request-ru@raidix.com
raidix.ru

RAIDIX 5.3.1
Руководство по мониторингу

Редакция 1

2024

Содержание

ГЛАВА 1. ОБ ЭТОМ РУКОВОДСТВЕ

Руководство содержит инструкции для интеграции системы хранения данных RAIDIX с системами мониторинга.

Что нового

Редакция	Изменения	Дата внесения изменения
1	Документ создан.	17.12.2025

ГЛАВА 2. НАСТРОЙКИ СХД

Подключение к пользовательскому веб-интерфейсу

Подключение к веб-инетрфейсу RAIDIX

Подключение к веб-интерфейсу выполняется с помощью веб-браузера на рабочей станции администратора, настроенной для подключения к СХД.

Чтобы подключиться к WEB UI:

1. Запустите веб-браузер на рабочей станции.
2. Введите в адресной строке IP-адрес контроллера системы.
3. Введите имя и пароль учетной записи и кликните **Войти**.

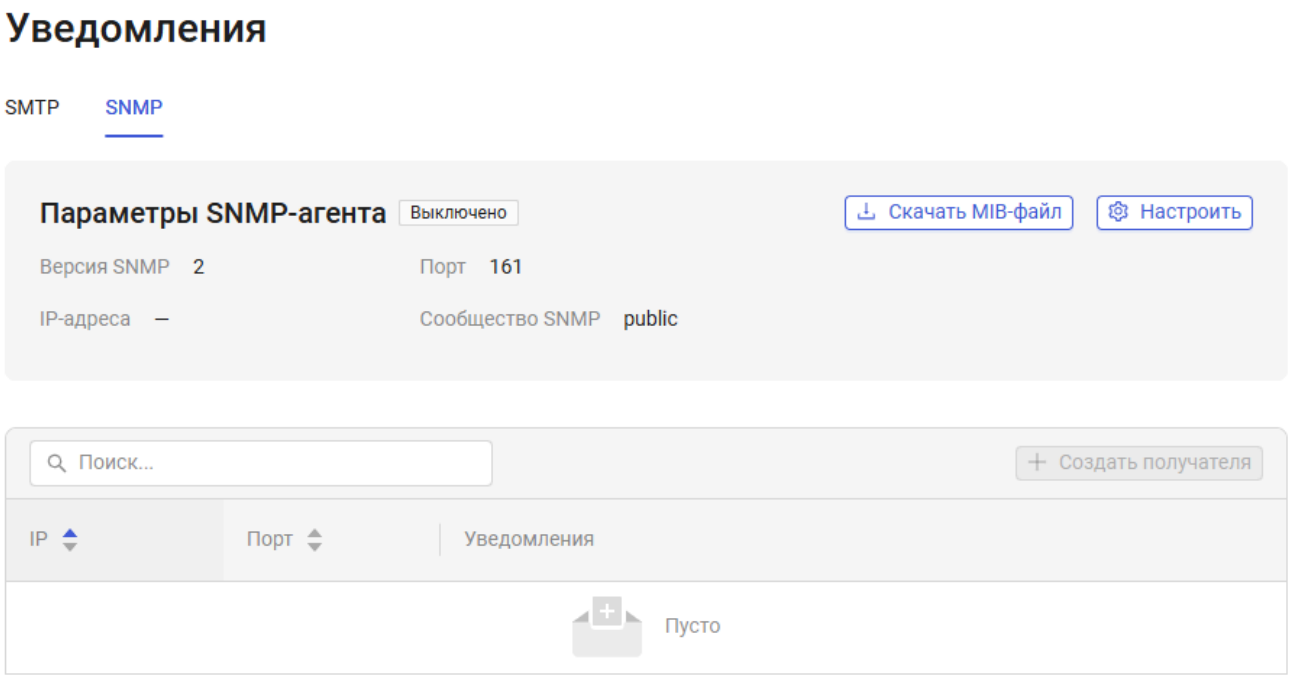
Настройка SNMP

Настройка подключения к серверу SNMP

Настройка подключения доступна во вкладке **SNMP**.

Вам доступны следующие операции:

- Настройка подключения к серверу SNMP.
- Скачивание MIB-файла.



Чтобы настроить подключение к серверу SNMP, кликните **Настроить**, настройте параметры сервера и кликните **Настроить**. Описание параметров см. ниже в этой секции.

Параметр	Назначение
Включено/Выключено	Состояние SNMP-агента.
Версия SNMP	Версия протокола SNMP.

