



# Zabbix communication

Server ↔ Agent

Server ↔ Proxy

Proxy ↔ Agent

# Two problems

Confidentiality  
Authentication

```
{  
  "globalmacro" : {  
    "fields" : ["globalmacroid", "macro", "value"],  
    "data" : [  
      [2, "{$SNMP_COMMUNITY}", "public"]  
    ]  
  },  
  "hosts" : {  
    "fields" : ["hostid", "host", "status", "ipmi_auth"],  
    "data" : [  

```

# Zabbix protocols

```
{  
  "globalmacro" : {  
    "fields" : ["globalmacroid", "macro", "value"],  
    "data" : [  
      [2, "{$SNMP_COMMUNITY}", "public"]  
    ]  
  },  
  "hosts" : {  
    "fields" : ["hostid", "host", "status", "ipmi_auth"],  
    "data" : [  

```

# What could be exposed?

Host names

SNMP community strings

SSH, IPMI passwords

```
{  
  "globalmacro" : {  
    "fields" : ["globalmacroid", "macro", "value"],  
    "data" : [  
      [{"id": 1, "macro": "SSH_PASSWORD", "value": "${SSNMP_COMMUNITY}"},  
      [{"id": 2, "macro": "IPMI_PASSWORD", "value": "public"}]  
    ],  
  },  
  "hosts" : {  
    "fields" : ["hostid", "host", "status", "ipmi_auth"],  
    "data" : [  
      [{"id": 1, "host": "192.168.1.1", "status": "up", "ipmi_auth": "123456"}]  
    ],  
  },  
}
```

# What else could be exposed?

Monitored data not that much...

Logfile contents?

```
{  "globalmacro" : {
    "fields" : ["globalmacroid", "macro", "value"],
    "data" : [
      [2, "{$SNMP_COMMUNITY}", "public"]
    ]
  },
  "hosts" : {
    "fields" : ["hostid", "host", "status", "ipmi_auth"],
    "data" : [
```

# What do you use today?

\*VPN?

stunnel?

SSH port forwarding?

# Who's there?

\*Knock Knock\*

- Who's there?

Maya.

- Maya who?

MAAAYAA HEEE

MAAYAA HUU

MAYAA HAA

MAYAAA HA HA

\*Knock Knock\*

- Who's there?

Zabbix server.

- Really?

TAKE ALL THIS DATA

# Encryption methods

PSK

Certificate based

~~Kerberos~~

```
{  "globalmacro" : {
    "fields" : ["globalmacroid", "macro", "value"],
    "data" : [
      [2, "{$SNMP_COMMUNITY}", "public"]
    ]
  },
  "hosts" : {
    "fields" : ["hostid", "host", "status", "ipmi_auth"],
    "data" : [
```

# Support must be compiled in

```
22104:20150911:103815.056 Starting Zabbix Server. Zabbix 3.0.0alpha2  
(revision {ZABBIX_REVISION}).
```

```
22104:20150911:103815.056 ***** Enabled features *****
```

```
22104:20150911:103815.057 SNMP monitoring: NO
```

```
22104:20150911:103815.057 IPMI monitoring: NO
```

```
22104:20150911:103815.057 Web monitoring: YES
```

```
22104:20150911:103815.057 VMware monitoring: NO
```

```
22104:20150911:103815.057 SMTP authentication: YES
```

```
22104:20150911:103815.057 Jabber notifications: NO
```

```
22104:20150911:103815.057 Ez Texting notifications: YES
```

```
22104:20150911:103815.057 ODBC: NO
```

```
22104:20150911:103815.057 SSH2 support: NO
```

```
22104:20150911:103815.057 IPv6 support: NO
```

```
22104:20150911:103815.057 TLS support: YES
```

```
22104:20150911:103815.057 *****
```

