Рисунок 21. Список доступных ресурсов

После выбора необходимо задать полномочия для всех доступных ресурсов (см. Рисунок *22*).

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рисунок 22. Доступные ресурсы

Можно выдать права на чтение ресурса , редактирование , сохранение  и удаление . Для этого необходимо нажать на необходимую кнопку и сделать её активной.

Для права «Open» предусмотрена каскадная модель доступа. А для прав «Create», «Save», «Delete» свободное назначение.

### **Редактирование роли**

Для редактирования роли необходимо выбрать её из выпадающего списка и внести изменения. После чего сохранить изменения нажатием на кнопку . Чтобы переименовать роль следует использовать кнопку . Или кликнуть ПКМ на роль и в контекстном меню выбрать соответствующий пункт.

### **Фильтры**

При необходимости можно разграничивать доступ к ресурсам с помощью фильтров. Для использования фильтров следует выбрать необходимую роль из ранее созданных в системе (см. Рисунок 23).

Изображение выглядит как снимок экрана, текст, черный

Автоматически созданное описание

Рисунок 23. Список ролей

Далее, следует выбрать необходимый фильтр из ранее созданных в системе (создание и редактирование фильтров подробно описано Руководстве пользователя). Для этого следует нажать на кнопку  и в появившемся выпадающем списке выбрать нужный фильтр (см. Рисунок *24*).

Изображение выглядит как текст, снимок экрана, компьютер, программное обеспечение

Автоматически созданное описание

Рисунок 24. Список фильтров

После чего выбранная роль будут доступны события только в соответствии с выбранным фильтром.

### **Расширенные привилегии**

U-SIEM позволяет назначить необходимой роль расширенные привилегии администратора ИБ для проведения аудита. Для этого в меню редактирования роли пользователя необходимо соответствующем разделе нажать на кнопку  и в появившемся списке выбрать необходимое (см. Рисунок *25*).

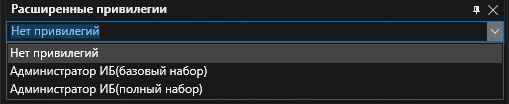


Рисунок 25. Список расширенных привилегий

## УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

Система U-SIEM поддерживаем многопользовательский режим работы. Для управления УЗ пользователей в меню ресурсов на вкладке «Администрирование» предусмотрен раздел «Пользователи» (см. Рисунок 26).

Изображение выглядит как снимок экрана, текст, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 26. Окно управления УЗ пользователей

### **Создание УЗ**

Для создания новой УЗ пользователя необходимо нажать ЛКМ на кнопку «новый пользователь» . Или в панели слева (под списком пользователей) формы управления УЗ пользователей щёлкнуть ПКМ и в контекстном меню выбрать соответствующий пункт. В появившейся форме (см. Рисунок 27) необходимо заполнить поля перечисленные в таблице Таблица 2.

Изображение выглядит как текст, снимок экрана, меню

Автоматически созданное описание

Рисунок 27. Форма создания нового пользователя

При работе с пользователями определяются следующие параметры, описанные в таблице ниже.

Таблица 2. Поля формы создания нового пользователя

|  |  |  |
| --- | --- | --- |
| Название поля | Описание | Примечание |
| ФИО | ФИО пользователя – владельца УЗ |  |
| Логин | Логин создаваемой УЗ пользователя |  |
| Пароль | Пароль создаваемой УЗ пользователя | Требования к паролю устанавливаются в соответствие с парольной политикой |
| Активный | Признак активности УЗ пользователя | Используется в целях временной блокировки УЗ пользователя в системе |
| E-mail | Электронная почта владельца УЗ пользователя |  |
| Удалён | Признак удаления УЗ пользователя | Используется в случае удаления УЗ пользователя из системы |
| Роль | Роль создаваемой УЗ пользователя | Создание и редактирование ролей представлено в разделе «АДМИНИСТРИРОВАНИЕ  УПРАВЛЕНИЕ РОЛЯМИ И ПРАВАМИ ДОСТУПА» |
| Должен сменить пароль | Признак необходимости смены пароля при первичном входе в Систему |  |
| Показывать удалённые ресурсы | Признак возможности УЗ пользователя управлять удалёнными ресурсами | Рекомендуется только для авторизованных пользователей Системы |
| Доменная аутентификация | Признак необходимости входа в систему с помощью доменной аутентификации |  |

