



SUMMIT
ONLINE / 2021

SECURING ZABBIX 6.0 LTS

■ KĀRLIS SALIŅŠ

Technical Support Engineer, Zabbix, Latvia



01

WHY DO WE NEED “SECURITY”?

- INDUSTRY STANDARDS
- BUSINESS NEEDS
- TO PREVENT DATA BREACH



ACHIEVING SECURE ENVIRONMENT

- ✓ Using encryption to protect data
- ✓ Role-based access
- ✓ Audit logging for visibility
- ✓ ISO standards

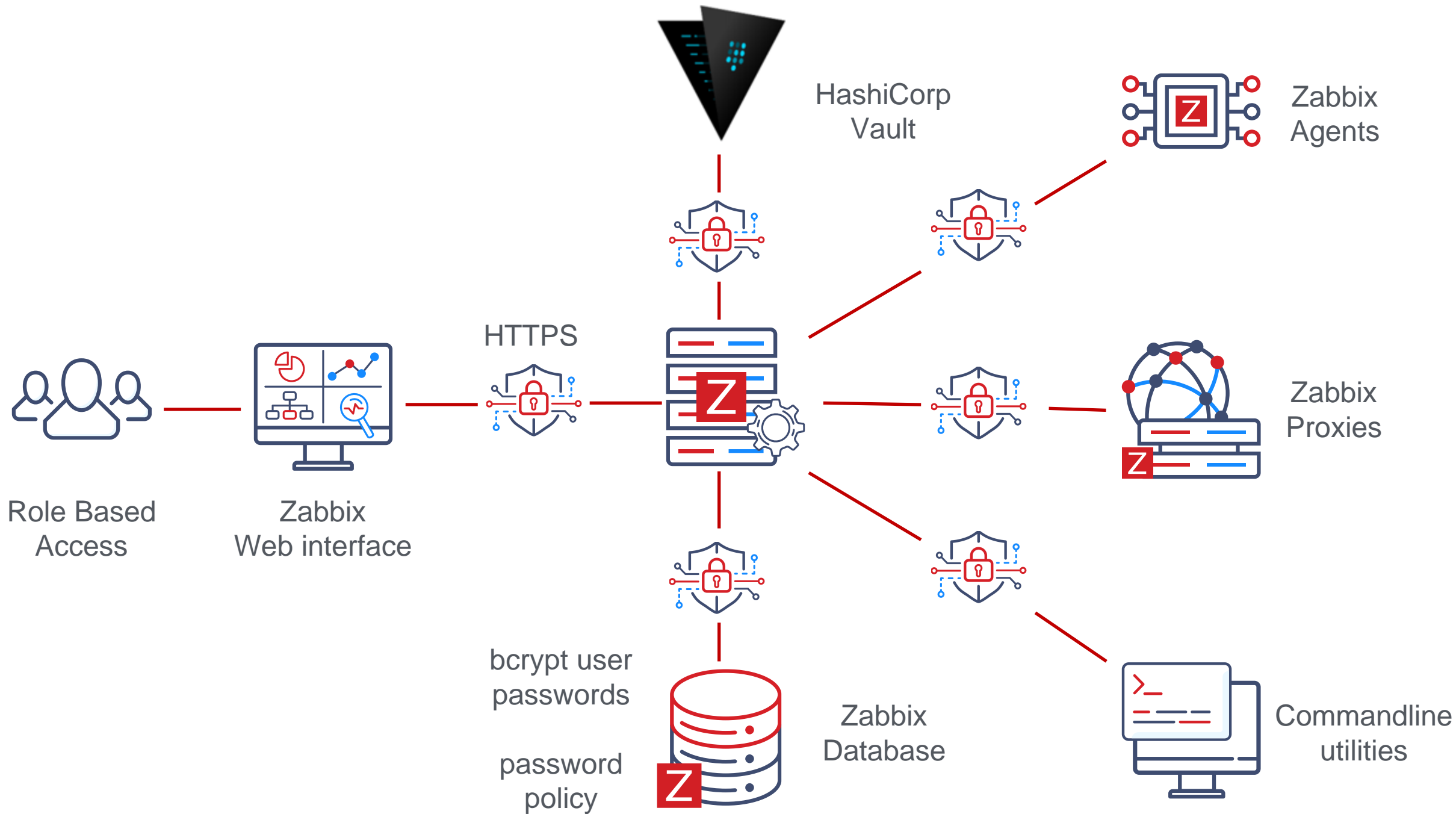


02

SECURITY IN ZABBIX

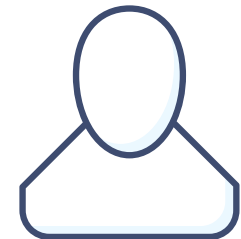
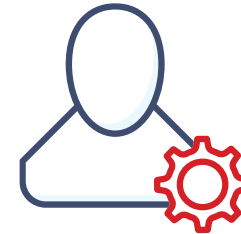
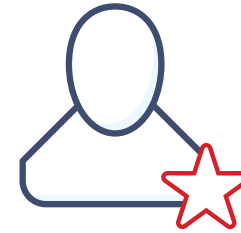
- Encryption
- Certificates
- PSK
- API tokens
- HashiCorp Vault





BUILT-IN USER TYPES

- ✓ Zabbix Super Admin
 - ✓ Unlimited Access
- ✓ Zabbix Admin
 - ✓ Can create hosts and templates
 - ✓ Permission based access
- ✓ Zabbix User
 - ✓ Permission based access
 - ✓ Can view monitoring

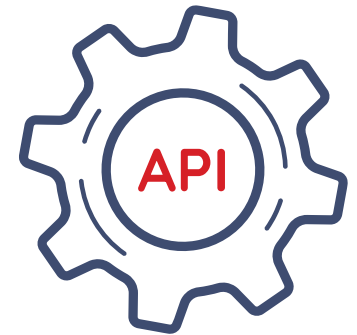


OBTAINING API TOKENS

```
{  
  "jsonrpc": "2.0",  
  "method": "user.login",  
  "params": {  
    "user": "Karlis",  
    "password": "K4rL!s"  
  },  
  "id": 1,  
  "auth": null  
}
```



```
{  
  "jsonrpc": "2.0",  
  "result": "0424bd59b807674191e7d77572075f33",  
  "id": 1  
}
```



NEW WAY OF OBTAINING API TOKENS

API tokens ▾

