ZABBIX 5.0

ZABBIX 5.0 SECURITY FEATURES AND IMPROVEMENTS

Simon Wetzstein, Convx GmbH
Zabbix Certified Expert

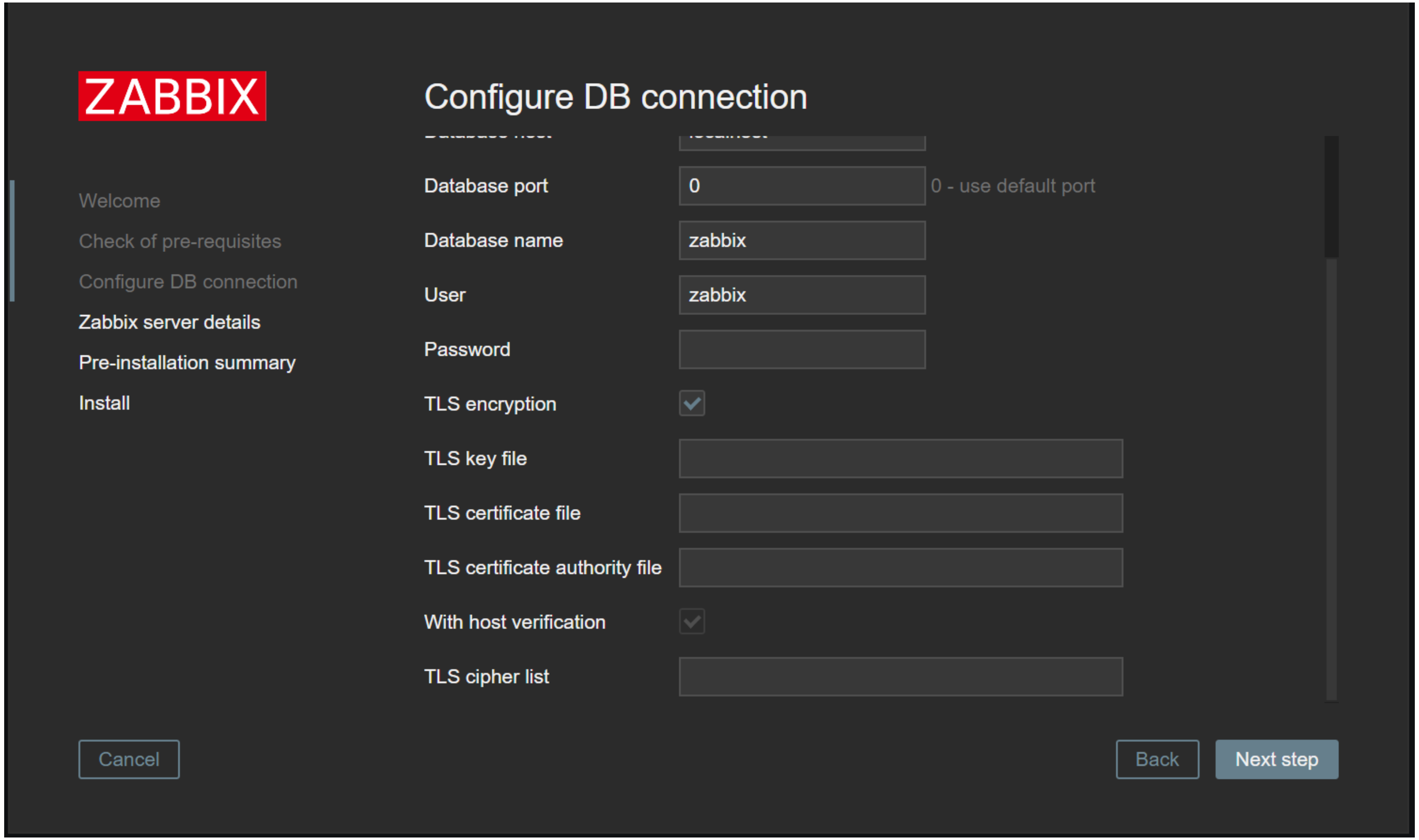
01

TLS SUPPORT FOR FRONTEND COMMUNICATION WITH DATABASE

ENCRYPT FRONTEND COMMUNICATION WITH THE ZABBIX DATABASE

- Uses already familiar TLS certificate encryption

CONFIGURING THE ENCRYPTION



Configure DB connection

Database port 0 0 - use default port

Database name zabbix

User zabbix

Password

TLS encryption ☑

TLS key file

TLS certificate file

TLS certificate authority file

With host verification ☑

TLS cipher list

CONFIGURING THE ENCRYPTION

- TLS certificate based encryption
- Supported for MySQL and PostgreSQL
- With host verification - the database server certificate is checked by comparing the host name specified in the certificate with the name of the host to which it is connected
- If the TLS parameters point to files that are open for writing, a warning will be displayed stating that the files should be read only

02

TLS SUPPORT FOR SERVER/PROXY COMMUNICATION WITH DATABASE

ENCRYPT ZABBIX SERVER COMMUNICATION WITH THE ZABBIX DATABASE

- Also uses the already familiar TLS certificate encryption

CONFIGURING THE ENCRYPTION

```
### Option: DBTLSConnect
DBTLSConnect=
### Option: DBTLSCAFile
DBTLSCAFile=
### Option: DBTLSCertFile
DBTLSCertFile=
### Option: DBTLSKeyFile
DBTLSKeyFile=
### Option: DBTLSCipher
DBTLSCipher=
### Option:DBTLSCipher13
DBTLSCipher13=
```