# Upgraded, what now?

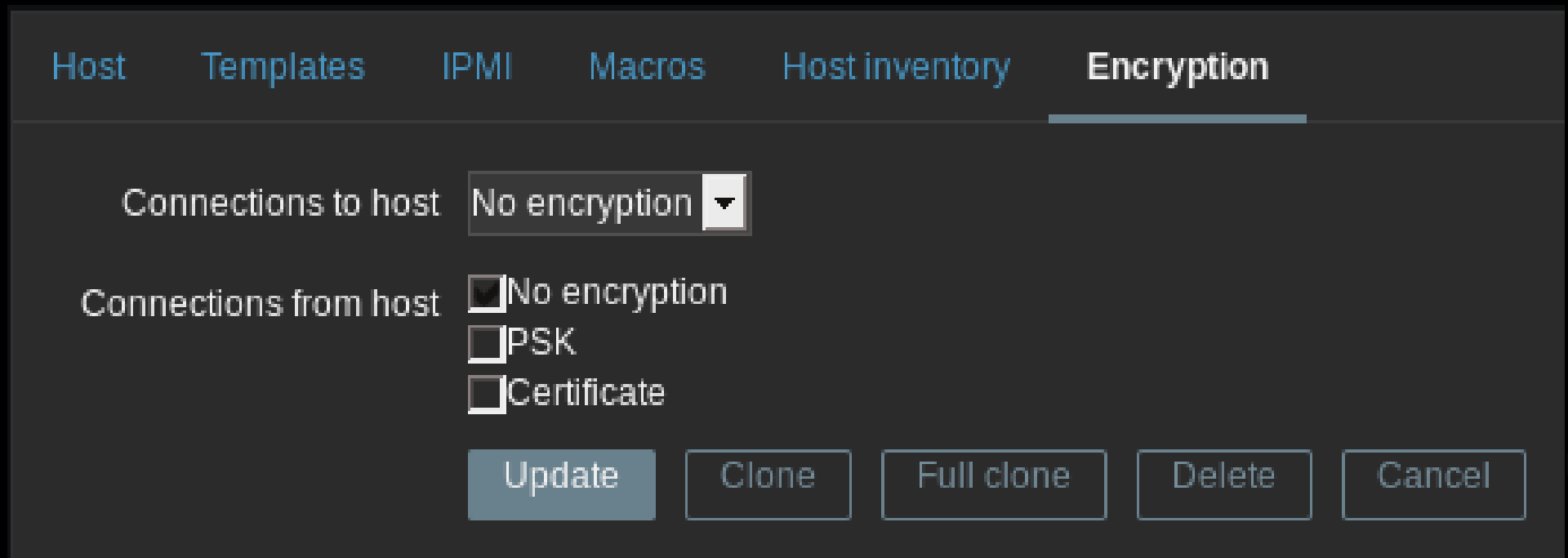
Passive agent

ENCRYPTION

NONE

NONE

# Host properties – new tab



The image shows a 'Host properties' dialog box with a dark theme. The 'Encryption' tab is selected, indicated by a blue underline. The dialog contains two main sections: 'Connections to host' and 'Connections from host'. The 'Connections to host' section has a dropdown menu currently set to 'No encryption'. The 'Connections from host' section has three radio buttons: 'No encryption' (which is selected), 'PSK', and 'Certificate'. At the bottom of the dialog, there are five buttons: 'Update' (highlighted in blue), 'Clone', 'Full clone', 'Delete', and 'Cancel'.

