



ZABBIX 5.0

КАК СДЕЛАТЬ МОНИТОРИНГ
ЕЩЕ БЕЗОПАСНЕЕ С ZABBIX 5.0

01

ШИФРОВАНИЕ МЕЖДУ ВЕБ-ИНТЕРФЕЙСОМ И БАЗОЙ ДАННЫХ

- ☑ Используется TLS-шифрование



НАСТРОЙКА ШИФРОВАНИЯ

ZABBIX

Welcome

Check of pre-requisites

Configure DB connection

Zabbix server details

Pre-installation summary

Install

Configure DB connection

Database port 0 - use default port

Database name

User

Password

TLS encryption

TLS key file

TLS certificate file

TLS certificate authority file

With host verification

TLS cipher list

НАСТРОЙКА ШИФРОВАНИЯ

- ✓ Основано на использовании сертификатов TLS
- ✓ Поддерживается для MySQL и PostgreSQL
- ✓ Верификация узлов – имя узла БД должно совпадать с именем узла (CN) на которое выдан сертификат
- ✓ Если TLS параметры указывают на файлы, доступные для записи, то появится предупреждение о необходимости доступности только для чтения

02

ШИФРОВАНИЕ МЕЖДУ СЕРВЕРОМ/ПРОКСИ И БАЗОЙ ДАННЫХ

- ☑ Также используется привычное TLS-шифрование



НАСТРОЙКА ШИФРОВАНИЯ

```
### Option: DBTLSConnect
```

```
DBTLSConnect=
```

```
### Option: DBTLSCAFile
```

```
DBTLSCAFile=
```

```
### Option: DBTLSCertFile
```

```
DBTLSCertFile=
```

```
### Option: DBTLSKeyFile
```

```
DBTLSKeyFile=
```

```
### Option: DBTLSCipher
```

```
DBTLSCipher=
```

```
### Option:DBTLSCipher13
```

```
DBTLSCipher13=
```

ПРИМЕР ПРИМЕНЕНИЯ – ПРОСТОЕ ШИФРОВАНИЕ

- ☑ Соединение к БД будет зашифровано (без аутентификации и проверки хоста)

```
### Option: DBTLSConnect  
DBTLSConnect=required
```

ПРИМЕР – ШИФРОВАНИЕ И ВЕРИФИКАЦИЯ

- ☑ Соединение к БД будет зашифровано а сертификат БД проверен

```
### Option: DBTLSConnect  
DBTLSConnect= verify_ca  
### Option: DBTLSCAFile  
DBTLSCAFile=/tmp/certs/cafile.crt
```


ПРИМЕР – ШИФРОВАНИЕ И ВЕРИФИКАЦИЯ

- ☑ Соединение к БД будет зашифровано, сертификат проверен так же как и имя узла должно соответствовать сертификату

```
### Option: DBTLSConnect  
DBTLSConnect= verify_full  
### Option: DBTLSCAFile  
DBTLSCAFile=/tmp/certs/cafile.crt
```

ПРИМЕР – МАКСИМУМ БЕЗОПАСНОСТИ

- ☑ Соединение к БД будет зашифровано, сертификат проверен, имя узла должно соответствовать сертификату, сам сервер\прокси Zabbix используют сертификат для аутентификации, а подключение будет установлено только если используются алгоритмы шифрования из списка

```
### Option: DBTLSConnect
DBTLSConnect= verify_full
### Option: DBTLSCAFile
DBTLSCAFile=/tmp/certs/cafile.crt
### Option: DBTLSCertFile
DBTLSCertFile=
### Option: DBTLSKeyFile
DBTLSKeyFile=
### Option: DBTLSCipher
DBTLSCipher=
### Option:DBTLSCipher13
DBTLSCipher13=
```

03



ВЫБОР РАЗРЕШЕННЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

- ☑ Возможность настроить наборы шифров в соответствии с вашей политикой безопасности
- ☑ Настройки на уровне Zabbix компонента

ФУНКЦИОНАЛЬНОСТЬ И ПРЕИМУЩЕСТВА

- ✓ Возможность переопределить встроенный набор шифров
- ✓ Можно переопределить для сертификатов, PSK ключей или для тех и других
- ✓ `zabbix_get` и `zabbix_sender` могут следовать тем же настройкам при помощи параметров `--tls_cipher13` или `--tls_cipher`
- ✓ Позволяет выбирать конкретные шифры на основе вашей политики безопасности или дополнительных требований
- ✓ Отдельные параметры для TLS 1.3 и 1.2
- ✓ Настраивается для входящих / исходящих соединений для каждого компонента