EXAMPLE SCENARIO – JUST ENCRYPT

- Make encrypted connection to the DB without authenticating or verifying the host identity

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

EXAMPLE SCENARIO – ENCRYPT AND VERIFY

- Make encrypted connection to the DB with authenticating and verifying the host identity

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

03

CONFIGURABLE CIPHERS

TLS CIPHERSUIT SELECTION

- Ability to configure ciphersuites according to your security policy
- Configurable per component

FUNCTIONALITY AND BENEFTS

- Ability to override the buil in ciphersuit selection
- Can override for certificates, PSK and combined
- Ability to override zabbix_get and zabbix_sender by passing --tls_cipher13 or --tls_cipher
- Allows to select specific ciphers based on your security policy or additional requirements
- Separate configuration parameters for TLS 1.3 and 1.2
- Configurable for incoming/outgoing connections per component

NEW CONFIGURATION PARAMETERS

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

### Option: TLSCipherCert
# TLSCipherCert=

### Option: TLSCipherPSK13
# TLSCipherPSK13=

### Option: TLSCipherPSK
# TLSCipherPSK=

### Option: TLSCipherAll13
# TLSCipherAll13=

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

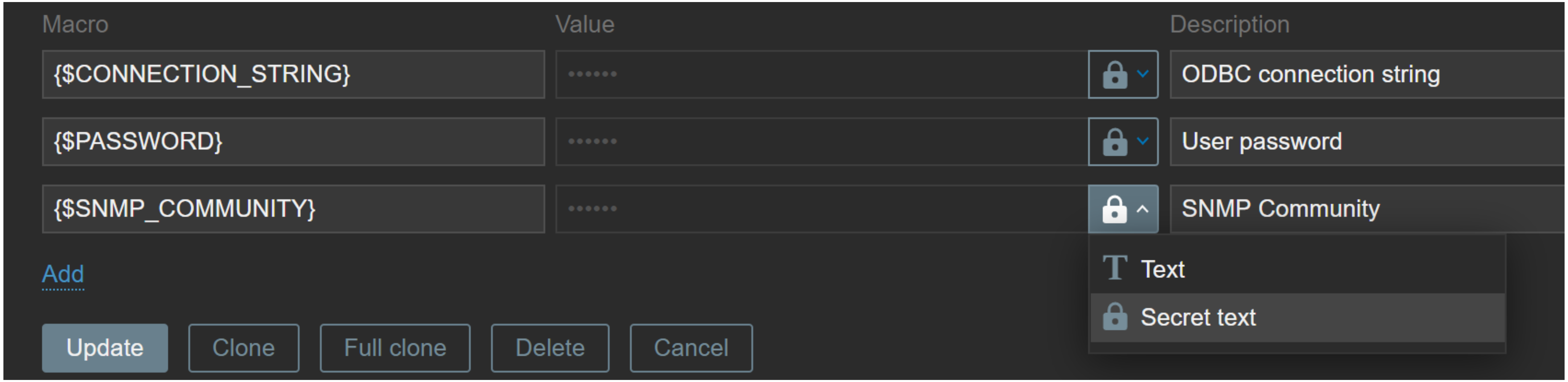
04

MASKED MACROS

ABILITY TO MASK YOUR MACROS IN THE FRONTEND

- A simple mask/unmask dropdown

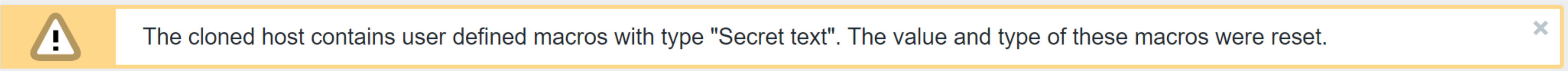
MASK YOUR SENSITIVE MACRO VALUES!



Macro	Value	Description
{$CONNECTION_STRING}	••••••	ODBC connection string
{$PASSWORD}	••••••	User password
{$SNMP_COMMUNITY}	••••••	SNMP Community

MASKED MACRO NOTES

- When attempting to clone a host/template with secret text macros, the values get reset:

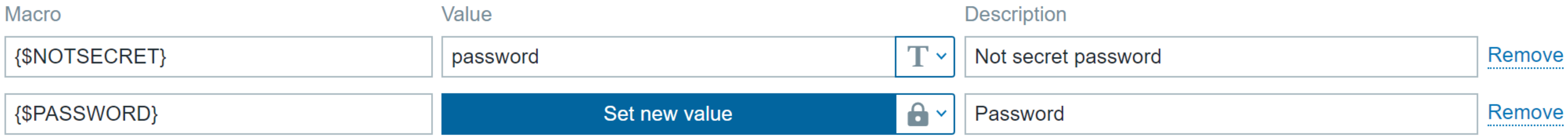


The cloned host contains user defined macros with type "Secret text". The value and type of these macros were reset.

- When exporting the host, the value of a secret macro is not exported.

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

- Once defined, you cannot edit it – you have to completely replace the Macro.