### **Внесение изменений в УЗ**

Для редактирования УЗ пользователя необходимо выбрать её и перейти в режим редактирования, нажав на кнопку  или из контекстного меню, вызываемого ПКМ. В основном окне отобразятся параметры УЗ, которые можно будет скорректировать. Для применения изменений необходимо нажать кнопку  . Возможна опция удаления УЗ пользователя из Системы при нажатии кнопки , для этого предварительно необходимо удалить или перенести ресурсы УЗ удаляемого профиля.

### **Мониторинг пользователей в системе**

Для мониторинга пользователей в системе следует в меню ресурсов на вкладке «Администрирование» выбрать раздел «Пользователи». В правой части окна располагается раздел для отслеживания залогиненных пользователей в системе (см. Рисунок 28). Для отключения пользователя необходимо нажать по нему ПКМ и в контекстном меню выбрать пункт «отключить».

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 28. Залогиненные пользователи

## ЛОГИРОВАНИЕ

Для просмотра логов системы U-SIEM необходимо в разделе «Администрирование» перейти на вкладку «Лог». Подробнее об уровнях логирования написано в разделе «Логирование в системе».

## НАСТРОЙКА ПАРОЛЬНОЙ ПОЛИТИКИ

Для настройки парольной политики необходимо во вкладке «Администрирование» выбрать раздел «Парольная политика».

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 29. Окно настройки парольной политики

Для редактирования парольной политики необходимо нажать на кнопку «Режим редактирования»  и внести изменения в пункты парольной политики.

После завершения редактирования необходимо нажать кнопку «Сохранить» .

Описание требований парольных политик, поддерживаемых системой, указаны в таблице ниже.

Таблица 3. Требования парольных политик

|  |  |  |
| --- | --- | --- |
| № | Наименование | Значение |
| 1 | Срок действия пароля, дней | Диапазон значений от 0-180 |
| 2 | За сколько дней необходимо напомнить об истечении срока действия пароля | Диапазон значений от 0-180 |
| 3 | Кол-во отличающихся символов при смене пароля | Диапазон значений от 0-50 |
| 4 | Не использовать последних введённых паролей | Диапазон значений от 0-50 |
| 5 | Попыток входа для блокировки | Диапазон значений от 3-10 |
| 6 | Таймер контроля неудачных попыток ввода, сек | Диапазон значений от 0-900 |
| 7 | Период блокировки пользователя, сек | Диапазон значений от 180-900 |
| 8 | Паттерн проверки сложности пароля | Настраиваемое регулярное выражение |

## Интеграция с почтовым сервером

Для подключения к почтовому серверу используется библиотека Curl.

Настройка отправки сообщений выполняется в модуле корреляции событий. Для этого необходимо запустить inforterCE следующей командой:

./inforter\_ce setup

В открывшемся меню выбираем пункт 1.

1 - change config

2 - test MySQL settings

3 - test Email settings

4 - save and exit

0 - exit

Далее выбираем пункт 2

1 - change MySQL settings

2 - change Email settings

0 - exit

После чего вводим необходимые настройки.

