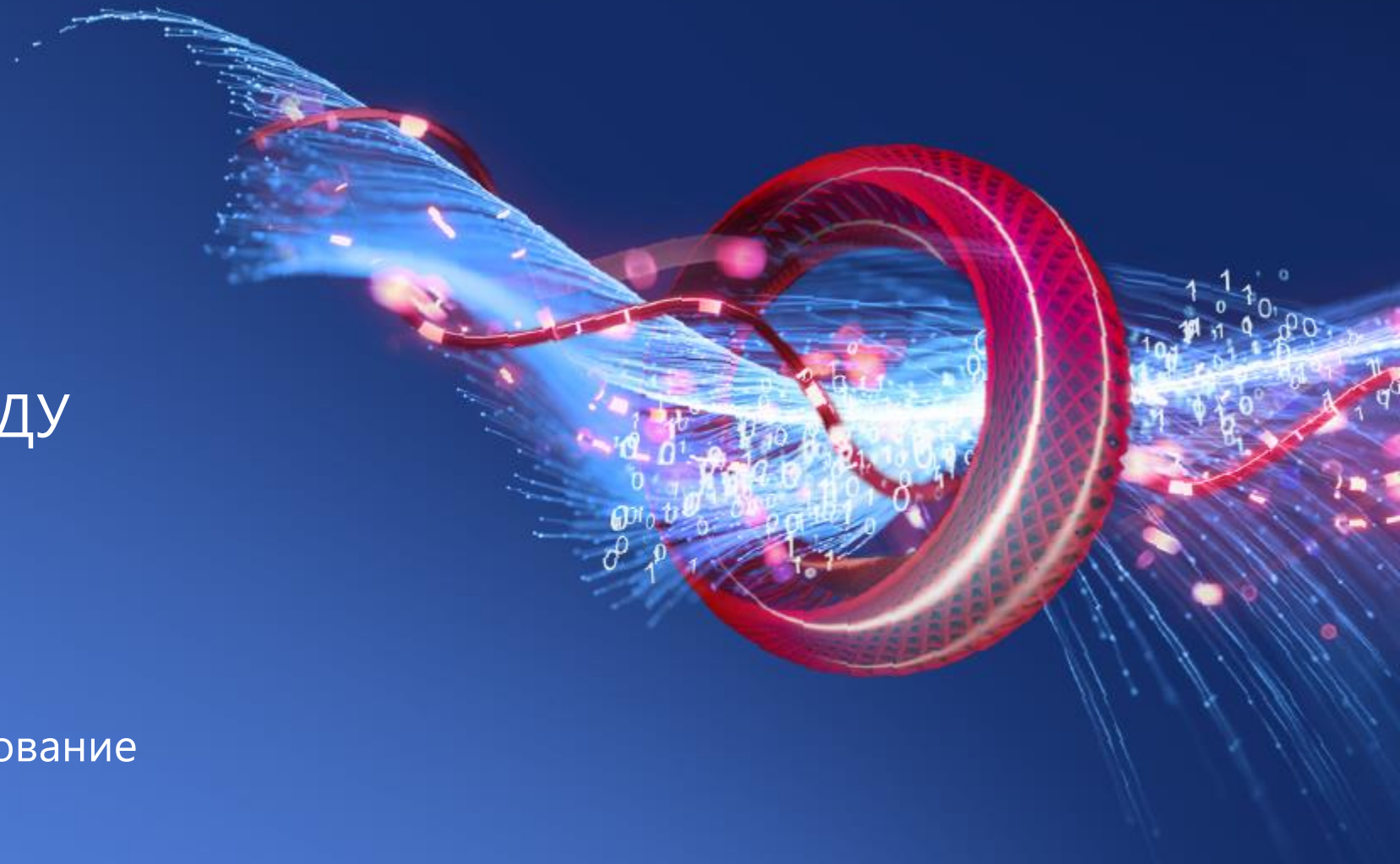
ZABBIX 5.0

КАК СДЕЛАТЬ МОНИТОРИНГ ЕЩЕ БЕЗОПАСНЕЕ С ZABBIX 5.0

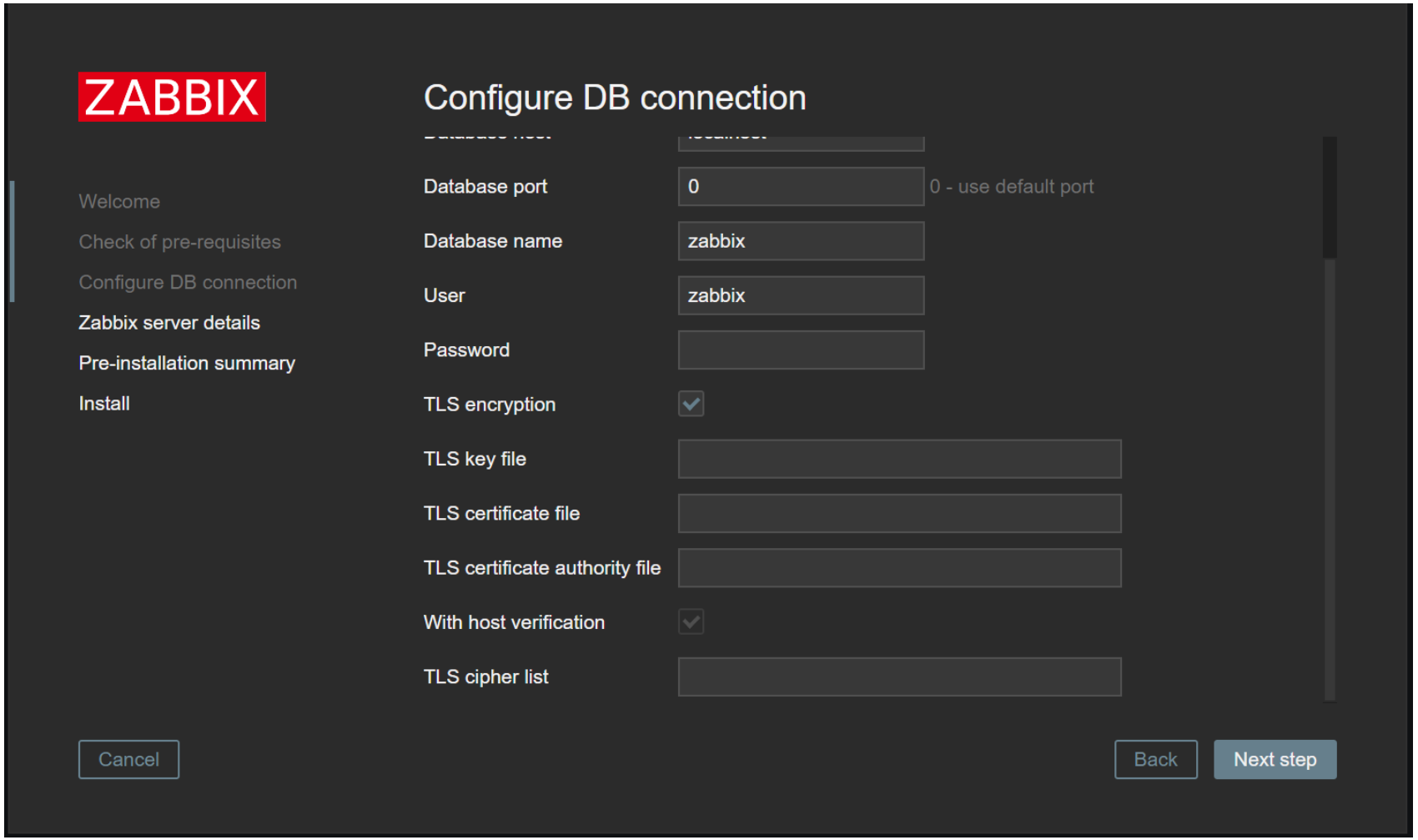
01

ШИФРОВАНИЕ МЕЖДУ ВЕБ-ИНТЕРФЕЙСОМ И БАЗОЙ ДАННЫХ



- Используется TLS-шифрование

НАСТРОЙКА ШИФРОВАНИЯ



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=
```

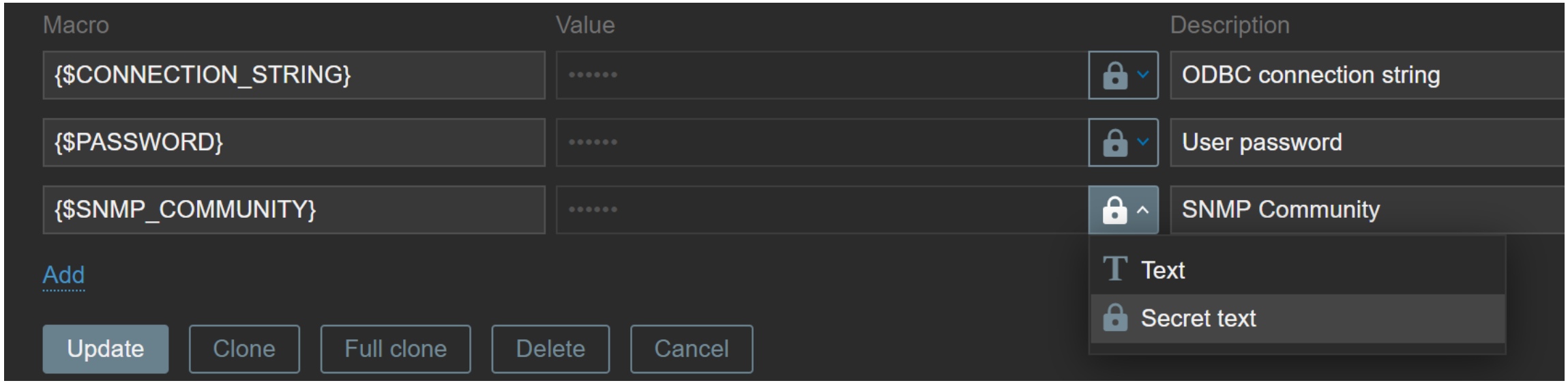
04

СКРЫТЫЕ МАКРОСЫ

ВОЗМОЖНОСТЬ СКРЫТЬ СВОИ МАКРОСЫ В ВЕБ-ИНТЕРФЕЙСЕ

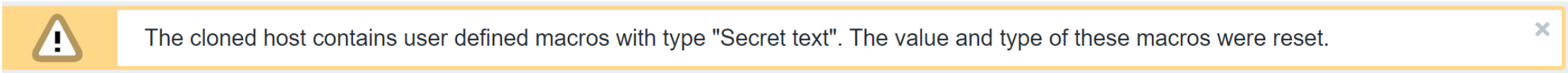
- Просто выберите из выпадающего списка должно ли значение этого макроса быть видимым

СПРЯЧЬТЕ СЕКРЕТНЫЕ ЗНАЧЕНИЯ МАКРОСОВ!