НОВЫЕ ПАРАМЕТРЫ КОНФИГУРАЦИИ

```
### Option: TLSCipherCert13
```

```
# TLSCipherCert13=
```

```
### Option: TLSCipherCert
```

```
# TLSCipherCert=
```

```
### Option: TLSCipherPSK13
```

```
# TLSCipherPSK13=
```

```
### Option: TLSCipherPSK
```

```
# TLSCipherPSK=
```

```
### Option: TLSCipherAll13
```

```
# TLSCipherAll13=
```

```
### Option: TLSCipherAll
```

```
# TLSCipherAll=
```

04






СКРЫТЫЕ МАКРОСЫ



ВОЗМОЖНОСТЬ СКРЫТЬ СВОИ МАКРОСЫ В ВЕБ-ИНТЕРФЕЙСЕ

- ☉ Просто выберите из выпадающего списка должно ли значение этого макроса быть видимым

СПРЯЧЬТЕ СЕКРЕТНЫЕ ЗНАЧЕНИЯ МАКРОСОВ!


Macro	Value		Description
<code>{\$CONNECTION_STRING}</code>	 v	ODBC connection string
<code>{\$PASSWORD}</code>	 v	User password
<code>{\$SNMP_COMMUNITY}</code>	 ^	SNMP Community

[Add](#)
.....

-  Text
-  Secret text

СКРЫТЫЕ МАКРОСЫ. ЗАМЕТКИ

- ✓ При клонировании узлов сети или шаблонов с макросами – значения сбрасываются :

 The cloned host contains user defined macros with type "Secret text". The value and type of these macros were reset. ✕

- ✓ Скрытое значение недоступно при экспорте узлов сети

```
<macro>
  <macro>{ $PASSWORD}</macro>
  <type>SECRET_TEXT</type>
  <description>Password</description>
</macro>
```

- ✓ Один раз определив, нет возможности изменить – макрос придется задать заново.

Macro	Value	Description	
<input type="text" value="{ \$NOTSECRET}"/>	<input type="text" value="password"/> T ▾	<input type="text" value="Not secret password"/>	Remove
<input type="text" value="{ \$PASSWORD}"/>	<input type="text" value="Set new value"/> 🔒 ▾	<input type="text" value="Password"/>	Remove

05

An abstract digital graphic featuring a central red ring with a grid pattern, surrounded by blue and red glowing lines and binary code (0s and 1s) scattered across the scene.

ДЛЯ ХЕШИРОВАНИЯ ПАРОЛЕЙ
ВЕБ-ИНТЕРФЕЙСА ИСПОЛЬЗУЕТСЯ
VSCRYPT ВМЕСТО MD5

- ☑ При хешировании паролей используется vscrypt
- ☑ Более безопасный подход

ПРЕИМУЩЕСТВО ПЕРЕХОДА НА **BCRYPT**

- ✓ Основан на алгоритме Blowfish
- ✓ Гораздо сложнее вычислить хеши, чем при использовании MD5
- ✓ Больше сложностей для атак перебором
- ✓ Старые хеши MD5 заменяются на bcrypt после первого входа
- ✓ Использует уникальное соль-значение
- ✓ Невозможность атак с использованием радужных таблиц

06

An abstract digital graphic featuring a central red ring with a grid pattern, surrounded by blue and red glowing lines and binary code (0s and 1s) scattered across the scene.

ВСТРОЕННАЯ ПОДДЕРЖКА SAML

- ⦿ Нативная поддержка zabbix saml-технологии единого входа

НАСТРОЙКА ИНТЕГРАЦИИ С SAML

Authentication HTTP settings LDAP settings **SAML settings**

Enable SAML authentication

* IdP entity ID

* SSO service URL

SLO service URL

* Username attribute

* SP entity ID

SP name ID format

Sign Messages
 Assertions
 AuthN requests
 Logout requests
 Logout responses

Encrypt Name ID
 Assertions

Case sensitive login

НАСТРОЙКА ИНТЕГРАЦИИ С SAML

- ✓ Соответствующий пользователь должен существовать в Zabbix, однако его пароль Zabbix не будет использоваться.
- ✓ Необходимо предварительно настроить провайдера идентификации
- ✓ Расположение по умолчанию для закрытого ключа и сертификата - `ui/conf/certs/`
- ✓ Некоторые настройки – SP-ключ, SP/IDP сертификаты и доп.параметры – можно сконфигурировать в файле `zabbix.conf.php`

07

An abstract digital graphic featuring a central red ring with a grid pattern, surrounded by glowing blue and red lines and binary code (0s and 1s) scattered across the scene. The background is a dark blue gradient.

