



ZABBIX 5.0

ZABBIX 5.0 SECURITY FEATURES AND IMPROVEMENTS

01

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.

TLS SUPPORT FOR FRONTEND COMMUNICATION WITH DATABASE

ENCRYPT FRONTEND COMMUNICATION WITH THE ZABBIX DATABASE

- ☑ Uses already familiar TLS certificate encryption

CONFIGURING THE ENCRYPTION

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:

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

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.

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

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.

CONFIGURABLE CIPHERS

TLS CIPHERSUITE SELECTION

- ④ Ability to configure ciphersuites according to your security policy
- ④ Configurable per component

FUNCTIONALITY AND BENEFITS

- ✓ Ability to override the built-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
<code>{\$CONNECTION_STRING}</code>	 v	ODBC connection string
<code>{\$PASSWORD}</code>	 v	User password
<code>{\$SNMP_COMMUNITY}</code>	 ^	SNMP Community

[Add](#)
.....

-  Text
-  Secret text

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	
<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="button" 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 glowing blue and red lines and binary code (0s and 1s) scattered across the scene.

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 algorithm
- ✓ 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

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.

OUT OF THE BOX SAML SUPPORT

INTEGRATE ZABBIX WITH SAML SINGLE SIGN-ON NATIVELY

CONFIGURING INTEGRATION WITH 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

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

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.

BLACKLISTING AND WHITELISTING OF ITEM KEYS

RESTRICT EXECUTION OF ITEM KEYS

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

CONFIGURING KEY RESTRICTIONS

- ✓ 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]
```

<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.

THE CONFIGURATION ORDER MATTERS!

```
### 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

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.

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 contain 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

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.

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

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

USE API TO RETRIEVE AUDIT LOG

- ④ Audit log object added
- ④ auditlog.get method added

EXAMPLE AUDITLOG.GET CALL

The image shows a REST client interface with two panels. The left panel, titled 'JSON', displays the request body as a JSON object. The right panel, titled 'Preview', displays the response body as a JSON object. The response contains an array of two audit log entries.

```
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 }
```

```
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      "resourceid": ""
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      "resourceid": "user2"
25    }
26  ],
27  "id": 1
28 }
```

At the bottom of the interface, there is a 'Beautify JSON' button on the left and a JSONPath expression `$.store.books[*].author` on the right, followed by a help icon.

