



Учебный центр АйТи Клауд

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ПРОСТЫМ
ЯЗЫКОМ

Преподаватель Груздев Павел Юрьевич

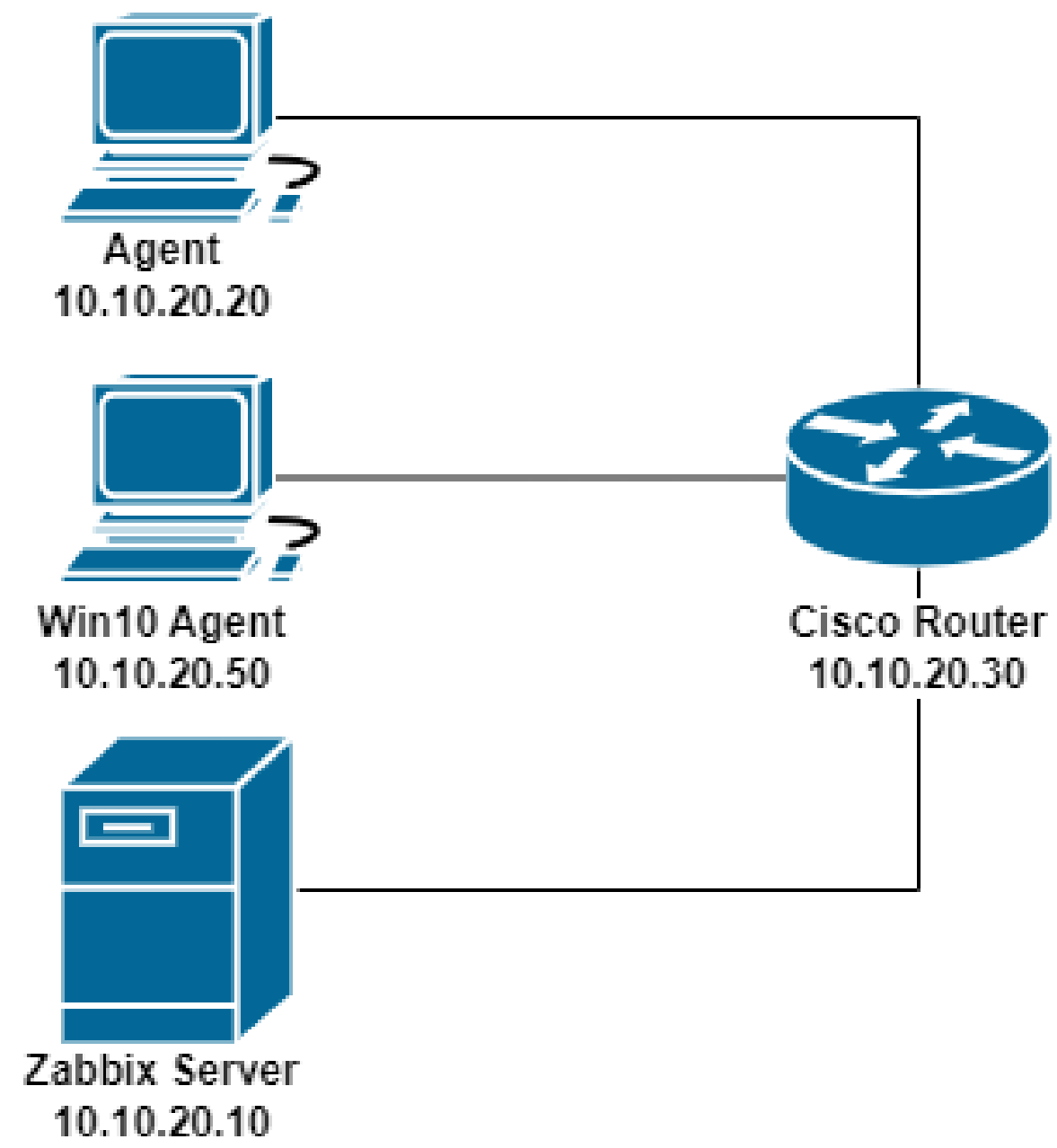
Учебный центр АйТи Клауд

Развертывание инфраструктуры

современные технологии простым языком



Схема стенда



Учебный центр АйТи Клауд

Знакомство с Zabbix

современные технологии простым языком



Что такое Zabbix

Zabbix - это решение распределенного мониторинга корпоративного класса с открытыми исходными кодами.

The logo for Zabbix, featuring the word "ZABBIX" in a bold, white, sans-serif font. The letters are closely spaced and set against a solid red rectangular background.

ZABBIX

Возможности Zabbix

- Сбор данных
- Гибкие определения порогов
- Множество настроек оповещений
- Построение графиков в режиме реального времени
- Возможности веб-мониторинга
- Широкие возможности визуализации
- Хранение данных истории
- Простая настройка
- Использование шаблонов
- Сетевое обнаружение
- Быстрый веб-интерфейс
- Zabbix API
- Система прав доступа
- Полнофункциональный и легко расширяемый агент
- Бинарные демоны
- Готовность к сложным средам

Архитектура Zabbix

- **Сервер** - центральный процесс программного обеспечения Zabbix, который выполняет мониторинг, взаимодействует с прокси и агентами Zabbix, вычисляет триггеры, отправляет оповещения; центральное хранилище данных.
- **База данных** - вся информация о конфигурации, а так же данные, собранные Zabbix, хранятся в базе данных.
- **Веб-интерфейс** - для легкого доступа к Zabbix из любого места и с любой платформы
- **Прокси** - процесс, который может собирать данные от имени Zabbix сервера, перенимая часть нагрузки сервера.
- **Агент** - процесс, разворачиваемый на наблюдаемых целях для активного мониторинга локальных ресурсов и приложений.

Потоки данных



Учебный центр АйТи Клауд

Установка Zabbix сервера

современные технологии простым языком



Системные требования

Размер инсталляции	Кол-во наблюдаемых метрик ¹	Ядра CPU/vCPU	Память (ГБ)	База данных
Маленькая	1 000	2	8	MySQL сервер, Percona сервер, MariaDB сервер, PostgreSQL
Средняя	10 000	4	16	MySQL сервер, Percona сервер, MariaDB сервер, PostgreSQL
Большая	100 000	16	64	MySQL сервер, Percona сервер, MariaDB сервер, PostgreSQL, Oracle
Очень большая	1 000 000	32	96	MySQL сервер, Percona сервер, MariaDB сервер, PostgreSQL, Oracle

¹ 1 метрика = 1 элемент данных + 1 триггер + 1 график

Поддерживаемые платформы

Платформа	Сервер	Агент	Агент 2
Linux	x	x	x
IBM AIX	x	x	-
FreeBSD	x	x	-
NetBSD	x	x	-
OpenBSD	x	x	-
HP-UX	x	x	-
Mac OS X	x	x	-
Solaris	x	x	-
Windows	-	x	x

Требуемое ПО

- Веб сервер:

- Apache
- Nginx

- База данных

- MySQL
- PostgreSQL

Подробнее про системные требования:

<https://www.zabbix.com/documentation/6.4/ru/manual/installation/requirements>

Очень важно иметь точное системное время на сервере с запущенным Zabbix. **ntpd** - один из самых популярных демонов синхронизации времени узла с временем на остальных серверах. Настоятельно рекомендуется поддерживать синхронизированное время на всех системах, где работают компоненты Zabbix.

Настройка брандмауэра

Компонент Zabbix	Номер порта	Протокол
Zabbix агент	10050	TCP
Zabbix агент 2	10050	TCP
Zabbix сервер	10051	TCP
Zabbix прокси	10051	TCP
Zabbix Java gateway	10052	TCP
Zabbix веб-сервис	10053	TCP
Zabbix веб-интерфейс	80	HTTP
	443	HTTPS
Zabbix траппер	10051	TCP

Эти номера портов должны быть открыты в брандмауэре, чтобы подключения Zabbix были разрешены. Исходящие TCP подключения обычно не требуют явных настроек брандмауэра.

Настройка SELinux

Для RHEL 7 (и более поздних версий), AlmaLinux, CentOS Stream, Oracle Linux, Rocky Linux 8 (и более поздних версий):

- `setsebool -P httpd_can_connect_zabbix on`

Если доступ к базе данных осуществляется по сети (в том числе через localhost для PostgreSQL), также разрешите веб-интерфейсу Zabbix подключение к базе данных:

- `setsebool -P httpd_can_network_connect_db on`

Для RHEL до версии 7:

- `setsebool -P httpd_can_network_connect on`
- `setsebool -P zabbix_can_network on`

После применения настроек SELinux перезапустите Apache:

- `systemctl restart httpd`

При желании можно установить пакет **zabbix-selinux-policy** из официального репозитория Zabbix. Это пакет предоставляется для всех поддерживаемых версий операционных систем, чтобы упростить развёртывание Zabbix и предотвратить отключение SELinux пользователями из-за сложности настройки.

Выбор варианта установки

Скачать и установить Zabbix

Пакеты Zabbix

Download and
install Zabbix
for free

Free trial

Zabbix Cloud

Available with
a 5-day free trial

Облачные образы Zabbix

Run Zabbix on
third-party cloud
platforms

Контейнеры Zabbix

Deploy Zabbix
components from
official Zabbix
containers

Готовое решение Zabbix

Run Zabbix from
a pre-configured
Zabbix virtual
appliance

Исходный код Zabbix

Download the
Zabbix source
code

Агенты Zabbix

Download Zabbix
agent for Unix-like
and Windows
environments

Обновление Zabbix между мажорными версиями

1. Остановите процессы Zabbix

```
systemctl stop zabbix-server zabbix-proxy zabbix-agent zabbix-agent2
```

2. Сделайте резервную копию базы данных Zabbix

3. Сделайте резервную копию файлов конфигурации, PHP и бинарных файлов Zabbix

```
mkdir /opt/zabbix-backup/
```

```
cp /etc/zabbix/zabbix_server.conf /opt/zabbix-backup/
```

```
cp /etc/apache2/conf-enabled/zabbix.conf /opt/zabbix-backup/
```

```
cp -R /usr/share/zabbix/ /opt/zabbix-backup/
```

```
cp -R /usr/share/zabbix-* /opt/zabbix-backup/
```

4. Обновите пакет конфигурации репозитория

```
rm -Rf /etc/apt/sources.list.d/zabbix.list
```

```
wget https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-release_latest+debian12_all.deb
```

```
dpkg -i zabbix-release_latest+debian12_all.deb
```

5. Обновите компоненты Zabbix

```
apt install --only-upgrade zabbix-server-mysql zabbix-frontend-php zabbix-agent
```

6. Проверьте параметры конфигурации компонентов

7. Запустите процессы Zabbix

```
systemctl start zabbix-server zabbix-proxy zabbix-agent zabbix-agent2
```

8. Очистите cookies и кэш в веб-браузере

Обновление Zabbix между минорными версиями

Сначала обновите информацию о репозитории:

apt update

Затем, чтобы обновить все компоненты Zabbix, выполните:

apt install --only-upgrade 'zabbix*'

Практическое задание

Выполнить лабораторную работу №1 – Установка Zabbix сервера.

Учебный центр АйТи Клауд

Пользователи и группы пользователей

современные технологии простым языком



Предустановленные пользователи

- *Admin* - Супер пользователь Zabbix с неограниченными правами доступа;
- *guest* - специальный пользователь Zabbix. Пользователь 'guest' по умолчанию деактивирован. Если вы добавите его в группу пользователей Guests, вы сможете получить доступ к страницам мониторинга в Zabbix без необходимости входа в систему. Обратите внимание, что по умолчанию пользователь 'guest' не имеет никаких прав доступа к объектам в Zabbix.

Типы пользователей

- *Пользователь* - по умолчанию имеет ограниченный доступ к разделам меню и не имеет доступа к ресурсам.
- *Администратор* - имеет неполный доступ к разделам меню. По умолчанию не имеет доступа к группам узлов сети.
- *Суперадминистратор* - имеет доступ ко всем разделам меню. Имеет доступ с правом чтения/записи ко всем группам узлов сети и шаблонов.

Роли пользователей

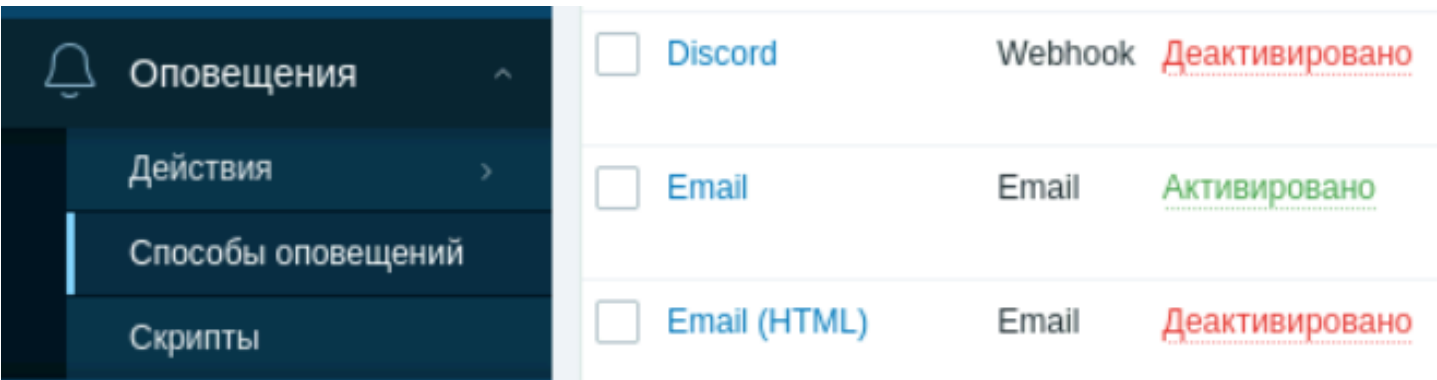
- Роли пользователей позволяют по необходимости изменять права доступа, определенные типом пользователя. Права доступа нельзя добавить сверх установленных для типа пользователя, но можно отозвать какие-то из них.
- Также роль пользователя определяет доступ не только к разделам меню, но и к услугам, модулям, методам API и различным действиям в веб-интерфейсе.

Группы пользователей

- Группы пользователей позволяют группировать пользователей для организационных целей и для назначения прав доступа к данным. Права доступа к наблюдаемым данным групп узлов сети назначаются на группы пользователей, а не индивидуально пользователям.
- Пользователь может входить в любое количество групп.

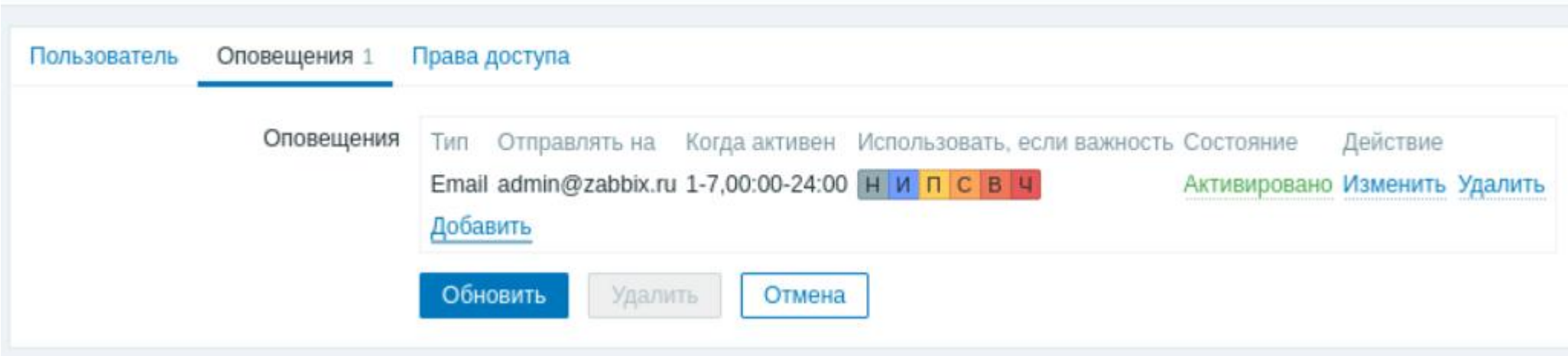
Оповещения пользователей

- Для того, чтобы иметь возможность получать оповещения – необходимо их включить в «Оповещения» - «Способы оповещений»



- Чтобы пользователь получал оповещения по конкретному способу оповещения, необходимо в профиле этого пользователя указать канал связи для этого способа оповещения. Например, действие, которое отправляет сообщения пользователю "Admin" с использованием вебхука "X", всегда будет сообщать об ошибке отправки, если в профиле пользователя не указан канал связи для вебхука "X".

Пользователи



Практическое задание

Выполнить лабораторную работу №2 – Создание и настройка пользователей.

Учебный центр АйТи Клауд

Узлы сети и группы узлов сети

современные технологии простым языком



Узлы сети и группы узлов сети

Host

HostIPMITagsMacros 5Inventory ●EncryptionValue mapping

* Host name

Zabbix server

Visible name

Zabbix server

Templates

Name	Action
Linux by Zabbix agent	Unlink Unlink and clear
Zabbix server health	Unlink Unlink and clear

type here to search

* Host groups

Zabbix servers

type here to search

Interfaces

Type	IP address	DNS name
Agent	127.0.0.1	
▼ SNMP	127.0.0.1	

Add

Description

Monitored by proxy

(no proxy) ▼

Enabled

☒

Инвентаризация

- Ручной режим
- Автоматический режим
- Деактивировано

Массовое обновление

Mass update

Host

IPMI

Tags

Macros

Inventory

Encryption

Value mapping

Link templates

☒

Link

Replace

Unlink

type here to search

Select

☐ Clear when unlinking

Host groups

☒

Add

Replace

Remove

type here to search

Select

Description

☐

Original

Monitored by proxy

☐

Original

Status

☐

Original

Update

Cancel

Шаблоны

Новый шаблон

Шаблон Теги Макросы Преобразование значений

* Имя шаблона

Видимое имя

Шаблоны

Выбрать

* Группы шаблонов

Выбрать

Описание

Практическое задание

Выполнить лабораторную работу №3 – Создание узла сети.

Учебный центр АйТи Клауд

Элементы данных

современные технологии простым языком



Элементы данных

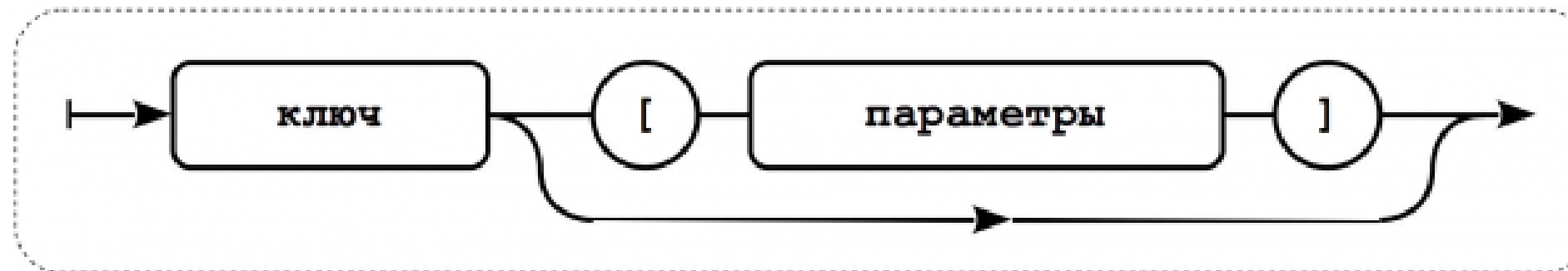
- Элементы данных являются теми сущностями, которые собирают данные с узлов сети.
- Ключ элемента данных – тип данных которые мы собираем
- Имя ключа может содержать в себе 0-9a-zA-Z_-.

Пример:

icmping[<цель>,<пакеты>,<интервал>,<размер>,<время ожидания>]

<параметр1> - не обязателен, при использовании ключа

параметр2 - обязателен при использовании ключа



Переменные интервалы

Интервал	Период	Описание
10	1-5,09:00-18:00	Элемент данных будет опрашиваться каждые 10 секунд в течение рабочего времени.
0	1-7,00:00-7:00	Элемент данных не будет опрашиваться в течение ночи.
0	7-7,00:00-24:00	Элемент данных не будет опрашиваться по воскресеньям.
60	1-7,12:00-12:01	Элемент данных будет опрошен ровно в 12:00 каждый день. Обратите внимание, что такой формат использовался как обходной путь при опросе по расписанию, и, начиная с Zabbix 3.0, рекомендуется использовать интервалы по расписанию для таких проверок.