Macro	Value	Description	
{$NOTSECRET}	password	Not secret password	Remove
{$PASSWORD}	Set new value	Password	Remove

05

FRONTEND PASSWORD HASHING IMPROVEMENTS

REPLACED MD5 ALGORITHM

- ✓ Passwords hashes by using bcrypt
- ✓ Much more secure approach

BENEFITS OF SWITCHING TO BCRYPT

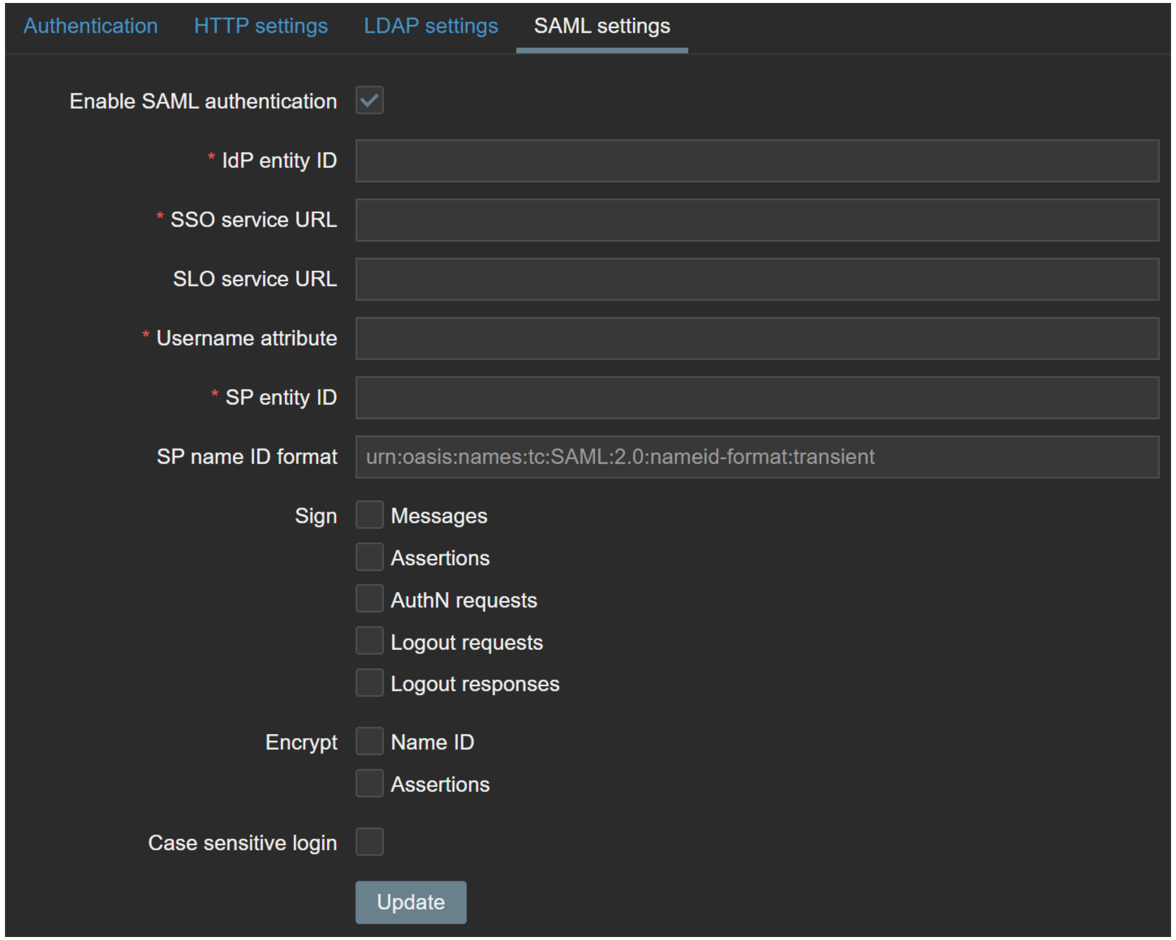
- Based on the Blowfish algorith
- A lot slower than MD5
- Not feasible for hardware acceleration – less vulnerable to brute-force attacks
- Old MD5 hashes replaced with bcrypt hashes after initial login
- Uses Unique salt value
- Not feasible for Rainbow table attacks