Параметр	Назначение
IP-адреса	Необязательно. IP-адреса, по которым клиент может обращаться к серверу для получения информации о его состоянии.
Порт	Номер порта, по которому SNMP агент обращается к серверу. По умолчанию: **161**.
Сообщество SNMP	Только для SNMPv1 и SNMPv2. Имя сообщества для аутентификации на сервере. По умолчанию: **public**.
Engine ID	Используется в SNMPv3 для уникальной идентификации устройств в сети. Стандартно формируется на основе MAC-адреса устройства. Должен быть уникальным в административном домене чтобы исключить совпадения между устройствами в сети.
Имя пользователя	Только для SNMPv3. Имя пользователя. Должно совпадать с именем на стороне клиента. Минимальная длина: 8 символов.
Протокол аутентификации	Только для SNMPv3. Протокол аутентификации. Должен совпадать с протоколом на стороне клиента. Возможные значения: • **md5** • **sha** По умолчанию: **md5**.
Пароль аутентификации	Только для SNMPv3. Пароль аутентификации. Значение должно совпадать с указанными на стороне клиента.
Мастер ключ аутентификации	Необязательно. Только для SNMPv3. Ключ, который используется для аутентификации вместо пароля.
Локализованный ключ аутентификации	Необязательно. Только для SNMPv3. Локализованный ключ, который используется для аутентификации вместо пароля.
Протокол шифрования	Только для SNMPv3. Протокол шифрования. Возможные значения: • **des** • **aes** По умолчанию: **des**.

Параметр	Назначение
Пароль конфиденциальности	Необязательно. Только для SNMPv3. Пароль, используемый для шифрования.
Мастер ключ конфиденциальности	Необязательно. Только для SNMPv3. Ключ, используемый для шифрования вместо пароля.
Конфиденциальный локализованный ключ	Необязательно. Только для SNMPv3. Ключ, используемый для шифрования вместо пароля.

Чтобы скачать MIB-файл, кликните **Скачать MIB-файл**.

Управление получателями уведомлений SNMP

После настройки параметров сервера SNMP вы можете настроить получателей уведомлений.

Управление получателями доступно во вкладке **SNMP**.

Вам доступны следующие операции:

- Добавление получателя.
- Изменение объектов и типов уведомлений для получателя.
- Удаление получателя.
- Тестовая отправка уведомления.

Чтобы добавить получателя, кликните **Создать получателя**, введите IP-адрес и порт получателя и выберите категорию и тип уведомлений, затем кликните **Создать**.

Параметр	Назначение
IP получателя	IP-адрес получателя.
Порт	Порт получателя. По умолчанию: **162**.

Чтобы изменить объекты и/или типы уведомлений для получателя, в строке с нужным получателем кликните ⋮ и выберите **Изменить**.

Чтобы удалить получателя, в строке с нужным получателем кликните ⋮ и выберите **Удалить**.

Чтобы отправить тестовое уведомление получателю, в строке с нужным получателем кликните ⋮ и выберите **Тест**.

ГЛАВА 3. НАСТРОЙКА ИНТЕГРАЦИИ С ZABBIX

Zabbix – система мониторинга для IT-инфраструктуры. Вы можете настроить интеграцию Zabbix с СХД RAIDIX, чтобы отслеживать состояние системы.

Для интеграции с Zabbix вам доступны два типа шаблонов:

- SNMP
- REST API

Рекомендуем использовать оба шаблона одновременно: каждый из них содержит свой набор метрик, дополняющих друг друга.

> Шаблоны доступны по *ссылке*. Инструкцию по загрузке MIB-файлов см. в разделе *Настройка SNMP (стр. 4)*.

Инструкции в этой главе подразумевают, что Zabbix установлен и настроен в соответствии с *официальной документацией Zabbix*.

Интеграция через шаблон SNMP

Чтобы настроить интеграцию с Zabbix:

1. На СХД *настройте передачу данных по протоколу SNMP (стр. 4)*.
2. В интерфейсе управления Zabbix:

   > Подробную информацию по каждой настройке см. в *официальной документации Zabbix*.

   a. При необходимости, настройте Zabbix-прокси.
   b. Настройте обработку SNMP Traps через Perl- или bash-скрипты. SNMPTT на данный момент не поддерживается.
   c. Импортируйте шаблон. Шаблон должен соответствовать версии Zabbix.
   d. Создайте «узел сети» для каждого контроллера СХД. При создании узла сети:
      - Настройте SNMP-интерфейс. Ключ SNMP Community должен совпадать с указанным в конфигурации службы SNMP на СХД.
      - Если мониторинг осуществляется через Zabbix-прокси, укажите имя Zabbix-прокси.
   e. Назначьте импортированный шаблон для каждого узла сети.