* Email from —адрес отправителя сообщений, например “U-SIEM@U-SIEM.ru”
* Email url –адрес почтового сервера в формате протокол://адрес\_сервера:порт, примеры:

smtp://localhost – используется локальный почтовый сервер с портом 25 по умолчанию

smtps://smtp.yandex.ru:465 – используется почтовый сервер smtp.yandex.ru и порт 465

* Email user – указываем пользователя для авторизации, если необходимо
* Email password – указываем пароль для авторизации, если необходимо
* Email encryption – указываем ”SSL”, если требуется шифрование

После настройки имеется возможность протестировать отправку сообщений. Для этого в корневом меню необходимо выбрать пункт 3

1 - change config

2 - test MySQL settings

3 - test Email settings

4 - save and exit

0 - exit

Далее при необходимости выбираем просмотр логов отправки и вводим адрес получателя сообщения.

* Show mail log? (Y/N) — отображение журнала отправки сообщений
* Enter email of recipient — получатель тестового сообщения, например ”root@localhost”

После успешной проверки отобразится сообщение «Email test is OK!» или "Email test failed!" при не успешной.

Применённый настройки будут отображаться в конфигурационном файле модуля корреляции.



## ПАРАМЕТРЫ СЕРВЕРА

В данном разделе настраивается ограничение на максимальное количество строк в активном списке и таймаут бездействия пользователя.

Ограничение на количество строк в активном списке необходимо для балансировки нагрузки на систему.

Для редактирования параметров необходимо нажать на кнопку «Режим редактирования»  и внести необходимые изменения.

Для сохранения изменений следует нажать на кнопку «Сохранить» .

# Приложение 1. Описание таблиц MariaDB

### **SAV\_ALC\_CustomZones**

**Хранимые данные:** служащее для хранения данных о геолокации.

Структура таблицы представлена ниже.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Имя поля** | **Формат поля** | **Описание** | **Примечание** |
| 1. | id | int(11) | Уникальный идентификатор |  |
| 2. | subnet | varchar(512) | Подсеть |  |
| 3. | zonename | varchar(512) | Имя зоны |  |
| 4. | country | varchar(512) | Страна |  |
| 5. | region | varchar(512) | Регион |  |
| 6. | city | varchar(512) | Город |  |
| 7. | description | varchar(512) | Описание |  |
| 8. | creationTime | bigint(20) | Время создания |  |
| 9. | lastModifiedTime | bigint(20) | Время последнего изменения файла. |  |
| 10. | count | int(11) | Количество |  |
| 11. | hashCode | bigint(20) | Хэш код |  |

### **SAV\_ALC\_NetModel\_Asset**

**Хранимые данные:** служащее для описания сетей и структуры сетевой модели.

Ниже представлено описание полей таблицы.

Таблица 4. SAV\_ALC\_NetModel\_Asset

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Имя поля** | **Формат поля** | **Описание** | **Примечание** |
| 1. | id | int(11) unsigned | Уникальный идентификатор |  |
| 2. | IPAddress | varchar(512) | IP адрес |  |
| 3. | Customer | varchar(512) | Клиент |  |
| 4. | Asset | varchar(512) | Выделенные сервера |  |
| 5. | Country | varchar(512) | Страна |  |
| 6. | Region | varchar(512) | Регион |  |
| 7. | City | varchar(512) | Город |  |
| 8. | Description | varchar(512) | Описание |  |
| 9. | creationTime | bigint(20) | Время создания |  |
| 10. | lastModifiedTime | bigint(20) | Время последнего изменения файла. |  |
| 11. | count | int(11) | Количество |  |
| 12. | hashCode | bigint(20) | Хэш код |  |

### **SAV\_ALC\_NetModel\_Network**

**Хранимые данные:** служащее для описания сетей и структуры сетевой модели.

Ниже представлено описание полей таблицы.