СКРЫТЫЕ МАКРОСЫ. ЗАМЕТКИ

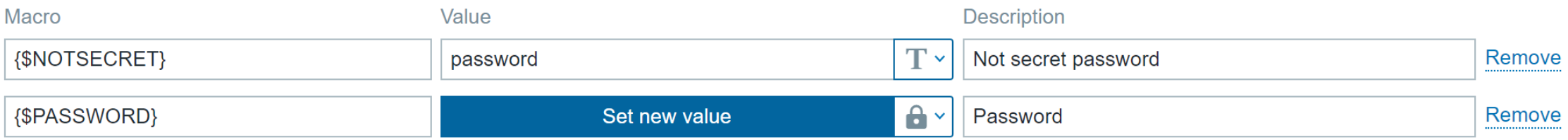
- При клонировании узлов сети или шаблонов с макросами – значения сбрасываются :



- 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.



05

ДЛЯ ХЕШИРОВАНИЯ ПАРОЛЕЙ ВЕБ-ИНТЕРФЕЙСА ИСПОЛЬЗУЕТСЯ BCRYPT ВМЕСТО MD5

- При хешировании паролей используется bcrypt
- Безопаснее подход

ПРЕИМУЩЕСТВО ПЕРЕХОДА НА BCRYPT

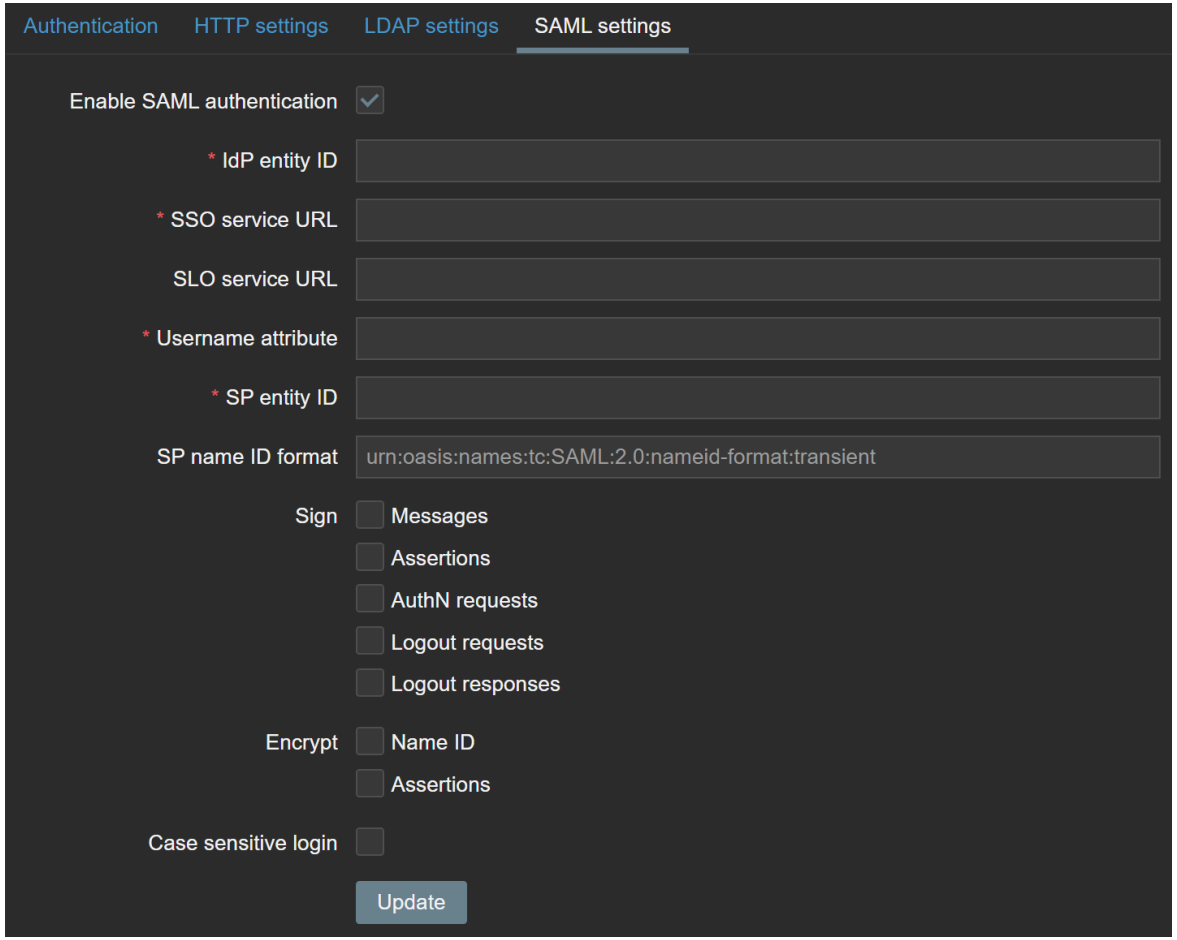
- Основан на алгоритме Blowfish
- Гораздо сложнее вычислить хеши, чем при использовании MD5
- Больше сложностей для атакам перебором