06

OUT OF THE BOX SAML SUPPORT

INTEGRATE ZABBIX WITH SAML SINGLE SIGN-ON NATIVELY

CONFIGURING INTEGRATION WITH SAML



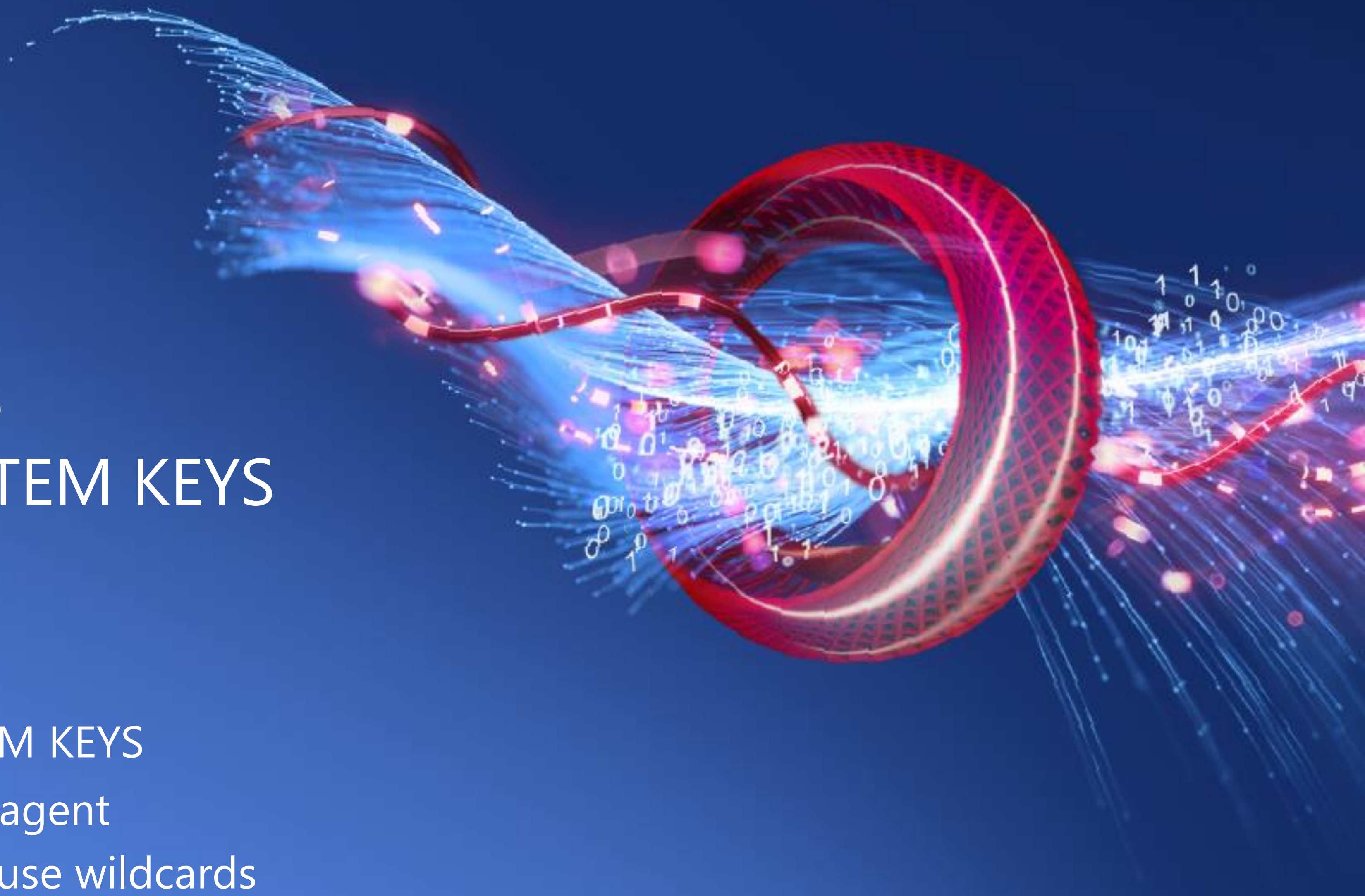
Enable SAML authentication	☑
* IdP entity ID	
* SSO service URL	
SLO service URL	
* Username attribute	
* SP entity ID	
SP name ID format	urn:oasis:names:tc:SAML:2.0:nameid-format:transient
Sign	□ Messages □ Assertions □ AuthN requests □ Logout requests □ Logout responses
Encrypt	□ Name ID □ Assertions
Case sensitive login	□

CONFIGURING INTEGRATION WITH SAML

- A corresponding user must exist in Zabbix, however, its Zabbix password will not be used.
- Need to preconfigure the identity provider
- Default location for private key and certificate is ui/conf/certs/
- Some settings - SP key, SP cert, IDP cert and additional settings can be configured in zabbix.conf.php file

07

BLACKLISTING AND WHITELISTING OF ITEM KEYS



RESTRICT EXECUTION OF ITEM KEYS

- Key whitelist/blacklist per agent
- Specify individual keys or use wildcards

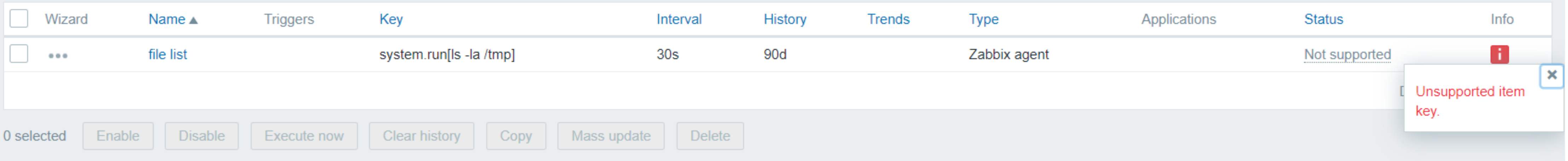
CONFIGURING KEY RESTICTIONS

- EnableRemoteCommands still required!
- Rule check stops after first match
- AllowKey can be used only if DenyKey is specified
- If a specific item key is disallowed in the agent configuration, the item will turn unsupported
- Zabbix agent with –print (-p) command line option will not show keys that are not allowed by configuration;
- Zabbix agent with –test (-t) command line option will return "Unsupported item key." status for keys that are not allowed by configuration.

THE CONFIGURATION ORDER MATTERS!