Интервалы по расписанию

Префикс	Описание	<от>	<до>
md	Дни месяца	1-31	1-31
wd	Дни недели	1-7	1-7
h	Часы	0-23	0-23
m	Минуты	0-59	0-59
s	Секунды	0-59	0-59

Интервал	Когда выполняется
m0-59	каждую минуту
h9-17/2	каждые 2 часа, начиная с 9:00 (9:00, 11:00 ...)
m0,30 или m/30	каждый час в чч:00 и чч:30
m0,5,10,15,20,25,30,35,40,45,50,55 или m/5	каждые пять минут
wd1-5h9	каждый день с понедельника по Пятницу в 9:00
wd1-5h9-18	каждый день с понедельник по Пятницу в 9:00,10:00,...,18:00
h9,10,11 или h9-11	каждый день в 9:00, 10:00 и 11:00
md1h9m30	каждое первое число каждого месяца в 9:30
md1wd1h9m30	каждое первое число каждого месяца в 9:30, если этот день понедельник
h9m/30	каждый день в 9:00, 9:30

Типы элементов данных

- Zabbix агент
- SNMP агент
- SNMP трапы
- Проверки IPMI
- Простые проверки
- Мониторинг файлов журналов
- Вычисляемые элементы данных
- Внутренние проверки
- Проверки через SSH
- Проверки через Telnet
- HTTP агент
- Внешние проверки
- Скриптовые элементы данных

Пользовательские параметры

1) Настройка файла конфигурации агента (zabbix_agent2.conf или zabbix_agentd.conf):

UserParameter=ключ[*],команда_или_скрипт

Пример:

UserParameter=system.custom.metric,/etc/zabbix/scripts/custom_monitor.sh

Содержание /etc/zabbix/scripts/custom_monitor.sh:

```
#!/bin/bash
```

```
# Проверка доступности сервиса
```

```
if systemctl is-active --quiet nginx; then
```

```
    echo 1
```

```
else
```

```
    echo 0
```

```
fi
```

Пользовательские параметры (продолжение)

2) Перезагрузка агента

sudo systemctl restart zabbix-agent.service

3) Создание элемента данных

Новый элемент данных

Элемент данных

Теги

Предобработка

* Имя Проверка статуса сервиса Nginx

Тип Zabbix агент

* Ключ system.custom.metric

Выбрать

Тип информации Числовой (целое положительное)

Использование Zabbix агента

- Zabbix агент
 - Эти проверки используют общение с Zabbix агентом для сбора данных.
 - Существуют пассивные и активные проверки. При настройке элемента данных, вы можете выбрать требуемый тип:
 - *Zabbix агент* - для пассивных проверок
 - *Zabbix агент (активный)* - для активных проверок

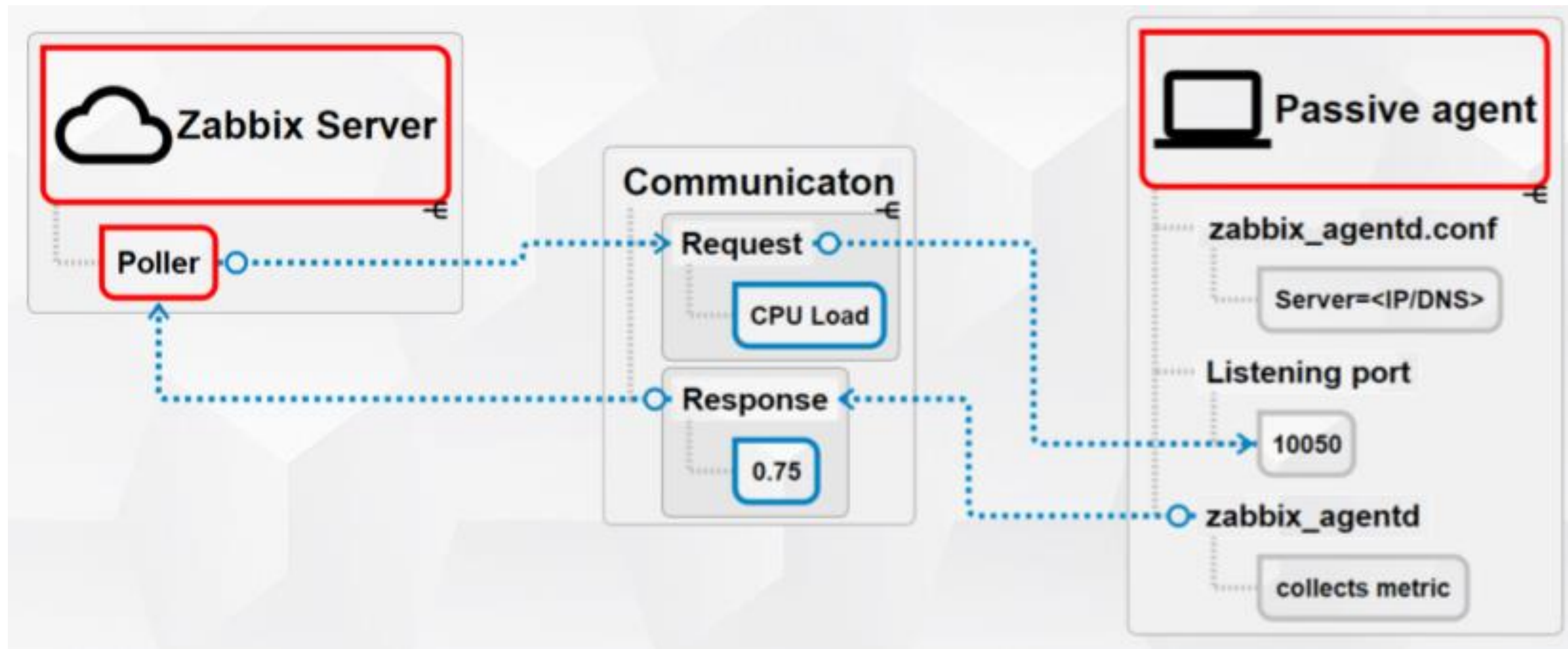
Пассивные проверки

- Пассивная проверка - это простой запрос данных.
 - ❖ Zabbix сервер или прокси запрашивает данные (например, CPU load) и Zabbix агент отправляет результат проверки обратно серверу (прокси).
- Настройка узла сети в веб-интерфейсе:
 - ❖ Настройка > Узлы сети > {host} > IP/DNS интерфейса и Порт

Интерфейсы	Тип	IP адрес	DNS имя	Подключаться через	Порт	По умолчанию
	Агент	127.0.0.1	zabbix-agent	☐ IP ☒ DNS	10050	☒ Удалить

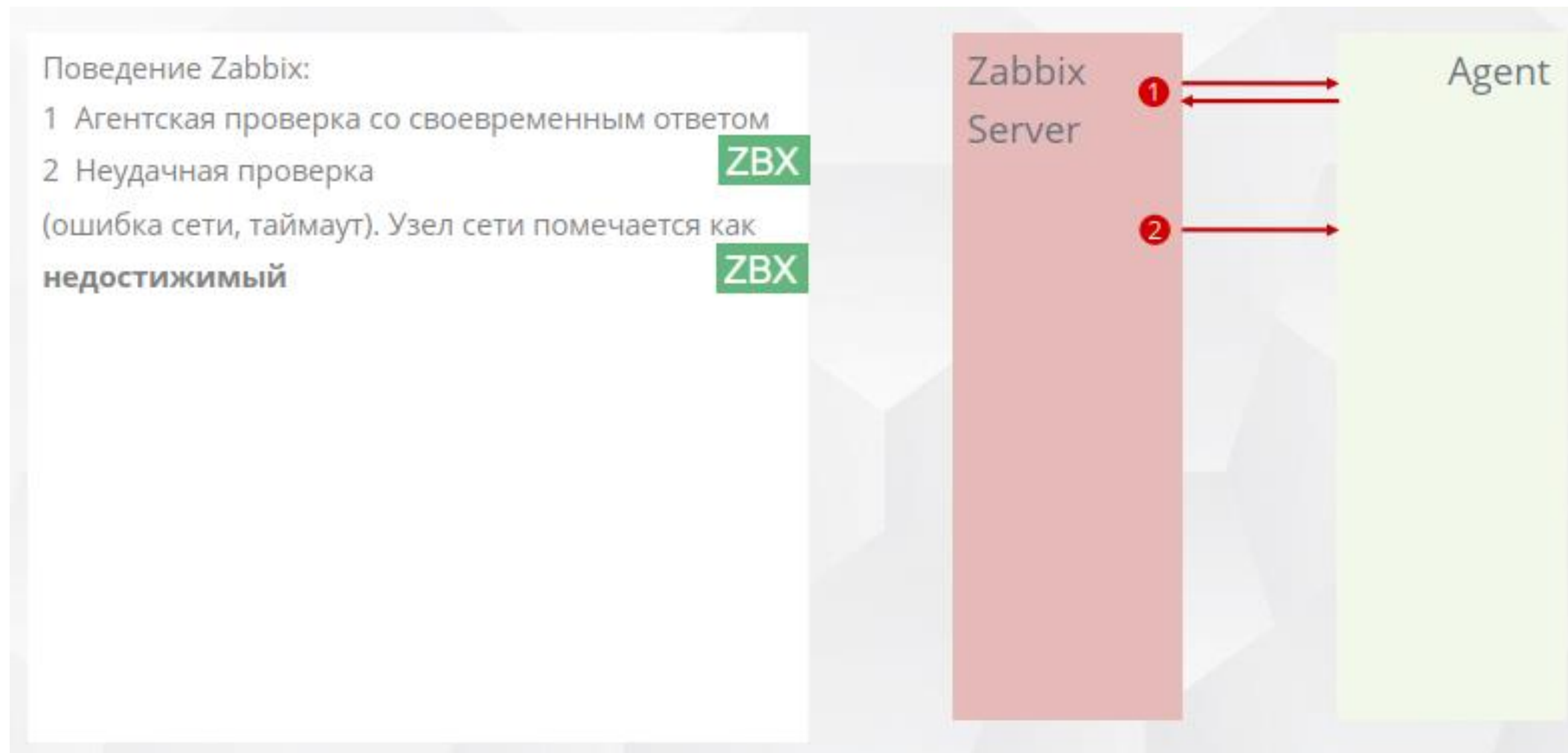
- zabbix_agentd.conf:
 - ❖ Server=IP/DNS
 - Например: Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,example.com
 - ❖ Дополнительно: порт по умолчанию (TCP/10050) можно изменить в настройках файла конфигурации агента:
 - Например: ListenPort=10050

Пассивные проверки



Поведение Zabbix сервера в зависимости от результата проверки

- Следующие настройки определяют, как Zabbix сервер должен вести себя, когда проверку (Zabbix, SNMP, IPMI, JMX) не возможно выполнить, и сервер/устройство недоступно.



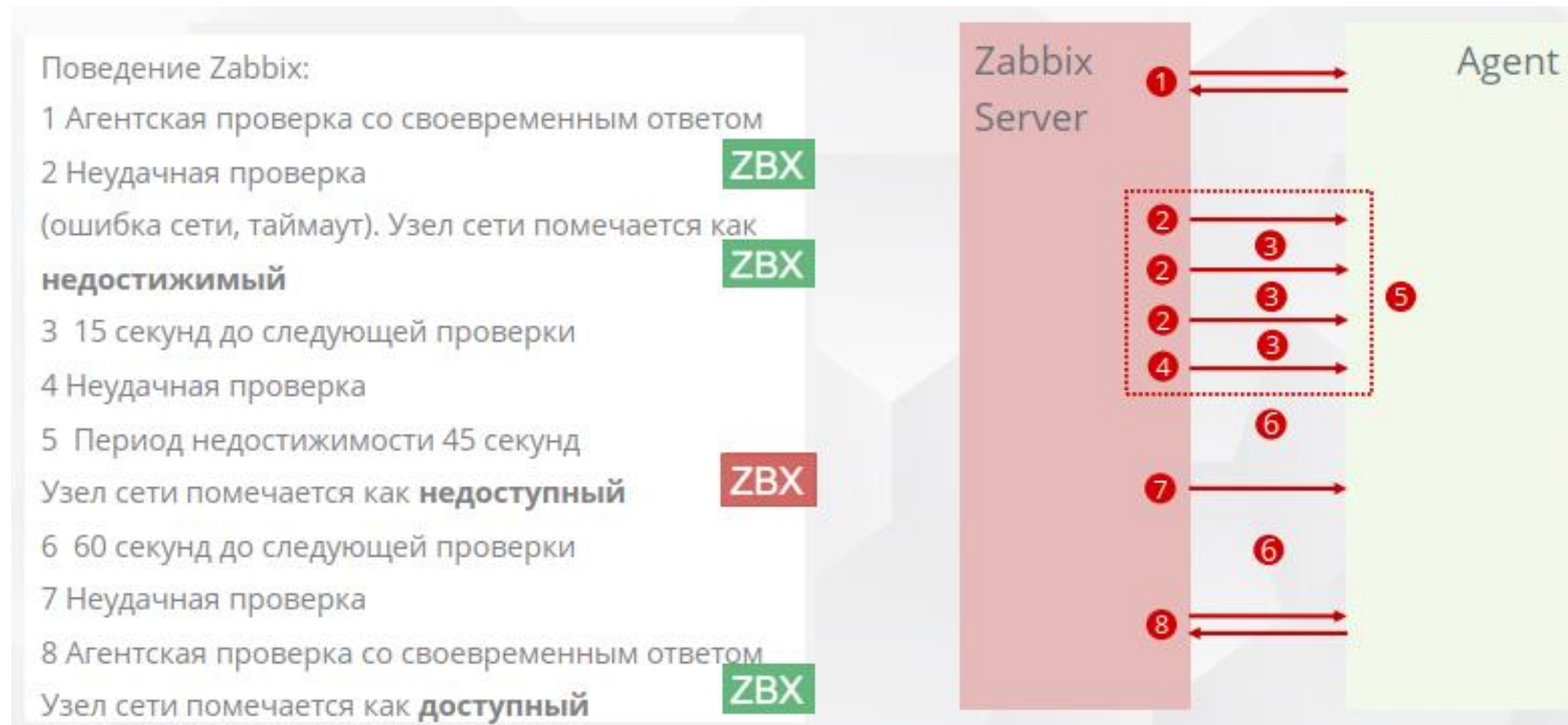
Настройки недоступности и недоступности

3 - UnreachableDelay

- Как часто недоступный узел сети будет перепроверяться одним из элементов данных соответствующего типа (15 секунд).

5 - UnreachablePeriod

- Общая продолжительность периода недоступности (45 секунд).

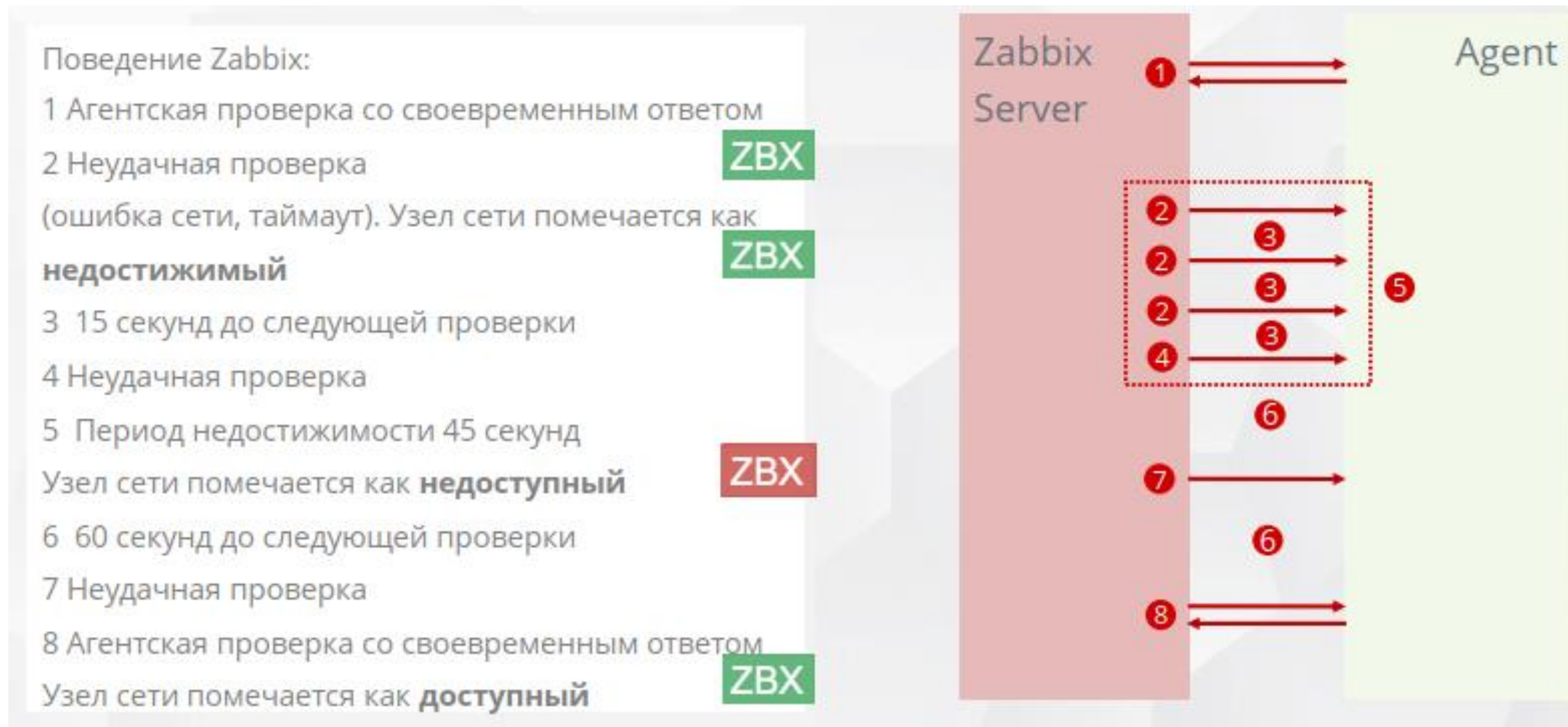


Настройки недоступности и недоступности

5 – Когда UnreachablePeriod закончился, но узел сети так и не ответил – он помечается как недоступный

6 - UnavailableDelay

- Как часто узел сети проверяется, когда он в состоянии недоступности.