Чтобы настроить приём и обработку SNMP Traps:

> Подробную информацию по каждой настройке см. в *официальной документации Zabbix*.

1. Установите `snmptrapd` (SNMP Trap Daemon).
2. Настройте приём SNMP Traps.

При использовании Bash- или Perl-скриптов дополнительных настроек не требуется.

Интеграция через шаблон REST API

Настройка интеграции выполняется в два этапа: создание на стороне СХД пользователя, учётные данные которого будут использоваться токеном доступа Zabbix, и настройка доступа в интерфейсе управления Zabbix.

На стороне СХД:

1. Создайте пользователя с правами администратора:

```
$ rdcli system user create -l <zabbix_adm> -p <password> -r administrators
```

2. Задайте продолжительность сессии для пользователя:

```
$ rdcli system settings session modify --users <zabbix_adm> --lifetime <new_value>
```

   По умолчанию продолжительность сессии для всех пользователей составляет 600 секунд, максимально возможное значение — 2678400 секунд (31 день).

В интерфейсе управления Zabbix:

> Подробную информацию по каждой настройке см. в *официальной документации Zabbix*.

1. Импортируйте шаблон.
2. Создайте «узел сети» для каждого контроллера СХД.
3. Для узла сети:
   - Назначьте импортированный шаблон.
   - Установите значение для макроса `{$RAIDIX_IP}` — IP-адрес основного интерфейса целевого контроллера СХД.
   - Установите значение для макроса `{$COOKIEAUTH}` — токен доступа.

     Токен доступа можно получить с помощью POST-эндпоинта `http://<ip:port>/api/auth` с телом вида: `{"login": "username", "password": "password"}`. Например:

```
curl -k -i -X POST -H "Content-Type: application/json" -d '{"login": "<zabbix_adm>", "password": "<password>"}'
 https://<controller_ip>/api/auth | grep -oP 'connect.sid=([^;]+)'
```

     где

     `<zabbix_adm>` – логин пользователя, созданного для доступа Zabbix;
     `<password>` – пароль пользователя, созданного для доступа Zabbix;
     `<controller_ip>` – IP-адрес основного интерфейса контроллера СХД.

Настройка интервалов сбора данных

Чтобы настроить интервал сбора данных, в интерфейсе Zabbix:

> Подробную информацию по каждой настройке см. в *официальной документацией Zabbix*.

1. Перейдите в раздел **Настройка > Шаблоны** и выберите шаблон `Raidix`.
2. В карточке шаблона откройте вкладку **Макросы**.
3. Задайте значения переменных:

`INV_POLL_INTERVAL`

Временной интервал сбора данных о компонентах СХД (пример: имя вендора).

`KEEP_LOST_RES`

Временной интервал хранения метрик для компонентов, которые больше нельзя обнаружить.

`LLD_POLL_INTERVAL`

Временной интервал поиска новых компонентов СХД.

PERF_POLL_INTERVAL

Временной интервал сбора показателей производительности СХД (пример: нагрузка на CPU).

ГЛАВА 4. ПЕРЕЧЕНЬ SNMP TRAPS

Типы оповещений SNMP Traps и объекты с соответствующими SNMP ID приведены ниже.

urgentNotification (.1.3.6.1.4.1.53647.0.1)

Срочное уведомление от системы. Использует следующие объекты для передачи информации:

Объект	SNMP ID	Описание
urgentNotificationMessage	1.3.6.1.4.1.53647.50.110.1	Текст уведомления.
urgentNotificationTime	1.3.6.1.4.1.53647.50.110.2	Время генерации уведомления.

alert (.1.3.6.1.4.1.53647.0.2)

Оповещение от системы. Использует следующие объекты для передачи информации:

Объект	SNMP ID	Описание
alertId	1.3.6.1.4.1.53647.50.110.3	Идентификатор объекта, который сгенерировал оповещение.
alertType	1.3.6.1.4.1.53647.50.110.4	Тип объекта, такой как `network.interface`.
alertName	1.3.6.1.4.1.53647.50.110.5	Название объекта, такое как `RAID`.
alertStart	1.3.6.1.4.1.53647.50.110.6	Время генерации оповещения.
alertMessage	1.3.6.1.4.1.53647.50.110.7	Текст оповещения.
alertStatus	1.3.6.1.4.1.53647.50.110.8	Статус оповещения, такой как `error`, `warning`, `info` или `ok`.