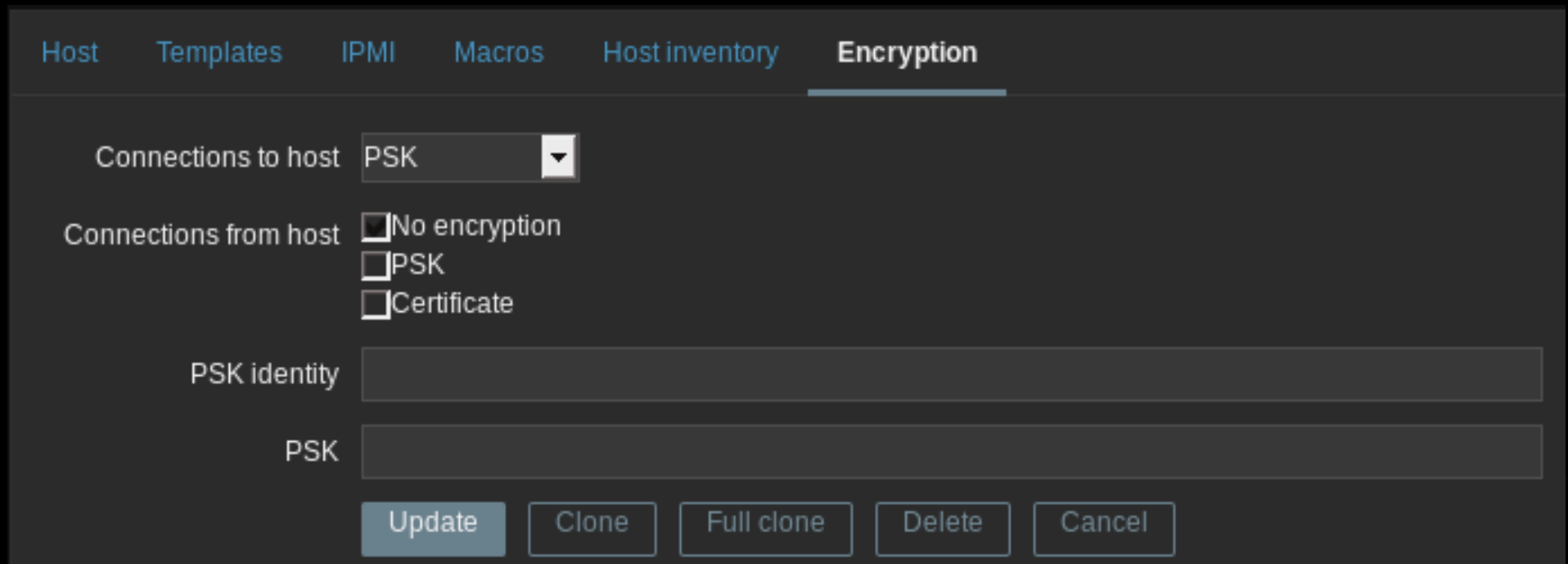
Host   Templates   IPMI   Macros   Host inventory   **Encryption**

Connections to host   No encryption ▼

Connections from host   ☒ No encryption  
☐ PSK  
☐ Certificate

Update   Clone   Full clone   Delete   Cancel

# Let's enable PSK



The screenshot shows a software interface with a top navigation bar containing the following tabs: Host, Templates, IPMI, Macros, Host inventory, and Encryption. The Encryption tab is currently selected and highlighted with a blue underline. Below the navigation bar, the interface is divided into two main sections. The first section, labeled 'Connections to host', features a dropdown menu with 'PSK' selected. The second section, labeled 'Connections from host', contains three radio button options: 'No encryption' (which is selected), 'PSK', and 'Certificate'. Below these options are two text input fields: the first is labeled 'PSK identity' and the second is labeled 'PSK'. At the bottom of the interface, there is a row of five buttons: 'Update' (highlighted in blue), 'Clone', 'Full clone', 'Delete', and 'Cancel'.

Host Templates IPMI Macros Host inventory **Encryption**

Connections to host PSK ▼

Connections from host ☒ No encryption  
☐ PSK  
☐ Certificate

PSK identity

PSK

**Update** Clone Full clone Delete Cancel

# Hostlist with enabled encryption

| ENCRYPTION                           |                            |
|--------------------------------------|----------------------------|
| <input checked="" type="radio"/> PSK | <input type="radio"/> NONE |

| ENCRYPTION                           |                                      |                                      |                                       |
|--------------------------------------|--------------------------------------|--------------------------------------|---------------------------------------|
| <input type="radio"/> NONE           | <input checked="" type="radio"/> PSK |                                      |                                       |
| <input checked="" type="radio"/> PSK | <input type="radio"/> NONE           | <input checked="" type="radio"/> PSK | <input checked="" type="radio"/> CERT |

# Agent side

TLSAccept

- unencrypted, psk, cert (multiple)

TLSPSKIdentity

TLSPSKFile

```
{
  "globalmacro" : {
    "fields" : ["globalmacroid", "macro", "value"],
    "data" : [
      [{"id": "1", "macro": "public", "value": "1"}]
    ],
  },
  "hosts" : {
    "fields" : ["hostid", "host", "status", "ipmi_auth"],
    "data" : [

```

That's it. Encrypted traffic.

