



RAIDIX 5.2.4

Руководство по мониторингу

Редакция 1

2024

Содержание

Глава 1. Об этом руководстве.....3

Глава 2. Настройки СХД..... 4

 Подключение к пользовательскому веб-интерфейсу..... 4

 Настройка SNMP..... 4

Глава 3. Настройка интеграции с Zabbix.....12

Глава 4. Перечень SNMP Traps..... 14

Глава 5. Настройка rsyslog.....15

ГЛАВА 1. ОБ ЭТОМ РУКОВОДСТВЕ

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

ГЛАВА 2. НАСТРОЙКИ СХД

Подключение к пользовательскому веб-интерфейсу

Подключение к RAIDIX WEB UI

Подключение к интерфейсу RAIDIX WEB UI 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 узла системы.
3. Введите имя и пароль учетной записи и кликните **Войти**.

Настройка SNMP

Настройка SNMP-агента с использованием SNMPv2

1. Откройте страницу **Система > Уведомления**.
2. Кликните **SNMP**.
3. В секции **Параметры SNMP-агента**:
 - a. переведите переключатель в положение **Включен**;
 - b. в списке **Версия SNMP** выберите 2;
 - c. добавьте IP-адрес и укажите порт SNMP-агента;
 - d. укажите сообщество (по умолчанию **public**);
 - e. кликните **Применить**.

Параметры SNMP-агента

Включен☐

Версия SNMP

2

▼

IP-адреса

IP-адрес

Добавить IP-адрес

Порт

161

Сообщество

public

ПРИМЕНИТЬ

ОТМЕНА

Скачать MIB-файл

Настройка SNMP-агента с использованием SNMPv3

1. Откройте страницу Система > Уведомления.
2. Кликните **SNMP**.
3. В секции **Параметры SNMP-агента**:

- a. переведите переключатель в положение **Включен**;
- b. в списке **Версия SNMP** выберите **3**;
- c. укажите необходимые параметры SNMP-агента;
- d. кликните **Применить**.

Параметры SNMP-агента

Включен

Версия SNMP

3

IP-адреса

IP-адрес

Добавить IP-адрес

Порт

161

Имя пользователя

Протокол аутентификации

md5

Пароль аутентификации

Мастер-ключ аутентификации

Engine Id

Локализованный ключ аутентификации

Протокол шифрования

des

Пароль конфиденциальности

Мастер-ключ конфиденциальности

Конфиденциальный локализованный ключ

ПРИМЕНИТЬ

ОТМЕНА

Скачать MIB-файл

Загрузка MIB-файлов

1. Откройте страницу Система > Уведомления.
2. Кликните SNMP.
3. В секции Параметры SNMP-агента кликните Скачать MIB-файл.

Параметры SNMP-агента

Включен

☒

Версия SNMP

2

▼

IP-адреса

IP-адрес

[Добавить IP-адрес](#)

Порт

161

Сообщество

public

ПРИМЕНИТЬ

ОТМЕНА

Скачать MIB-файл

Создание получателей

1. Откройте страницу Система > Уведомления.
2. Кликните SNMP.
3. В секции Получатели SNMP Trap:

- a. кликните **Добавить получателя**;
- b. выберите типы системных уведомлений и кликните **Применить**:

Типы уведомлений



Имя компонента	Ошибки	Предупреждения	Информация
	☐	☐	☐
Диск	☐	☐	☐
Сеть	☐	☐	☐
Набор резервных дисков	☐	☐	☐
Лицензия	☐	☐	☐
Датчики контроллера	☐	☐	☐
Датчики корзины	☐	☐	☐
Гостевые VM	☐	☐	☐
NVMe-oF	☐	☐	☐
Оптимизатор SAN	☐	☐	☐
Общая папка Samba	☐	☐	☐
Общая папка AFP	☐	☐	☐
Общая папка FTP	☐	☐	☐
Общая папка NFS	☐	☐	☐
ИБП	☐	☐	☐
RAID	☐	☐	☐
LUN	☐	☐	☐
iSCSI	☐	☐	☐
DC	☐	☐	☐

Системные уведомления



ОТМЕНА

ПРИМЕНИТЬ

с. укажите IP-адрес и порт:

IP-адрес

162

Системные уведомления
[Выбрать](#)

СОЗДАТЬ

ОТМЕНА

d. кликните Создать.