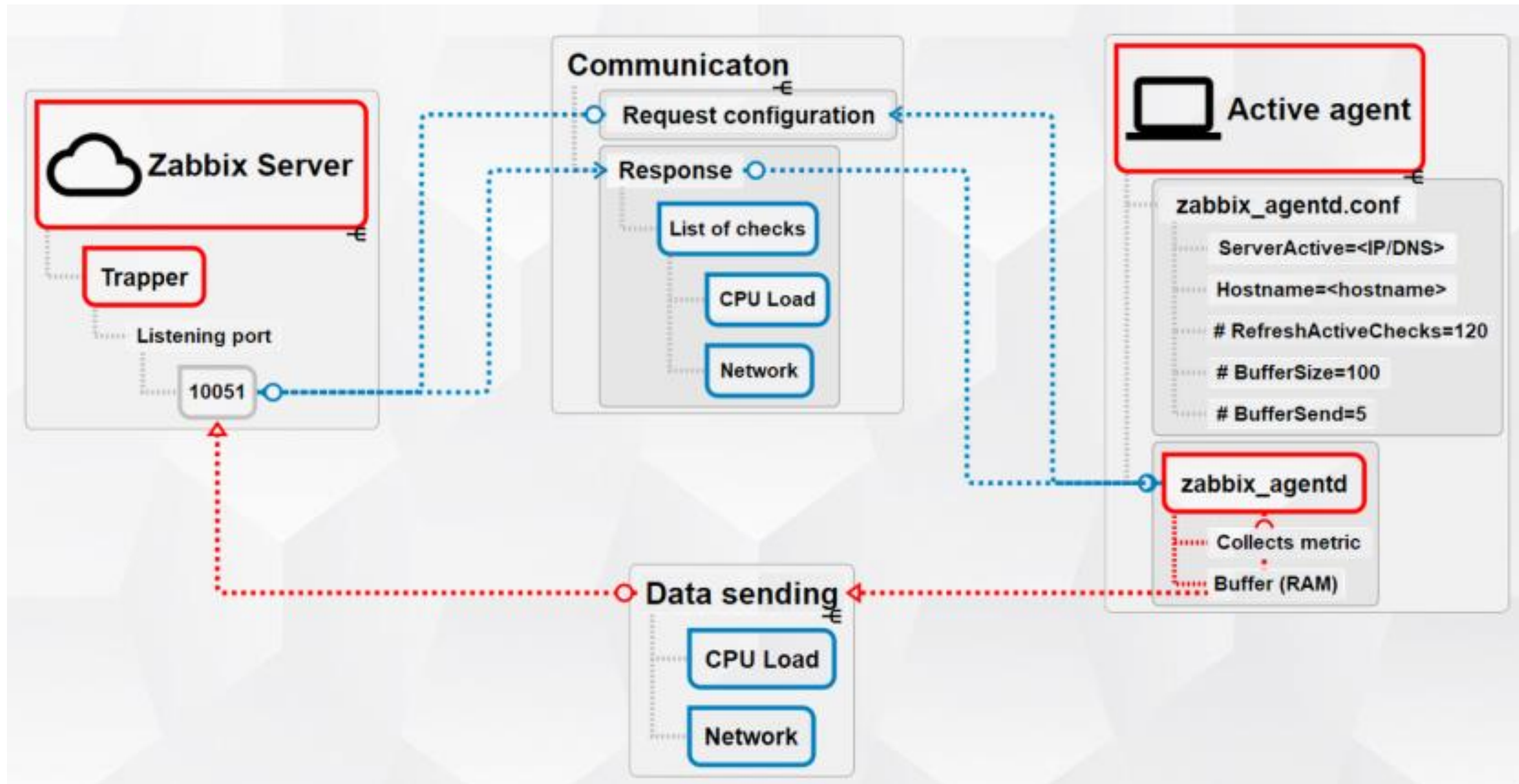
Основные ключи элементов данных

Область мониторинга	Предлагаемый ключ
Имя узла сети	system.hostname[<type>]
Доступность	agent.ping
Удаленные службы	net.tcp.service[service,<ip>,<port>]
Процессы	proc.num[<name>,<user>,<state>,<cmdline>]
Доступное место на диске	vfs.fs.size[fs,<mode>]
Количество объектов в папке	vfs.dir.count[dir]
Сеть	net.if.in/out/total[interface]
Доступная память	vm.memory.size[<mode>]
Загрузка CPU (Unix)	system.cpu.load[<cpu>,<mode>]
Утилизация CPU (Win)	system.cpu.util[<cpu>,<type>,<mode>]

Активные проверки

- Активные проверки требуют более сложной обработки.
 - ❖ Агент получает список элементов данных от Zabbix сервера для сбора данных:
 - При старте агента
 - Каждые 120 секунд
 - ❖ Периодически пакетно отправляет собранные значения серверу:
 - Каждые 5 секунд и очищает буфер
 - Когда буфер заполнен (если это случиться быстрее, чем за 5 секунд)
 - Локальное время используется для метки времени собранных значений
 - ❖ Может буферизировать данные в памяти при отсутствии связи:
 - По умолчанию размер буфера – 100 значений Zabbix сервер или прокси запрашивает данные (например, CPU load) и Zabbix агент отправляет результат проверки обратно серверу (прокси).

Активные проверки – поток данных



Активные проверки настройки

Настройки узла сети в веб-интерфейсе:

❖ Настройки > Узлы сети > {host}

- Явно установлено: «Имя узла сети» = student-XX

zabbix_agentd.conf

ServerActive=<IP/DNS>

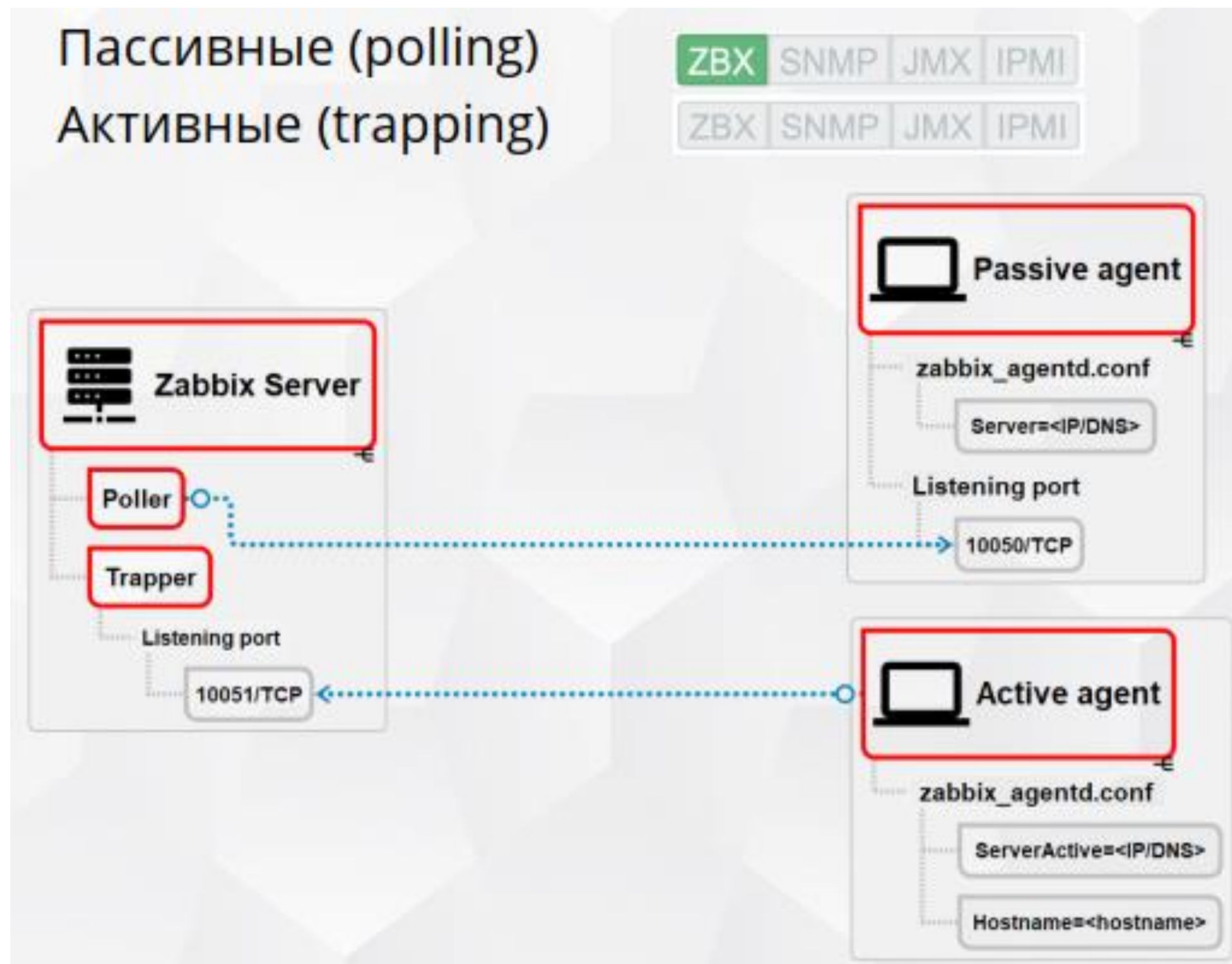
Hostname=student-XX

#HostnameItem=system.hostname

Автоматически использует system.hostname, если оба параметра не заданы.



Пассивные vs активные проверки



Zabbix get

`zabbix_get` — это утилита командной строки, которая используется для получения данных от агента Zabbix.

Синтаксис:

`zabbix_get -s имя-узла-сети-или-IP [-p номер-порта] [-I IP-адрес] [-t тайм-аут] -k ключ-элемента-данных`

Пример:

```
zabbix_get -s 127.0.0.1 -p 10050 -k "system.cpu.load[all,avg1]"
```

Zabbix sender

zabbix_sender — это утилита командной строки для отправки значений мониторинга на Zabbix сервер или Zabbix прокси. На Zabbix сервере должен быть создан элемент данных типа Zabbix траппер с соответствующим ключом.

Синтаксис:

`zabbix_sender [-v] -z сервер [-p порт] [-I IP-адрес] [-t тайм-аут] -s узел-сети -k ключ -o значение`

Пример:

`zabbix_sender -z <IP адрес сервера> -p 10051 -s "New host" -k trap -o "тестовое значение"`

Zabbix trapper

Item Tags Preprocessing

* Name

Trapper item

Type

Zabbix trapper

* Key

trap

Select

Type of information

Text

* History

Do not store

Store up to

31d

Allowed hosts

Populates host inventory field

-None-

Description

Enabled

☒

Add

Test

Cancel

Практическое задание

Выполнить лабораторные работы:

№4 – Безагентный мониторинг – простые проверки

№5 – Установка и настройка агента на ОС Windows

№6 – Установка и настройка агента на ОС GNU/Linux

№7 – Пассивные проверки

№8 – Активные проверки

№9 – Активные проверки Windows

Учебный центр АйТи Клауд

Триггеры

современные технологии простым языком



Триггеры – Обзор

Триггеры - это логические выражения, которые «оценивают» собранные данные.

- ⚡ Представляют текущее состояние системы.
- ⚡ Позволяют определить пороговые значения (какое состояние данных можно считать приемлемым , а какое нет).
- ⚡ Триггер может находиться в одном из двух статусов:

ОК

Нормальное состояние триггера

ПРОБЛЕМА

Произошло что-то требующее внимания

- ⚡ Когда триггер меняет состояние – создается новое событие.
- ⚡ Если триггер переходит в состояние ПРОБЛЕМА, это также называется – «сработал».
- ⚡ Состояние триггера (выражение) пересчитывается каждый раз, когда Zabbix сервер получает новое значение элемента данных, который участвует в выражении.
- ⚡ Триггеры вычисляются только на основании данных истории, данные динамики изменений не участвуют.
- ⚡ Возможно построение триггерных выражений разной степени сложности.

Триггеры – Настройка

Настройка > Узлы сети > Триггеры > Создать триггер

* Name	High CPU utilization (over {CPU.UTIL.CRIT}% for 5m)					
Operational data	Current utilization: {ITEM.LASTVALUE1}					
Severity	Not classified	Information	Warning	Average	High	Disaster
* Expression	{Template Module Linux CPU by Zabbix agent:system.cpu.util.min(5m)}>{CPU.UTIL.CRIT}					Add
	Expression constructor					
OK event generation	<input checked="" type="button" value="Expression"/> Recovery expression None					
PROBLEM event generation mode	<input checked="" type="button" value="Single"/> Multiple					
OK event closes	<input checked="" type="button" value="All problems"/> All problems if tag values match					
Allow manual close	☐					
URL						
Description	CPU utilization is too high. The system might be slow to respond.					

Имя и важность триггера

Имя триггера

⚡ Поддерживаются макросы:

- {HOST.HOST}, {HOST.NAME}, {HOST.CONN}, {HOST.DNS}, {HOST.IP}, {ITEM.VALUE}
- Пользовательские макросы {\$MACRO}

⚡ Например:

- Сервер mail.example.com не доступен
- Высокая загрузка CPU на db2.example.com
- Служба "DHCP" (DHCP Client) не запущена

⚡ Использование макросов делает имя триггера динамичным и дает дополнительную информацию об элементах данных или их значениях.

Оперативные данные:

⚡ Можно задать произвольной строкой вместе с макросами (информативно)

⚡ Макросы будут динамически раскрываться в текущие данные в Мониторинг > Проблемы

⚡ Если не настроено, будут отображаться последние значения по каждому элементу данных из выражения триггера

Важность триггера:

Severity

Not classified

Information

Warning

Average

High

Disaster

Триггеры – синтаксис выражения

Упрощенно выражение триггера можно представить в следующем виде:

функция(/узел сети/ключ,параметр)<оператор><константа>

Например:

min(/Zabbix server/net.if.in[eth0,bytes],5m)>100K

Функции: min(), max(), avg(), last(), diff(), count(), delta() и многие другие

Операторы: -, *, /, +, <, <=, >, >=, =, <>, and, not, or

Параметры:

sum(/узел сети/ключ,**10m**) - Сумма значений за последние 10 минут.

sum(/узел сети/ключ,**#10**) - Сумма последних десяти значений.

Сдвиг по времени: avg(/узел сети/ключ,1h:now-1d)

Триггеры – примеры

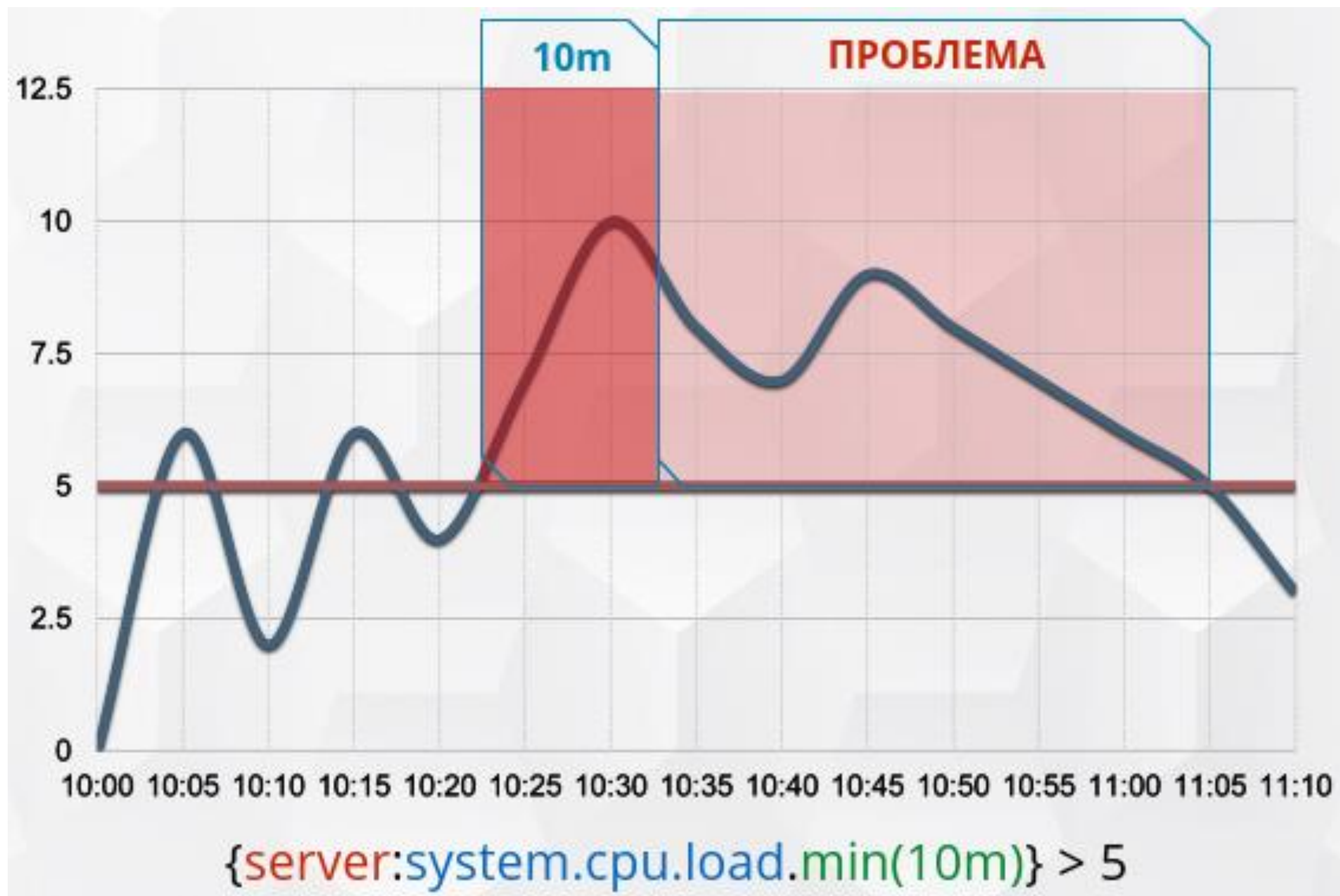
`last(/Zabbix server/system.cpu.load[all,avg1])>5`

`last(/www.example.com/system.cpu.load[all,avg1])>5 or min(/www.example.com/system.cpu.load[all,avg1],10m)>2`

`last(/www.example.com/vfs.file.cksum[/etc/passwd],#1)<>last(/www.example.com/vfs.file.cksum[/etc/passwd],#2)`

`min(/www.example.com/net.if.in[eth0,bytes],5m)>100K`

Чувствительность триггеров



Выражение триггера

Выражение триггера можно добавить или изменить:

⚡ Вручную (набрать соответствующий текст в поле Выражение)

* Expression Add

⚡ При помощи помощника (Нажав кнопку «Добавить»)

Condition

* Item student-XX: CPU load Select

Function last() - Last (most recent) T value

Last of (T) Count

Time shift Time

* Result >

Insert Cancel

Выражение триггера

«Конструктор выражения» может помочь при создании более сложных условий

* Problem expression

Edit Insert expression

And Or Replace

A or B

Target	Expression	Action	Info
☒	Or	Remove	
☐	A [Training-VM-XX:net.if.in[eth0].last()]>10	Remove	
☐	B [Training-VM-XX:net.if.out[eth0].last()]>10	Remove	

[Test](#)

Упрощает работу с И/ИЛИ сценариями

Используйте скобки, чтобы не нарушить логики:

⚡ (A or B) and (C or D)

Триггеры – тестирование выражений

Укажите примеры значений, чтобы увидеть результат выражения и его частей.

Test

Test data	Expression	Variable	Elements	Result type	Value	Value
	{Training-VM-XX:net.if.in[eth0].last()}			Numeric (integer)	9	9
	{Training-VM-XX:net.if.out[eth0].last()}			Numeric (integer)	11	9

Result

Expression

Or

A {Training-VM-XX:net.if.in[eth0].last()}>10

B {Training-VM-XX:net.if.out[eth0].last()}>10

A or B

Result

TRUE

FALSE

TRUE

TRUE

Test Cancel

PROBLEM

Result

FALSE

FALSE

FALSE

FALSE

OK

⚡ Выражение верно (TRUE) / ошибочно (FALSE)

⚡ Состояние триггера перейдет в «Проблема», если конечный результат будет TRUE.

Триггеры – генерация ОК события

Выражение:

- Событие ОК генерируется на основе выражения проблемы (TRUE->FALSE).

* Expression
[Expression constructor](#)

OK event generation ☒ Expression ☐ Recovery expression ☐ None

Выражение восстановления:

- Событие ОК генерируется, если выполнены оба условия:
 - Выражение проблемы не верно (FALSE)
 - Выражение восстановления верно (TRUE)

* Problem expression
[Expression constructor](#)

OK event generation ☐ Expression ☒ Recovery expression ☐ None

* Recovery expression
[Expression constructor](#)

Нет: в этом случае триггер никогда самостоятельно не сменит состояние на ОК.

Триггеры – генерация генерации событий ПРОБЛЕМА

PROBLEM event generation mode **Single** Multiple

Одиночная:

- Когда триггер переходит в состояние «Проблема», генерируется одно событие.

Time ▾	Recovery time	Status	Info	Host	Problem • Severity	Operational data	Duration	Ack	Actions
18:11:26		PROBLEM		Training-VM-XX	CPU Load is very high on Training-VM-XX	2.33/2.18	1m 36s	No	

Множественный:

- Каждый раз, когда триггер пересчитывается в состояние «Проблема» генерируется новое событие.
 - Полезно для мониторинга логов, журнала событий или для SNMP трапов.