Таблица 5. SAV\_ALC\_NetModel\_ Network

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Имя поля** | **Формат поля** | **Описание** | **Примечание** |
| 1. | id | int(11) unsigned | Уникальный идентификатор |  |
| 2. | Subnet | varchar(512) | Подсеть |  |
| 3. | Customer | varchar(512) | Клиент |  |
| 4. | Network | varchar(512) | Сеть |  |
| 5. | Country | varchar(512) | Страна |  |
| 6. | Region | varchar(512) | Регион |  |
| 7. | City | varchar(512) | Город |  |
| 8. | Description | varchar(512) | Описание |  |
| 9. | creationTime | bigint(20) | Время создания |  |
| 10. | lastModifiedTime | bigint(20) | Время последнего изменения файла. |  |
| 11. | count | int(11) | Количество |  |
| 12. | hashCode | bigint(20) | Хэш код |  |

### **SAV\_ALC\_NetModel\_Zone**

**Хранимые данные:** служащее для описания сетей и структуры сетевой модели.

Ниже представлено описание полей таблицы.

Таблица 6. SAV\_ALC\_NetModel\_Zone

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Имя поля** | **Формат поля** | **Описание** | **Примечание** |
| 1. | id | int(11) unsigned | Уникальный идентификатор |  |
| 2. | Subnet | varchar(512) | Подсеть |  |
| 3. | Customer | varchar(512) | Клиент |  |
| 4. | Zone | varchar(512) | Зона |  |
| 5. | Country | varchar(512) | Страна |  |
| 6. | Region | varchar(512) | Регион |  |
| 7. | City | varchar(512) | Город |  |
| 8. | Description | varchar(512) | Описание |  |
| 9. | creationTime | bigint(20) | Время создания |  |
| 10. | lastModifiedTime | bigint(20) | Время последнего изменения файла. |  |
| 11. | count | int(11) | Количество |  |
| 12. | hashCode | bigint(20) | Хэш код |  |

### **SAV\_ALC\_RVision\_Incidents**

**Хранимые данные:** служащее для для интеграции с RVision.

Ниже представлено описание полей таблицы.