СПИСОК ЗАПРЕЩЁННЫХ/РАЗРЕШЁННЫХ ЭЛЕМЕНТОВ ДАННЫХ ДЛЯ УЗЛА СЕТИ

- ☉ Белый/чёрный список ключей элементов данных
- ☉ Указывайте конкретные ключи или используйте * (символ подстановки)

НАСТРОЙКА ОГРАНИЧЕНИЙ ДЛЯ МЕТРИК

- ✓ EnableRemoteCommands также требуется!
- ✓ Проверка правил останавливается после первого совпадения
- ✓ AllowKey может быть использован только если DenyKey определён
- ✓ Если ключ элемента данных запрещён в конфигурации агента, ЭД станет неподдерживаемым
- ✓ Zabbix_agentd с опцией `-print (-p)` не покажет список ЭД, которые не разрешены в конфигурации;
- ✓ Zabbix_agentd с опцией `-test (-t)` вернёт статус "Unsupported item key." для не разрешённых в конфигурации ключей ЭД. Эквивалентно для запросов с помощью `zabbix_get` с опцией `-k`


ПОРЯДОК ПАРАМЕТРОВ **ИМЕЕТ ЗНАЧЕНИЕ!**

```
### Option: DenyKey
```

```
DenyKey=system.run[*]
```

```
### Option: AllowKey
```

```
AllowKey=system.run[ls -la /tmp]
```

<input type="checkbox"/>	Wizard	Name ▲	Triggers	Key	Interval	History	Trends	Type	Applications	Status	Info
<input type="checkbox"/>	...	file list		system.run[ls -la /tmp]	30s	90d		Zabbix agent		Not supported	

0 selected

Unsupported item
key.

ПОРЯДОК ПАРАМЕТРОВ **ИМЕЕТ ЗНАЧЕНИЕ!**

```
### Option: AllowKey
```

```
AllowKey=system.run[ls -la /tmp]
```

```
### Option: DenyKey
```

```
DenyKey=system.run[*]
```

<input type="checkbox"/>	Wizard	Name ▲	Triggers	Key	Interval	History	Trends	Type	Applications	Status	Info
<input type="checkbox"/>	...	file list		system.run[ls -la /tmp]	30s	90d		Zabbix agent		Enabled	

Displaying 1 of 1 found

0 selected

Enable

Disable

Execute now

Clear history

Copy

Mass update

Delete

08



ПОДДЕРЖКА ПАРАМЕТРОВ ПОДКЛЮЧЕНИЯ ODVC ПРЯМО В КЛЮЧЕ ЭЛЕМЕНТА ДАННЫХ

- ☉ Параметр DSN теперь опционален
- ☉ Новый параметр ключа для опций подключения

DSN ИЛИ СТРОКА ПОДКЛЮЧЕНИЯ?

- ✓ У пользователей может отсутствовать доступ к `odbc.ini`
- ✓ Определение параметров подключения на уровне элемента данных
- ✓ Строка подключения или DSN должны присутствовать. Если присутствуют оба – DSN игнорируется
- ✓ Строка подключения может содержать особые настройки драйверов

ИЗМЕНЕНИЯ В КЛЮЧЕ ЭЛЕМЕНТА ДАННЫХ **ODBC**

Старый ключ:

```
db.odbc.select[<unique short description>,dsn]
```

Новый ключ:

```
db.odbc.select[<unique short description>,<dsn>,<connection string>]
```

