

Table of Contents

Table of Contents	1
Сенсоры	2
Общие сведения	3
Сенсоры SNMP	4
Сенсоры WMI	6
Конечные устройства	7
Управление SNMP MIB	8

Общие сведения

Documentation: 

Product: LogAn, SIEM

Version: 6.1.9, 7.0.1, 7.1.0

Для сбора информации с различных устройств и последующего ее анализа LogAn использует сенсоры. Сенсор — это совместимое с LogAn устройство, которое может передавать определенные данные на сервер LogAn. Сенсорами могут выступать устройства UserGate NGFW, конечные устройства UserGate Client, а также любые другие сетевые устройства, способные передавать данные по протоколу SNMP.

Сенсоры SNMP

Documentation: ☒
Product: LogAn, SIEM
Version: 6.1.9, 7.0.1, 7.1.0

С помощью сенсора SNMP администратор может подключить SNMP-совместимое сетевое устройство к серверу LogAn для сбора и анализа его метрик. LogAn может отображать любые счетчики, полученные по SNMP с помощью запросов SNMP. Для настройки сенсора SNMP необходимо иметь базы MIB (Management Information Base) на управляемое устройство. Подробнее об управлении базами MIB смотрите раздел данного руководства [Управление SNMP MIB](#).

Для настройки сенсора SNMP необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Загрузите базу MIB того устройства, которое хотите добавить для мониторинга.	На сервере LogAn в разделе Сенсоры → Управление SNMP MIB загрузите файл с MIB.
Шаг 2. Создайте сенсор SNMP	На сервере LogAn в разделе Сенсоры → Сенсоры SNMP нажмите кнопку Добавить и заполните необходимые поля.

При создании сенсора SNMP необходимо заполнить следующие поля:

Наименование	Описание
Включено	Включает или выключает данный сенсор SNMP.
Название	Название сенсора SNMP.
Описание	Опциональное описание сенсора SNMP.
Адрес сервера	IP-адрес сенсора SNMP.
Порт	Порт сенсора SNMP. Обычно для запросов данных по протоколу SNMP используется порт TCP 161.
Версия	Указывает версию протокола SNMP, которая будет использоваться в данном сенсоре. Возможны варианты SNMP v2 и SNMP v3.
Community	SNMP community - строка для идентификации сервера LogAn и сетевого устройства для версии SNMP v2. Используйте только латинские буквы и цифры.
Интервал опроса (сек)	Интервал, через который сервер LogAn будет инициировать получение данных с сетевого устройства.
Пользователь	Только для SNMP v3. Имя пользователя для аутентификации сетевом устройстве.
Тип аутентификации	Выбор режима аутентификации. Возможны варианты: - Без аутентификации, без шифрования (noAuthNoPriv). - С аутентификацией, без шифрования (authNoPriv). - С аутентификацией, с шифрованием (authPriv). Наиболее безопасным считается режим работы authPriv.
Алгоритм аутентификации	Алгоритм, используемый для аутентификации.
Пароль аутентификации	Пароль, используемый для аутентификации.

Наименование	Описание
Алгоритм шифрования	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
Пароль шифрования	Пароль, используемый для шифрования.
Счётчики	Укажите здесь все требуемые данные, которые LogAp будет запрашивать на сетевом устройстве. Счетчики выбираются из баз MIB, которые загружены на устройство. Выберите в дереве SNMP необходимый раздел и добавьте соответствующий счетчик либо укажите в строке SNMP OID счетчика и его тип.

После успешного добавления сенсора в разделе **Дашборд** появится возможность добавить виджет с графиками данных SNMP, полученными с данного сенсора.

Сенсоры WMI

Documentation: 

Product: LogAn, SIEM

Version: 7.0.1, 7.1.0

С помощью сенсора WMI администратор может подключить WMI-совместимое сетевое устройство (компьютер под управлением ОС Windows) к серверу LogAn для сбора и анализа его метрик.

Documentation: ☒

Product: LogAn, SIEM

Version: 7.0.1, 7.1.0

Данный раздел содержит список конечных устройств с установленным программным обеспечением UserGate Client.

Примечание Конечное устройство будет отображено при выборе на UGMC данного устройства LogAn в качестве сервера для передачи информации о событиях, соответственно, LogAn должен быть предварительно зарегистрирован на UGMC.

Отображена следующая информация:

- Название конечного устройства, заданное на UGMC.
- Версия ПО UserGate Client, установленная на устройстве.
- Время последнего подключения к устройству.
- IP-адрес устройства.
- Netbios имя.
- Версия операционной системы (ОС) устройства.
- Телеметрическая информация.

В LogAn реализована возможность удалённого управления устройствами UserGate Client. Для этого нажмите **Послать команду** и выберите необходимое действие:

- Отключить от сети.
- Разрешить передачу данных по сети.
- Завершить процесс. При выборе данного действия необходимо указать идентификатор процесса.
- Запустить/остановить службу. Для выполнения данных действий необходимо указать название службы.

Управление SNMP MIB

Documentation: 

Product: LogAn, SIEM

Version: 6.1.9, 7.0.1, 7.1.0

В данном разделе администратор может добавлять и удалять базы MIB (Management Information Base) на сервере LogAn.

Для получения специфических MIB обратитесь к производителю вашего устройства. LogAn уже содержит наиболее популярные базы сетевых устройств.