Time ▾	Recovery time	Status	Info	Host	Problem • Severity	Operational data	Duration	Ack	Actions
18:14:46		PROBLEM		Training-VM-XX	CPU Load is very high on Training-VM-XX	2.4/2.4	6s	No	
18:14:36		PROBLEM		Training-VM-XX	CPU Load is very high on Training-VM-XX	2.47/2.4	16s	No	
18:14:26		PROBLEM		Training-VM-XX	CPU Load is very high on Training-VM-XX	2.56/2.4	26s	No	
18:14:16		PROBLEM		Training-VM-XX	CPU Load is very high on Training-VM-XX	2.48/2.4	36s	No	
18:14:06		PROBLEM		Training-VM-XX	CPU Load is very high on Training-VM-XX	2.1/2.4	46s	No	

Триггеры – тэги

Триггеры позволяют настроить тэги для событий

- ⚡ После определений тэгов в настройках триггера – события на основе него будут помечены этими тэгами.
- ⚡ Варианты использования:
 - Разделять проблемы на основе одного лога и закрывать их по отдельности.
 - Проще определить принадлежность события к тому или другому сервису/приложению и т.д.
 - Дополнительные возможности по фильтрации, как для отображения, так и при настройке оповещений.
 - Глобальная корреляция событий.

The screenshot shows a configuration window for a trigger. At the top, there are three tabs: 'OK event closes', 'All problems', and 'All problems if tag values match' (which is selected). Below the tabs, there is a label '* Tag for matching' followed by a text input field containing 'Service'. Underneath this, there is a section labeled 'Tags' containing a table of tag pairs. The first row has 'Service' and 'MySQL' with a 'Remove' link. The second row has 'DC' and 'Los Angeles DC1' with a 'Remove' link. At the bottom left of the table is an 'Add' link.

Tags		
Service	MySQL	Remove
DC	Los Angeles DC1	Remove

[Add](#)

Событие ОК закрывает:

- ⚡ Все проблемы – все проблемы на основе этого триггера.
- ⚡ Все проблемы, если значения тэгов совпадают - все проблемы на основе этого триггера, если у этих проблем совпадают тэги.

Триггеры – обновление, подтверждение, закрытие вручную

Чтобы подтвердить проблему (снять подтверждение), нажмите на **Да** / **Нет** в колонке «Подтверждение».

Time	☐	Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack
14:51:26	☐	High				Training-VM-XX	CPU Load is very high on Training-VM-XX	33s	No

Нажмите чтобы обновить проблему

При подтверждении проблемы можно:

Оставить сообщение:

Message Working on it!

History

Time

User

User action

Message

Scope

☒ Only selected problem

☐ Selected and all other problems of related triggers 1 event

Изменить важность:

Change severity ☒

Not classified

Information

Warning

Average

High

Disaster

Подтвердить:

Acknowledge ☒

Закрыть проблему:

Close problem ☒

⚡ Ручное закрытие проблемы возможно при соответствующей настройке триггера:

- Полезно, если используется «Нет» для генерации ОК события.
- Если проблема не решена, Zabbix создаст новую проблему.

Практическое задание

Выполнить лабораторные работы:

№10 – Триггеры

№11 – Определение проблем

Учебный центр АйТи Клауд

Макросы

современные технологии простым языком



Встроенные макросы

Есть встроенные макросы:

Синтаксис: {MACRO.NAME}

Макрос заменяется конкретным значением в зависимости от контекста.

Разные области использования:

- Узлы сети и шаблоны: {HOST.NAME}, {HOST.CONN}
- Триггеры: {ITEM.VALUE}, {ITEM.LASTVALUE}
- Тэги
- Оповещения: {EVENT.DATE}
- Веб мониторинг
- И т.д.

Макросы экономят время и позволяют сделать конфигурацию Zabbix прозрачнее.

Полный список поддерживаемых макросов есть в документации.

Настройка пользовательских макросов

Пользовательские макросы:

Переменные для большей гибкости настроек.

Синтаксис (A-Z 0-9 _ .): {\$MACRO.NAME}

Два варианта:

- «Текст» – отображать данные как есть (по умолчанию).
- «Скрытый текст» – скрыть значение.

Три уровня:

- Глобальный
- Шаблон
- Узел сети

Если макрос не определен на уровне узла сети:

- Будет использоваться значение макроса уровня шаблонов с учетом вложенности
- Если значение все еще не найдено – будет использоваться «Глобальные макросы», если там есть соответствующий



Настройка пользовательских макросов

- Глобальные макросы: Администрирование > Макросы

Macros ▾

Macro	Value		Description	
{S1.GLOBAL.MACRO}	443	T ▾	Example of Global user macro	Remove
{S1.GLOBAL.MACRO.MASKED}	*****	🔒 ▾	Example of masked Global user macro	Remove

[Add](#)

T ▾

Text

🔒 Secret text

- Макросы шаблона: Сбор данных > Шаблоны > {template} > Макросы

Template macros Inherited and template macros

Macro	Value		Description	
{S2.TEMPLATE.MACRO}	80	T ▾	Example macro from template	Remove
{S2.TEMPLATE.MACRO2}	22	T ▾	SSH connection default port.	Remove

[Add](#)

- Макросы узла сети: Сбор данных > Узлы сети > {host} > Макросы

Macros Inventory Encryption

Host macros Inherited and host macros

Macro	Value		Description	
{S3.HOST.USER.MACRO}	1024	T ▾	Example of Host macro	Remove
{S3.HOST.USER.MACRO.MASKED}	*****	🔒 ▾	Example of masked Host macro	Remove

[Add](#)

Функционал пользовательских макросов

Один шаблон – разные параметры:

Разные параметры ключа элемента данных

- `net.tcp.service[ssh,{SSH.PORT}]`

Разные пороговые значения в выражении триггеров

- `{server:system.cpu.load.last()} > {$MAX.CPU.LOAD}`
- `{server:system.cpu.load[,avg1].min({CPU.LOAD. PERIOD})}>{$MAX.CPU.LOAD}`

Разные учетные данные

- `ssh.run[remote.command]`
- `{SSH.USERNAME}`
- `{SSH.PASSWORD}`



Наследование макросов

Наследование макросов можно проследить и изменить значение в настройках шаблонов и узлов сети:

The screenshot displays a web interface for managing macros. At the top, a navigation bar includes 'Host', 'Templates', 'IPMI', 'Tags', 'Macros' (selected), 'Inventory', and 'Encryption'. Below this, a sub-navigation bar shows 'Host macros' and 'Inherited and host macros'. A callout box with the text 'Нажмите [Изменить]' (Click [Edit]) points to the 'Change' button next to the first macro entry.

Macro	Effective value	Actions
Host macros		
Example of Global user macro		
Global macro	443	T Change
Example of Global user macro		
Masked Global macro	*****	Change
Example of masked Global user macro		
Template macro	8080	T Remove
Example of Template macro (override)		
Template macro 2	22	T Change
SSH connection default port		
Host macro	1024	T Remove
Example of Host macro		
Masked Host macro	*****	Remove
Example of masked Host macro		

On the right side, two panels provide details for selected macros:

- Шаблоны (Templates):** Shows the 'Template value' for 'Example Template - Macros: "80"' and 'Example Template - Macros: "22"'. It also includes a 'Global value (configure)' section with a value of '443'.
- Глобальные (Global):** Shows the 'Global value (configure)' for the selected macro, which is '443'.

At the bottom left, a blue box labeled 'Узел сети' (Network node) is visible.

Пользователям не видны глобальные значения макросов на уровне узла / шаблона.

Практическое задание

Выполнить лабораторные работы:

№12 – Продвинутое определение проблем и макросы

№13 – Шаблоны

Учебный центр АйТи Клауд

Обнаружение

современные технологии простым языком



SNMP

Simple Network Management Protocol (SNMP) - стандартный интернет-протокол для управления устройствами в IP-сетях.

MIB — это иерархическая база данных со сведениями об устройстве.

OID — идентификатор объекта в MIB.

Иерархия MIB

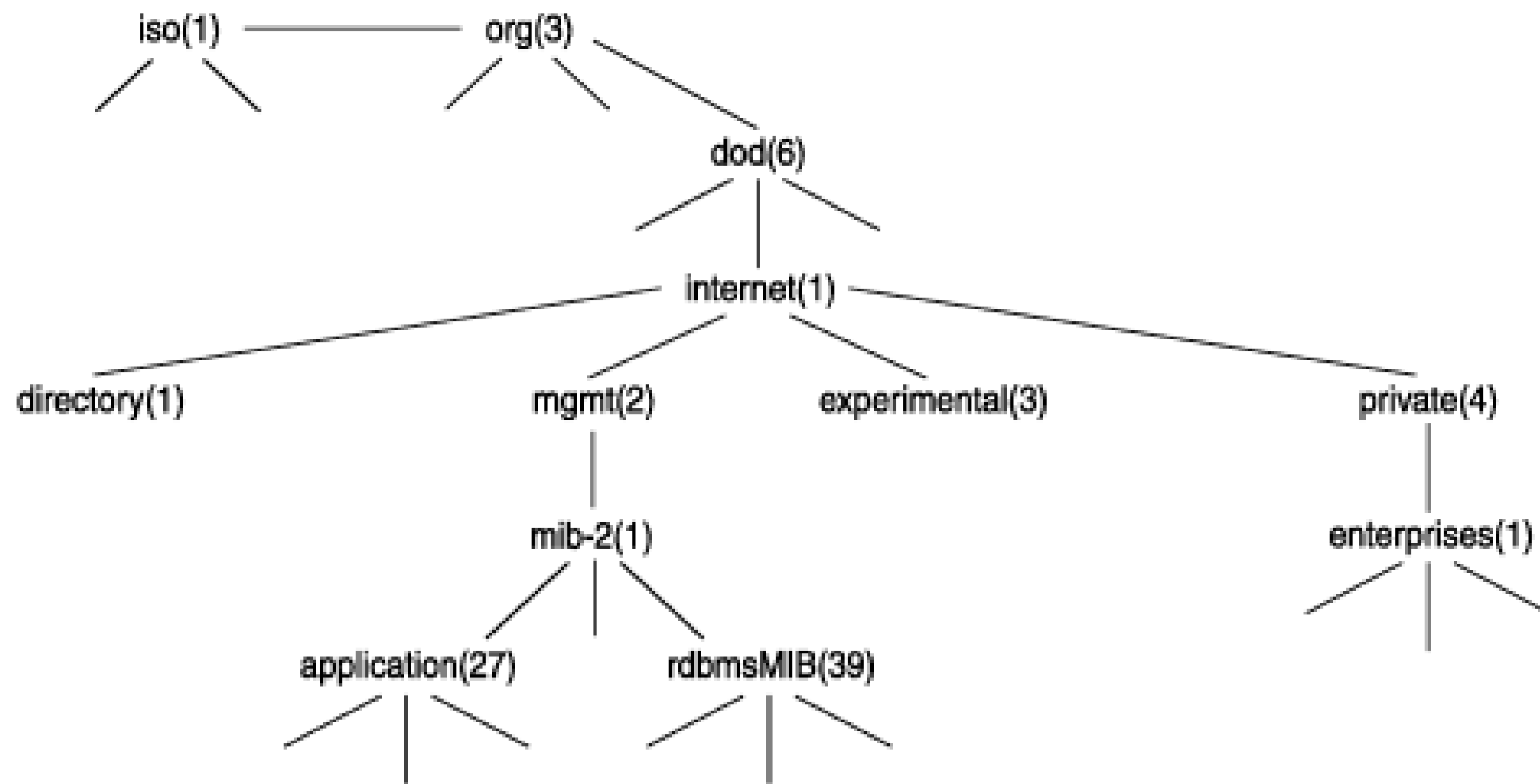


Схема PDU

Версия SNMP	v1/v2/v3
Строка сообщества	Public, Private
Тип PDU	Get, GetNext, Response, Set, Trap, GetBulk, Inform
ID запроса	Идентификатор запроса
Статус ошибки	0, 1, 2, 3, 4, 5
Индекс ошибки	0, 1
Связанные переменные	Одна или несколько переменных в запросе

Настройка мониторинга по SNMP

Узел сети для мониторинга

Host

Templates

IPMI

Tags

Macros

Inventory

Encryption

Value mapping

* Host name

SNMP device host

Visible name

SNMP device host

* Groups

Discovered hosts

type here to search

Interfaces

Type	IP address	DNS name
Agent	127.0.0.1	

SNMP

127.0.0.1

* SNMP version

SNMPv2

* SNMP community

{ \$SNMP_COMMUNITY }

Max repetition count

10

☒ Use combined requests

Элемент данных для мониторинга

Item

Tags

Preprocessing

* Name

Interface wlp3s0: Bits received

Type

SNMP agent

* Key

net.if.in[ifHCInOctets.3]

Type of information

Numeric (unsigned)

* Host interface

127.0.0.1:161

* SNMP OID

get[1.3.6.1.2.1.31.1.1.1.6.3]

Units

bps

* Update interval

3m

Настройка мониторинга по SNMP

Узнать OID элемента данных можно:

- Из документации
- Используя команды SNMP

Получить список OID:

```
snmpwalk -v 2c -c public <IP хоста>
```

Пример результата выполнения команды:

```
IF-MIB::ifHCInOctets.3 = Counter64: 3409739121
```

- Идентификатор объекта: IF-MIB::ifHCInOctets.3
- Значение объекта: 3409739121

Получить OID в числовом виде:

```
snmpget -v 2c -c public -On <IP хоста> IF-MIB::ifHCInOctets.3
```

Пример результата выполнения команды:

```
.1.3.6.1.2.1.31.1.1.1.6.3 = Counter64: 3472126941
```

- Идентификатор OID: 1.3.6.1.2.1.31.1.1.1.6.3
- Значение объекта: 3409739121

Сетевое обнаружение

Обнаружение сетевых устройств в Zabbix базируется на основе следующей информации:

- диапазоны IP
- доступность внешних сервисов (FTP, SSH, WEB, POP3, IMAP, TCP и т.д.)
- информация, полученная от Zabbix агента (поддерживается только режим без шифрования)
- информация, полученная от SNMP агента

Обнаружение NE предоставляет:

- обнаружение топологии сети

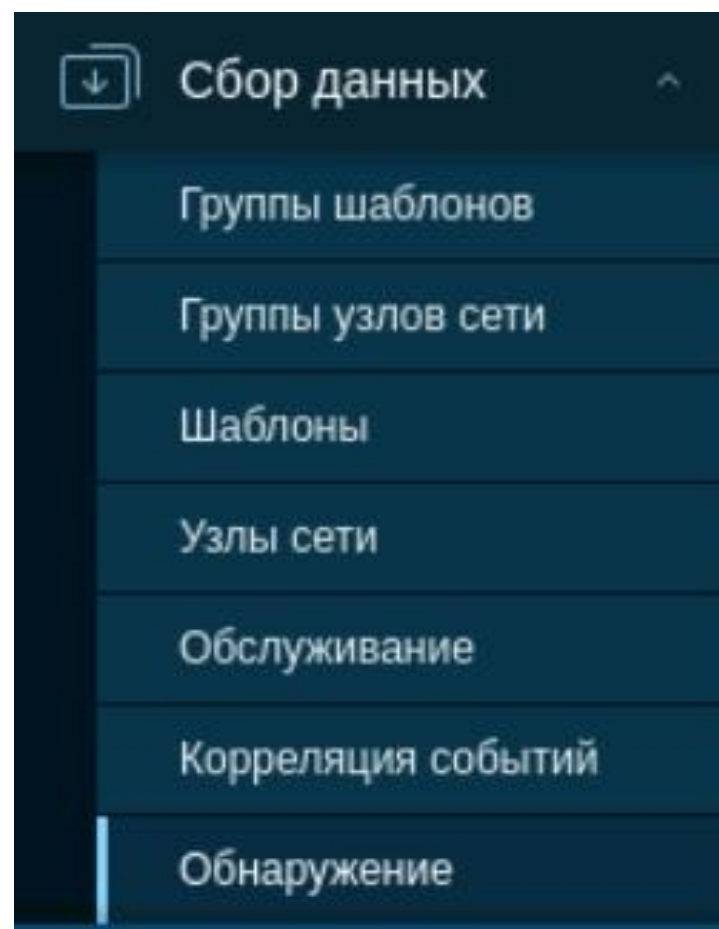
Сетевое обнаружение, по сути, состоит из двух этапов: обнаружение и действия.

Действия обнаружения

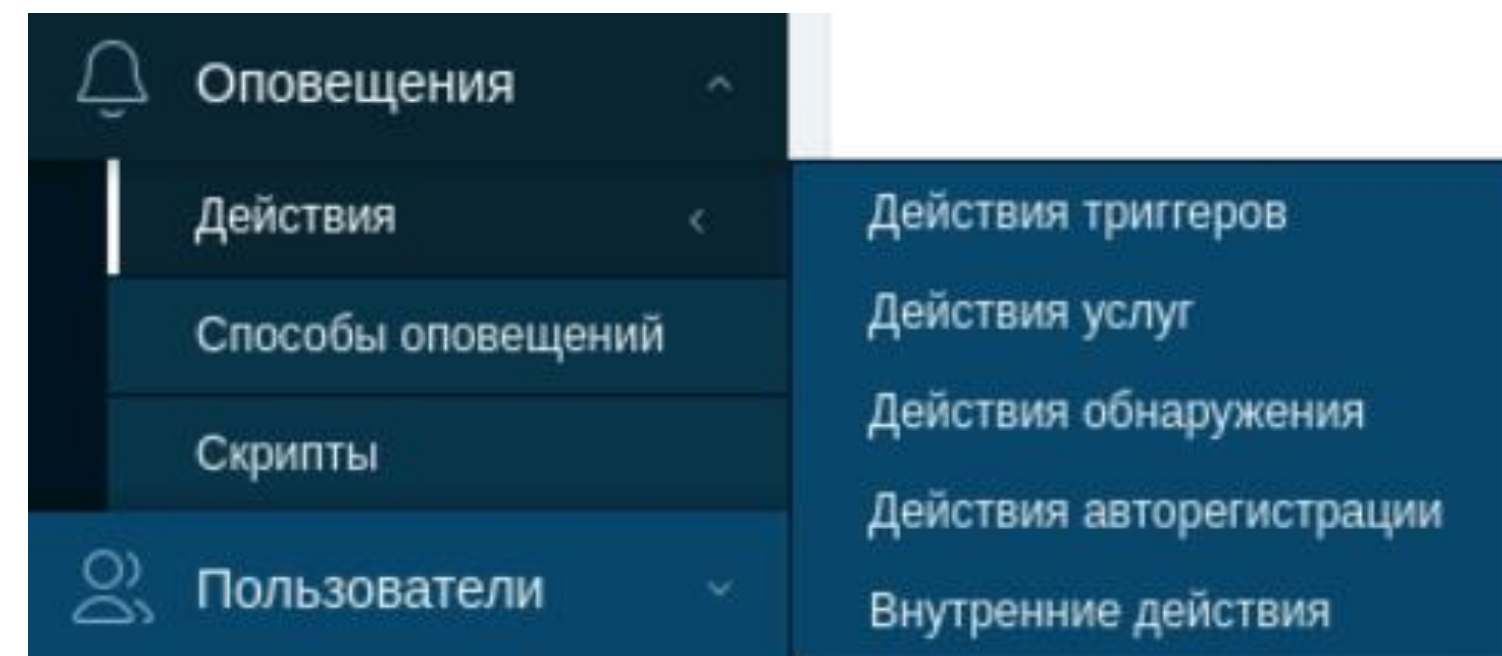
- Отправка оповещений
- Добавление/удаление узлов сети
- Активация/деактивация узлов сети
- Добавление узлов сети в группу
- Удаление узлов сети из группы
- Присоединение/отсоединение узлов сети к/от шаблона
- Выполнение удаленных скриптов

Настройка сетевого обнаружения

- Настройка правил сетевого обнаружения выполняется в разделе «Сбор данных» - «Обнаружение»



- Настройка действий сетевого обнаружения выполняется в разделе «Оповещения» - «Действия» - «Действия обнаружения»



Авторегистрация активных агентов

Авторегистрация активных агентов — это механизм, при котором Zabbix агенты в активном режиме самостоятельно регистрируются на Zabbix сервере без ручного добавления хостов.

Авторегистрация активного агента также поддерживает мониторинг добавленных узлов сети с пассивными проверками. Когда активный агент запрашивает проверки, при условии, что параметры конфигурации «ListenIP» или «ListenPort» определены в файле конфигурации, они отправляются на сервер.

