

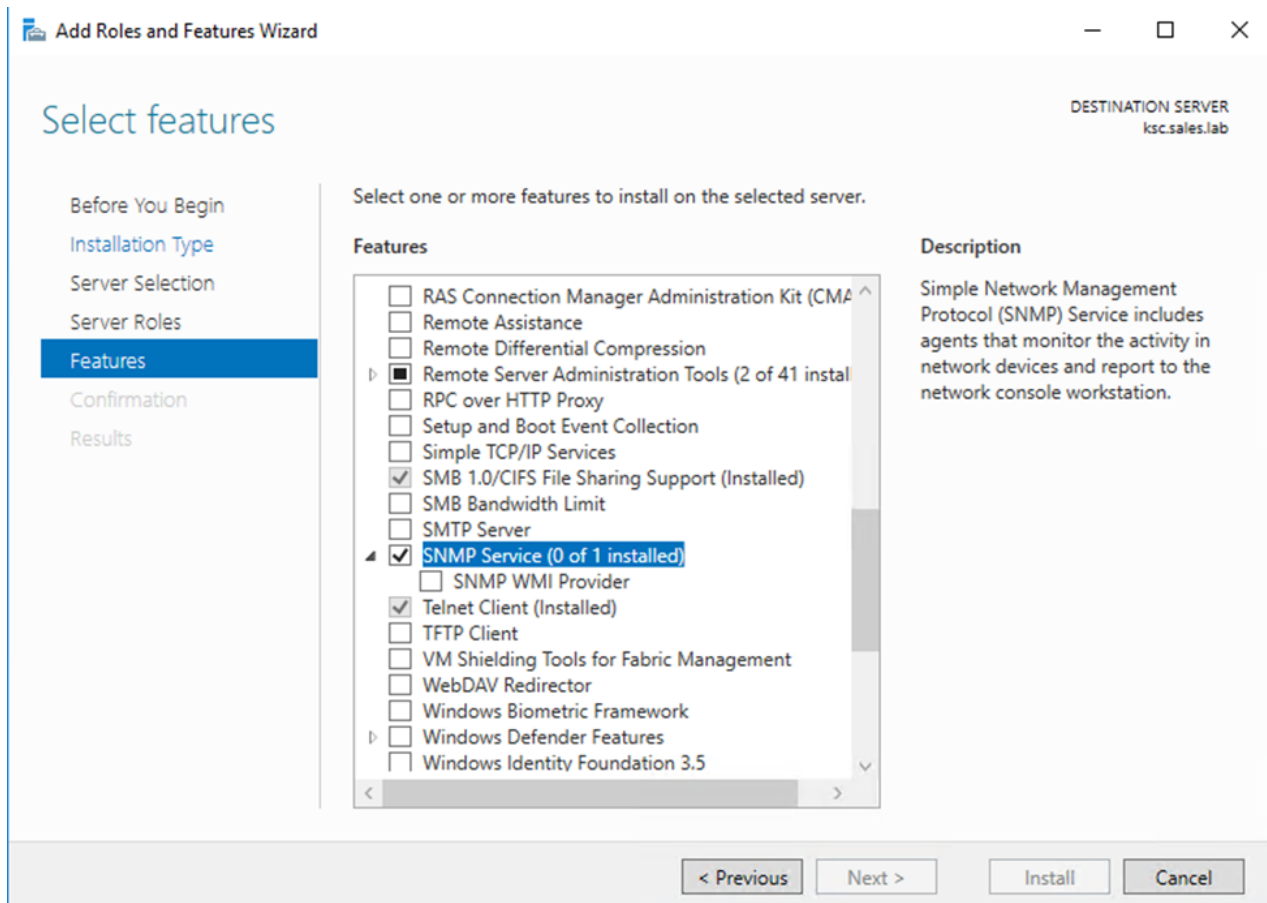
MS Windows Server 2016 SNMP

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

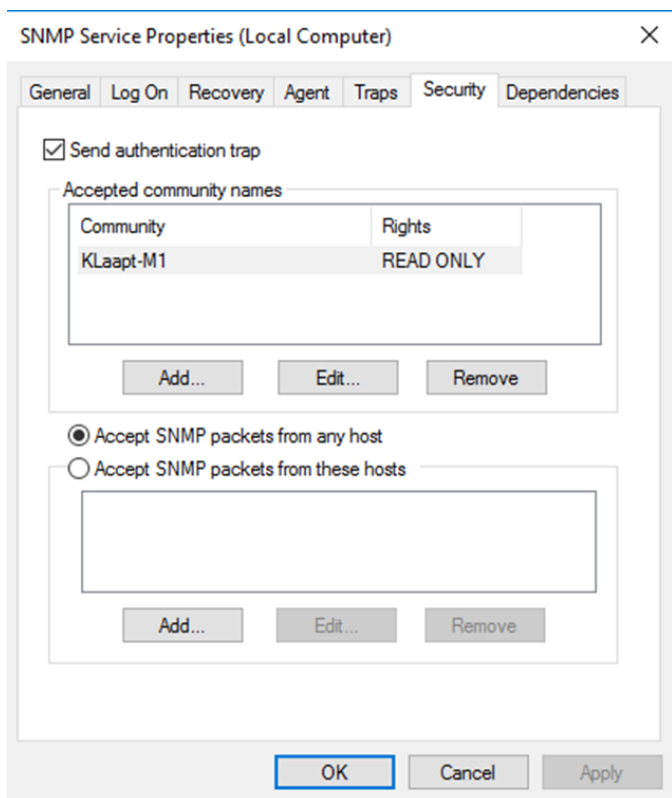
?????????? ?? ???????? Windows.

?????????? ???????? SNMP

1. Включить поддержку SNMP на Windows



2. В свойствах сервиса SNMP Service настроить community (фактически, это можно использовать как пароль) и добавить адрес KUMA в разрешенные (либо any)