- Старые хеши MD5 заменяются на bcrypt после первого входа
- Использует уникальное соль-значение
- Невозможность атак с использованием радужных таблиц

06

ВСТРОЕННАЯ ПОДДЕРЖКА SAML

- Нативная поддержка zabbix saml-технологии единого входа

НАСТРОЙКА ИНТЕГРАЦИИ С SAML



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

СПИСОК ЗАПРЕЩЁННЫХ/РАЗРЕШЁННЫХ ЭЛЕМЕНТОВ ДАННЫХ ДЛЯ УЗЛА СЕТИ

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

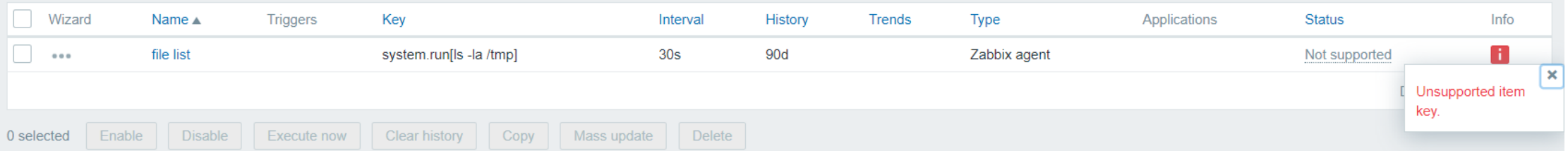
НАСТРОЙКА ОГРАНИЧЕНИЙ ДЛЯ МЕТРИК

- 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]
```