Таблица 44. SAV\_ALC\_RVision\_Incidents

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Имя поля** | **Формат поля** | **Описание** | **Примечание** |
| 1. | id | int(11) unsigned | Уникальный идентификатор |  |
| 2. | seid | bigint(20) | Уникальный идентификатор события |  |
| 3. | status | int(11) | Статус |  |
| 4. | status\_desc | varchar(512) | Описание |  |
| 5. | logging | varchar(1024) | Время логирования |  |
| 6. | eventId | varchar(512) | Уникальный идентификатор, который присваивает значение каждому событию. |  |
| 7. | startTime | bigint(20) | Время, когда началось действие, на которое ссылается событие |  |
| 8. | endTime | bigint(20) | Время, когда закончилось действие, на которое ссылается событие |  |
| 9. | externalId | varchar(512) | Идентификатор, используемый исходным устройством. |  |
| 10. | severity | int(11) | Уровень критичности |  |
| 11. | name | varchar(512) | Название события |  |
| 12. | message | varchar(512) | Произвольное сообщение, содержащее более подробную информацию о событии. |  |
| 13. | sourceUserName | varchar(512) | Идентифицирует исходного пользователя по имени. |  |
| 14. | sourceUserId | varchar(512) | Идентифицирует исходного пользователя по идентификатору. |  |
| 15. | sourceUserPrivileges | varchar(512) | Определяет привилегии исходного пользователя. |  |
| 16. | sourceNtDomain | varchar(512) | Доменное имя Windows для исходного адреса. |  |
| 17. | sourceAddress | varchar(512) | Определяет источник, на который ссылается событие в IP-сети. |  |
| 18. | sourceHostName | varchar(512) | Определяет источник, на который ссылается событие в IP-сети. |  |
| 19. | sourceMacAddress | varchar(512) | Шесть шестнадцатеричных чисел, разделенных двоеточием. |  |
| 20. | sourcePort | int(11) | Порт источника события. |  |
| 21. | sourceZoneUri | varchar(512) | URI для зоны, которой был назначен исходный ресурс |  |
| 22. | sourceServiceName | varchar(512) | Служба, которая отвечает за генерацию этого события. |  |
| 23. | destinationUserName | varchar(512) | Идентифицирует конечного пользователя по имени. |  |
| 24. | destinationUserId | varchar(512) | Идентифицирует конечного пользователя по ID. |  |
| 25. | destinationUserPrivileges | varchar(512) | Представляет привилегии конечного пользователя. |  |
| 26. | destinationNtDomain | varchar(512) | Доменное имя Windows для адреса назначения. |  |
| 27. | destinationAddress | varchar(512) | Определяет адрес назначения, на который ссылается событие в IP -сети. Формат представляет собой IPv4 -адрес. |  |
| 28. | destinationHostName | varchar(512) | Определяет пункт назначения, к которому относится событие в IP-сети. |  |
| 29. | destinationMacAddress | varchar(512) | Шесть шестнадцатеричных чисел, разделенных двоеточием. |  |
| 30. | destinationPort | int(11) | Номер порта |  |
| 31. | destinationZoneUri | varchar(512) | URI для зоны, в которой был назначен целевой ресурс |  |
| 32. | destinationServiceName | varchar(512) | Сервис, на который направлено данное событие. Пример: "sshd" |  |
| 33. | destinationProcessName | varchar(512) | Имя процесса назначения события. |  |
| 34. | deviceProcessName | varchar(512) | Имя процесса, связанного с событием. |  |
| 35. | fileId | varchar(512) | Идентификатором, связанным с файлом |  |
| 36. | fileHash | varchar(512) | Хэш файла. |  |
| 37. | fileName | varchar(512) | Имя файла. |  |
| 38. | filePath | varchar(512) | Полный путь к файлу, включая само имя файла. |  |
| 39. | oldFileId | varchar(512) | Полный путь к старому файлу, включая само имя файла. |  |
| 40. | oldFileHash | varchar(512) | Хэш старого файла. |  |
| 41. | requestUrlHost | varchar(512) | Получение текущего имени домена |  |
| 42. | flexDate1 | varchar(512) | Пользовательское поле временной метки |  |
| 43. | reason | varchar(512) | Причина, по которой было сгенерировано событие аудита. |  |
| 44. | deviceCustomDate1 | bigint(20) | Пользовательское временное поле |  |
| 45. | deviceCustomDate2 | bigint(20) | Пользовательское временное поле |  |
| 46. | deviceCustomString1 | varchar(512) | Пользовательское строковое поле |  |
| 47. | deviceCustomString2 | varchar(512) | Пользовательское строковое поле |  |
| 48. | deviceCustomString3 | varchar(512) | Пользовательское строковое поле |  |
| 49. | deviceCustomString4 | varchar(512) | Пользовательское строковое поле |  |
| 50. | deviceCustomString5 | varchar(512) | Пользовательское строковое поле |  |
| 51. | deviceCustomString6 | varchar(512) | Пользовательское строковое поле |  |
| 52. | deviceDomain | varchar(512) | Полное доменное имя |  |
| 53. | devicePayloadId | varchar(512) | Уникальный идентификатор для полезной нагрузки, связанной с событием. |  |
| 54. | creationTime | bigint(20) | Время создания |  |
| 55. | lastModifiedTime | bigint(20) | Время последнего изменения файла. |  |
| 56. | count | int(11) | Количество |  |
| 57. | hashCode | bigint(20) | Хэш код |  |

### **actualresources**

**Хранимые данные:** Данная таблица служит для хранение созданных в системе U-SIEM ресурсов.

Ниже представлено описание полей таблицы.