# Certificates

Host Templates IPMI Macros Host inventory **Encryption**

Connections to host Certificate ▼

Connections from host ☐ No encryption  
☐ PSK  
☐ Certificate

Issuer

Subject

# Certificates, agent side

TLSCAFile

TLSCRLFile

TLSServerCertIssuer

TLSServerCertSubject

TLSCertFile

TLSKeyFile

# Active agent

Host

Templates

IPMI

Macros

Host inventory

Encryption

Connections to host

Certificate

Connections from host

☐ No encryption

☐ PSK

☐ Certificate

PSK identity

PSK

Issuer

Subject

Update

Clone

Full clone

Delete

Cancel

# Active agent, agent side

TLSCConnect

- unencrypted, psk, cert (one of)

TLSPSKIdentity

TLSPSKFile

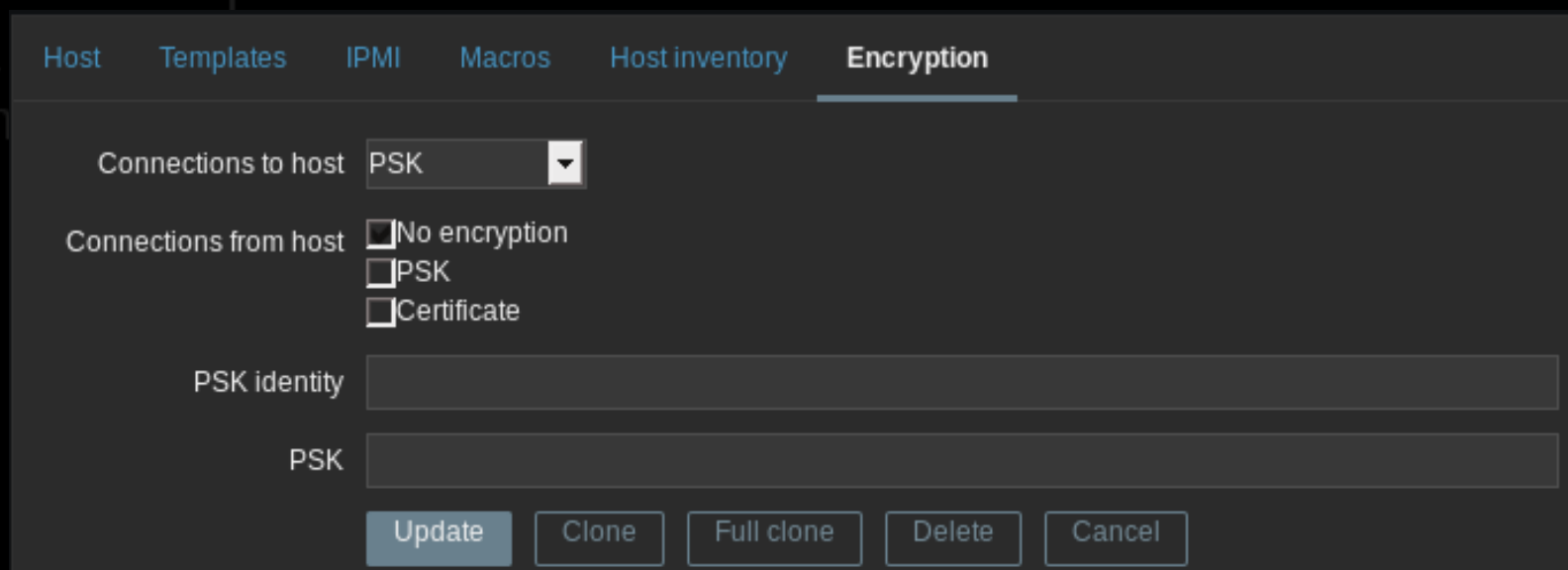
I don't follow, when upgrading I do what?