ПОРЯДОК ПАРАМЕТРОВ ИМЕЕТ ЗНАЧЕНИЕ!

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

### Option: DenyKey
DenyKey=system.run[*]
```

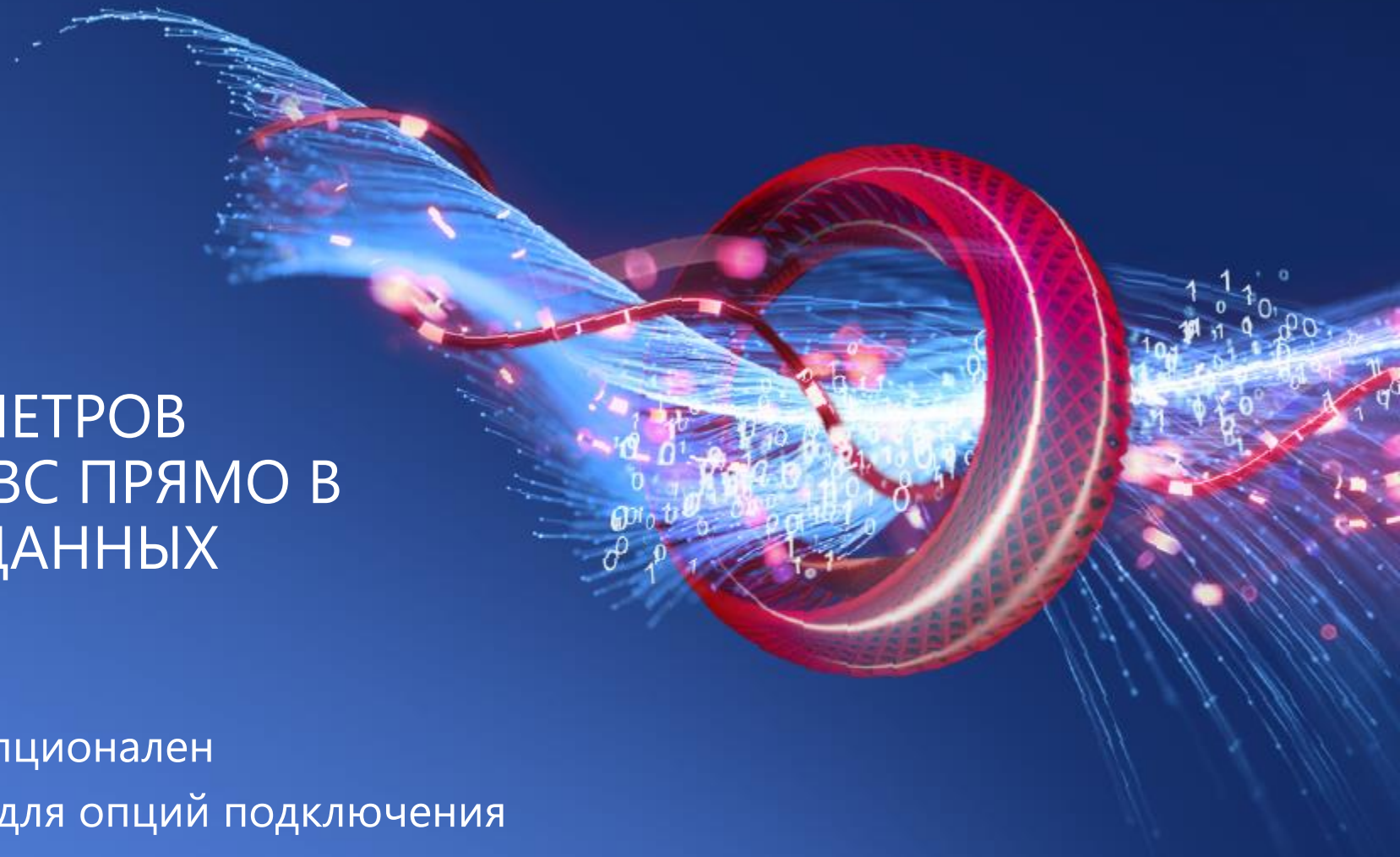
Wizard	Name ▲	Triggers	Key	Interval	History	Trends	Type	Applications	Status	Info
•••	file list		system.run[ls -la /tmp]	30s	90d		Zabbix agent		Enabled	

Displaying 1 of 1 found

0 selected | Enable | Disable | Execute now | Clear history | Copy | Mass update | Delete

08

ПОДДЕРЖКА ПАРАМЕТРОВ ПОДКЛЮЧЕНИЯ ODBC 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

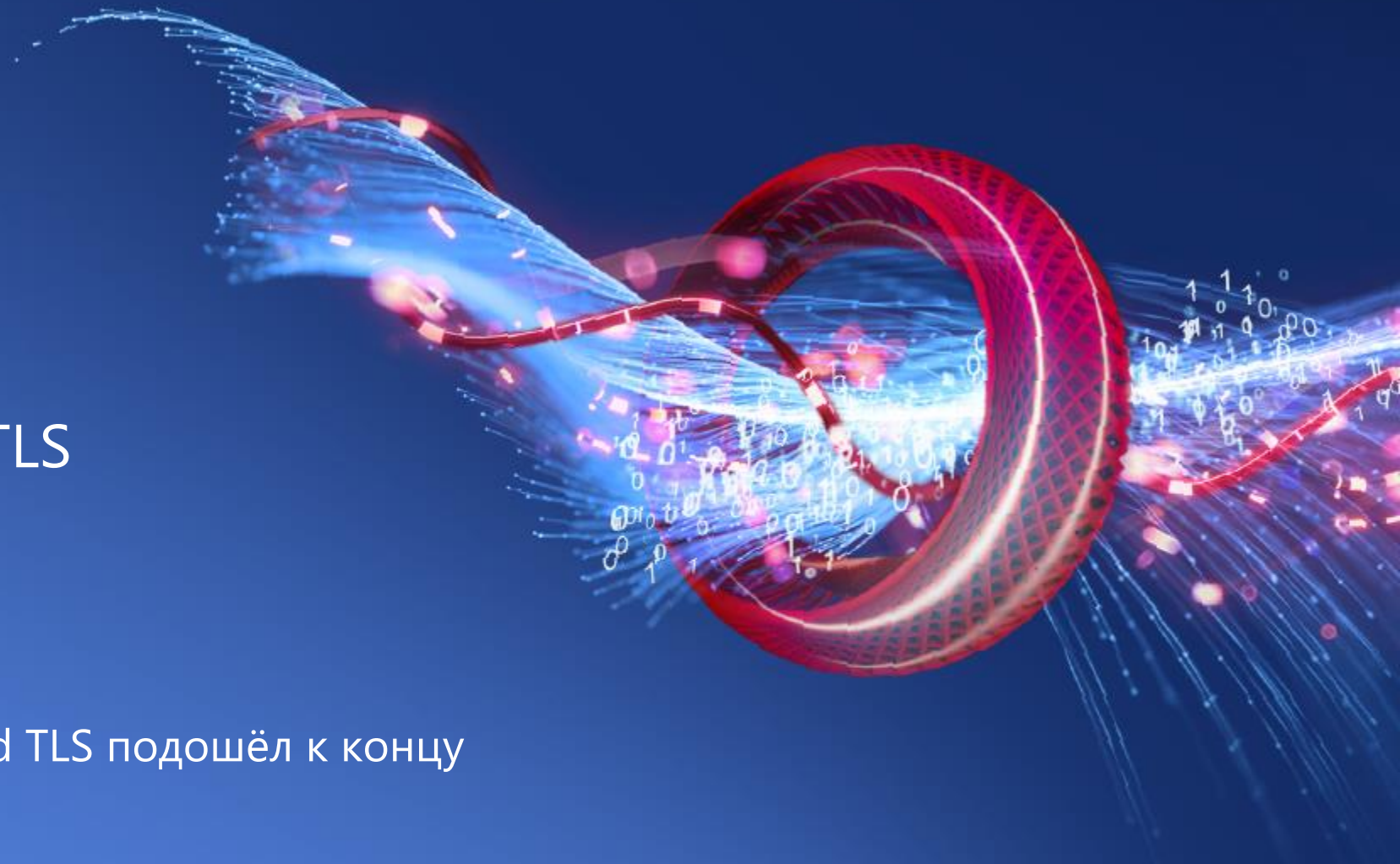
ИЗМЕНЕНИЯ В КЛЮЧЕ ЭЛЕМЕНТА ДАННЫХ ODBC