Настройка авторегистрации активных агентов

Убедитесь, что у вас в файле конфигурации на агенте — `zabbix_agentd.conf` — указан Zabbix сервер.
Например:

```
ServerActive=10.0.0.1
```

Если вы не указали параметр *Hostname* в `zabbix_agentd.conf`, то в качестве имени узла сети будет использоваться системное имя узла сети, на котором находится агент.

Перезапустите агента после любых изменений, сделанных в файле конфигурации.

В веб-интерфейсе Zabbix перейдите к *Оповещения* → *Действия* выберите *Действия авторегистрации* и нажмите *Создать действие*:

- На вкладке «Действие» дайте название вашему действию.
- По желанию укажите условия. В условиях вы можете выполнить сопоставление подстроки или регулярного выражения для имени узла сети/метаданных узла сети.
- На вкладке «Операции» добавьте соответствующие операции, такие как «Добавить узел сети», «Добавить в группу узлов сети», «Присоединить шаблон» и т. д.

Использование метаданных узла для авторегистрации

Когда агент отправляет запрос на авторегистрацию на сервер, он отправляет свое имя хоста (hostname). В некоторых случаях (например, облачные узлы Amazon) имени хоста недостаточно, чтобы сервер Zabbix различал обнаруженные узлы сети. Для отправки другой информации от агента на сервер могут быть дополнительно использованы метаданные узла сети.

Метаданные узла настраиваются в файле конфигурации агента — `zabbix_agentd.conf`. Существует 2 способа указать метаданные узла сети в файле конфигурации:

`HostMetadata`

`HostMetadataItem`

Низкоуровневое обнаружение (LLD)

Низкоуровневое обнаружение (англ. Low-level discovery, LLD) даёт возможность автоматического создания элементов данных, триггеров и графиков для различных объектов на компьютере.

Правило обнаружения состоит из двух частей – элемента данных и прототипов.

Элемент данных – обычный элемент данных, но значения представлены в формате JSON. По сути возвращаемые значения представлены в виде пар – макрос – значение.

Эти макросы затем используются в именах, ключах и других полях прототипов, где они заменяются на полученные значения для создания реальных элементов данных, триггеров, графиков и даже узлов сети для каждого обнаруженного объекта.

Когда сервер получает значение элемента данных обнаружения, он смотрит на пары макрос → значение и для каждой пары создаёт реальные элементы данных, триггеры и графики, основанные на их прототипах.

Настройка LLD

- Настройка LLD выполняется в разделе «Сбор данных» - «Шаблоны», и далее необходимо перейти в «Обнаружение» для шаблона.

Сбор данных										
Имя	Узлы сети	Элементы данных	Триггеры	Графики	Панели	Обнаружение	Веб	Поставщик	Версия	
☐ Template Windows	Узлы сети 1	Элементы данных 34	Триггеры 13	Графики 5	Панели	Обнаружение 5	Веб			
☐ Windows by SNMP	Узлы сети	Элементы данных 15	Триггеры 7	Графики 1	Панели 3	Обнаружение 3	Веб	Zabbix	7.0-0	
☐ Windows by Zabbix agent	Узлы сети	Элементы данных 34	Триггеры 13	Графики 5	Панели 3	Обнаружение 4	Веб	Zabbix	7.0-0	
☐ Windows by Zabbix agent active	Узлы сети	Элементы данных 34	Триггеры 13	Графики 5	Панели 3	Обнаружение 4	Веб	Zabbix	7.0-0	

Настройка LLD

☐ Шаблон	Имя ▲	Элементы данных	Триггеры	Графики	Узлы сети	Ключ	Интервал	Тип	Состояние
☐ Template Windows	Monted filesystem discovery	Прототипы элементов данных 3	Прототипы триггеров 1	Прототипы графиков 1	Прототипы узлов сети	vfs.fs.discovery	1m	Zabbix агент	Активировано
☐ Template Windows	Windows by Zabbix agent: Get filesystems : Mounted filesystem discovery	Прототипы элементов данных 5	Прототипы триггеров 2	Прототипы графиков 2	Прототипы узлов сети	vfs.fs.dependent.discovery		Зависимый элемент данных	Активировано
☐ Template Windows	Windows by Zabbix agent: Windows: Network interfaces WMI get : Network interfaces discovery	Прототипы элементов данных 9	Прототипы триггеров 4	Прототипы графиков 1	Прототипы узлов сети	net.if.discovery		Зависимый элемент данных	Активировано
☐ Template Windows	Windows by Zabbix agent: Physical disks discovery	Прототипы элементов данных 8	Прототипы триггеров 3	Прототипы графиков 4	Прототипы узлов сети	perf_instance_en.discovery[PhysicalDisk]	1h	Zabbix агент	Активировано
☐ Template Windows	Windows by Zabbix agent: Windows services discovery	Прототипы элементов данных 1	Прототипы триггеров 1	Прототипы графиков	Прототипы узлов сети	service.discovery	1h	Zabbix агент	Активировано

Практическое задание

Выполнить лабораторные работы:

№14 – SNMP проверки и обнаружение

№15 – Авторегистрация активных агентов

Учебный центр АйТи Клауд

Веб-мониторинг

современные технологии простым языком



Веб-мониторинг

Каждым веб-сценарием собирается следующая информация:

- средняя скорость загрузки в секунду для всех шагов для всего сценария
- номер шага, который завершился с ошибкой
- последнее сообщение об ошибке

На каждом шаге веб-сценария собирается следующая информация:

- скорость загрузки в секунду
- время ответа
- код ответа

Настройка веб-мониторинга

Шаг веб-сценария

* Имя

Первая страница

* URL

https://{HOST.CONN}/index.php

Анализ

Поля запроса

Имя

название

Значение

значение

Удалить

Добавить

Тип Post

Данные формы

Сырые данные

Post поля

Имя

название

Значение

значение

Удалить

Добавить

Переменные

Имя

название

Значение

значение

Удалить

Добавить

Заголовки

Имя

название

Значение

значение

Удалить

Добавить

Следовать перенаправлениям

☒

Режим получения

Тело

Заголовки

Тело и заголовки

* Время ожидания

15s

Требуемая строка

Zabbix SIA

Требуемые коды состояния

200

Обновить

Отмена

Просмотр результатов работы веб-сценария



Практическое задание

Выполнить лабораторную работу №16 – Веб-проверки

Учебный центр АйТи Клауд

Мониторинг бизнес уровня

современные технологии простым языком



Мониторинг услуг

Мониторинг услуг — это мониторинг бизнес-уровня, который можно использовать для обзора всего дерева услуг IT инфраструктуры, выявлять слабые места инфраструктуры, вычислять SLA по различным IT услугам, а также проверять другую информацию на более высоком уровне.

SLI (Service Level Indicator) - Индикатор уровня сервиса. Отвечает на вопрос – «Что мы измеряем?».

SLO (Service Level Objective) - Цель уровня сервиса. Отвечает на вопрос – «Чего мы хотим достичь?»

SLA (Service Level Agreement) - Соглашение об уровне сервиса. Отвечает на вопрос – «Что мы гарантируем?»

Дерево услуг

Услуги?

Все услуги / web-server

web-server Родительские услуги: Состояние: Высокая SLA: Доступность web-server: 1.0171 ? Теги: service: web-server				
Имя	Состояние	Основная причина	Создано в	Теги
apache	Высокая	Проблемы с Веб-сервером на сервере Debian, Проблемы с Веб-сервером на сервере Debian Active	30.10.2025	service: apache
connection	OK		30.10.2025	service: connection

SLA

SLA



SLA [Исключения времени простоя](#)

* Имя

Доступность web-server

* SLO

99.9

%

Период отчета

Ежедневно

Еженедельно

Ежемесячно

Ежеквартально

Ежегодно

Часовой пояс

Системное по умолчанию: (UTC+00:00) UTC

Запланировано

24x7

Пользовательское

* Действительно с

2025-10-30

* Теги услуг

Имя	Операция	Значение	Действие
service	Равно	apache	Удалить
service	Равно	connection	Удалить
service	Равно	web-server	Удалить

Обновить

Клонировать

Удалить

Отмена

Отчёт SLA

Отчет SLA

SLA

Доступность web-server ×

Выбрать

От

ГГГГ-ММ-ДД

Услуга

web-server ×

Выбрать

К

ГГГГ-ММ-ДД

Применить

Сбросить

День	SLO	SLI	Доступен	Недоступен	Бюджет времени простоя	Исключения времени простоя
05.11.2025	99.9%	0.9938	7м 4с	11ч 43м 59с	-11ч 43м 59с	
04.11.2025	99.9%	0	0	1д	-1д	
03.11.2025	99.9%	0	0	1д	-1д	
02.11.2025	99.9%	0	0	1д	-1д	
01.11.2025	99.9%	0	0	1д	-1д	
31.10.2025	99.9%	20.6504	4ч 57м 22с	19ч 2м 38с	-19ч 2м 21с	
30.10.2025	99.9%	23.7054	1ч 31м 52с	4ч 55м 40с	-4ч 55м 35с	

Практическое задание

Выполнить лабораторную работу №17 – Мониторинг услуг

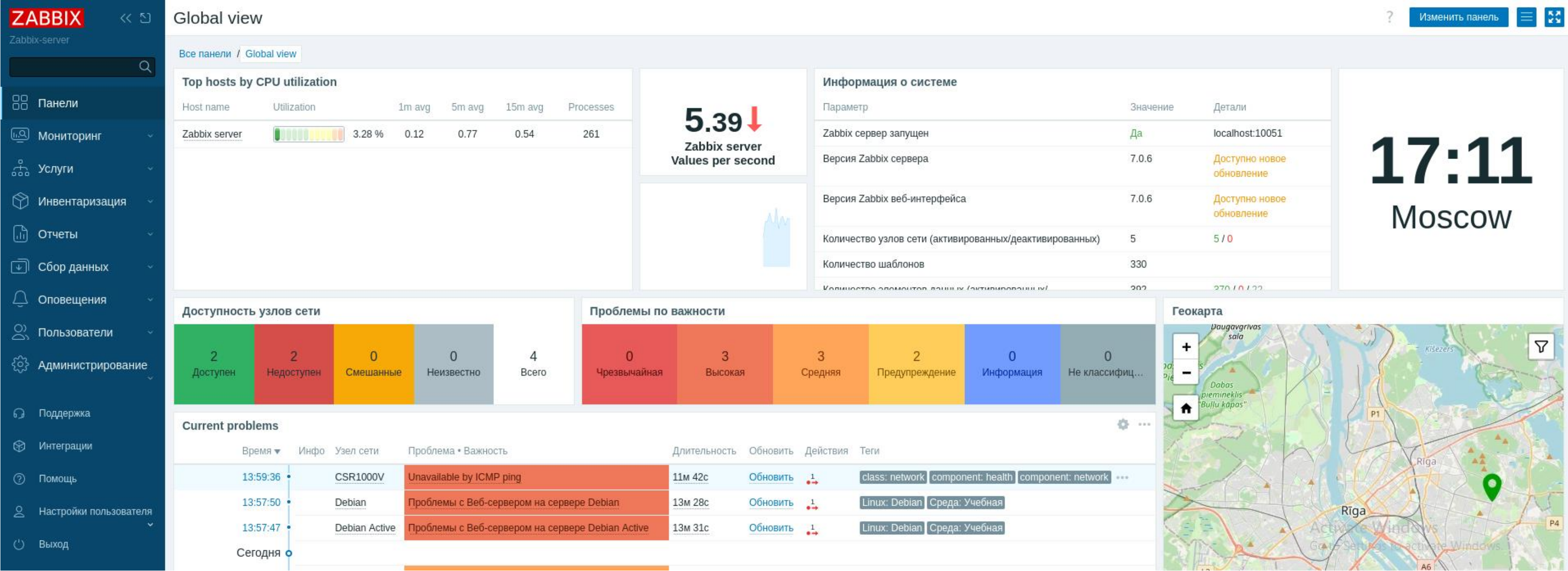
Учебный центр АйТи Клауд

Визуализация данных

современные технологии простым языком



Панели мониторинга



Все панели

 Dashboards



Create dashboard



Filter



Name ▲



Apache info

My

Shared



Global view

My

Shared



HyperV (John's custom)

My



Problems (quick view)

My



Zabbix server

My

Shared

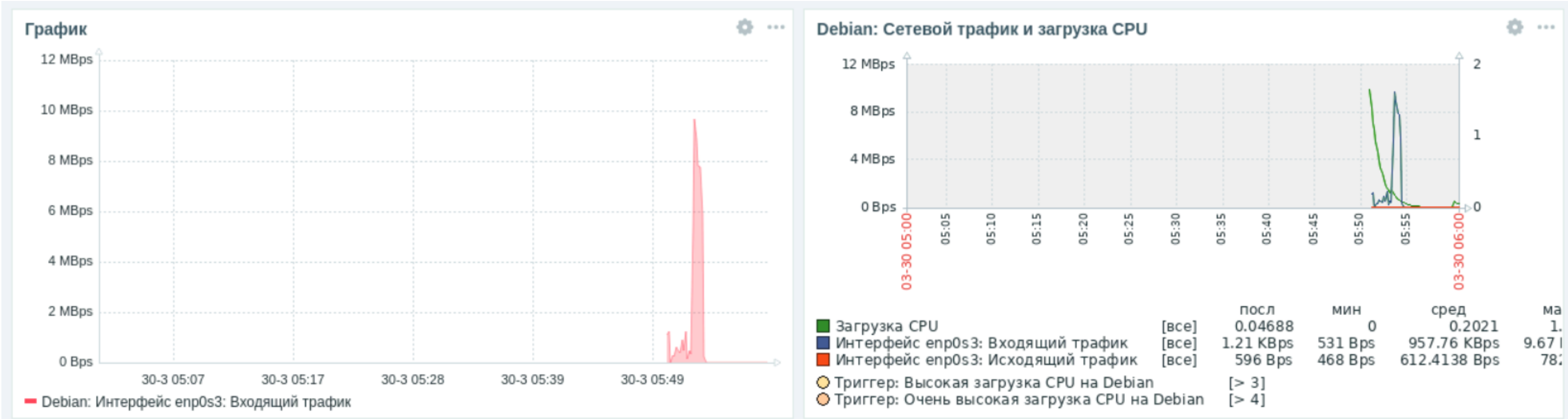


Zabbix server health

My

Shared

Виджеты: Графики



Виджеты: Доступность узлов сети и Журнал действий

Доступность узлов сети

Доступно

Недоступен

Всего узлов сети	5	0
Агент (активный)	0	0
Агент (пассивный)	4	0
SNMP	1	0

Журнал действий

Время

Действие

Способ оповещений

Получатель

Сообщение

Состояние

Инфо

Данные не найдены

Виджеты: Значение элемента данных, информация о системе и история элементов данных

Debian: Загрузка С... ⚙️ ...

30.03.2025 06:01:19

0.02↓

Загрузка CPU

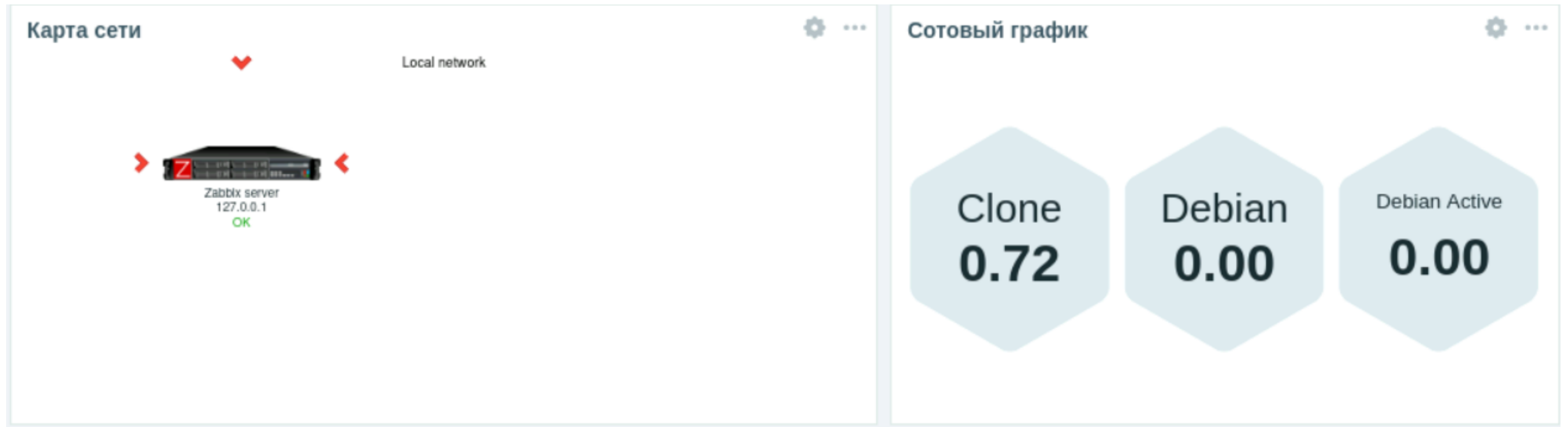
Информация о системе ⚙️ ...

Параметр	Значение	Детали
Версия Zabbix веб-интерфейса	7.0.6	Доступно новое обновление
Количество узлов сети (активированных/деактивированных)	5	5 / 0
Количество шаблонов	330	
Количество элементов данных (активированных/деактивированных/неподдерживаемых)	392	370 / 0 / 22
Количество триггеров (активированных/деактивированных [проблема/ок])	185	185 / 0 [5 / 180]
Количество пользователей (в сети)	3	2
Требуемое быстродействие сервера, новые значения в	7.67	

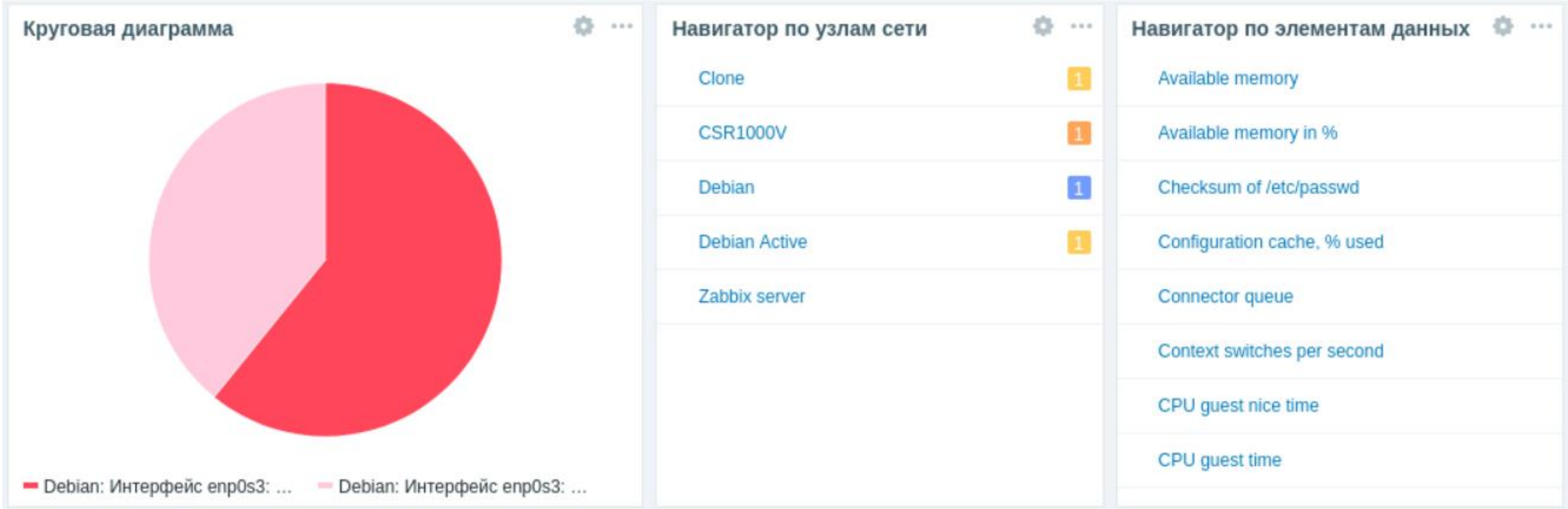
История элементов данных ⚙️ ...