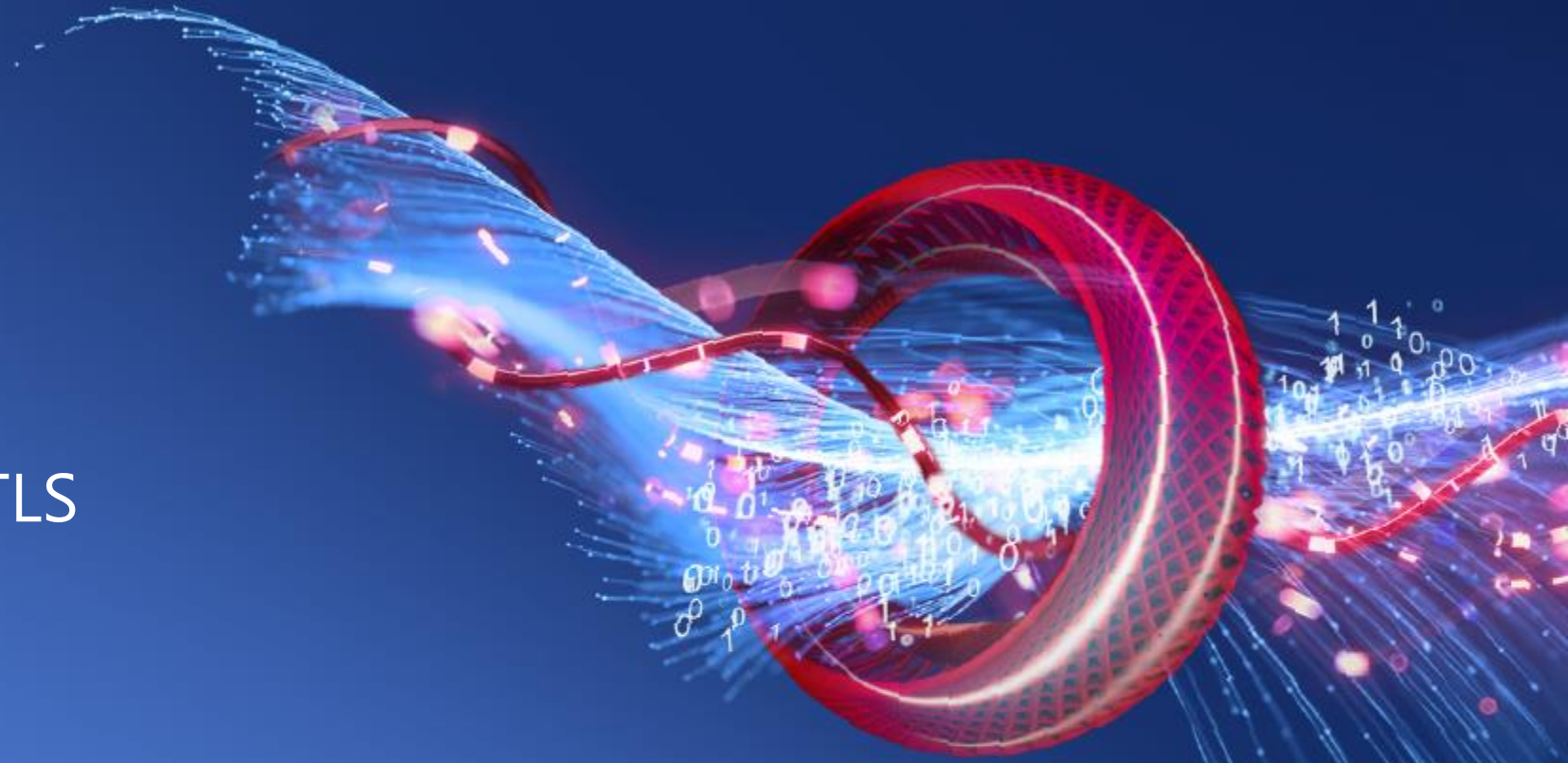
Пример строки подключения:

```
"Driver=/usr/local/lib/libmyodbc5a.so;Database=master;Server=127.0.0.1;Port=3306"
```

09

ПОДДЕРЖКА MBED TLS ПРЕКРАЩЕНА

- ☞ Поддержка версий mbed TLS подошёл к концу



ПОЧЕМУ?

- ✓ Ранее поддерживались версии mbed TLS 1.3.9 и поздние версии 1.3.x.
- ✓ Отсутствие интереса/вариантов применения со стороны сообщества
- ✓ Экономит накладные расходы на разработку
- ✓ Лучше сфокусироваться на поддержке OpenSSL и GnuTLS

10

An abstract digital graphic featuring a central red ring with a grid pattern, surrounded by blue and red light trails and binary code (0s and 1s) floating in the background.