* Name

Karlis token

* User

Karlis ✕

Select

Description


Token generated from Zabbix GUI

Set expiration date and time

☒

* Expires at

2021-12-31 00:00:00



Enabled

☒

Add

Cancel

NEW WAY OF OBTAINING API TOKENS

API tokens ▾

✓

API token added

Name:

Karlis token

User:

Karlis

Auth token:

cf759668fd86b9376cea9025678201f5f6524fd57bce1e311a51c7d7c557349e

i

[Copy to clipboard](#)

Expires at:

2021-12-31 00:00:00

Description:

Token generated from Zabbix GUI

Enabled:

☒

Close

NEW WAY OF OBTAINING API TOKENS

API tokens ▾

Create API token

Filter 

Name

Created by users

Select

Users

Select

Status Any Enabled Disabled

Expires in less than days

Apply

Reset

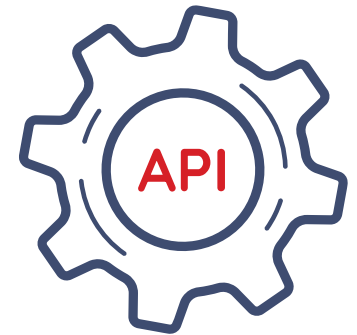
<input type="checkbox"/>	Name ▲	User	Expires at	Created at	Created by user	Last accessed at	Status
<input type="checkbox"/>	Admin token	Admin (Zabbix Administrator)	Never	2021-11-03 07:48:46	Admin (Zabbix Administrator)	Never	Enabled
<input type="checkbox"/>	Karlis token	Karlis	2021-12-31 00:00:00	2021-11-03 07:45:44	Admin (Zabbix Administrator)	Never	Enabled
<input type="checkbox"/>	Unique token	guest	2021-11-30 00:00:00	2021-11-03 07:41:22	Admin (Zabbix Administrator)	Never	Enabled