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.

i 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:

i 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 узла 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:

i 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

Чтобы настроить интеграцию с Zabbix, в интерфейсе управления Zabbix:

i Подробную информацию по каждой настройке см. в [официальной документации Zabbix](#).

1. Импортируйте шаблон.
2. Создайте «узел сети» для каждого узла СХД.
3. Для узла сети:
 - Назначьте импортированный шаблон.
 - Установите значение для макроса `{ $RAIDIX_IP }` — IP-адрес менеджмент-интерфейса целевого узла RAIDIX.
 - Установите значение для макроса `{ $COOKIEAUTH }` — токен доступа. Если токен не используется, то он перестает действовать через 10-20 минут.

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": "<adm_login>", "password": "<adm_password>"}' https://<node_ip>/api/auth | grep -oP 'connect.sid=([^;]+)'
```

где

`<adm_login>` – логин пользователя СХД с правами администратора;

`<adm_password>` – пароль пользователя СХД с правами администратора;

`<node_ip>` – IP-адрес менеджмент-интерфейса узла СХД.

Настройка интервалов сбора данных

Чтобы настроить интервал сбора данных, в интерфейсе Zabbix:

 Подробную информацию по каждой настройке см. в [официальной документации 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 <code>network.interface</code> .
alertName	1.3.6.1.4.1.53647.50.110.5	Название объекта, такое как <code>RAID</code> .
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 <code>error</code> , <code>warning</code> , <code>info</code> или <code>ok</code> .

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`:

```
snmtrap -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

Для отправки журналов событий (логов) через сервис rsyslog настройте

- отправителя: узел RAIDIX;
- получателя: удалённую Linux-систему.

Настройка отправителя

Чтобы настроить узел RAIDIX для сбора и отправки логов, выполните

```
$ rdcli param logger modify [-ra <remote_address>] [-rp <remote_port>] [-re {yes|no}]
```

где

- **<remote_address>** – IP-адрес удалённой системы для получения логов;
- **<remote_port>** – номер порта удалённой системы для получения логов (по умолчанию – 514);
- **{yes|no}** – включить или выключить отправку логов.

Настройка получателя

Чтобы настроить Linux-систему, принимающую логи:

i Для настройки приёма сообщений необходимы права root.

i В этом примере сообщения будут логироваться в файлы `/var/log/remote-%HOSTNAME%.log`.

1. Создайте или отредактируйте файл `/etc/rsyslog.d/20-raidix-core-from-remote.conf` следующим образом:

```
## Receiving logs from remote hosts

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

Описание используемых настроек:

- module (подробнее на официальном сайте rsyslog.com)
 - load
Модуль для загрузки сообщений.
imtcp – обеспечивает отправку syslog сообщений через TCP.
Подробнее на официальном сайте rsyslog.com
 - MaxSessions
Максимальное количество сессий. По умолчанию: **200**.
- input (подробнее на официальном сайте rsyslog.com)
 - type
Тип модуля входных параметров.
 - port
Порт для TCP-сервера.

■ ruleset

Имя используемого набора правил.

◦ template (подробнее на официальном сайте rsyslog.com)

■ name

Имя шаблона.

■ type

Тип шаблона.

string – содержит шаблонную строку, которая будет применена.

■ string

Текст строки для типа шаблона «string».

◦ ruleset (подробнее на официальном сайте rsyslog.com)

■ name

Имя набора правил.

2. Перезапустите сервис **rsyslog**:

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