```
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

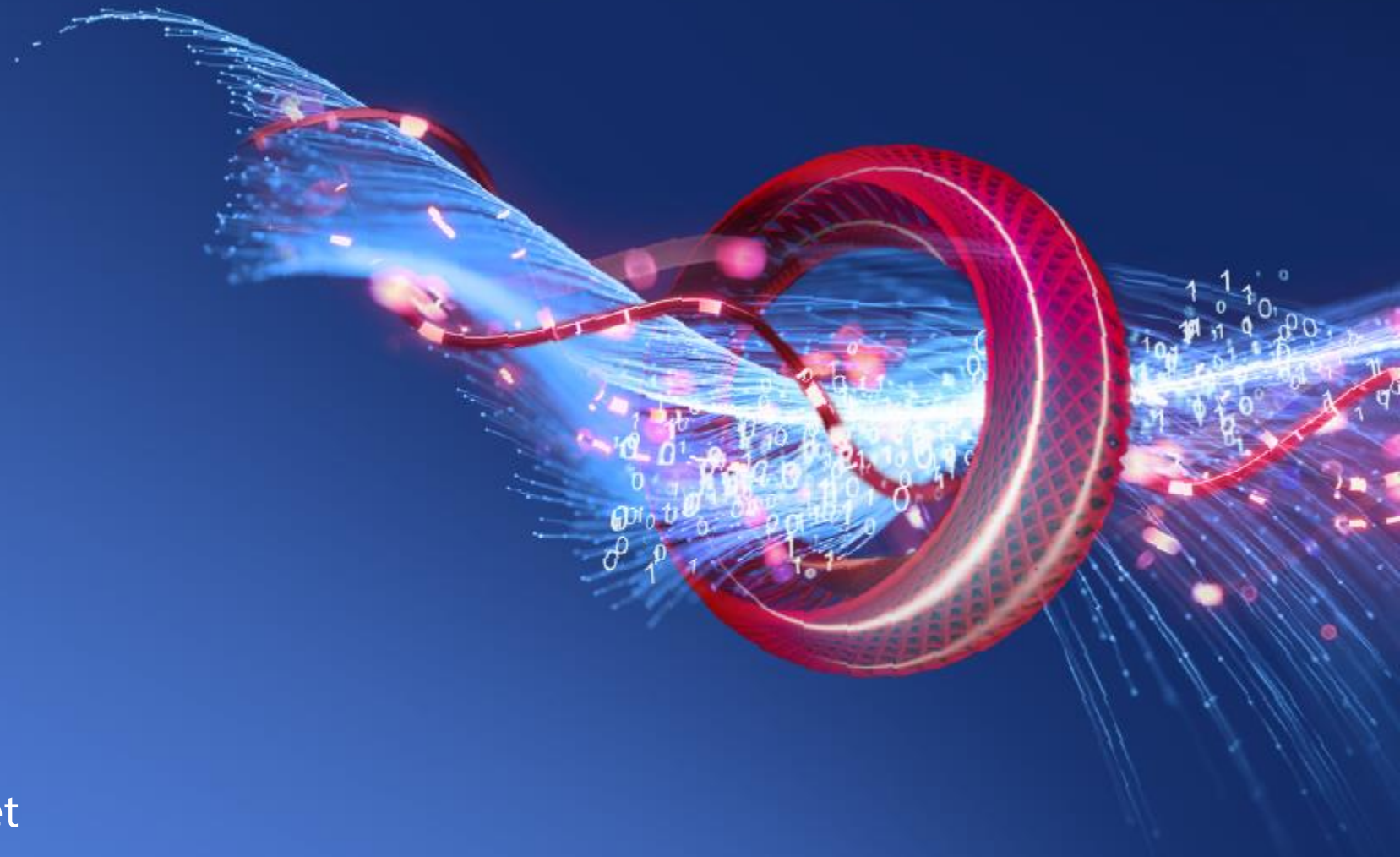
- Поддержка версий mbed TLS подошёл к концу

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

AUDITLOG.GET



- Новый объект API
- Новый метод auditlog.get

ПРИМЕР РАБОТЫ AUDITLOG.GET

JSON | Auth | Query | Header 1 | Docs

```
{
    "jsonrpc": "2.0",
    "method": "auditlog.get",
      "params": {
        "output": "extend",
        "sortfield": "clock",
        "sortorder": "DESC",
        "limit": 2
    },
    "id": 1,
    "auth": "5c4e8ee5e42b556535f1a6e512877d7f"
}
```

Beautify JSON