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


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



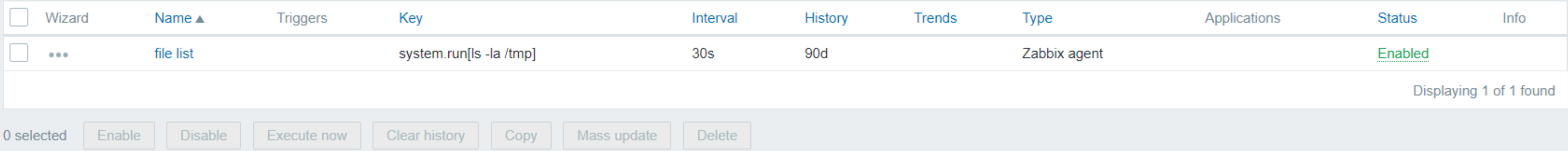
□	Wizard	Name ▲	Triggers	Key	Interval	History	Trends	Type	Applications	Status	Info
□	•••	file list		system.run[ls -la /tmp]	30s	90d		Zabbix agent		Not supported	i

Unsupported item key.

THE CONFIGURATION ORDER MATTERS!

```
### 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

08

ODBC CONNECTION STRING SUPPORT

ANOTHER WAY TO SPECIFY A CONNECTION STRING

- dsn parameter now optional
- New connection string parameter

DSN OR CONNECTION STRING?

- In some cases users may not have access to the odc.ini file
- Connection string works around that by defining the connection parameters on the item level
- Either dsn OR connection string should be present. If both are present – the dsn will be ignored
- The connection string may containt drivers specific arguments

ODBC KEY CHANGES

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

New key:
db.odbc.select[<unique short description>,<dsn>,<connection string>]

Example connection string:
“Driver=/usr/local/lib/libmyodbc5a.so;Database=master;Server=127.0.0.1;Port=
3306”
```

09

LEGACY ENCRYPTION LIBRARY SUPPORT DROPPED

MBED TLS SUPPORT DISCONTINUED

- Currently supported mbed TLS versions have reached end of life

WHY?

- Previous versions supported mbed TLS 1.3.9 and later 1.3.x versions – by now these versions have reached end of life.
- Lack of interest/use cases from the community
- Saves the development overhead
- Better focus on support of OpenSSL and GnuTLS