Таблица 7. actualresources

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Имя поля** | **Формат поля** | **Описание** | **Примечание** |
| 1. | id | int(11) | Уникальный идентификатор |  |
| 2. | parentId | int(11) | Идентификатор родительского ресурса |  |
| 3. | type | int(11) | Тип |  |
| 4. | name | varchar(512) | Имя ресурса |  |
| 5. | def | mediumtext | XML файл, описывающий структуру и состав ресурса |  |
| 6. | subType | int(11) | Подтип |  |
| 7. | isSystem | tinyint(1) | Системный |  |
| 8. | shared | tinyint(1) | Общий |  |
| 9. | personal | tinyint(1) | Персональный |  |
| 10. | deleted | tinyint(1) | Ресурс помечен на удаление |  |
| 11. | userId | int(11) | Уникальный идентификатор пользователя |  |
| 12. | resourceId | varchar(50) | Уникальный идентификатор ресурса |  |
| 13. | Disabled | tinyint(1) | Выключенный |  |
| 14. | DateCreation | datetime | Дата создания |  |
| 15. | DateChanged | datetime | Дата последнего изменения |  |

### **config\_properties**

**Хранимые данные:** хранит параметры парольной политики.

Таблица 46 config\_properties

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Имя поля** | **Формат поля** | **Описание** | **Примечание** |
| 1. | id | int(11) | Уникальный идентификатор записи |  |
| 2. | pwd\_sym\_to\_change | int(11) | кол-во символов, на которое новый пароль пользователя должен отличаться от старого при смене пароля пользователем |  |
| 3. | pwd\_exp\_days | int(11) | срок действия пароля пользователя в днях |  |
| 4. | pwd\_ban\_last\_used | int(11) | кол-во последних введенных паролей, запрещенных к использованию при смене пароля пользователем |  |
| 5. | max\_auth\_attempts | int(11) | максимальное кол-во попыток входа в систему, после которого блокируется учетная запись пользователя |  |
| 6. | auth\_attempts\_timer | int(11) | время фиксации последовательных неудачных попыток входа пользователя в систему, в секундах |  |
| 7. | user\_ban\_timer | int(11) | время, на которое блокируется учетная запись пользователя после превышения максимального количества неудачных попыток входа, в секундах |  |
| 8. | pwd\_pattern | varchar(300) | REGEXP-выражение, описывающее минимально допустимый набор символов и минимальную длину пароля пользователя при создании нового пользователя или смене пароля пользователем |  |
| 9. | pwd\_exp\_days\_remind | int(11) | за сколько дней необходимо начать напоминать пользователю об истечении пароля |  |

### **core\_properties**

**Хранимые данные:** используется для хранения служебных данных, характерных для всех пользователей сервиса.

Таблица 47 core\_properties

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Имя поля** | **Формат поля** | **Описание** | **Примечание** |
| 1. | id | int(11) | Уникальный идентификатор записи |  |
| 2. | al\_rows\_limit\_default | int(11) | Лимит количества записей активного списка |  |
| 3. | user\_inactivity\_timeout | int(11) | Таймаут бездействия пользователя в сессии |  |

### **roles**

**Хранимые данные:** Данная таблица служит хранения данных о существующих в системе U-SIEM ролях пользователей.

Ниже представлено описание полей таблицы.

Таблица 8. roles

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Имя поля** | **Формат поля** | **Описание** | **Примечание** |
| 1. | id | int(11) | Уникальный идентификатор |  |
| 2. | Name | varchar(128) | Имя роли |  |
| 3. | parent\_id | int(11) | Ссылка на родителя |  |
| 4. | roleFilter | varchar(50) | Идентификатор фильтра, прикрепленного к роли |  |
| 5. | rolePermission | int(11) | Дополнительные привилегии роли |  |

### **roles\_access**

**Хранимые данные:** служащее для описания прав роли пользователя на выполнение действий над определенным типом ресурсов.

Ниже представлено описание полей таблицы.