Preview | Header 9 | Cookie | Timeline

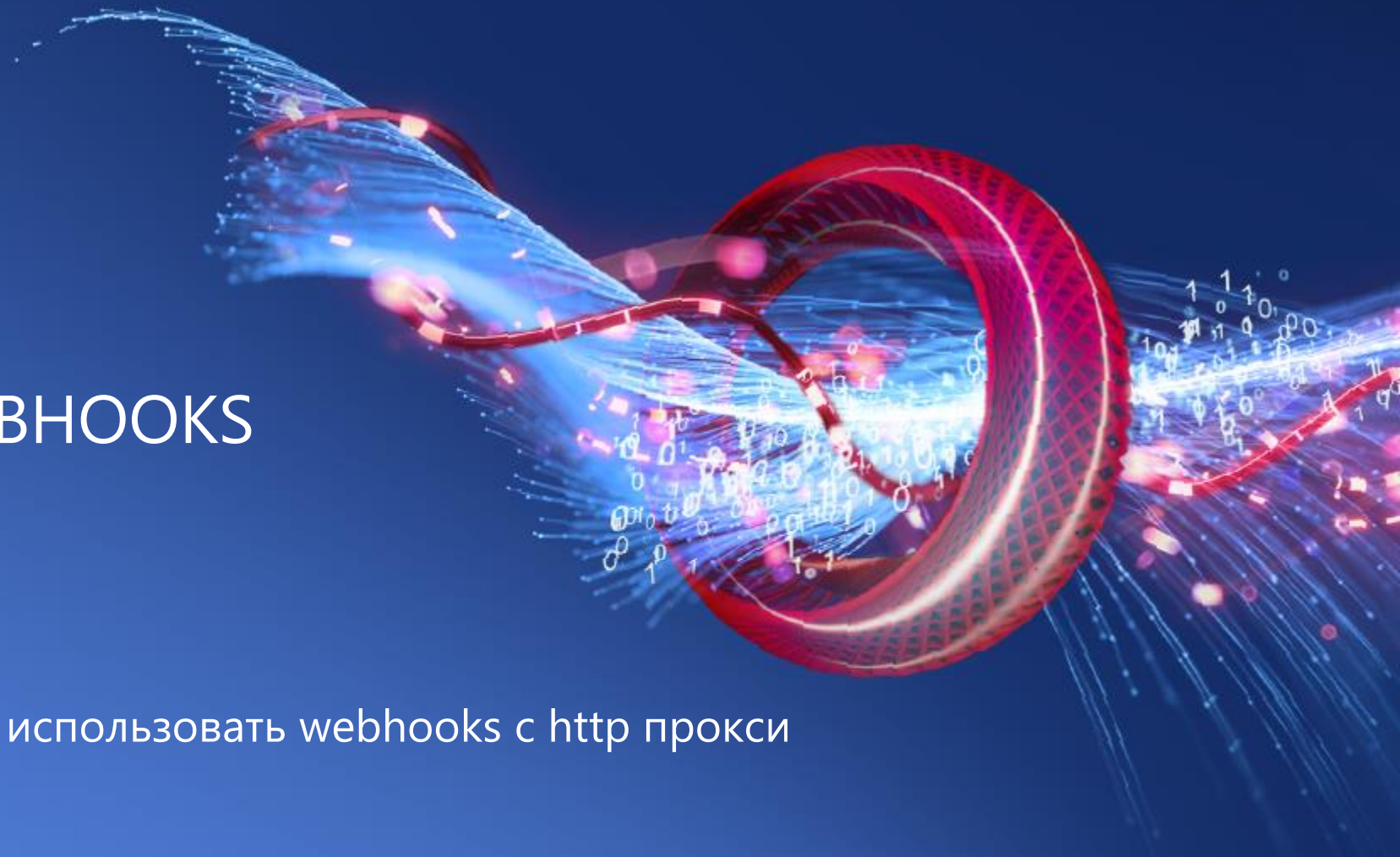
```
{
  "jsonrpc": "2.0",
  "result": [
    {
      "auditid": "188",
      "userid": "1",
      "clock": "1589506616",
      "action": "3",
      "resourcetype": "0",
      "note": "",
      "ip": "192.168.1.141",
      "resourceid": "0",
      "resourcename": ""
    },
    {
      "auditid": "187",
      "userid": "1",
      "clock": "1589388014",
      "action": "0",
      "resourcetype": "0",
      "note": "",
      "ip": "192.168.1.141",
      "resourceid": "5",
      "resourcename": "user2"
    }
  ],
  "id": 1
}
```