# Upgrading passive agents

Set TLSAccept=unencrypted,psk

Set TLSPSKIdentity, TLSPSKFile

Set connections to PSK in host properties

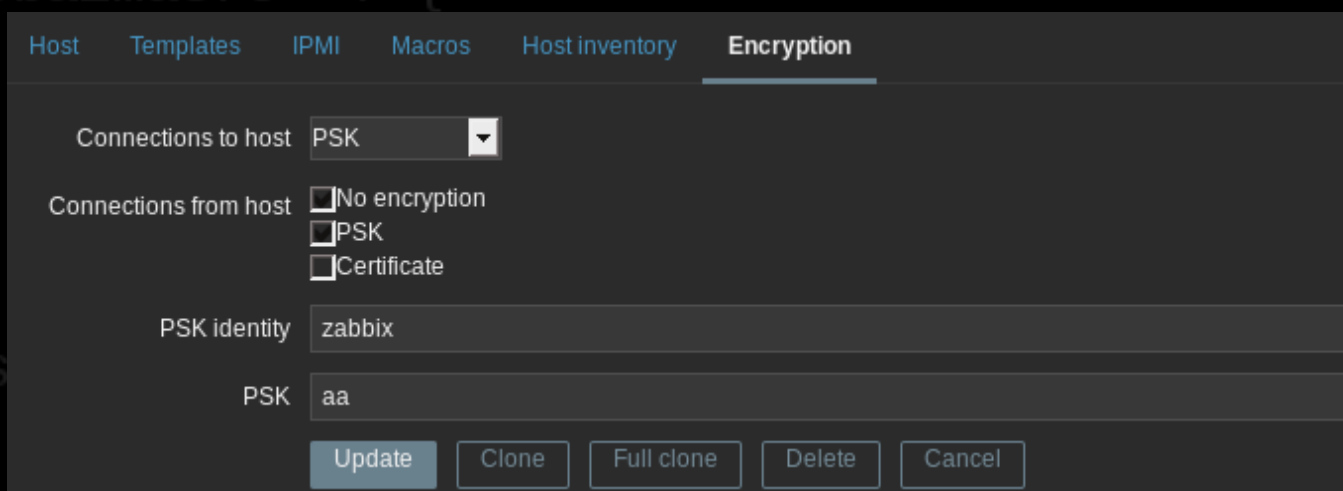


The screenshot shows a configuration window with several tabs: Host, Templates, IPMI, Macros, Host inventory, and Encryption. The Encryption tab is selected. It contains the following fields and controls:

- Connections to host:** A dropdown menu currently set to "PSK".
- Connections from host:** Three radio button options: "No encryption", "PSK", and "Certificate". The "PSK" option is selected.
- PSK identity:** A text input field.
- PSK:** A text input field.
- Buttons:** "Update", "Clone", "Full clone", "Delete", and "Cancel".

# Upgrading active agents

Enable unencrypted & PSK in host properties



The screenshot shows the Zabbix web interface with the 'Encryption' tab selected. The 'Connections to host' dropdown is set to 'PSK'. Under 'Connections from host', the 'No encryption' checkbox is checked, and the 'PSK' and 'Certificate' checkboxes are unchecked. The 'PSK identity' field contains 'zabbix' and the 'PSK' field contains 'aa'. At the bottom, there are buttons for 'Update', 'Clone', 'Full clone', 'Delete', and 'Cancel'.

| Host                                                                                                                                                                                                                                                                                  | Templates | IPMI | Macros | Host inventory | Encryption |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|--------|----------------|------------|
| <p>Connections to host: PSK</p> <p>Connections from host:<br/><input checked="" type="checkbox"/> No encryption<br/><input type="checkbox"/> PSK<br/><input type="checkbox"/> Certificate</p> <p>PSK identity: zabbix</p> <p>PSK: aa</p> <p>Update Clone Full clone Delete Cancel</p> |           |      |        |                |            |

Set TLSConnect=psk in the agent config

Set TLSPSKIdentity, TLSPSKFile

# Reminder

Encryption is optional

```
{  
  "globalmacro" : {  
    "fields" : ["globalmacroid", "macro", "value"],  
    "data" : [  
      ["$ONIE_COMMUNITY", "public"]  
    ]  
  },  
  "hosts" : {  
    "fields" : ["hostid", "host", "status", "ipmi_auth"],  
    "data" : [  
      ["$ONIE_COMMUNITY", "public"]  
    ]  
  }  
}
```