На данный момент нет возможности инициировать отправку SNMP Traps с RAIDIX без воспроизведения алертных ситуаций (кроме тестового `urgentNotification`), однако можно сэмулировать отправку SNMP Traps с помощью команды `snmtrap`:

```
snmptrap -v 2c -c public 127.0.0.1:162 '' 1.3.6.1.4.1.53647.0.2 1.3.6.1.2.1.1.3.0 t 536531000
 1.3.6.1.4.1.53647.50.110.6.0 s "2023-10-24 10:10:10" 1.3.6.1.4.1.53647.50.110.5.0 s "ens5f0np0"
 1.3.6.1.4.1.53647.50.110.7.0 s "ens5f0np0 is down" 1.3.6.1.4.1.53647.50.110.4.0 s "network.interface"
 1.3.6.1.4.1.53647.50.110.3.0 s "ens5f0np0" 1.3.6.1.4.1.53647.50.110.8.0 s "warning"
```

Где:

- `127.0.0.1:162` — IP целевой системы;
- `public` — ключ SNMP community;
- `t 536531000` — время работы системы;
- `1.3.6.1.4.1.53647.50.110.6.0 s "2023-10-24 10:10:10"` и другие — значения полей alert-trap.

ГЛАВА 5. НАСТРОЙКА RSYSLOG

В главе представлено описание настроек отправки и получения логов и уведомлений через «rsyslog». Вам доступны следующие операции:

- *Настройка отправки и получения логов на СХД (стр. 12)*;
- *Настройка отправки и получения уведомлений на СХД (стр. 12)*;
- *Настройка получения логов и уведомлений на Linux-системе (стр. 12)*.

«rsyslog» – сервис для Linux-систем, предназначенный для управления журналами событий (далее – логами), в том числе уведомлений. Сервис поддерживает приём данных по протоколу Syslog из разных источников, их фильтрацию, преобразование и отправку.

Syslog – протокол для отправки и получения сообщений между устройствами или приложениями по сети по протоколам UDP и TCP. Структура сообщений в Syslog включает приоритет, временную метку, имя хоста, имя приложения, идентификатор процесса и текст сообщения.

Уведомления от СХД передаются в формате CEF. *CEF* (англ. аббр. «Common Event Format», «общий формат событий») – независимый от поставщика устройств формат для логирования данных из устройств и приложений. Формат был разработан специально для решений по управлению информацией и событиями безопасности (англ. «Security Information and Event Management», англ. аббр. «SIEM»).

Структура CEF:

```
CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension
```

Пример уведомления в формате CEF:

```
May 27 15:38:43.218289 0OY5CC rdnotify[81421]: CEF:0|Raidix||5.3.1|100|system.state|10|src=10.78.188.121 msg=The system
 is in NORMAL state. spt=514 shost=0OY5CC
```

Описание структуры CEF:

Поле	Назначение
CEF:Version	Обязательный префикс с версией CEF.
Device Vendor	Имя вендора продукта.
Device Product	Имя продукта. В RAIDIX 5.3.1 значение всегда пустое.
Device Version	Версия ПО RAIDIX.
Signature ID	Уникальный идентификатор типа события. В RAIDIX 5.3.1 значение всегда **100**.
Name	Тип объекта и, если применимо, имя объекта события.
Severity	Важность события. В зависимости от типа уведомления: • **0** – уведомления с типом «информация». • **5** – уведомления с типом «предупреждения». • **10** – уведомления с типом «ошибки».

Поле	Назначение
Extension	Дополнительные поля: • msg – текст уведомления. • spt – порт источника события (контроллера СХД). • src – IP-адрес источника события (контроллера СХД). • shost – имя устройства источника (контроллера СХД).

Особенности и ограничения

- Для отправки с СХД доступны логи только уровня **info**.
- С СХД отправляются все уведомления без возможности фильтрации по типу и объекту.
- Отправка доступна только для *одной* принимающей системы.
- В DC-системе настройки на одном контроллере автоматически применяются на втором.
- Если «rsyslog» настроен на контроллере, не входящем в DC, после включения DC-режима настройте «rsyslog» на другом контроллере вручную.

Настройка отправки и получения логов на СХД

Выполните команду

```
$ rdcli param logger modify [-ra <remote_address>] [-rpo <remote_port>] [-rpr <remote_protocol>] [-re 1]
```

где

`<remote_address>` – IP-адрес принимающей системы;
`<remote_port>` – номер порта принимающей системы;
`<remote_protocol>` – транспортный протокол.
`-re 1` – включение отправки логов.