$.store.books[*].author

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

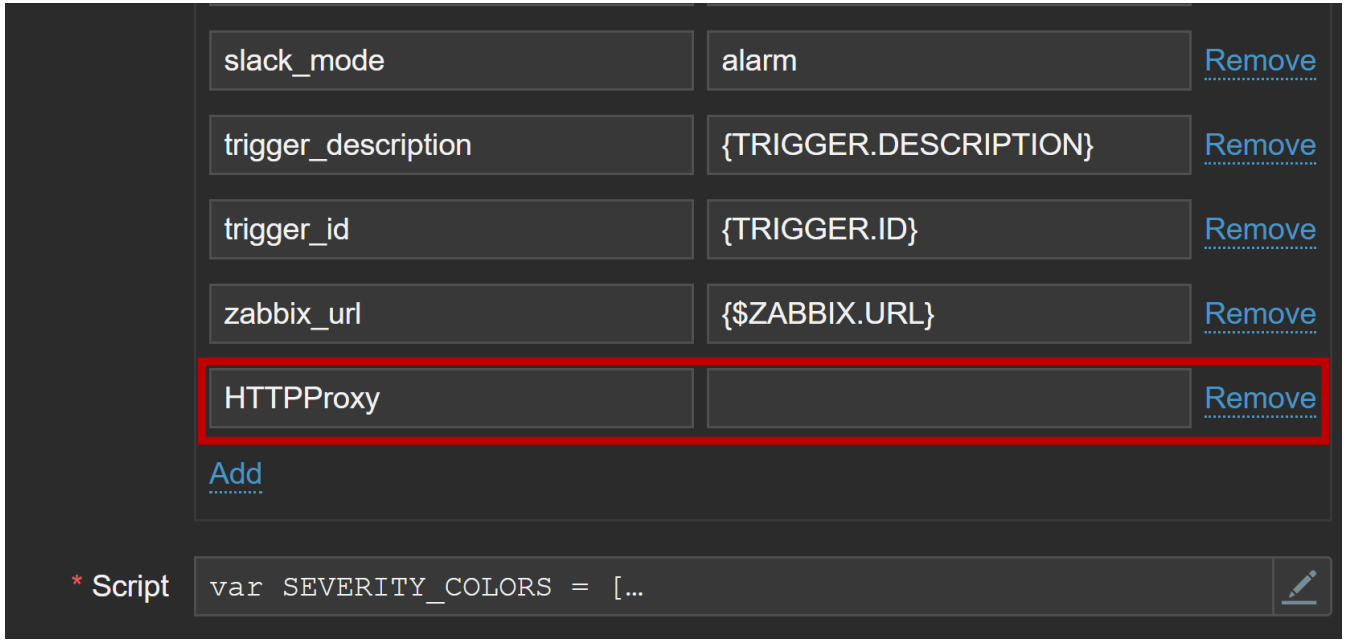


HTTP PROXY В WEBHOOKS

- Добавлена возможность использовать webhooks с http прокси

НАСТРОЙКА WEBHOOK С HTTP ПРОКСИ

- Вы можете указать HTTP прокси



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

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

