

Table of Contents

Table of Contents	1
Сборщик логов	2
Описание	3
Syslog	4

Описание

Documentation: ☒

Product: SIEM

Version: 7.1.x

Сборщик логов предназначен для централизованного сбора информации с сетевых устройств, что помогает облегчить мониторинг сети, виртуальных машин, серверов, пользовательских устройств, приложений.

Documentation: ☒
Product: SIEM
Version: 7.2.x

В данном разделе настраиваются правила сбора событий системных журналов Unix-систем (syslog), которые содержат информацию о работе системы, её состоянии и безопасности, наличии ошибок, сбоях в работе. Правила syslog позволяют осуществлять фильтрацию записей событий (по времени, критичности событий, объектам, названию устройств, приложениям), упрощая поиск необходимой информации.

Для работы сборщика логов необходимо настроить сервер, с которого будет происходить сбор информации, и правила syslog.

Для настройки сервера необходимо в веб-консоли администратора перейти в раздел **Сборщик логов → Syslog**, нажать кнопку **Настроить сервер** и указать следующие данные в открывшемся окне **Настройки syslog**:

Наименование	Описание
Включено	Включение/отключение приёма syslog событий.
Протокол	Сетевой протокол, использующийся для сбора информации: - TCP. - UDP.
Порт	Номер порта, использующегося для сбора syslog событий. По умолчанию — порт 514.
Максимальное количество сессий	Максимальное количество устройств, подключённых одновременно с целью отправки сообщений.
Безопасное соединение	Включение/отключение шифрования потока данных. Подробнее об использовании TLS в Syslog читайте в соответствующей документации.
Файл сертификата УЦ	Сертификат удостоверяющего центра (центра сертификации), который используется для установления безопасного соединения.
Файл сертификата	Сертификат, сгенерированный пользователем и подписанный центром сертификации (ЦС); необходимо указать при настройке безопасного соединения.
Разрешённые соседи	Список устройств, с которых SIEM будет получать информацию в случае использования безопасного соединения.

Для настройки правил фильтрации записей событий syslog необходимо указать следующие данные:

Наименование	Описание
Включено	Включение/отключение правила syslog.
Название	Название правила syslog.
Описание	Описание правила syslog (опционально).
Действие	Действие: Разрешить — разрешение приёма сообщений, подходящих под условия правила. Запретить — блокировка приёма сообщений, подходящих под условия правила.
Часовой пояс	Часовой пояс, настроенный на удалённых устройствах. Приём сообщений будет разрешён или запрещён с устройств, у которых сохранение записей происходит в указанном часовом поясе.

Наименование	Описание
Вставить	Место вставки создаваемого правила в списке правил: вверх, вниз или выше выбранного существующего правила.
Критичность	Критичность событий syslog: • Экстренная: критическое состояние, которое сказывается на работоспособности системы. • Тревога: состояние, требующее незамедлительного вмешательства. • Критическая: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе. • Ошибки: сообщения о сбоях в системе. • Предупреждения: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия. • Уведомительная: события, которые относятся к необычному поведению системы, но не являются ошибками. • Информативная: информационные уведомления. • Отладочная: информация, полезная разработчикам для отладки приложений.
Объект	Категория события: • Сообщения ядра. • Сообщения пользовательские. • Почтовая система. • Системный сервис. • Безопасность/авторизация. • Сообщения syslog. • Система печати LPR. • Система сетевых новостей. • Подсистема UUCP. • Сервис времени. • Безопасность/аутентификация. • FTP сервис. • Система NTP. • Аудит. • Тревога. • Сервис времени 2. • Local 0 — Local 7.
Имя хоста	Название устройства.
Название приложения	Название приложения, сбор информации о котором необходимо разрешить/запретить. Подробнее читайте в разделе Приложения syslog.

Примечание При парсинге syslog-сообщений в отдельные поля журналов будут записаны поля syslog из RFC 3164 (facility, severity, timestamp, hostname, tag, pid). Все дополнительные поля из RFC 5424 будут записаны в поле data.

Записи событий будут отображены в журнале **Syslog**, подробнее читайте в разделе [Системный журнал](#).

