


Zabbix-агент

Zabbix-агент — программа контроля локальных ресурсов и приложений (таких как накопители, оперативная память, статистика процессора и т. д.) на сетевых системах. Zabbix-агенты являются чрезвычайно эффективными из-за использования специфических системных вызовов для сбора информации и подготовки статистики.

 В данном разделе приведена информация по настройке агентов. Полная информация по настройке средств мониторинга приведена на странице [Мониторинг серверов и сетей: интеграция с Zabbix \(агент, SNMP, JMX, IPMI\)](#).

Содержание:

- [Установка агентов](#)
 - [Установка в среде ОС Windows](#)
 - [Установка в среде Linux](#)
- [Проверка доступности хостов](#)
- [Настройка узла в Zabbix](#)

Общие сведения

Zabbix agent устанавливается на мониторируемый узел работает в режиме демона. Агент может быть как в активном режиме (сам запрашивает список нужных параметров), так и в пассивном (ждёт запросов от сервера Zabbix). Это мощный механизм проверок, однако информацию с устройства можно получить при помощи других интерфейсов: SNMP, JMX и IPMI. Если настроено несколько, будет выполнен поиск доступных интерфейсов у узла сети в следующем порядке: АгентSNMPJMXIPMI, и узел будет связан с первым подходящим ему интерфейсом. Также доступны проверки через SSH, Telnet, HTTP, ODBS и другие.

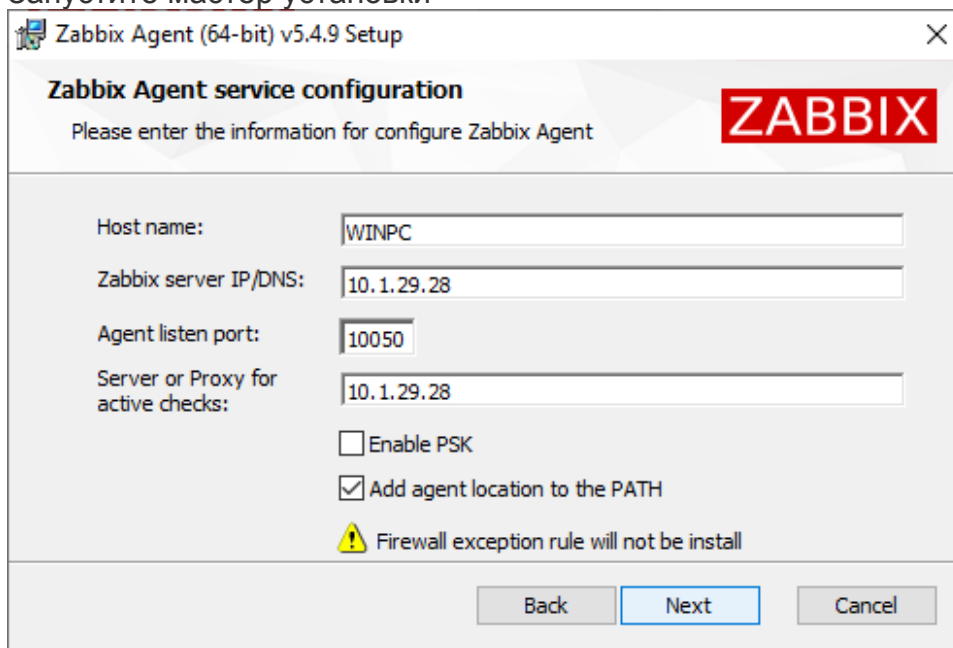
Установка агентов

 Дистрибутивы Zabbix-агентов для различных операционных систем доступны по адресу https://www.zabbix.com/ru/download_agents.

Установка в среде ОС Windows

Установка производится из MSI-инсталлятора с помощью мастера установки. Также доступна установка в silent-режиме.

1. Запустите мастер установки



- a. Проверьте, что имя в поле Host name совпадает с именем текущего узла.
 - b. Укажите IP-адрес Zabbix-сервера, порт по умолчанию: 10050.
 - c. Укажите IP-адрес сервера для активных проверок (чаще всего совпадает с адресом сервера)
- ## 2. Добавьте агент zabbix в исключения брандмауэра Windows.
- a. Выберите Панель управления > Система и безопасность > Брандмауэр защитника Windows > Дополнительные параметры > Правила для входящих подключений > Создать правило».
 - b. Выберите Для программы > Далее > Путь программы.
 - c. Укажите путь к zabbix_agentd > Далее > Разрешить подключение > Далее.
 - d. Оставьте флажки на всех профилях > Далее > Имя – zabbix-agent > Далее.

Установка в среде Linux

Для установки на сервер Платформы НЕЙРОСС, работающий под управлением ОС Ubuntu 18, выполните:

⚠ Ниже приведён вариант установки агента. При отсутствии доступа к сети Интернет, недоступности данного DEB-пакета или наличии ошибок, следуйте инструкции производителя.