> Подробнее о командах см. в «Справочнике CLI RAIDIX 5.3.1».

Настройка отправки и получения уведомлений на СХД

Выполните команду

```
$ rdcli notify syslog profile modify [-a <remote_address>] [-po <remote_port>] [-pr <remote_protocol>] [-e 1]
```

где

`<remote_address>` – IP-адрес принимающей системы;
`<remote_port>` – номер порта принимающей системы;
`<remote_protocol>` – транспортный протокол.
`-e 1` – включение отправки уведомлений.

> Подробнее о командах см. в «Справочнике CLI RAIDIX 5.3.1».

Настройка получения логов и уведомлений на Linux-системе

> Для настройки принимающей системы необходимы права root.

На принимающей Linux-системе конфигурация «rsyslog» едина для логов и уведомлений.

1. Создайте файл `/etc/rsyslog.d/some_name.conf` и пропишите настройки сервиса «rsyslog» для получения логов и уведомлений с СХД.

   Пример конфигурации для протокола TCP с сохранением уведомлений в файл `/var/log/remote-CEF.log` и логов в файл `/var/log/remote-%HOSTNAME%/%PROGRAMNAME%.log`:

```
module(load="imtcp" MaxSessions="500")
input(type="imtcp" port="514" ruleset="remote")
template(name="RemoteCEF" type="string" string="/var/log/remote-CEF.log")
template(name="RemoteHost" type="string" string="/var/log/remote-%HOSTNAME%/%PROGRAMNAME%.log")
ruleset(name="remote") {
    if $msg startswith " CEF" then {
        action(type="omfile" dynaFile="RemoteCEF")
        stop
    }

    action(type="omfile" dynaFile="RemoteHost")
    stop
}
```

   > Для настройки через UDP замените в конфигурации модуль `imtcp` на `imudp`.

   Описание параметров, используемых в примерах, см. в разделе *Параметры конфигурации «rsyslog» (стр. 13)*. Полная информация о сервисе «rsyslog» доступна на *официальном сайте rsyslog*.

2. Перезапустите сервис **rsyslog**:

```
# systemctl restart rsyslog.service
```

Чтобы отправить тестовое уведомление, после настройки СХД и принимающей стороны, на контроллере выполните

```
$ rdcli notify syslog test
```

Пример тестового уведомления:

```
Jun 19 17:21:59.098126 0OY5CC rdcmd[2395939]: CEF:0|Raidix||5.3.1|100|test|10|src=10.78.188.121 spt=514 shost=0OY5CC
 msg=Test CEF message
```

Пример сортировки получаемых логов с DC-системы с контроллерами «pro10» и «pro9»:

```
# ls /var/log/remote-pro10
attomdnsd.log  kernel.log  login-hook.log  rdbroker.log  rdconfig.log  rdmetadata.log  rdscan.alua_scst_watch.log
 rdscan.net_watch.log     rdscan.raid_watch.log  rsyslogd.log  sshd.log
crond.log       ledmon.log  multipath.log   rdcmd.log     rdhb.log      rdnotify.log    rdscan.log
 rdscan.nvmeof_watch.log  rdstat.log             smartd.log    sudo.log

# ls /var/log/remote-pro9/
crond.log  kernel.log     rdbroker.log  rdhb.log        rdscan.alua_scst_watch.log  rdscan.mpath_watch.log
 rdscan.nvme_fabrics_subsystem_wa.log  rdscan.raid_watch.log  run-parts.log  sudo.log
CROND.log  multipath.log  rdcmd.log     rdmetadata.log  rdscan.drive_watch.log      rdscan.net_watch.log
 rdscan.nvmeof_watch.log               rsyslogd.log           sshd.log
```

Параметры конфигурации «rsyslog»

В секции представлено описание параметров конфигурационного файла «rsyslog», используемых в примерах. Полная информация о сервисе «rsyslog» доступна на *официальном сайте rsyslog*.

Параметр	Значение	Описание
module	load	Модуль для загрузки сообщений. **imtcp** – обеспечивает отправку syslog-сообщений через TCP. **imudp** – обеспечивает отправку syslog-сообщений через UDP.
	MaxSessions	Максимальное количество сессий для модуля TCP.

Параметр	Значение	Описание
input	type	Тип модуля входных параметров.
	port	Порт сервера.
	ruleset	Имя используемого набора правил.
template	name	Имя шаблона.
	type	Тип шаблона. **string** – содержит строку с шаблоном, который будет применён.
	string	Текст строки для типа шаблона «string».
ruleset	name	Имя набора правил.