AUDITLOG.GET

- ☑ Новый объект API
- ☑ Новый метод `auditlog.get`

ПРИМЕР РАБОТЫ **AUDITLOG.GET**

The screenshot displays a REST client interface with two main panels: 'JSON' on the left and 'Preview' on the right. The 'JSON' panel shows a request body with the following structure:

```
1 {
2   "jsonrpc": "2.0",
3   "method": "auditlog.get",
4   "params": {
5     "output": "extend",
6     "sortfield": "clock",
7     "sortorder": "DESC",
8     "limit": 2
9   },
10  "id": 1,
11  "auth": "5c4e8ee5e42b556535f1a6e512877d7f"
12 }
```

The 'Preview' panel shows the response body, which is a JSON array of two objects:

```
1 {
2   "jsonrpc": "2.0",
3   "result": [
4     {
5       "auditid": "188",
6       "userid": "1",
7       "clock": "1589506616",
8       "action": "3",
9       "resourcetype": "0",
10      "note": "",
11      "ip": "192.168.1.141",
12      "resourceid": "0",
13      "resourceidname": ""
14    },
15    {
16      "auditid": "187",
17      "userid": "1",
18      "clock": "1589388014",
19      "action": "0",
20      "resourcetype": "0",
21      "note": "",
22      "ip": "192.168.1.141",
23      "resourceid": "5",
24      "resourceidname": "user2"
25    }
26  ],
27  "id": 1
28 }
```

At the bottom of the interface, there are two tabs: 'Beautify JSON' on the left and '\$.store.books[*].author' on the right, with a help icon on the far right.

ЖУРНАЛ АУДИТА: **ОБЪЕКТ И МЕТОД**

- ✓ Фильтрация по ID аудита и/или ID пользователей
- ✓ Возможность поиска по старому/новому значениям
- ✓ Объект содержит информацию о типе действия, типе ресурса, IP-адресе, идентификаторах ресурса, именах и другие сведения.
- ✓ Большой потенциал для анализа данных аудита и уведомлений о критических изменениях

11

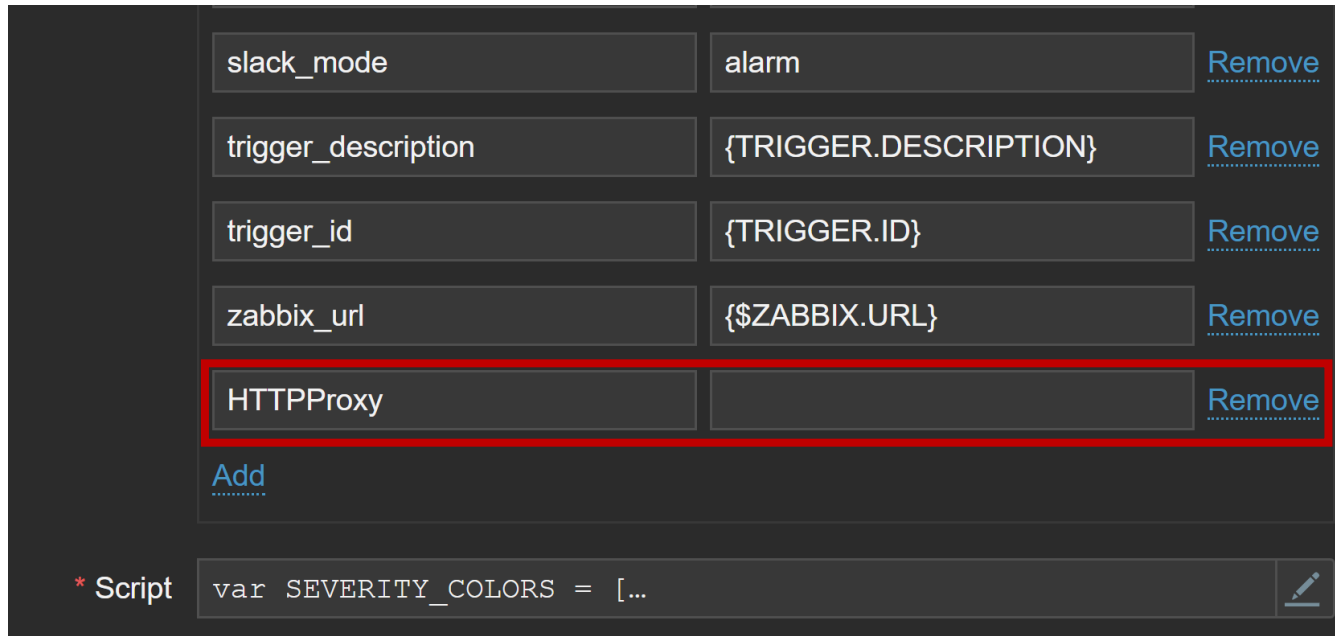


HTTP PROXY В WEBHOOKS

- ⊙ Добавлена возможность использовать webhooks с http прокси

НАСТРОЙКА **WEBHOOK** С HTTP ПРОКСИ

- ✓ Вы можете указать HTTP прокси



slack_mode	alarm	Remove
trigger_description	{TRIGGER.DESCRPTION}	Remove
trigger_id	{TRIGGER.ID}	Remove
zabbix_url	{\$ZABBIX.URL}	Remove
HTTPProxy		Remove