1. Скачайте с сайта производителя и установите агент

```
wget https://repo.zabbix.com/zabbix/5.0/ubuntu/pool/main/z/zabbix-release
/zabbix-release_5.0-1+bionic_all.deb
sudo dpkg -i zabbix-release_5.0-1+bionic_all.deb
sudo apt update
sudo apt install zabbix-agent
```

2. Откройте файл конфигурации:

```
sudo nano /etc/zabbix/zabbix_agentd.conf
```

3. В конфигурационный файл добавьте строки:

```
Server=10.0.29.47  
ServerActive=10.0.29.47  
EnableRemoteCommands=1
```


Где:

Server — IP-адрес сервера Zabbix;

ServerActive — адрес сервера для активных проверок (чаще всего совпадает с адресом сервера);

Hostname — имя текущего хоста; отсылается агентом на сервер, который пересылает список активных проверок для хоста с указанным именем; имя должно совпадать с тем именем, которое указано для хоста в web-интерфейсе Zabbix-сервера;

EnableRemoteCommands=1 — разрешает запуск команд, которые сервер передает агенту; запускать команды будет агент;

 Включать удалённое выполнение команд надо ТОЛЬКО после настройки шифрования между агентом и сервером\прокси.

4. Сохраните изменения: нажмите Ctrl+X, введите Y (для подтверждения изменений) и нажмите Enter.
5. Включите сервис в автозапуск при загрузке системы:

```
sudo systemctl enable zabbix-agent.service
```

6. Перезапустите сервис:

```
sudo systemctl restart zabbix-agent.service
```

7. Откройте порт 10050:

```
sudo iptables -A INPUT -p TCP --dport 10050 -j ACCEPT  
sudo iptables -A OUTPUT -p TCP --dport 10050 -j ACCEPT
```


8. Сохраните правила iptables:

```
sudo iptables -L  
sudo iptables-save > /etc/iptables.rules
```

9. Выполните перезагрузку:

```
sudo reboot
```

Проверка доступности хостов

 Проверка работоспособности проводится посредством службы telnet. Может потребоваться установка службы.

Чтобы убедиться в работоспособности агента:

1. Зайдите на сервер Zabbix и в интерфейсе командной строки выполните:

```
telnet [IP-addr] 10050
```

Где [IP-addr] — Ip-адрес хоста, например:

```
telnet 10.1.29.26 10050
```

2. Если все в порядке, вы увидите:

```
Connected to [IP-addr]  
Escape character is '^'.
```


и через небольшой интервал времени:

```
Connection closed by foreign host.
```

3. Если агент не запущен или не работает, вы увидите:

```
telnet: connect to address [IP-addr]: Connection refused
```

Настройка узла в Zabbix

 Ниже дана краткая информация по добавлению узла. Полное описание настройки Zabbix приведена в разделе [[Мониторинг серверов и сетей: интеграция с Zabbix \(агент, SNMP, JMX, IPMI\)](#)].

Для добавления узла с установленным Zabbix-агентом:

Новый узел сети

Узел сети | IPMI | Теги | Макросы | Инвентаризация | Шифрование | Преобразование значений

* Имя узла сети:

Видимое имя:

Шаблоны:
начните печатать для поиска

* Группы:
начните печатать для поиска

Интерфейсы	Тип	IP адрес	DNS имя	Подключаться через	Порт	По умолчанию
Агент		<input type="text" value="10.1.29.38"/>	<input type="text"/>	<input checked="" type="radio"/> IP <input type="radio"/> DNS	<input type="text" value="10050"/>	<input checked="" type="radio"/> Удалить

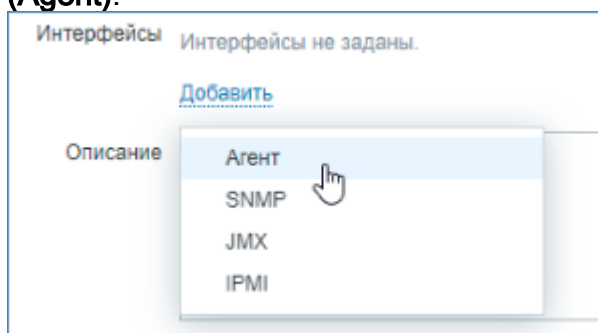
[Добавить](#)

Описание:

Наблюдение через прокси:

Активировано: ☒

1. Введите уникальное **Имя узла (Host name)**, заданное при установке агента.
2. В поле **Видимое имя (Visible name)** впишите имя для отображения в интерфейсах Zabbix и Платформы НЕЙРОСС.
3. В поле **Шаблоны (Templates)** выберите один из шаблонов для узла данного типа. Все объекты (элементы данных (items), триггеры (triggers), графики и группы элементов данных) будут унаследованы из шаблона
4. В поле **Группы (Groups)** выберите группу узлов **NEYROSS**. Узел может принадлежать нескольким группам узлов. Поэтому для работы с интерфейсом Zabbix вы можете использовать и другие группы узлов. Для работы только с Платформой НЕЙРОСС используйте одну группу.
5. В поле **Интерфейсы (Interfaces)** нажмите [Добавить \(Add\)](#) и выберите **Агент (Agent)**.



6. Укажите IP-адрес или DNS-имя узла. Задайте номер TCP/UDP порта. Значения по умолчанию: 10050.
7. Оставьте флаг **Активировано (Enabled)**, чтобы узел сети был активным, готовым к мониторингу. Если не отмечено, узел сети неактивен, его состояния не отслеживаются.
8. Нажмите на кнопку **Добавить (Add)**.