Таблица 9.roles\_access

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Имя поля** | **Формат поля** | **Описание** | **Примечание** |
| 1. | roleid | int(11) | Уникальный идентификатор роли |  |
| 2. | resourcetype | int(11) | Тип ресурса | Тип ресурса, на который определяются права |
| 3. | CREATE | tinyint(1) | Создан | Право роли выполнять команду «Создать» |
| 4. | OPEN | tinyint(1) | Открыт | Право роли выполнять команду «Открыть» |
| 5. | SAVE | tinyint(1) | Сохранён | Право роли выполнять команду «Сохранить» |
| 6. | DEL | tinyint(1) | Удален | Право роли выполнять команду «Удалить» |

### **roles\_resources**

**Хранимые данные:** служащее для описания прав роли пользователя на выполнение действий над определенным типом ресурсов.

Ниже представлено описание полей таблицы.

Таблица 109.roles\_resources

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Имя поля** | **Формат поля** | **Описание** | **Примечание** |
| 1. | role\_id | int(11) | Уникальный идентификатор роли | Роль пользователя |
| 2. | res\_id | int(11) | ИД ресурса | Ресурса, на который определяются права (папка в дереве ресурсов) |
| 3. | CREATE | tinyint(1) | Создан | Право роли выполнять команду «Создать» |
| 4. | OPEN | tinyint(1) | Открыт | Право роли выполнять команду «Открыть» |
| 5. | SAVE | tinyint(1) | Сохранён | Право роли выполнять команду «Сохранить» |
| 6. | DEL | tinyint(1) | Удален | Право роли выполнять команду «Удалить» |

### **user\_auth\_attempts**

**Хранимые данные:** используется для хранения данных о неудачных попытках входа пользователя в систему.

Таблица 53 user\_auth\_attempts

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Имя поля** | **Формат поля** | **Описание** | **Примечание** |
| 1. | user\_id | int(11) | Уникальный идентификатор пользователя |  |
| 2. | attempts\_count | int(11) | Количество неудачных попыток входа за контролируемый промежуток времени |  |
| 3. | attempts\_start | timestamp | Время первой неудачной попытки |  |
| 4. | banned\_until | timestamp | Время окончания блокировки входа по количеству неудачных попыток входа |  |

### **users**

**Хранимые данные:** служащее для описания пользователей.

Ниже представлено описание полей таблицы.

Таблица 51. users

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Имя поля** | **Формат поля** | **Описание** | **Примечание** |
| 1. | id | int(11) | Уникальный идентификатор |  |
| 2. | FIO | varchar(45) | Фамилия имя отчество |  |
| 3. | UserLogin | varchar(45) | Логин пользователя |  |
| 4. | Active | tinyint(1) | Является ли пользователь активным |  |
| 5. | EMail | varchar(255) | Электронная почта пользователя |  |
| 6. | Deleted | tinyint(1) | Является ли пользователь удалённым |  |
| 7. | Pwd | varchar(300) | Хэш пароля пользователя |  |
| 8. | userRole | int(11) | Роль пользователя |  |
| 9. | needChangePass | tinyint(1) | Признак необходимости смены пароля пользователем |  |
| 10. | showDeletedResources | tinyint(1) | Показывать ли пользователю удалённые ресурсы |  |
| 11. | adAuth | tinyint(1) | Пользователь использует доменную аутентификацию |  |
| 12. | userFilter | varchar(50) | Фильтр пользователя | Сейчас не используется |

### **usersPasswords**

**Хранимые данные:** служащее для хранения хэш значения введенных ранее паролей. Используется для реализации требования парольной политики не допускать использование последних N введенных паролей.

Ниже представлено описание полей таблицы.

Таблица 52 userPasswords

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Имя поля** | **Формат поля** | **Описание** | **Примечание** |
| 1. | id | int(11) | Уникальный идентификатор пароля |  |
| 2. | userId | int(11) | Уникальный идентификатор пользователя |  |
| 3. | pwd | varchar(300) | Хэш пароля |  |
| 4. | dateCreation | datetime | Дата создания |  |
| 5. | dateExpiration | datetime | Дата истечения пароля |  |
| 6. | active | int(11) | Пароль активен | Текущий используемый хэш пароля |