3. Перезапустить сервис SNMP Service

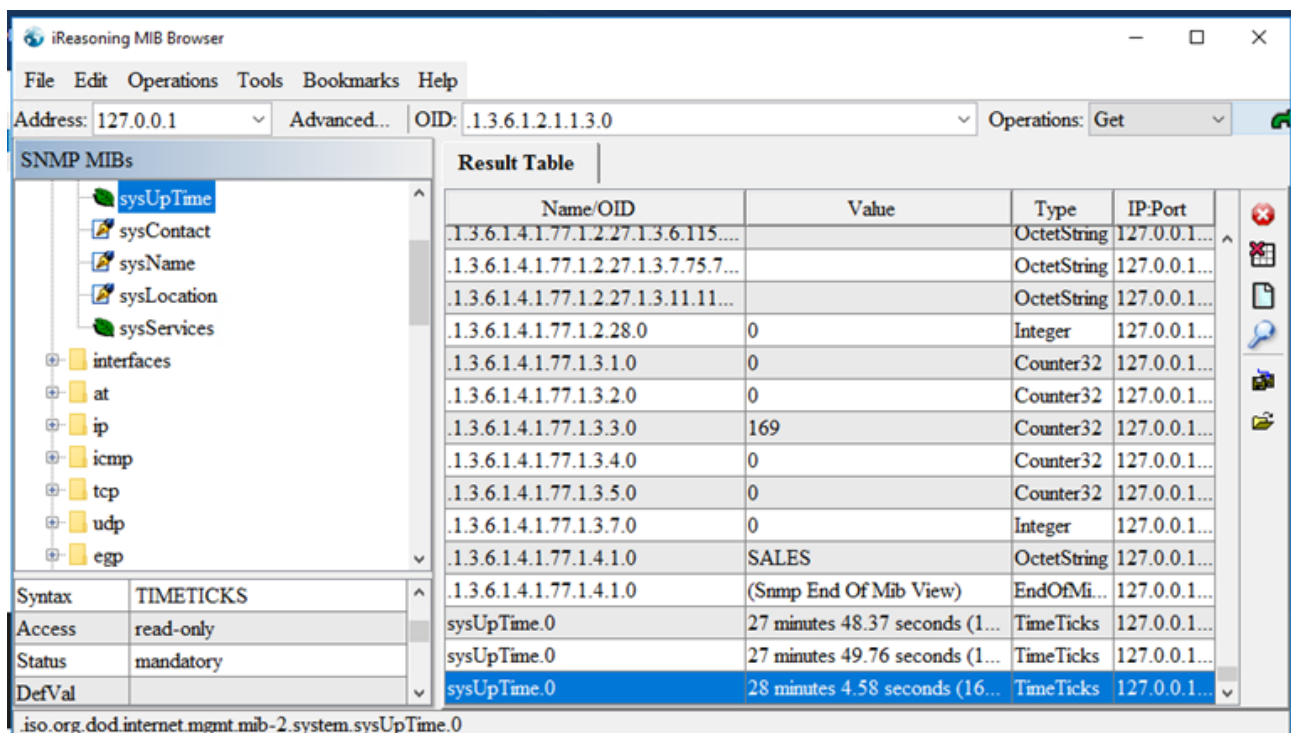
????????? ?? ??????? KUMA

Добавить новый источник, тип SNMP. Community – это та же строка, указанная в SNMP Service в Windows - KLaapt-M1

Порт 161 – по умолчанию.

Чтобы настроить мапинг полей нужно

- обратиться к документации источника SNMP
- <https://oidref.com/>
- использовать MIB браузеры. Для Windows, например, <https://www.ireasoning.com/downloadmibbrowserfree.php>



?????????? ?? ????????? KUMA

Создайте коллектор со следующим транспортом:

1 Подключение источников

2 **Транспорт**

3 Парсинг событий

4 Фильтрация событий

5 Агрегация событий

6 Обогащение событий

7 Маршрутизация

8 Проверка параметров

Основные параметры

Дополнительные параметры

*Коннектор

Создать

?

*Тип

snmp

?

*Версия SNMP

snmpV2

?

*Хост

ksc.sales.lab

?

*Порт

161

?

*Секрет

[SNMP] Windows Community

+

+ SNMP-ресурс

*Данные источника

Название параметра	OID	Ключ
sysUpTime	1.3.6.1.2.1.1.3.0	sysUpTime

+ Добавить строку

Назад

Вперед

Установить сервис коллектора, проверить, что события поступают



Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

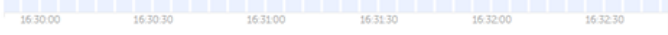
Устройства

Дней до истечения срока годности лицензионного ключа: 8. Добавьте лицензионный ключ.

События

SELECT * FROM 'events' WHERE ServiceID = '9aba1246-c217-4df4-b5bb-f9b40f1775e5' LIMIT 250

Скор: 60



Тенант	Timestamp	Name	DeviceProduct	DeviceVendor