[Add](#)

* Script `var SEVERITY_COLORS = [...]`

- ✓ Логика таже что и при работе с HTTP агентом
- ✓ Нужно просто указать HTTPProxy. Синтаксис:

```
[protocol://] [username[:password]@] proxy.mycompany.com[:port]
```

12

An abstract digital graphic featuring a central red ring with a grid pattern, surrounded by glowing blue and red lines and binary code (0s and 1s) scattered across the scene.

ПРОВЕРКА КОДИРОВКИ БД

- ⊙ Предупреждение отображается во время начальной настройки интерфейса
- ⊙ Предупреждение отображается на уже запущенных экземплярах

ПРИМЕР КАК НЕ НАДО ДЕЛАТЬ

Hostid:10325



ABC

Hostid:10326



Abc

Hostid:10327



AbC

Warning: Cannot update host

Host "Abc" already exists. [hosts.php:856 → CApiWrapper->__call() → CFrontendApiWrapper->callMethod() → CApiWrapper->callMethod() → CFrontendApiWrapper->callClientMethod() → CLocalApiClient->callMethod() → CHost->update() → CHost->massUpdate() → CApiService::exception() in include/classes/api/services/CHost.php:1063]

All hosts / **Abc** Enabled ZBX SNMP JMX IPMI Applications 2 Items 44 Triggers 3 Graphs 5 Discovery rules 2 Web scenarios

Host **Templates** IPMI Tags Macros Inventory Encryption

Linked templates	Name	Action
Link new templates	Template App Docker ✕ type here to search	Select

Update Clone Full clone Delete Cancel

ПРЕДУПРЕЖДЕНИЕ В ХОДЕ ПЕРВОНАЧАЛЬНОЙ НАСТРОЙКИ

ZABBIX

Welcome

Check of pre-requisites

Configure DB connection

Zabbix server details

Pre-installation summary

Install

Configure DB connection

Please create database manually, and set the configuration parameters for connection to this database. Press "Next step" button when done.



[Details ▲](#) Cannot connect to the database.

Unsupported charset or collation for tables: acknowledges, actions, alerts, application_discovery, application_prototype, applications, auditlog, auditlog_details, autoreg_host, conditions, config, config_autoreg_tls, corr_condition_tag, corr_condition_tagpair, corr_condition_tagvalue, correlation, dashboard, dchecks, drules, dservices, event_tag, events, expressions, functions, globalmacro, graph_theme, graphs, graphs_items, group_discovery, group_prototype, history_log, history_str, history_text, host_discovery, host_inventory, host_tag, hostmacro, hosts, housekeeper, hstgrp, httpstep, httpstep_field, httpstest, httpstest_field, icon_map, icon_mapping, ids, images, interface, interface_snmp, item_condition, item_discovery, item_preproc, item_rtdata, items, lld_macro_path, lld_override, lld_override_condition, lld_override_operation, lld_override_ophistory, lld_override_opperiod, lld_override_optag, lld_override_optrends, maintenance_tag, maintenances, mappings, media, media_type, media_type_message, media_type_param, module, opcommand, opconditions, operations, opmessage, problem, problem_tag, profiles, proxy_autoreg_host,

Back

Next step

ПРЕДУПРЕЖДЕНИЯ В ЛОГЕ СЕРВЕРА

```
Zabbix supports only "utf8_bin" collation. Database "zabbix" has default  
collation "utf8_general_ci"
```

```
character set name or collation name that is not supported by Zabbix found  
in 421 column(s) of database "zabbix"
```

```
only character set "utf8" and collation "utf8_bin" should be used in  
database
```

ПОЧЕМУ ЭТО ТАК ВАЖНО?

- ✓ Гарантированно, что БД знает о чувствительности к регистру
- ✓ До 5.0 нет проверок со стороны Zabbix, но можно проверить со стороны БД
- ✓ Если сортировка `utf8_bin` не используется, пользователь может в конечном итоге столкнуться с SQL ошибками о дублях или другим странным поведением веб-интерфейса.

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

- ✓ Уведомление пользователей о неправильной конфигурации БД
- ✓ Любые проблемы лучше (и легче!) увидеть и исправить их при начальной настройке БД



СПАСИБО!