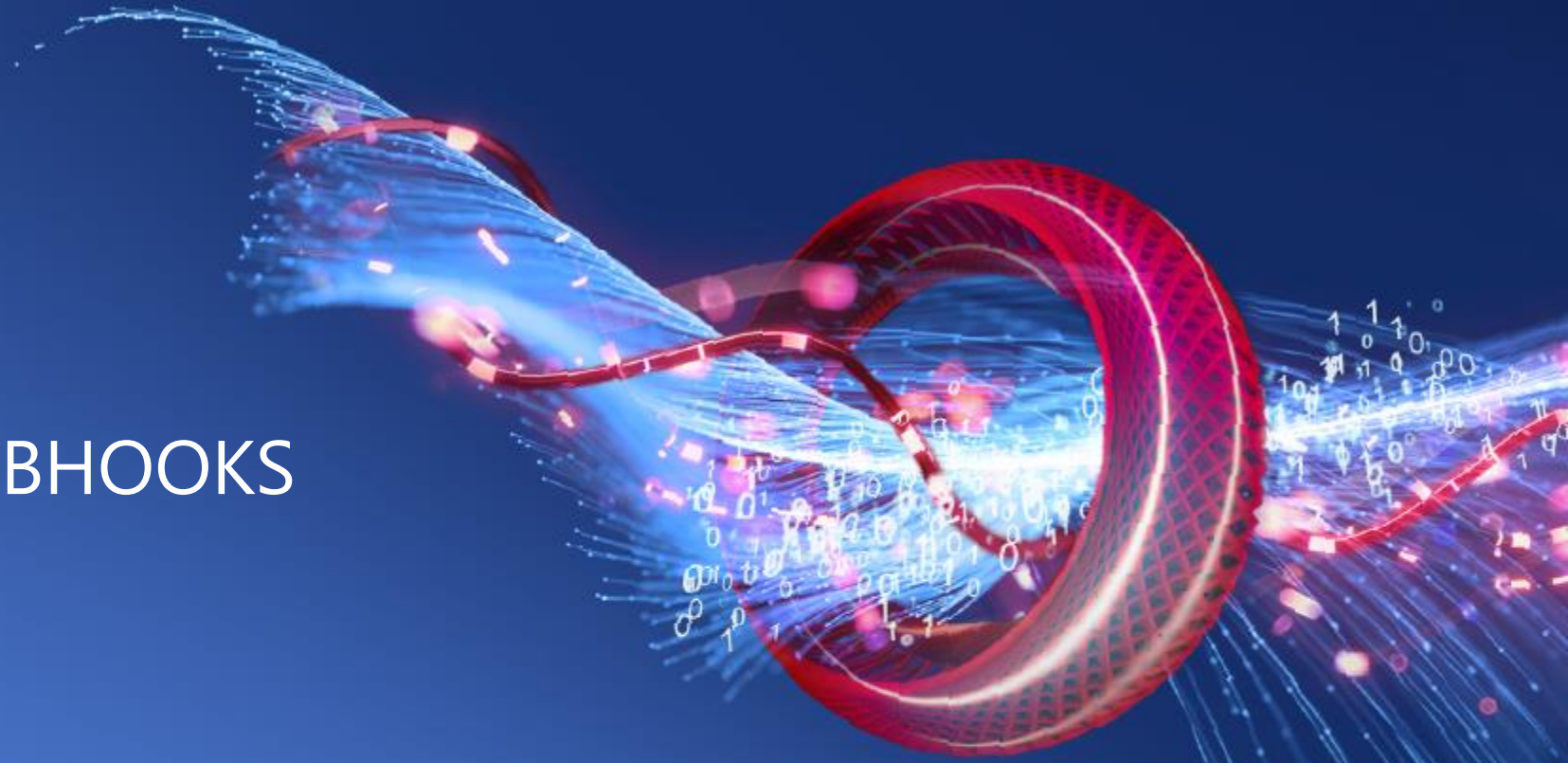
AUDIT LOG OBJECT AND METHOD

- ✓ 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

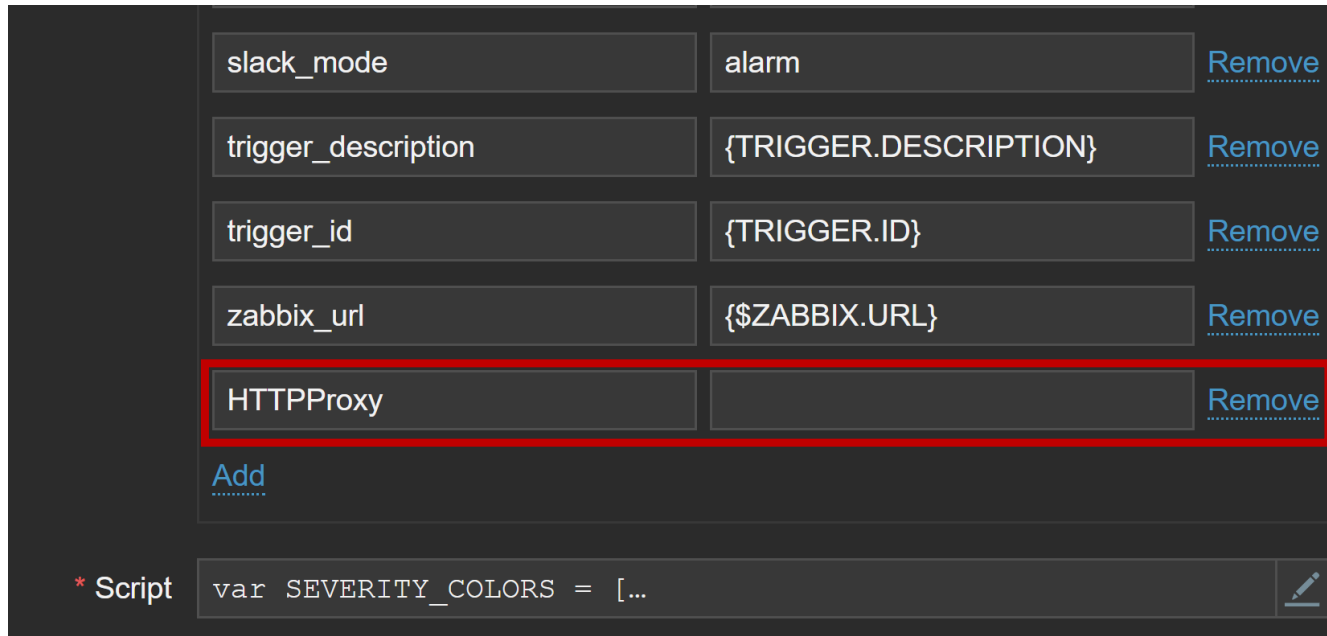
HTTP PROXY IN WEBHOOKS

ADDED ABILITY TO USE WEBHOOKS WITH HTTP PROXY



HTTP PROXY WEBHOOK CONFIGURATION

- ✓ Ability to specify HTTP proxy when configuring a webhook



The screenshot shows a configuration interface for a webhook. It features a list of parameters, each with a text input field and a 'Remove' button. The parameters are:

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

Below the list is an 'Add' button. At the bottom, there is a script editor with the label '* Script' and the following code: `var SEVERITY_COLORS = [...]` with a pencil icon for editing.

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

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

12

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.

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

Warning 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]

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

DISPLAYED DURING INITIAL SETUP

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

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!