12

ПРОВЕРКА КОДИРОВКИ БД

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

ПРИМЕР КАК НЕ НАДО ДЕЛАТЬ

Hostid:10325

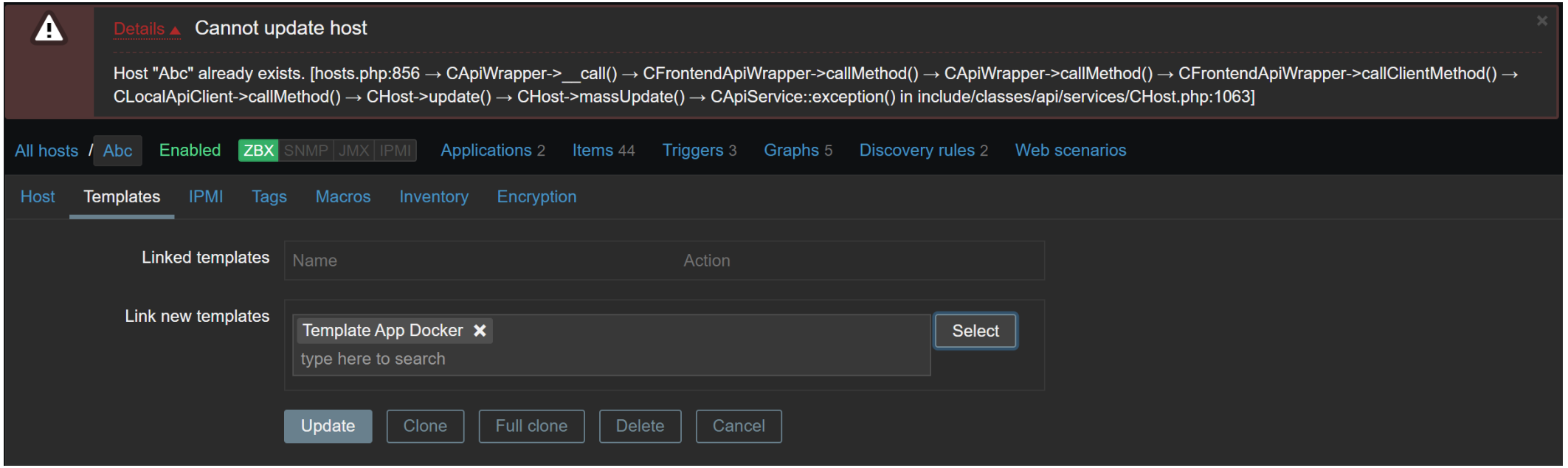
ABC

Hostid:10326

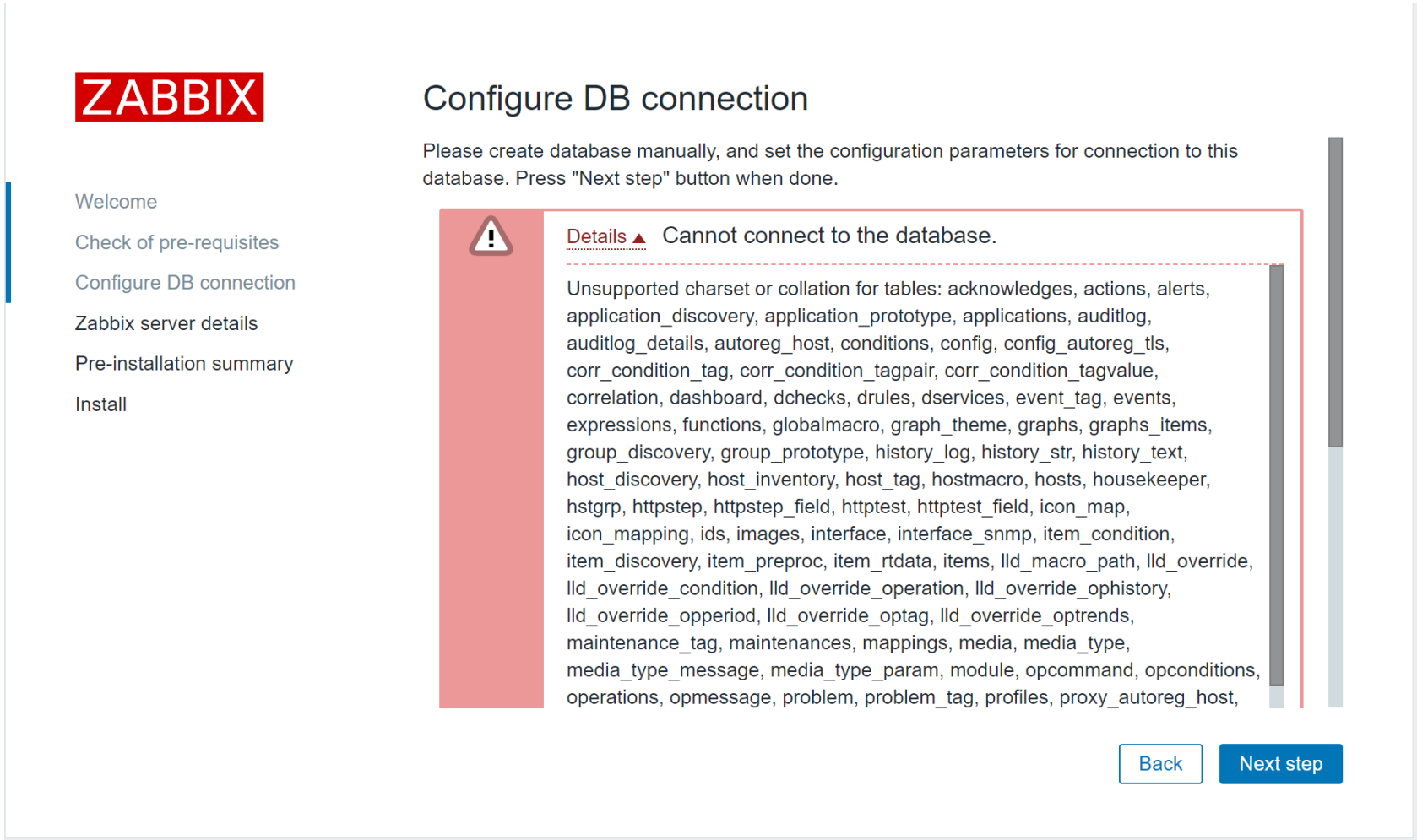
Abc

Hostid:10327

AbC



ПРЕДУПРЕЖДЕНИЕ В ХОДЕ ПЕРВОНАЧАЛЬНОЙ НАСТРОЙКИ



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!