Имя	Значение
Debian: Загрузка CPU	0.009766
Debian: Загрузка CPU	0.01221
Debian: Загрузка CPU	0.01514
Debian: Загрузка CPU	0.01856
Debian: Загрузка CPU	0.02246
Debian: Загрузка CPU	0.02734
Debian: Загрузка CPU	0.03272
Debian: Загрузка CPU	0.03906
Debian: Загрузка CPU	0.04688
Debian: Загрузка CPU	0.05615

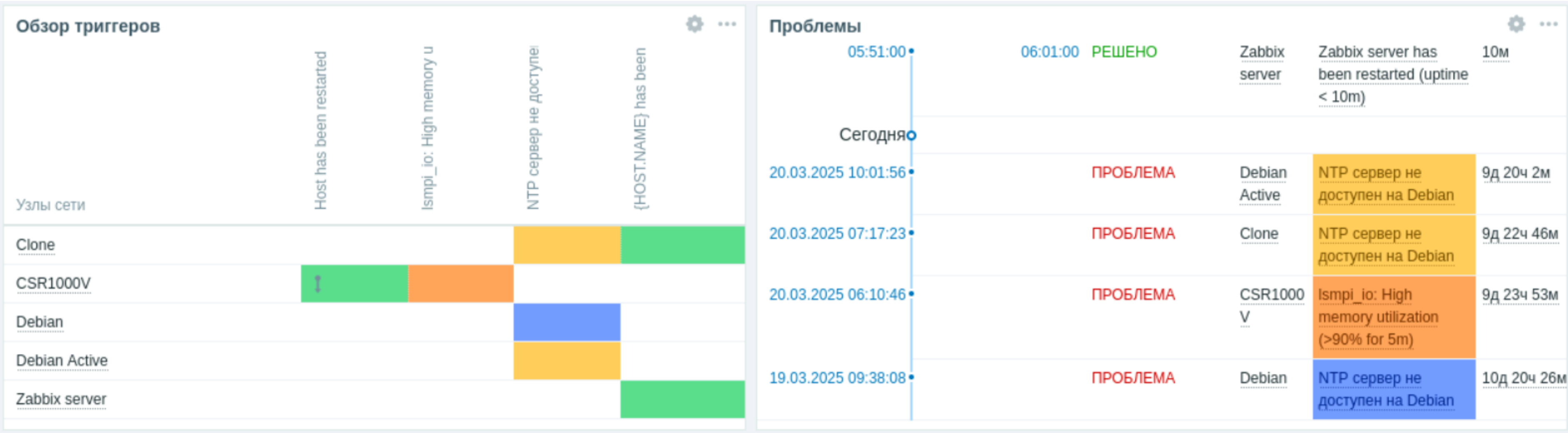
Виджеты: Карта сети и сотовый график



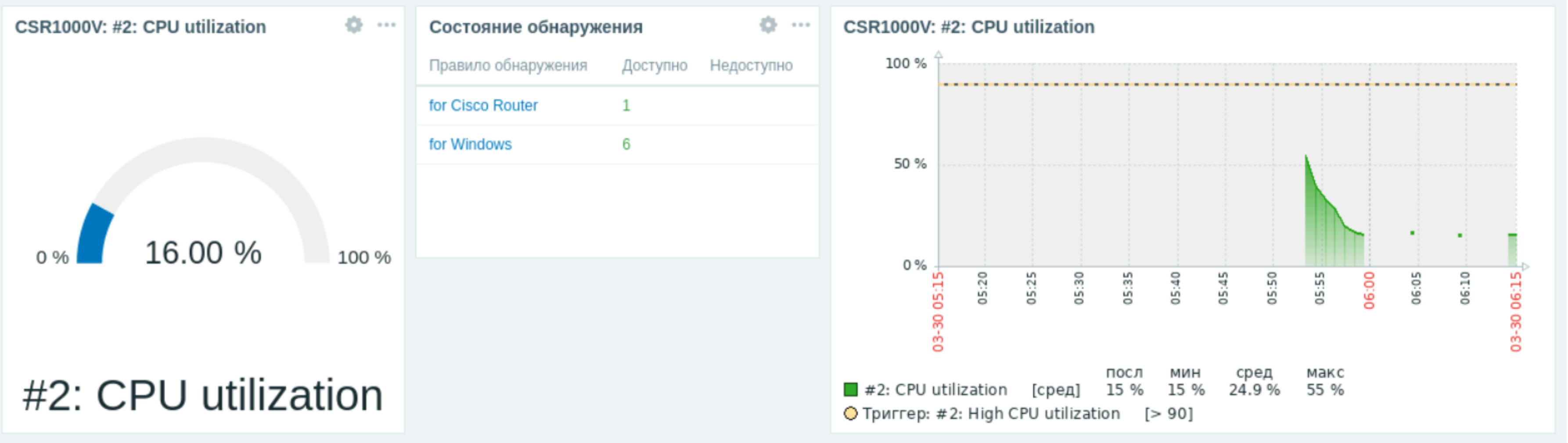
Виджеты: Круговая диаграмма, навигатор по узлам сети и навигатор по элементам данных



Виджеты: Обзор триггеров и проблемы



Виджеты: Радиальный датчик, состояние обнаружения и прототип графиков



Виджеты: Геокарта, веб-мониторинг и часы

Геокарта



Leaflet | © OpenStreetMap contributors

Веб-мониторинг

Группа узлов сети ▲ Ok Неудачно Неизвестно

Training/Servers	1	2
------------------	---	---

Локальное



Локальное

09:20:45

Мониторинг: Проблемы

Мониторинг

Проблемы

Узлы сети

Последние данные

Карты сетей

Обнаружение

Услуги

Инвентаризация

Отчеты

Сбор данных

Оповещения

Пользователи

Сохранить как

Применить

Сбросить

☐	Время ▼	Важность	Время восстановления	Состояние	Инфо	Узел сети	Проблема
☐	13:59:36	Высокая		ПРОБЛЕМА		CSR1000V	Unavailable by ICMP ping ?
☐	13:57:50	Высокая		ПРОБЛЕМА		Debian	Проблемы с Веб-сервером на сервере Debian
☐	13:57:47	Высокая		ПРОБЛЕМА		Debian Active	Проблемы с Веб-сервером на сервере Debian Active
Сегодня							
☐	30.03.2025 17:27:53	Средняя		ПРОБЛЕМА		Debian Active	Узел сети Debian не доступен по ICMP
☐	30.03.2025 17:27:53	Средняя		ПРОБЛЕМА		Debian	Узел сети Debian не доступен по ICMP
Вчера							
☐	20.03.2025 10:01:56	Предупреждение		ПРОБЛЕМА		Debian Active	NTP сервер не доступен на Debian
☐	20.03.2025 07:17:23	Предупреждение		ПРОБЛЕМА		Clone	NTP сервер не доступен на Debian
☐	20.03.2025 06:10:46	Средняя		ПРОБЛЕМА		CSR1000V	Ismpi_io: High memory utilization (>90% for 5m) ?

Симптомы

Problems

☐	Time ▼	Severity	Recovery time	Status	Info	Host	Problem	Duration
☒	18:15:01 •	Not classified				Zabbix server	Application unavailable on (23)	1m 4s
☒	18:15:01 •	Not classified				Zabbix server	Host (23) unavailable	1m 4s
☐	18:15:01 •	Not classified				Zabbix server	Power outage on (23)	1m 4s
Today ○								
☐	2022-10-17 10:38:52 •	Average		PROBLEM		Zabbix server	Interface e	13d 8h
October ○								
☐	2022-09-16 12:38:25 •	Not classified		PROBLEM		Zabbix server	A class: trigge	14d 6h
☐	2022-09-16 12:12:47 •	Not classified		PROBLEM		Zabbix server	A class: trigge	14d 7h
☐	2022-09-16 12:09:28 •	Not classified		PROBLEM		Zabbix server	A class: trigge	14d 7h
☐	2022-09-16 12:04:06 •	Not classified		PROBLEM		Zabbix server	A class: trigge	14d 7h
☐	2022-09-16 11:59:30 •	Not classified		PROBLEM		Zabbix server	A class: trigge	14d 7h

- VIEW
- Problems
- History ▶
- CONFIGURATION
- Trigger
- Items ▶
- PROBLEM
- Mark as cause
- Mark selected as symptoms

Действия над проблемами

Обновление проблемы

? X

Проблема Unavailable by ICMP ping

Сообщение

История

Время	Пользователь	Действие пользователя	Сообщение
-------	--------------	-----------------------	-----------

Границы

☒ Только выбранная проблема

☐ Выбранные и все другие проблемы связанные с триггерами 1 событие

Изменение важности

☐ Не классифицир...☐ Информация☐ Предупреждение☐ Средняя☐ Высокая☐ Чрезвычайная

Подавление ?

☐ Бессрочно☐ До pow+1d 

Отмена подавления ?

☐

Подтвердить ?

☐

Конвертация в причину ?

☐

Закрыть проблему

☐

Мониторинг: Узлы сети

Узлы сети

Имя

Состояние

Любое

Активировано

Деактивировано

Группы узлов сети

начните печатать для поиска

Выбрать

Теги

И/ИЛИ

Или

IP

тег

Содержит

▼

значение

Удалить

DNS

Добавить

Порт

Узлы сети в обслуживании

☒

Подавленные проблемы

☐

Важность

☐ Не классифицировано

☐ Предупреждение

☐ Высокая

☐ Информация

☐ Средняя

☐ Чрезвычайная

Сохранить как

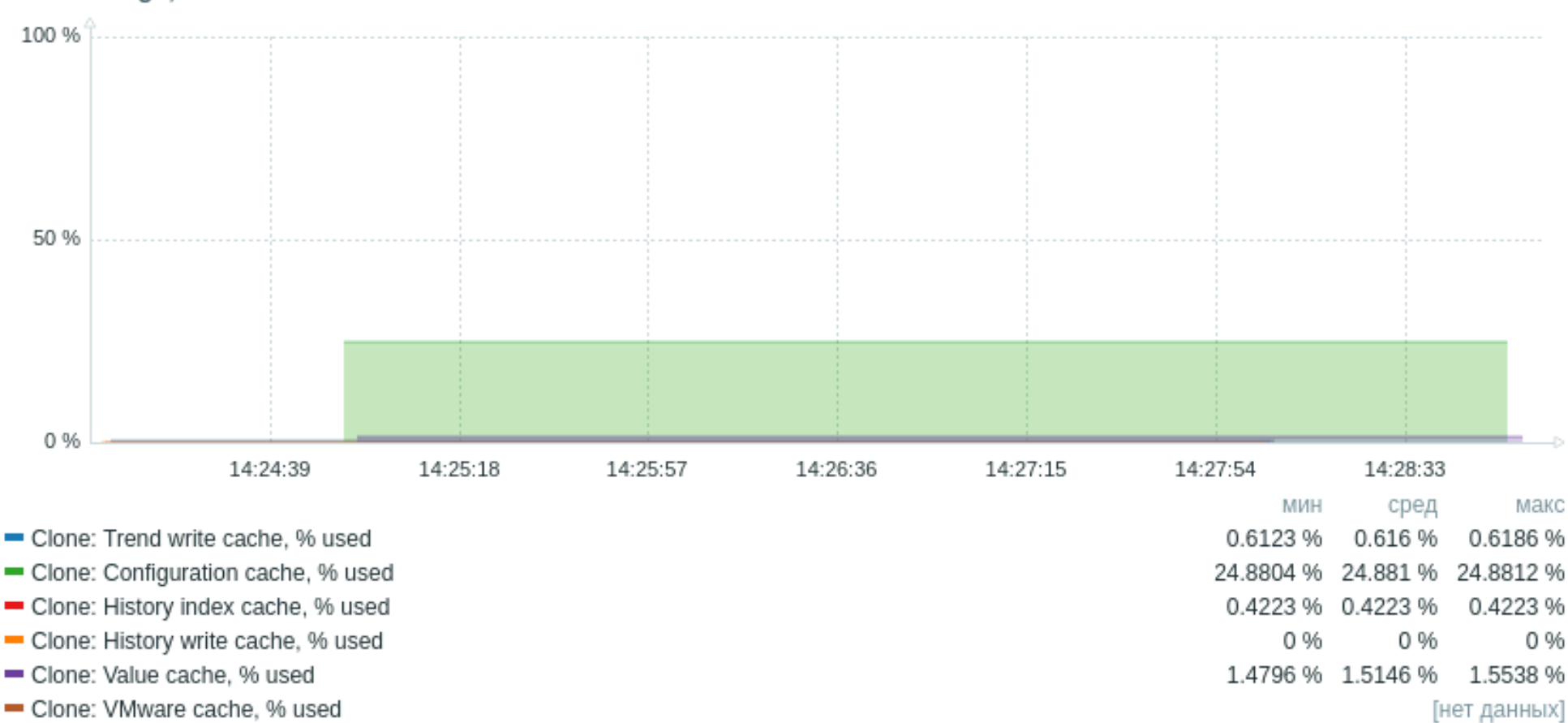
Применить

Сбросить

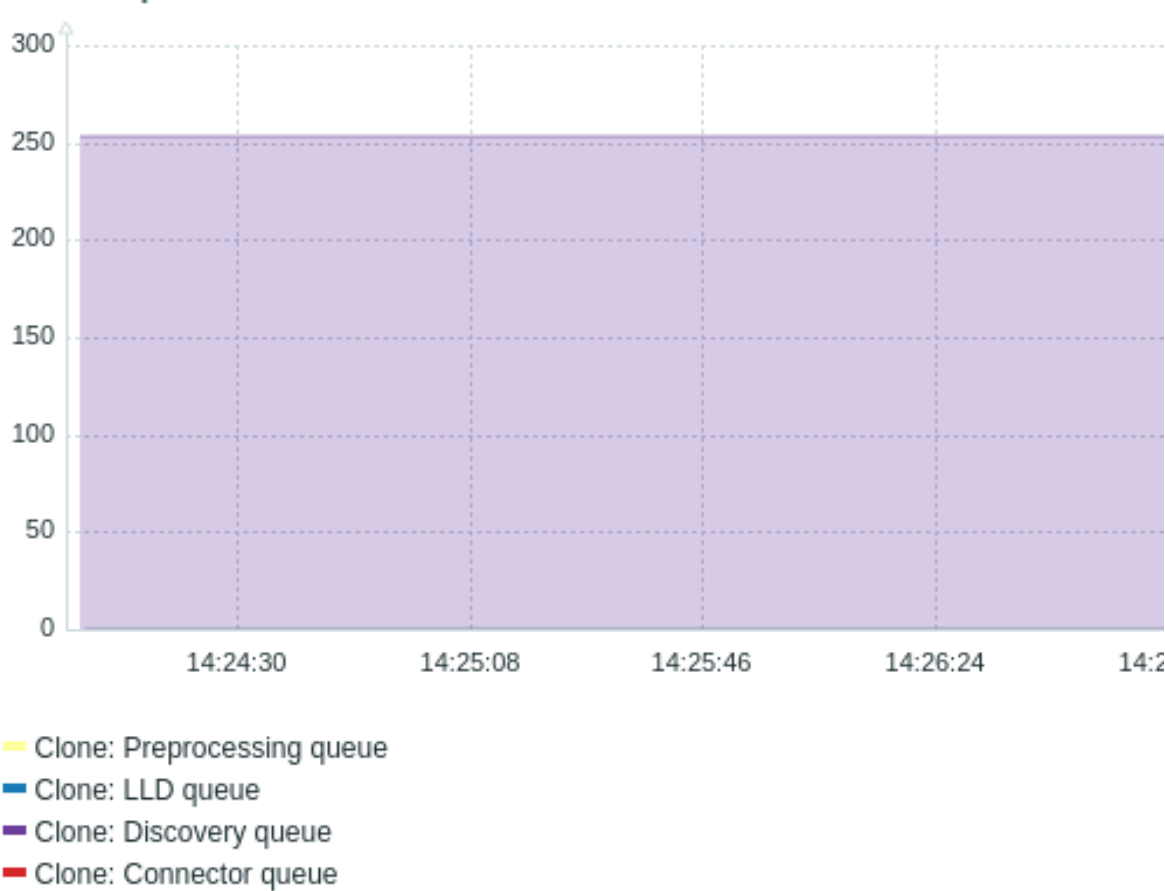
Имя ▲	Интерфейс	Доступность	Теги	Состояние	Последние данные	Проблемы	Графики
Clone	127.0.0.1:10050	ZBX	class: os class: software target: linux ...	Активировано	Последние данные 164	1	Графики 15
CSR1000V	10.10.20.30:161	SNMP	class: network target: cisco target: cisco-ios	Активировано	Последние данные 40	1 1	Графики 4
Debian	10.10.20.20:10050	ZBX	Linux: Debian Среда: Учебная	Активировано	Последние данные 24	1 1	Графики 1
Debian Active	10.10.20.20:10050	ZBX	Linux: Debian Среда: Учебная	Активировано	Последние данные 24	1 1 1	Графики 1
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux ...	Активировано	Последние данные 140	Проблемы	Графики 14

Панели мониторинга узлов сети

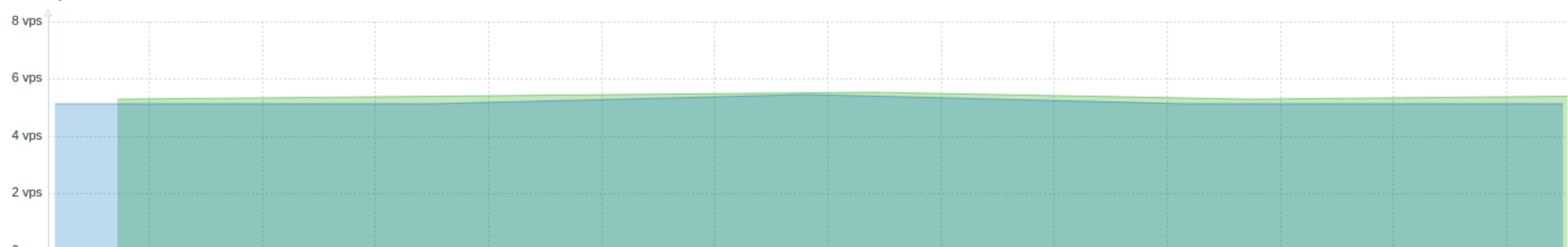
Cache usage, in %



Internal queues



Server performance



Веб-мониторинг

Веб-мониторинг

Группы узлов сети

начните печатать для поиска

Выбрать

Узлы сети

Clone ×
начните печатать для поиска

Выбрать

Теги

ИЛИИли

тег

Содержит

▼

значение

Удалить

Добавить

Применить

Сбросить

Узел сети	Имя ▲	Количество шагов	Последняя проверка	Состояние
Clone	Веб-интерфейс Zabbix	5	31с	OK

Последние данные

☐	Clone	Available memory	44c	5.58 GB	+14.89 MB	component: memory	График
☐	Clone	Available memory in %	42c	71.8902 %	+0.1845 %	component: memory	График
☐	Clone	Checksum of /etc/passwd	20м 46с	9ec6497026c023da9dc4e...		component: security	История
☐	Clone	Configuration cache, % used	48c	24.8811 %		component: system	График
☐	Clone	Connector queue				component: system	График
☐	Clone	Context switches per second	7c	2052.137	+152.5876	component: cpu	График
☐	Clone	CPU guest nice time	5c	0 %		component: cpu	График
☐	Clone	CPU guest time	7c	0 %		component: cpu	График
☐	Clone	CPU idle time	4c	90.6173 %	+0.1817 %	component: cpu	График
☐	Clone	CPU interrupt time	4c	0 %		component: cpu	График
☐	Clone	CPU iowait time	3c	0.6044 %	+0.007648 %	component: cpu	График
☐	Clone	CPU nice time	1c	0 %		component: cpu	График
☐	Clone	CPU softirq time	0	0.2469 %	-0.02589 %	component: cpu	График
☐	Clone	CPU steal time	1м	0 %		component: cpu	График
☐	Clone	CPU system time	58c	1.5598 %	-0.6172 %	component: cpu	График
☐	Clone	CPU user time	57c	7.4551 %	-5.078 %	component: cpu	График

Обнаружение

Обнаруженное устройство ▲	Наблюдаемый узел сети	Доступен/Недоступен
for Cisco Router (1 устройство)		
10.10.20.30	CSR1000V	00:35:11
for Windows (6 устройств)		
10.10.20.1 (_gateway)		11 дней, 08:12:05
10.10.20.2		11 дней, 08:12:05
10.10.20.10 (debian)		11 дней, 08:12:05
10.10.20.20	Debian	00:35:05
10.10.20.30	CSR1000V	00:35:05
10.10.20.50		00:35:05

Карты сетей

Карты сетей

Имя

Применить

Сбросить

☐ Имя ▲	Ширина	Высота	Действия
☐ Local network	680	200	Свойства Изменить

Услуги

Services

[View](#)[Edit](#)[Filter](#)

Name	Status	Root cause	Created at	Tags
Cloud services 3	OK		2018-10-01	sla-id: 695871
Database services 5	High	Service is down, Version has changed	2018-10-01	sla-id: 714492
Network services 2	OK		2018-10-01	sla-id: 293983

Displaying 3 of 3 found

Инвентаризация

Инвентарные данные узла сети

Группы узлов сети

Выбрать

Поле

MAC адрес A

▼

содержит

▼

Применить

Сбросить

Отчеты

Журнал действий

От 

К 

Применить

- Последние 2 дня
- Последние 7 дней
- Последние 30 дней
- Последние 3 месяца
- Последние 6 месяцев
- Последний 1 год
- Последние 2 года
- Вчера
- За день до вчера
- Этот день прошлой недели
- Предыдущая неделя
- Предыдущий месяц
- Предыдущий год

Время	Действие	Способ оповещений	Получатель	Сообщение
31.03.2025 14:07:25	Оповещения по проблемам учебных узлов сети	Email	Admin (Zabbix Administrator) zabbix@training.ru	Тема: Resolved in 9m 31s: Clone has been restarted (uptime < 10m) Сообщение: Problem has been resolved at 17:07:25 on 2025.03.31 Problem name: Clone has been restarted (uptime < 10m) Problem duration: 9m 31s Host: Clone Severity: Warning Original problem ID: 27922

Практическое задание

Выполнить лабораторную работу №18 – Визуализация данных

Учебный центр АйТи Клауд

Оповещения

современные технологии простым языком



Оповещения на события

Чтобы была возможность отправлять и получать оповещения от Zabbix, вы должны:

- настроить какие-нибудь способы оповещения
- настроить действия, которые отправляют сообщения по одному из заданных способов оповещения

Действия состоят из условий и операций. В общем смысле, когда условия удовлетворяются, выполняются операции.