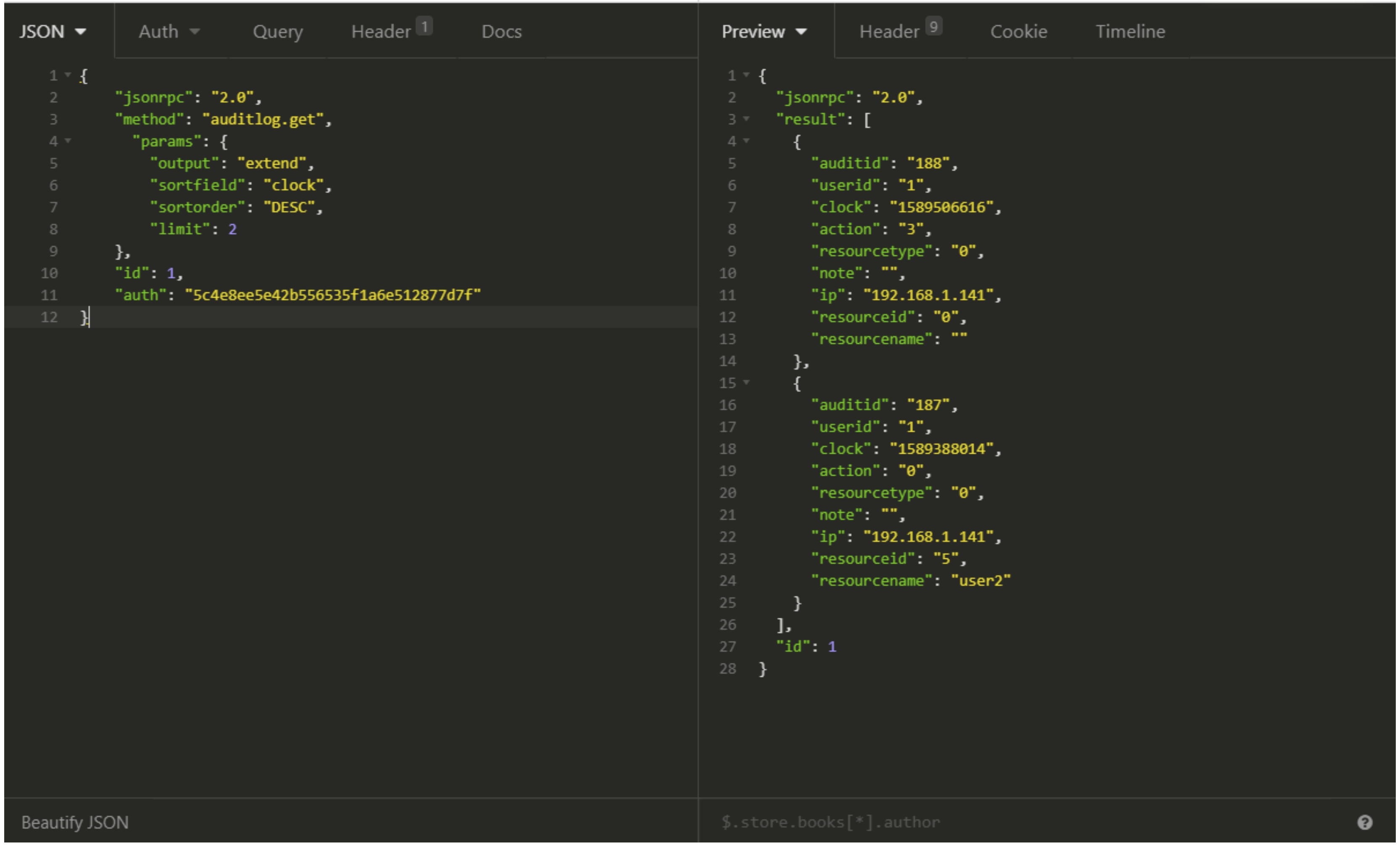
10

AUDITLOG.GET

USE API TO RETRIEVE AUDIT LOG

- Audit log object added
- auditlog.get method added

EXAMPLE AUDITLOG.GET CALL



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

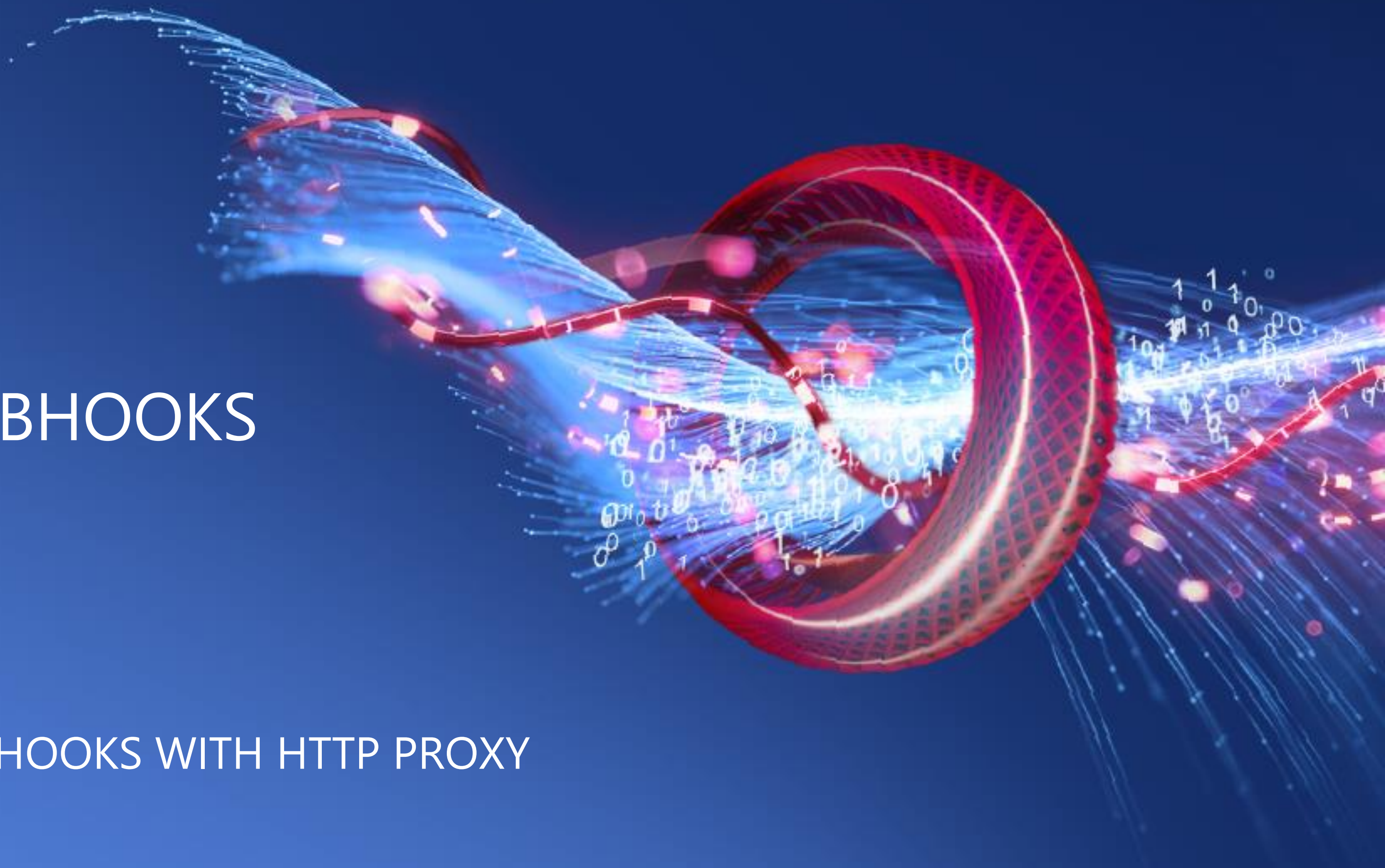
```
{
  "jsonrpc": "2.0",
  "result": [
    {
      "auditid": "188",
      "userid": "1",
      "clock": "1589506616",
      "action": "3",
      "resourcetype": "0",
      "note": "",
      "ip": "192.168.1.141",
      "resourceid": "0",
      "resourcename": ""
    },
    {
      "auditid": "187",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

AUDIT LOG OBJECT AND METHOD

- Filter by audit ID’s and/or user ID’s
- Ability to search by old value and new value
- The object contains information about Action type, Resource type, IP address, Resource ID’s, Names and other details
- Potentially very useful for parsing audit data and notifying you when critical changes have been made