# Backend library support

OpenSSL

GnuTLS

PolarSSL/mbedTLS

```
{  "globalmacro" : {
    "fields" : ["globalmacroid", "macro", "value"],
    "data" : [
      ["{$SNMP_COMMUNITY}", "public"]
    ]
  },
  "hosts" : {
    "fields" : ["hostid", "host", "status", "ipmi_auth"],
    "data" : [
```

# Doing things properly

You want your developers pedantic

You want your beer at room temperature

```
{  
  "globalmacro" : {  
    "fields" : ["globalmacro", "value"],  
    "data" : [  
      [2, "{$SNMP_COMMUNITY}", "public"]  
    ]  
  },  
  "hosts" : {  
    "fields" : ["hostid", "host", "status", "ipmi_auth"],  
    "data" : [  
      [2, "192.168.1.1", "up", "12345678"]  
    ]  
  }  
}
```

# Less hair pulling

Good error messages

Error messages

```
{  "globalmacro" : {
    "fields" : ["globalmacroid", "macro", "value"],
    "data" : [
      [2, "{$SNMP_COMMUNITY}", "public"]
    ]
  },
  "hosts" : {
    "fields" : ["hostid", "host", "status", "ipmi_auth"],
    "data" : [
```

# What about other tools?

Yep, also supported for:

- zabbix\_get
- zabbix\_sender

```
{  "globalmacro" : {
    "fields" : ["globalmacroid", "macro", "value"],
    "data" : [
      [2, "{$SNMP_COMMUNITY}", "public"]
    ]
  },
  "hosts" : {
    "fields" : ["hostid", "host", "status", "ipmi_auth"],
    "data" : [
```

# zabbix\_get pre-3.0

## usage:

```
zabbix_get -s host-name-or-IP [-p port-number] [-I IP-address] -k item-key
```

```
zabbix_get -h
```

```
zabbix_get -V
```

Get data from Zabbix agent.

## Options:

-s --host host-name-or-IP Specify host name or IP address of a host

-p --port port-number Specify port number of agent running on the host. Default is 10050

-I --source-address IP-address Specify source IP address

-k --key item-key Specify key of the item to retrieve value for

-h --help Display this help message

-V --version Display version number

# zabbix\_get in 3.0

## usage:

zabbix\_get -s host-name-or-IP [-p port-number] [-I IP-address] -k item-key

zabbix\_get -s host-name-or-IP [-p port-number] [-I IP-address]

    --tls-connect cert --tls-ca-file CA-file

    [--tls-crl-file CRL-file] [--tls-agent-cert-issuer cert-issuer]

    [--tls-agent-cert-subject cert-subject]

    --tls-cert-file cert-file --tls-key-file key-file -k item-key

zabbix\_get -s host-name-or-IP [-p port-number] [-I IP-address]

    --tls-connect psk --tls-psk-identity PSK-identity

    --tls-psk-file PSK-file -k item-key

zabbix\_get -h

zabbix\_get -V

Get data from Zabbix agent.

## General options:

-s --host host-name-or-IP Specify host name or IP address of a host

-p --port port-number Specify port number of agent running on the host.  
Default is 10050

-I --source-address IP-address Specify source IP address

-k --key item-key Specify key of the item to retrieve value for

-h --help Display this help message

-V --version Display version number

## TLS connection options:

--tls-connect value How to connect to agent. Values:

unencrypted - connect without encryption

psk - connect using TLS and a pre-shared  
key

cert - connect using TLS and a  
certificate

--tls-ca-file CA-file Full pathname of a file containing the top-level  
CA(s) certificates for peer certificate  
verification

--tls-crl-file CRL-file Full pathname of a file containing revoked  
certificates

--tls-agent-cert-issuer cert-issuer Allowed agent certificate issuer

--tls-agent-cert-subject cert-subject Allowed agent certificate subject

--tls-cert-file cert-file Full pathname of a file containing the certificate  
or certificate chain