Способы оповещений

Способы оповещений являются каналами доставки при отправке оповещений и предупреждений из Zabbix.

Способы оповещений поддерживают следующие методы доставки:

- Email
- SMS
- Пользовательские скрипты
- Вебхук

Требования для доставки уведомлений от Zabbix конечным пользователям:

- Необходимо определить операцию действия, которая отправляет оповещения
- Необходимо определить работающий способ оповещений (например, Email, который отправляет уведомления через SMTP)
- Информация о доставке на уровне пользователя (например, адреса e-mail, номера телефонов и т.п.) должна быть задана в оповещениях пользователей

Действия

Действия можно задать для событий со всех поддерживаемых источников:

- Действия на триггеры — на события при изменениях состояния триггеров с ОК на ПРОБЛЕМА и обратно
- Действия на услуги — на события при изменениях состояния услуги с ОК на ПРОБЛЕМА и обратно
- Действия на обнаружения — на события, когда производится сетевое обнаружение
- Действия на авторегистрацию — на события автоматической регистрации новых активных агентов (или при изменениях в метаданных узла сети, который уже был зарегистрирован)
- Внутренние действия — на события, когда элементы данных становятся неподдерживаемыми или триггеры переходят в неизвестное состояние

Условия

Действие

Действие [Операции 2](#)

* Имя

Тип вычисления ▼ A and B

Условия

Подпись

Имя

Действие

A

Группа узлов сети равно *Training/Servers*

[Удалить](#)

B

Проблема не подавлена

[Удалить](#)

[Добавить](#)

Активировано ☒

* Должна существовать по крайней мере одна операция.

Обновить

Клонировать

Удалить

Отмена

Операции

Операции по всем событиям:

- Отправка сообщений
- Выполнение удалённых команд

Для событий обнаружения и авторегистрации доступны дополнительные операции:

- Добавление узла сети
- Удаление узла сети
- Активация узла сети
- Деактивация узла сети
- Добавление в группу узлов сети
- Удаление из группы узлов сети
- Добавление тегов уровня узла сети
- Удаление тегов уровня узла сети
- Присоединение шаблона
- Отсоединение шаблона
- Установка режима инвентарных данных узлам сети

При изменении статуса проблемы:

- Операции восстановления
- Операции обновления

Выполнение удаленных команд

По умолчанию удалённые команды отключены как у Zabbix агента, так и у Zabbix прокси. Их можно включить:

- добавив параметр `AllowKey=system.run[*]` в конфигурацию агента;
- изменив параметр `EnableRemoteCommands` на значение «1» в конфигурации прокси.

Эскалации и превентивный мониторинг

С практической точки зрения эскалации означают, что:

- Пользователей можно информировать о новых проблемах незамедлительно
- Оповещения могут повторяться до решения проблемы
- Отправка оповещения может быть выполнена с задержкой
- Оповещения могут эскалироваться другой "более высокой" группе пользователей
- Удаленные команды могут быть выполнены незамедлительно или когда проблема не будет решена за длительный период времени

Пример эскалации №1

New action

Action

Operations 1

* Default operation step duration

30m

Operations

Steps

Details

Start in

Duration

Action

1 - 5

Send message to user groups: MySQL Administrators via Email

Immediately

Default

[Edit](#) [Remove](#)

[Add](#)

Пример эскалации №2

New action



Action

Operations 1

* Default operation step duration

10h

Operations

Steps

Details

Start in

Duration

Action

2

Send message to user groups: Managers via SMS

10:00:00

Default

[Edit](#) [Remove](#)

[Add](#)

Пример эскалации №3

New action

Action

Operations 2

* Default operation step duration

30m

Operations

Steps

Details

Start in

Duration

Action

1 - 0

Send message to user groups: MySQL Administrators via Email

Immediately

Default

[Edit](#) [Remove](#)

5

Send message to users: Database manager (JS) via all media

02:00:00

Default

[Edit](#) [Remove](#)

[Add](#)

Детали операции 2

Operation details

×

Operation

Send message

Steps

5

-

5

(0 - infinitely)

Step duration

0

(0 - use action default)

* At least one user or user group must be selected.

Send to user groups

type here to search

Select

Send to users

Database manager (JS) ×

type here to search

Select

Send to media type

All available

▼

Custom message

☒

Subject

Unacknowledged problem: {EVENT.NAME}

Message

Problem started at {EVENT.TIME} on {EVENT.DATE}
Problem name: {EVENT.NAME}
Host: {HOST.NAME}
Severity: {EVENT.SEVERITY}

Original problem ID: {EVENT.ID}
{TRIGGER.URL}
{ESC.HISTORY}

Conditions

Label	Name	Action
A	Event is not acknowledged	Remove
Add		

Add

Cancel

Пример эскалации №4

New action

Action

Operations 5

* Default operation step duration

30m

Operations

Steps	Details	Start in	Duration	Action
1 - 0	Send message to user groups: MySQL Administrators via Email	Immediately	Default	Edit Remove
5	Send message to users: Database manager (JS) via all media	02:00:00	Default	Edit Remove
6	Run script "Restart MySQL" on current host	02:30:00	Default	Edit Remove
7	Send message to user groups: Guests via all media	03:00:00	Default	Edit Remove
9	Run script "Restart server" on current host	04:00:00	Default	Edit Remove
Add				

Пример эскалации №5

New action



Action

Operations 4

* Default operation step duration

30m

Operations

Steps	Details	Start in	Duration	Action
1 - 4	Send message to user groups: MySQL Administrators via Email	Immediately	Default	Edit Remove
5 - 6	Send message to users: Database manager (JS) via all media	02:00:00	1h	Edit Remove
5 - 7	Send message to user groups: Zabbix administrators via Email	02:00:00	10m	Edit Remove
11	Send message to user groups: Guests via Email	04:00:00	Default	Edit Remove
Add				

Обслуживание

New maintenance period

* Name

DB regular maintenance

Maintenance type

With data collection

No data collection

* Active since

2021-01-01 00:00

* Active till

2031-01-01 00:00

* Periods

Period type	Schedule	Period	Action
Monthly	At 18:00 on day 1 of every January, February, March, April, May, June, July, August, September, October, November, December	1h	Edit Remove

Add

Host groups

Databases

×

type here to search

Select

Hosts

type here to search

Select

* At least one host group or host must be selected.

Tags

And/Or

Or

tag

Contains

Equals

value

Remove

Add

Description

Monthly DB maintenance.

Add

Cancel

Обслуживание узла сети

Zabbix server 	Lack of free swap space on Zabbix server	2015-08-11 23:29:28	3m 3d 10h
	Weekly maintenance [Maintenance with data collection] We break and fix things at this time.		

Подавление проблем

	<u>New host </u>	<u>CPU load too high on New host for</u>
	Suppressed till: 13:05	on New host for
	Maintenance: Weekly maintenance	been restarted

Отслеживание действий

Вы можете увидеть состояние отправленных сообщений в Мониторинг → Проблемы.

В Отчёты → Журнал действий вы увидите подробную информацию обо всех действиях, предпринятых для тех событий, которые имеют какое-либо настроенное действие.

×

Время	Пользователь/Получатель	Действие	Сообщение/Команда	Состояние	Инфо
05.11.2025 07:16:40	Admin (ZabbixAdministrator)	✉	Email	Неудачно	ⓘ
05.11.2025 07:16:40	Admin (ZabbixAdministrator)	✉	Telegram	Отправлено	
05.11.2025 07:16:40	Admin (ZabbixAdministrator)	✉	Email	Неудачно	ⓘ
05.11.2025 07:16:40		📅			

05.11.2025 07:16:40	Оповещение в telegram	Telegram	Admin (Zabbix Administrator) -1003248682874	Тема: Problem: Проблемы с Веб-сервером на сервере Debian Сообщение: Problem started at 10:16:40 on 2025.11.05 Problem name: Проблемы с Веб-сервером на сервере Debian Host: Debian Severity: High Operational data: Web performance 0s Original problem ID: 46526	Отправлено
---------------------	-----------------------	----------	---	---	------------

Практическое задание

Выполнить лабораторную работу №19 – Действия

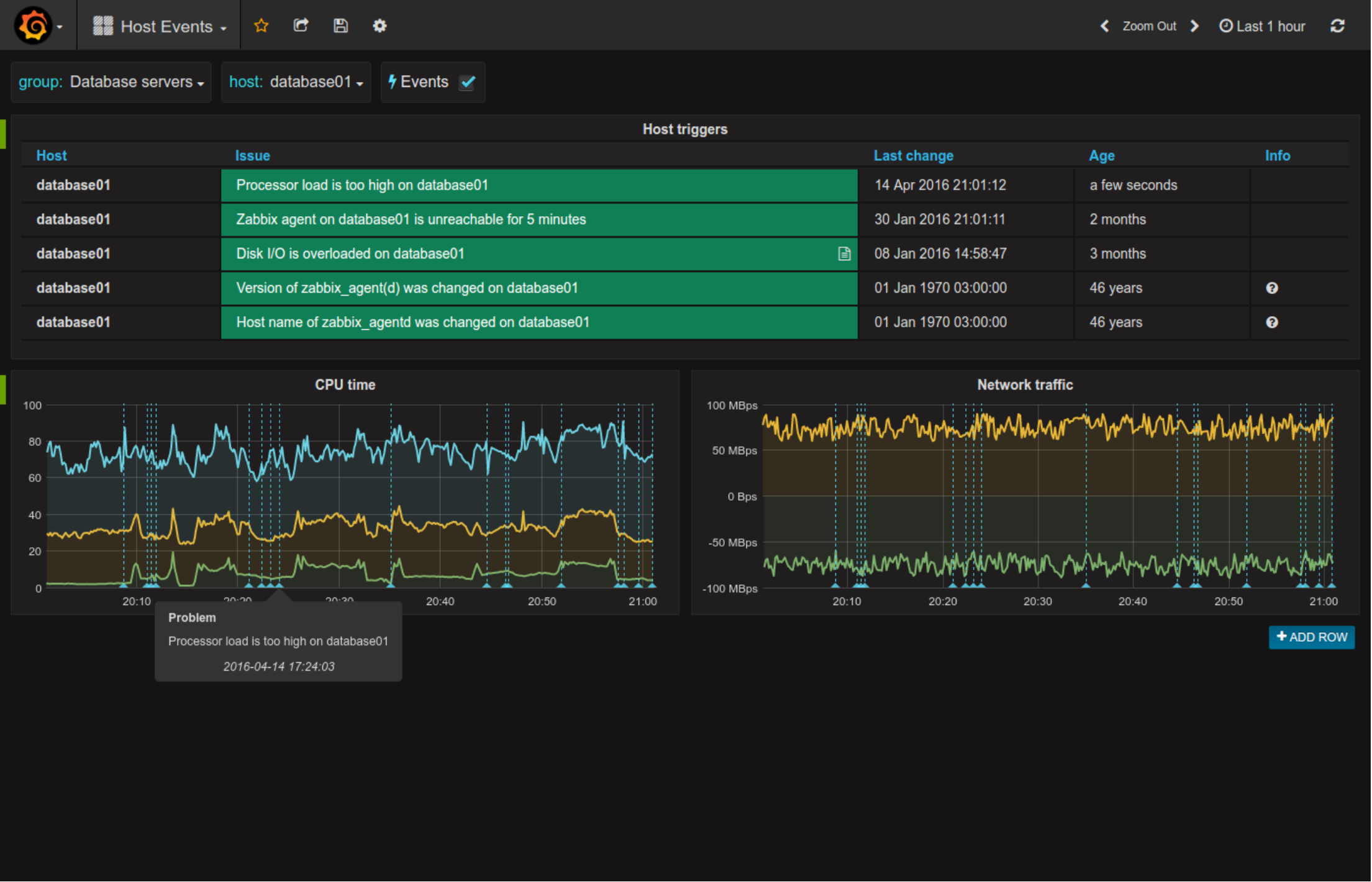
Учебный центр АйТи Клауд

Дополнительные возможности Zabbix

современные технологии простым языком



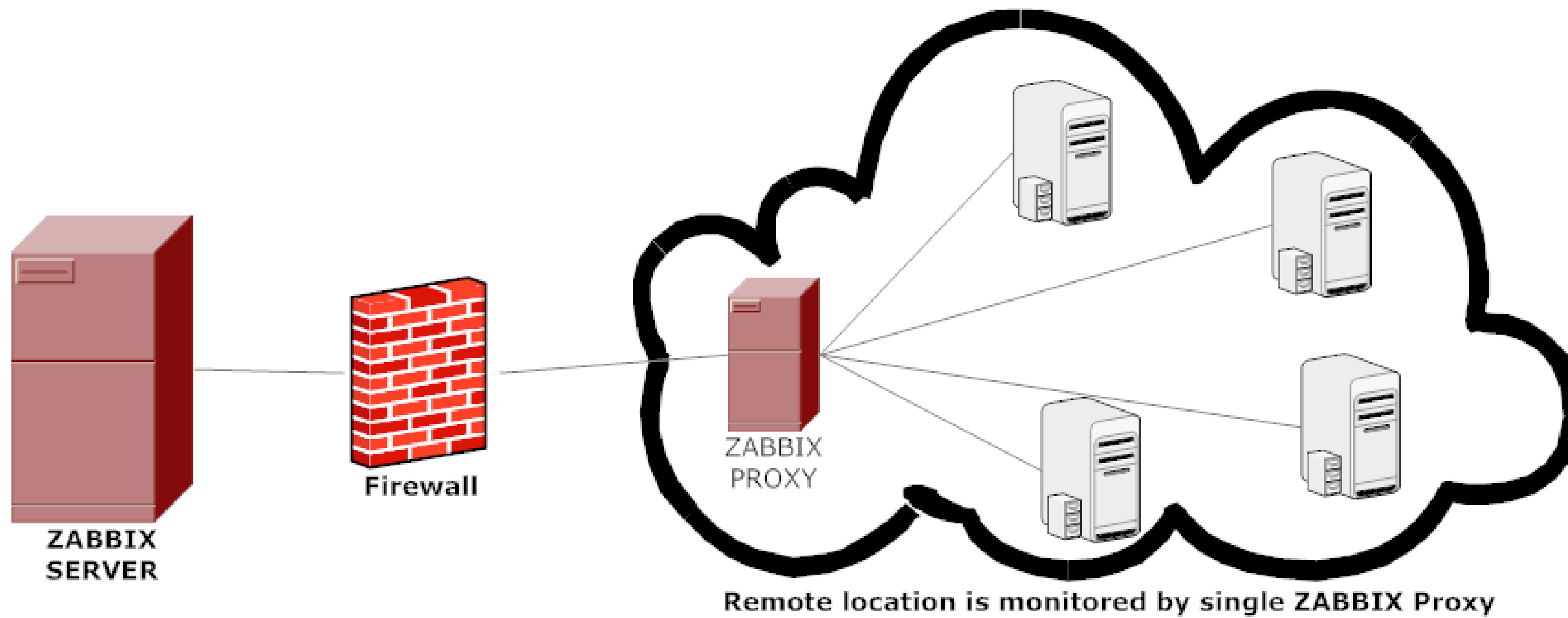
Zabbix API



Пример получения списка хостов с помощью Zabbix API

```
#!/usr/bin/env python3
import requests
import json
URL = "http://ваш-zabbix-сервер/zabbix/api_jsonrpc.php"
USER = "Admin"
PASS = "zabbix"
login = requests.post(URL, json={
    "jsonrpc": "2.0",
    "method": "user.login",
    "params": {"user": USER, "password": PASS},
    "id": 1
}).json()
if "error" in login:
    print("Ошибка:", login["error"])
    exit()
token = login["result"]
print("Авторизация успешна")
hosts = requests.post(URL, json={
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "output": ["host"],
        "limit": 5
    },
    "auth": token,
    "id": 2
}).json()
print(f"\nНайдено хостов: {len(hosts['result'])}")
for i, host in enumerate(hosts["result"], 1):
    print(f"{i}. {host['host']}")
```

Zabbix Proxy



Скрипты

Scripts

Create script

Filter 

☐ Name ▲	Type	Execute on	Commands	User group	Host group	Host access
☐ Detect operating system	Script	Server	sudo /usr/bin/nmap -O {HOST.CONN}	Zabbix administrators	All	Read
☐ MyScripts/Check disk space	Script	Agent	sleep 5 df -h	All	All	Read
☐ MyScripts/Check disk space no sleep	Script	Agent	df -h	All	All	Read
☐ MyScripts/Check disk space S	Script	Server	sleep 11 df -h	All	All	Read
☐ Ping	Script	Server	/bin/ping -c 3 {HOST.CONN}	All	All	Read
☐ Traceroute	Script	Server	/usr/bin/traceroute {HOST.CONN}	All	All	Read

Displaying 6 of 6 found

Практическое задание

Дополнительно:

Выполнить:

Лабораторная работа №20 – Глобальные скрипты

Лабораторная работа №21 – Установка и настройка Zabbix proxy

Учебный центр АйТи Клауд

Zabbix Agent 2 и плагины

современные технологии простым языком

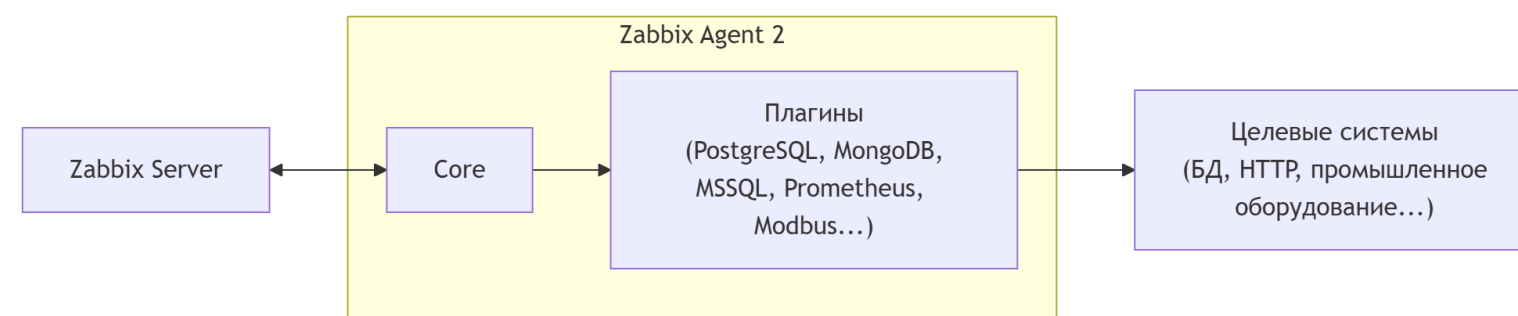


Отличия Zabbix Agent 2 от классического агента

- Язык разработки: Go (Agent 2) vs C (Agent 1)
- Модель выполнения: Goroutine (легковесные потоки) vs fork на каждый запрос
- Плагины: Нативные Go-модули vs UserParameter (внешние скрипты)
- Производительность: Высокая — пул соединений, in-memory кэш
- Persistent Buffer: Да (store-and-forward) — отсутствует в Agent 1
- Горячая перезагрузка: Да (SIGHUP) — Agent 1 требует перезапуска
- Windows PerfCounter: Нативная поддержка без WMI

Архитектура Agent 2

- Модульная архитектура: ядро (Core) + изолированные плагины
- Core: управляет конфигурацией, кэшем, связью с сервером
- Plugins Manager: загрузка/выгрузка/контроль Go-плагинов
- Плагины работают изолированно: сбой плагина не влияет на агент
- Каждый плагин имеет секцию Plugins.<Name> в конфигурации



Установка Zabbix Agent 2

- Linux (Debian/Ubuntu): `apt install zabbix-agent2 zabbix-agent2-plugin-postgresql`
- Linux (RHEL/Rocky): `dnf install zabbix-agent2 zabbix-agent2-plugin-postgresql`
- Windows: MSI-инсталлятор с параметрами SERVER, HOSTNAME, LISTENPORT

Установка подключаемых плагинов

- Linux: `apt/dnf install zabbix-agent2-plugin-<name>` — автоматическая загрузка
- Windows (мастер): запустить MSI, выбрать плагины, завершить
- Windows (CLI): `msiexec /i ... ADDLOCAL=PostgresqlPlugin,MongodbPlugin /qn`
- Конфигурация: `/etc/zabbix/agent2.d/plugins.d/*.conf` или `zabbix_agent2.d\`

Persistent Buffer (буферизация данных)

- Назначение: хранение данных при потере связи с сервером (store-and-forward)
- Хранилище: SQLite-база на диске
- Ключевые параметры: EnablePersistentBuffer, PersistentBufferPeriod, PersistentBufferFile, PersistentBufferSize
- Применение: удалённые площадки, мобильные объекты, нестабильные каналы связи
- FIFO: данные отправляются в порядке очереди после восстановления связи

Учебный центр АйТи Клауд

Мониторинг баз данных PostgreSQL

современные технологии простым языком



Обзор мониторинга PostgreSQL в Zabbix 7.0+

- Рекомендуемый способ: нативный Go-плагин в составе Zabbix Agent 2
- Протокол: pgproto3 (прямое подключение без внешних утилит)
- Преимущества: пул постоянных соединений, prepared statements, кэширование
- UserParameter + psql: устарел — каждый элемент данных создаёт отдельный процесс
- Производительность: выигрыш в 10-50 раз по сравнению с UserParameter

Создание пользователя мониторинга

- Роль pg_monitor: встроенная роль PostgreSQL 10+ для чтения системных представлений
- SQL: CREATE USER zbx_monitor WITH PASSWORD '...' INHERIT; GRANT pg_monitor TO zbx_monitor;
- Безопасность: не использовать суперпользователя, пароль в файле с правами 0640
- TLS: обязателен для Production-сред

Настройка плагина и именованных сессий

- Файл конфигурации: `/etc/zabbix/zabbix_agent2.d/plugins.d/postgresql.conf`
- Default-сессия: `Plugins.PostgreSQL.Default.Uri/User/Password/Database`
- Множественные сессии: `Plugins.PostgreSQL.Sessions.<name>.<param>` для разных инстансов
- Сессия в шаблоне: указывается через макрос `{$PG.SESSION}`

Ключи элементов данных плагина PostgreSQL

- postgresql.ping/up/version/uptime
- postgresql.connections / db.stat / db.size
- postgresql.bgwriter / slow.queries
- postgresql.replication.*: status, recovery, role, lag (bytes/sec), count
- postgresql.custom.query: пользовательские SQL-запросы из файлов
- Все ключи опционально принимают [<session>]

Шаблоны Zabbix для PostgreSQL

- PostgreSQL by Zabbix agent 2: пассивный режим, основной шаблон
- PostgreSQL by Zabbix agent 2 active: активный режим (для >1000 хостов)
- Шаблоны Agent 1: считаются устаревшими в Zabbix 7.0+
- Мониторинг PgBouncer: через отдельную сессию к БД pgbouncer

Основные плагины Zabbix Agent 2

- Prometheus: сбор метрик из /metrics endpoints. Ключ: prometheus.get[<url>]
- MongoDB: мониторинг MongoDB 4.4+ через Wire Protocol. Ключи: mongodb.*
- MSSQL: мониторинг SQL Server через TDS-протокол. Ключи: mssql.*
- Modbus: промышленное оборудование (PLC, SCADA). Ключ: modbus.get[...]
- Каждый плагин: оформлен как отдельный Go-модуль

Учебный центр АйТи Клауд

Оптимизация производительности Zabbix

современные технологии простым языком



Узкие места в архитектуре Zabbix

- База данных: самое частое узкое место (медленные INSERT, блокировки)
- Preprocessing Manager: JavaScript, JSON/XML парсинг — CPU-интенсивные задачи
- Pollers: нехватка поллеров приводит к росту очереди
- History Syncer: частые сбросы кэша — сигнал нехватки HistoryCacheSize
- Housekeeper: DELETE-блокировки при очистке истории

Оптимизация базы данных

- TimescaleDB: гипертаблицы с автоматическим партиционированием и сжатием (рекомендуется)
- Партиционирование MySQL: RANGE по clock с месячными секциями + процедура очистки
- PostgreSQL: `shared_buffers=RAM*0.25`, `effective_cache_size=RAM*0.75`, `work_mem`, `wal_buffers`
- MySQL: `innodb_buffer_pool_size=70% RAM`, `innodb_log_file_size=1-4GB`
- Для SSD: `random_page_cost=1.1`, `effective_io_concurrency=200`

Оптимизация параметров Zabbix Server

- StartPollers = NVP / 50 (один поллер $\approx$ 50 NVP)
- CacheSize: 12-64MB на 1000 элементов данных
- ValueCacheSize: кэш последних значений — ускоряет вычисление триггеров
- HistoryCacheSize / TrendCacheSize: снижают частоту сбросов на диск
- StartPreprocessors, PreprocessingThreads: для тяжёлой предобработки
- Симптом: pfree < 20% — увеличьте соответствующий кэш

Формула расчёта NVP

- $NVP = (\text{элементов_данных} \times \text{коэффициент_изменений}) / 60$
- Коэффициент изменений: 0.3 для стандартных шаблонов, 0.8 для высокодинамичных
- Пример: $50\,000 \text{ элементов} \times 0.8 / 60 = 666 \text{ NVP}$
- NVP 50-200: StartPollers=5, 2 vCPU, 4GB RAM
- NVP 500-1000: StartPollers=20, 4 vCPU, 8GB RAM
- NVP 2000+: StartPollers=40+, 8 vCPU, 16GB+ RAM, кластер БД

Оптимизация элементов данных и housekeeper

- Интервалы: CPU 30-60с, диск 300-600с, inventory 24ч
- Предобработка: Discard unchanged — снижает нагрузку в 10+ раз
- Housekeeper: отключить при TimescaleDB/партиционировании
- Прокси: ProxyBufferSize = NVP × период_хранения × 24
- Сеть: Compression=1 (сжатие трафика), активные проверки для >1000 хостов

Учебный центр АйТи Клауд

Интеграция Zabbix и Grafana

современные технологии простым языком



Зачем Grafana при наличии Zabbix?

- 30+ типов визуализации: против стандартных графиков Zabbix
- Мульти-источники: Zabbix + Prometheus + InfluxDB + SQL на одном дашборде
- Templating: каскадные переменные (Group → Host → Item)
- Annotations: проблемы Zabbix на временной шкале
- Public dashboards: kiosk-режим, расшаривание без аутентификации

Компоненты интеграции

- Grafana OSS: сервер визуализации
- Плагин alexanderzobnin-zabbix-app: источник данных Zabbix
- Два режима подключения: Zabbix API (через веб) или Direct DB Connection
- Установка: grafana-cli plugins install alexanderzobnin-zabbix-app

Типы запросов и переменные

- Metrics: числовые временные ряды от элементов данных
- Text: логи, статусы, версии (нечисловые данные)
- Problems: активные/исторические проблемы с цветовой кодировкой
- Services: SLA-статистика из сервисного дерева
- Переменные: Group, Host, Item, Application — с каскадной фильтрацией

Функции обработки данных

- `groupBy(1m, avg)`: агрегация по времени
- `rate`: преобразование счётчика в скорость (traffic → bits/sec)
- `consolidateBy(max)`: выбор метода консолидации
- `movingAverage(5)`: скользящее среднее для сглаживания
- `asPercent`: расчёт процента (used/total)

Учебный центр АйТи Клауд

Глобальная корреляция событий

современные технологии простым языком



Понятие и необходимость корреляции

- Проблема: один root-cause порождает сотни алертов (каскадный сбой)
- Пример: отказ питания → 500 алертов vs 1 причина + N симптомов
- Решение: глобальная корреляция автоматически закрывает проблемы-симптомы
- Типы корреляции: ручная, по тегам триггеров, правила корреляции, сервисное дерево

Корреляция через теги триггеров

- Теги на триггерах определяют отношения: причина-следствие
- Схема тегов: correlation, cause, root_id, impact, layer, depends_on
- Правило: Оповещения > Корреляция событий > Создать правило
- Условия: фильтр по тегам, важности, группам хостов
- Операции: закрыть связанные проблемы, изменить важность, добавить тег

Практические сценарии

- 1. Отказ коммутатора: `parent_switch` — закрыть проблемы всех хостов за ним
- 2. Плановое обслуживание: `maintenance=true` — подавить все связанные алерты
- 3. Каскад БД: `layer=db` → закрыть проблемы сервисов, понизить важность
- Рекомендации: стандартизировать теги, тестировать в `sandbox`, документировать

Учебный центр АйТи Клауд

Регулярные PDF-отчёты

современные технологии простым языком



Обзор Scheduled Reports в Zabbix 7.0+

- Генерация: PDF из любого дашборда по расписанию
- Расписание: ежедневно, еженедельно, ежемесячно, ежегодно
- Доставка: по Email через Media Type
- Макросы в теме: {TIME}, {DATE}, {HOSTNAME}
- Архитектура: Zabbix Web Service (Chromium) → Report Writers → Email

Установка и настройка

- Web Service: `apt install zabbix-web-service`
- Конфиг: `/etc/zabbix/zabbix_web_service.conf` (ListenPort, AllowedIP, DashboardTimeout)
- Zabbix Server: `WebServiceURL=http://127.0.0.1:10053/report`, `StartReportWriters=3`
- Frontend URL: Администрирование > Общие > Другие — указать URL фронтенда
- Email: создать тип оповещения Email, назначить пользователю

Создание и тестирование отчёта

- Отчёты > Регулярные отчеты > Создать отчет
- Параметры: имя, дашборд, период (прошлый день/неделя/месяц), цикл, время
- Получатели: пользователи и группы пользователей
- Права: отчёт содержит данные, которые видит генератор (пользователь)
- Тестирование: кнопка Test — PDF приходит на Email

Сценарии использования

- 1. Ежедневный SLA: IT-менеджеру в 09:00 — дашборд SLA Compliance
- 2. Еженедельный тех. отчёт: администраторам в Пн 08:00 — все метрики за неделю
- 3. Ежемесячный бизнес-отчёт: руководству 1-го числа — аптайм, инциденты, тренды

Учебный центр АйТи Клауд

Прогнозирующие функции Zabbix

современные технологии простым языком



Обзор прогнозирующих функций

- Функции:
- `forecast()` — «Какое значение примет метрика через заданное время?» — прогноз в будущее
- `timeleft()` — «Через сколько времени метрика достигнет порога?» — время до достижения
- Принцип: анализ исторических данных → аппроксимация кривой → прогноз
- Применение: заполнение диска, тренды CPU, планирование памяти, перегрев
- Результат: проактивное оповещение — замена «скорой помощи» на превентивную диагностику

Функция *forecast()*

- Синтаксис: `forecast(period, time_shift, fit, mode, duration)`
- `period`: окно обучения (1h, 7d, 30d)
- `time_shift`: смещение прогноза (900 — 15 мин, 3600 — 1 час)
- `fit`: linear, polynomial2, exponential, logarithmic, power
- `mode`: value, max, min, avg, delta, count
- # Прогноз CPU через 15 минут:
`forecast(/host/system.cpu.load, 30m, 15m, linear, max) > 90`

Trigger: `forecast(...) > 90` # CPU >90% через 15 мин

Функция *timeleft()*

- Синтаксис: `timeleft(period, threshold, fit, mode, duration)`
- `period`: окно обучения (1h, 7d)
- `threshold`: пороговое значение (95%, 5G, 100M)
- `fit`: linear, polynomial2, exponential, logarithmic, power
- Результат: время в секундах до достижения порога
- # Когда диск / будет заполнен на 95%?
`timeleft(/host/vfs.fs.size[/,pused], 7d, 95, linear, value) < 604800`

Trigger: `timeleft(...) < 604800` # Менее 7 дней до 95%

Модели аппроксимации (*fit*)

- linear: $y = a \cdot t + b$ — для линейных трендов (диск, память, лог-файлы)
- polynomial2: $y = a_0 + a_1 t + a_2 t^2$ — для нелинейных процессов с ускорением
- exponential: $y = a \cdot e^{(b \cdot t)}$ — для экспоненциального роста (ошибки, цепные реакции)
- logarithmic: $y = a \cdot \ln(t) + b$ — для насыщающихся процессов (кэш, архивация)
- Рекомендация: для большинства метрик IT используйте linear — устойчив к шумам

Режимы обработки данных (mode)

- value: аппроксимация по всем исходным значениям (по умолчанию) — для метрик с низкой частотой опроса
- min: по минимальным значениям в каждом интервале — поиск нижней границы тренда (мин. свободное место)
- max: по максимальным значениям — поиск верхней границы (пиковый CPU, макс. температура)
- avg: по средним значениям — наиболее устойчив к выбросам (средняя загрузка CPU, трафик)
- delta: по разности значений за интервал duration — скорость изменения (счётчики net.if.in, disk.io)
- count: по количеству изменений в интервале — метрики количества событий (ошибки в логе)

Проактивное оповещение о заполнении диска

- Задача: Через сколько времени диск / будет заполнен на 95%?
- `timeleft(/host/vfs.fs.size[/,pused], 7d, 95, linear, value)`
- Период обучения: 7 дней исторических данных
- Порог: 95% заполнения
- Модель: `linear` — консервативный прогноз по прямой
- Режим: `value` — все исходные значения без агрегации
- Триггер: `timeleft(...) < 604800 AND timeleft(...) > 0` (7 дней до заполнения)

Прогнозирование пиковой нагрузки CPU

- Задача: Какая будет максимальная загрузка CPU через 15 минут?
- `forecast(/host/system.cpu.load, 30m, 15m, linear, max)`
- Период обучения: 30 минут истории
- Прогноз: на 15 минут вперёд
- Модель: `linear` — линейная регрессия
- Режим: `max` — по пиковым значениям в каждом интервале
- Триггер: `forecast(...) > 90` (CPU превысит 90% через 15 мин)

Планирование увеличения памяти

- Задача: Через сколько дней использование памяти достигнет 90%?
- `timeleft(/host/vm.memory.size[pused], 30d, 90, linear, avg)`
- Период обучения: 30 дней исторических данных
- Порог: 90% использования ОЗУ
- Модель: `linear` — устойчива к кратковременным пикам
- Режим: `avg` — средние значения для сглаживания выбросов
- Триггер: `last(...) < 90 AND timeleft(...) < 2592000` (30 дней до 90%)

Прогноз температуры в серверной

- Задача: Какая будет температура в серверной через 2 часа?
- `forecast(/host/sensor.temp[rack_01], 2h, 7200, linear, value)`
- Период обучения: 2 часа истории
- Прогноз: на 7200 секунд (2 часа) вперёд
- Модель: `linear` — температура меняется плавно
- Режим: `value` — без агрегации
- Триггер: `forecast(...) > 40` (температура превысит 40°C через 2ч)

Рост лог-файла приложения

- Задача: Через сколько времени лог-файл достигнет 100 МБ?
- `timeleft(/host/vfs.file.size[/var/log/app.log], 3h, 100M, linear, value)`
- Период обучения: 3 часа истории роста лога
- Порог: 100M (104 857 600 байт)
- Модель: `linear` — рост лога обычно равномерный
- Режим: `value` — все исходные значения
- Триггер: `timeleft(...) < 1h` (менее часа до 100 МБ)

Исчерпание *inode* на файловой системе

- Задача: Через сколько дней количество свободных *inode* упадёт ниже 1000?
- `timeleft(/host/vfs.fs.inode[/,free], 1d, 1000, linear, value)`
- Период обучения: 24 часа истории
- Порог: 1000 свободных *inode*
- Модель: `linear` — линейное потребление *inode*
- Режим: `value` — без агрегации
- Триггер: `timeleft(...) < 2d` (менее 2 дней до исчерпания *inode*)

Рост таблицы базы данных

- Задача: Через сколько дней таблица main_table достигнет 50 ГБ?
- timeleft(/host/db.size[main_table], 7d, 50G, linear, value)
- Период обучения: 7 дней истории роста таблицы
- Порог: 50G (53 687 091 200 байт)
- Модель: linear — рост таблиц БД близок к линейному
- Режим: value — исходные значения
- Триггер: timeleft(...) < 14d (менее 14 дней до 50 ГБ)

Рекомендации по применению

- Минимум 10–20 точек данных: для достоверного прогноза. Период сбора ≥ 10 интервалов опроса.
- Ограничьте период прогноза: не дальше 30–50% от длины исторического периода.
- Тестируйте forecast: сначала в вычисляемом элементе, сравнивайте с фактическими данными за прошлый период.
- Комбинируйте с триггерами: прогноз + традиционный триггер для предотвращения ложных срабатываний.
- Учитывайте сезонность: функции не учитывают ежедневные/еженедельные циклы — для сезонных метрик прогнозы могут быть неточными.
- Мониторьте качество: дашборд с forecast() за прошлые периоды для постоянной оценки точности.
- Комбинированный триггер:
(timeleft(/host/key,30d,95,linear,value) < 604800
AND timeleft(...) > 0)
OR
last(/host/key) > 90

Ограничения прогнозирующих функций

- Отсутствие сезонности: модели не учитывают периодические паттерны (часы, дни недели) — только общий тренд.
- Чувствительность к выбросам: один аномальный замер может исказить прогноз. Используйте `mode=avg` для сглаживания.
- Нагрузка на CPU: аппроксимация на Zabbix Server. Избегайте `period > 90` дней при сотнях вычисляемых элементов.
- Нет доверительного интервала: точечный прогноз без `confidence interval`. Добавьте запас в триггерах.
- Отрицательные значения/NaN: для `logarithmic/power` при неподходящих данных. Проверьте `forecast(...) > 0`.
- Не поддерживается на прокси: только пассивный режим на Zabbix Server (до Zabbix 7.0).

Спасибо, что выбрали обучение в УЦ АйТи Клауд!

Желаем успешно применить полученные знания
на практике!

И будем ждать новых
встреч!

Связаться с преподавателем pgruzdev@itcloud-edu.ru

Наш сайт