11

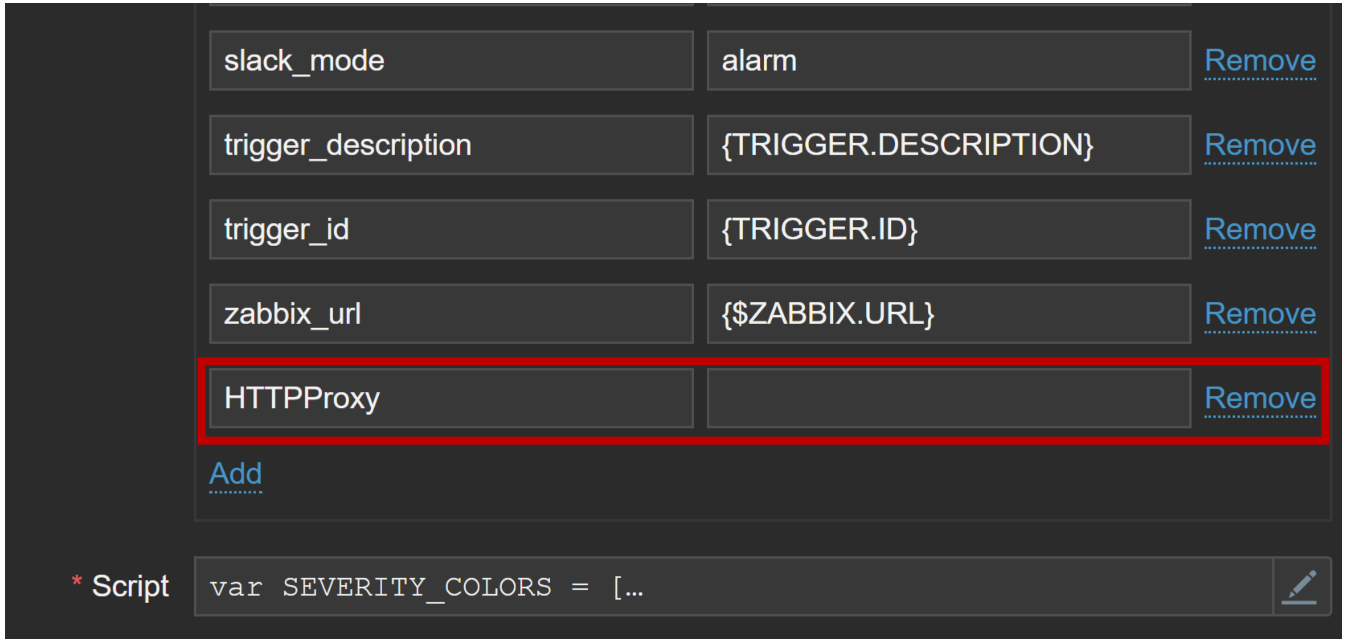
HTTP PROXY IN WEBHOOKS



ADDED ABILITY TO USE WEBHOOKS WITH HTTP PROXY

HTTP PROXY WEBHOOK CONFIGURATION

- Abilty to specify HTTP proxy when configuring a webhook



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

Add

* Script `var SEVERITY_COLORS = […`

- Same logic as in HTTP agent
- Need to specify the HTTPProxy parameter:

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

12

DB CHARACTER SET CHECK

WARN USERS OF CHARACTER SET MISCONFIGURATION

- Warning is displayed during the initial frontend setup
- Warning is displayed on already running instances

EXAMPLE OF AN ISSUE

Hostid:10325

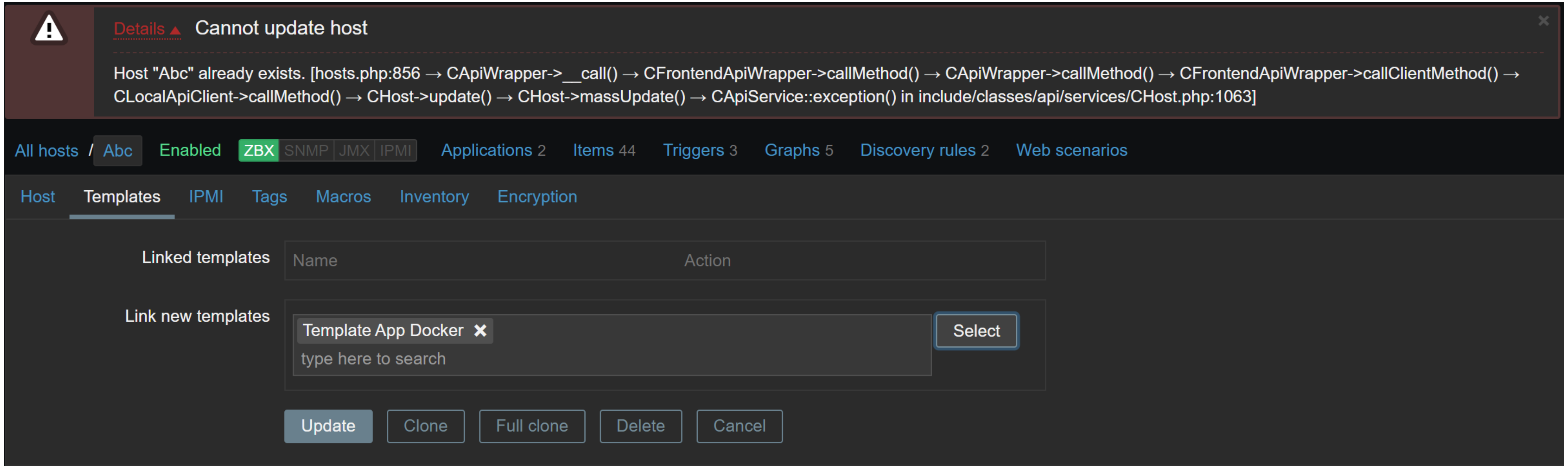
ABC

Hostid:10326

Abc

Hostid:10327

AbC



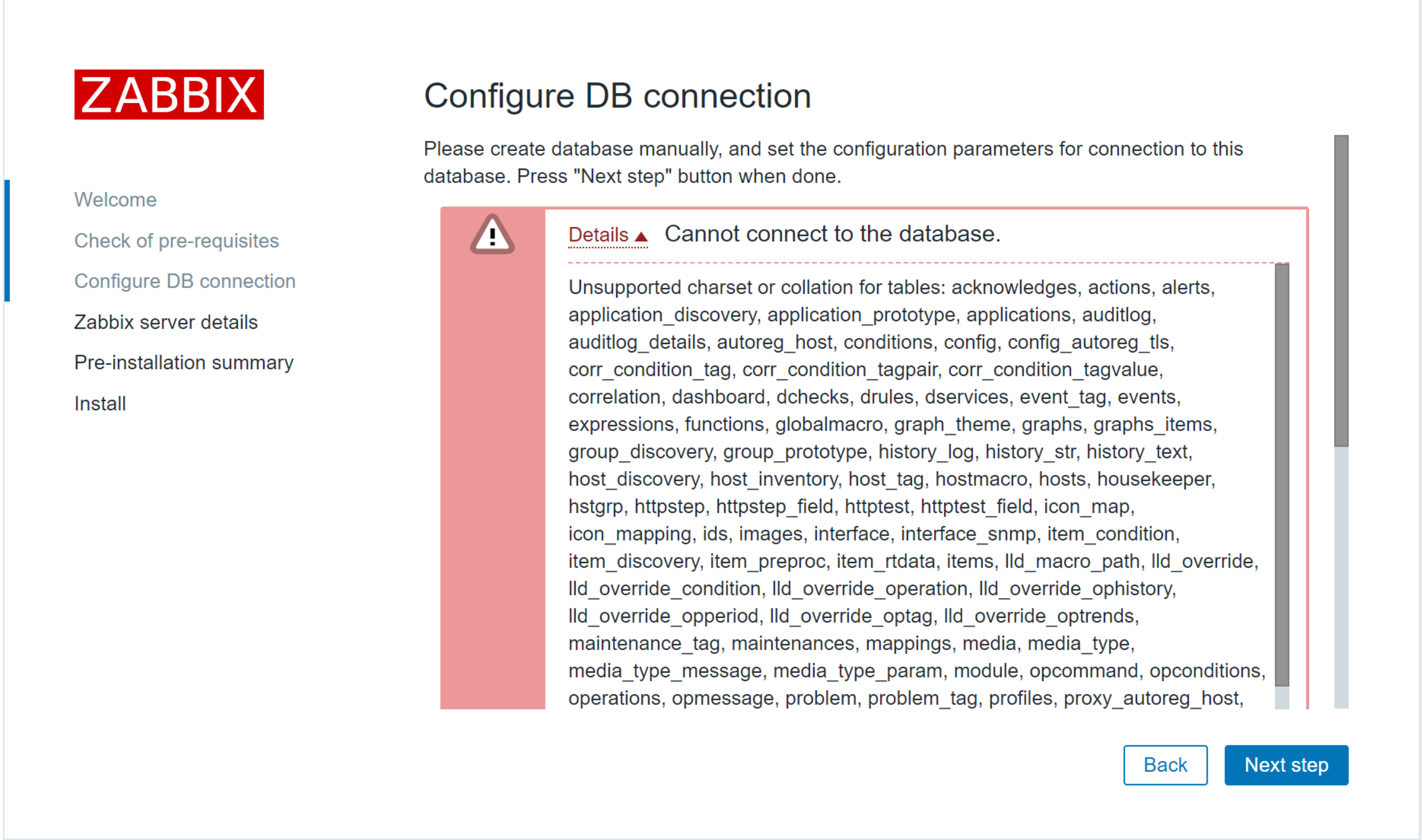
Details ▲ Cannot update host

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]

Linked templates: Name | Action

Link new templates: Template App Docker ✖ | type here to search

DISPLAYED DURING INITIAL SETUP



Configure DB connection

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

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, httptest, httptest_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,

DISPLAYED IN THE SERVER LOG

```
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
```

WHY DOES COLLATION MATTER?

- Ensures that the DB backend is aware of object case sensitivity
- No way to detect before 5.0 but to take a look at the DB table structure from the DB side
- If utf8_bin collation is not used, the user may eventually encounter duplicate SQL errors or other unexpected behavior in the frontend

MAIN BENEFITS OF DETECTING MISCONFIGURATION

- Letting users know that there’s DB misconfiguration
- It’s better to catch any issues and fix them during the initial setup of the DB
- Users should avoid running any extra queries on DB’s that have over time substantially grown in size

THANK YOU!