--tls-key-file key-file Full pathname of a file containing the private key

--tls-psk-identity PSK-identity Unique, case sensitive string used to  
identify the pre-shared key

--tls-psk-file PSK-file Full pathname of a file containing the pre-shared  
key

## Example(s):

zabbix\_get -s 127.0.0.1 -p 10050 -k "system.cpu.load[all,avg1]"

```
zabbix_get -s 127.0.0.1 -p 10050 -k "system.cpu.load[all,avg1]" \  
--tls-connect cert --tls-ca-file /home/zabbix/zabbix_ca_file \  
--tls-agent-cert-issuer \  
"CN=Signing CA,OU=IT operations,O=Example Corp,DC=example,DC=com" \  
--tls-agent-cert-subject \  
"CN=server1,OU=IT operations,O=Example Corp,DC=example,DC=com" \  
--tls-cert-file /home/zabbix/zabbix_get.crt \  
--tls-key-file /home/zabbix/zabbix_get.key
```

```
zabbix_get -s 127.0.0.1 -p 10050 -k "system.cpu.load[all,avg1]" \  
--tls-connect psk --tls-psk-identity "PSK ID Zabbix agentd" \  
--tls-psk-file /home/zabbix/zabbix_agentd.psk
```

# zabbix\_sender in 3.0

...even longer help output

Same functionality – TLS, PSK, unencrypted

```
{
  "globalmacro" : {
    "macro" : [
      [1, "{$SNMP_COMMUNITY}", "public"],
      [2, "{$SNMP_COMMUNITY}", "public"]
    ]
  },
  "hosts" : {
    "fields" : ["hostid", "host", "status", "ipmi_auth"],
    "data" : [

```

# Sender commandline

```
$ zabbix_sender -z 127.0.0.1  
-s host -k item_key -o value
```

# Sender commandline

```
$ zabbix_sender -z 127.0.0.1  
-s host -k item_key -o value  
--tls-connect psk --tls-psk-file psk  
--tls-psk-identity zabbix
```

# tcpdump before, after

```
E...T.@.@.....  
.....W'/.1W...w..  
...V.....@  
...?ZBXD.^.....  
.{"request":"sen  
der.data","data"  
:[{"host":"impor  
tant.host","key"  
:"secret","value  
":"revealed"}]}
```

```
E..<.X@.@.xa....  
.....'/qO.....  
.....0.....  
.....  
E..4.Y@.@.xh....  
.....'/qO..D.h  
...V.(.....  
....  
E....Z@.@.x....  
.....'/qO..D.h  
...V.....  
.....^...Z.]  
..)pk...2..qz.-0  
.....h.Ww..  
.....-.#.....  
.....  
.....
```

```
.....  
E..4.[@.@.xf.... E....]@.@.w....  
.....'/qO..D.. .....'/qPQ.D..  
...^.....  
.....=..  
.... J..*5.mmP^..''  
E....\@.@.x.... ..5.....X..'H+.b  
.....'/qO..D.. ..).q....b....1..  
...V..... ..x./L..%...R..3  
.....Z ..g.|...AGH....!  
abbix.....@ ..KU...K....6S./~  
...{...,oN.].. ....".....;u....  
..Ry..{..*.W...{. &.....qPw.O....a  
....%....l.*]+.H ..W..1.x]
```

# Executive summary

Built-in encryption (easy to use)

Strong authentication

Painless upgrade – encryption is optional

Can be enabled for selected proxies, agents

# Technical summary

Built-in encryption  
Painless upgrade

# Technical summary

## Connection methods

- PSK
- TLS
- Unencrypted

## Supported libraries

- OpenSSL
- GnuTLS
- PolarSSL/mbetTLS

# Things to keep in mind

Not for plain agent

Overhead – problem with passive, less with active

- Increase BufferSend for the active agent

# Proxy, you said "proxy"!

**Proxy**   **Encryption**

Connections to proxy   No encryption ▼

Connections from proxy   ☒ No encryption  
☐ PSK  
☐ Certificate

Add   Cancel

# WORKSFORME

Do you plan to use encryption?

Have you tested it already?

Devs, involved in encryption work, are on IRC

# Question time

IRC

Developers are here, use the chance

Encrypt away