Main	18 февр. 2022 г. 16:34:47			
Main	18 февр. 2022 г. 16:34:42			
Main	18 февр. 2022 г. 16:34:37			
Main	18 февр. 2022 г. 16:34:32			
Main	18 февр. 2022 г. 16:34:27			

Информация о событии

TenantName	Main
Timestamp	18 февр. 2022 г. 16:34:47:304
DeviceReceiptTime	18 февр. 2022 г. 16:34:47:304
Service	[SNMP] Windows
Priority	Низкий
Type	Base
Raw	("sysUpTime":144441)

Настроить нормализацию для типа данных json

Парсинг событий

*Название

[SNMP] Windows

*Тенант

Main

*Метод парсинга

json

*Хранить исходное событие

Не хранить

*Сохранить дополнительные поля

Нет

Описание

Описание

Примеры событий

Сопоставление

Исходные данные	Поле KUMA	Подпись	
sysUpTime	DeviceCustomString1	Uptime	

OK

Отмена

Проверить парсинг событий

Информация о событии

TenantName	Main
Timestamp	18 февр. 2022 г. 16:38:12.428
DeviceReceiptTime	18 февр. 2022 г. 16:38:12.428
DeviceCustomString1	164954
DeviceCustomString1Label	Uptime
Service	[SNMP] Windows
Priority	Низкий
Type	Base

Траблшутить можно со стороны KUMA утилитой snmpget
yum install net-snmp
yum install net-snmp-utils
snmpget -v 2c -c KLaapt-M1 ksc.sales.lab .1.3.6.1.2.1.1.3.0

```
[root@kuma15 ~]# snmpget -v 2c -c KLaapt-M1 ksc.sales.lab .1.3.6.1.2.1.1.3.0  
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (107135) 0:17:51.35
```

Revision #2

Created 2026-07-29 11:11:44 UTC by Boris RZR

Updated 2026-07-29 11:17:44 UTC by Boris RZR