Displaying 3 of 3 found

USING API TOKENS

0424bd59b807674191e7d77572075f33

```
{  
  "jsonrpc": "2.0",  
  "method": "choose.method",  
  "params": {  
    "param": "one",  
    "param": "two"  
  },  
  "id": 1,  
  "auth": 0424bd59b807674191e7d77572075f33  
}
```



SECRET MACROS

- ✓ Value of macro is not displayed
- ✓ Value is not cloned / exported with Host / Template
- ✓ Secret macros are stored in database
- ✓ Database connection and access **MUST** be secured

{ \$MACRO }

The screenshot shows a web interface for managing host macros. It has two tabs: 'Host macros' (selected) and 'Inherited and host macros'. Below the tabs is a table with columns: 'Macro', 'Value', a dropdown menu, and 'Description'. There are four rows of macros. The first two are standard macros with visible values. The last two are secret macros, indicated by a red box around them and masked values (dots) in the 'Value' column. Each row has a 'Remove' button to its right. At the bottom, there are buttons for 'Update', 'Clone', 'Full clone', 'Delete', and 'Cancel'.

Macro	Value		Description	
{CPU.LOAD.HIGH}	3	T v	Threshold for CPU load	Remove
{DISK.SPACE.LOW}	100M	T v	Free disk space threshold	Remove
{ROOT.PASSWORD}	👁 v	Root password	Remove
{SNMP.COMMUNITY}	👁 v	SNMP community	Remove

Add

[Update](#) [Clone](#) [Full clone](#) [Delete](#) [Cancel](#)

VAULT USAGE

- ✓ HashiCorp vault can be used as storage for secrets
- ✓ Vault is a tool for securely accessing secrets, such as passwords
- ✓ Vault provides a unified interface to any secret, while providing tight access control and recording a detailed audit log
- ✓ Initially vault is sealed and must be unsealed using unseal keys
- ✓ Secrets are stored in Zabbix configuration cache
- ✓ The values of secrets are retrieved on every Zabbix configuration update



VAULT CONFIGURATION

Option: VaultToken

Vault authentication token that should have been generated

exclusively for Zabbix server with read only permission

VaultToken=verysecretrandomlygeneretedvaultstring

Option: VaultURL

Vault server HTTP[S] URL. System-wide CA certificates directory

will be used if SSLCALocation is not specified.

VaultURL=https://my.organization.vault:8200

Option: VaultDBPath

Vault path from where credentials for database will be retrieved

by keys 'password' and 'username'.

VaultDBPath=my/secret/location



03

WHAT'S NEW IN ZABBIX 6.0 LTS

- Audit log upgrades
- Password complexity requirements
- TLS/SSL website certificate monitoring
- User permissions for the service tree



UPGRADED AUDIT LOG

- ✓ Better API operations logging
- ✓ Better support regarding high amount of items/devices/etc.
- ✓ Overall quality of life improvements
- ✓ Added various new metrics to be logged:
 - ✓ Script execution
 - ✓ Global macro change
 - ✓ LLD changes
 - ✓ etc.



UPGRADED AUDIT LOG

Time	User	IP	Resource	Action	ID	Description	Details
2021-11-03 10:43:33	karlis	192.168.100.200	<u>Macro</u>	<u>Update</u>	6	{TEST_MACRO}	globalmacro.value: testvalue => testvalue23
2021-11-03 10:43:00	karlis	192.168.100.200	User	Add	68	karlis1	
2021-11-03 10:42:00	karlis	192.168.100.200	<u>Macro</u>	<u>Add</u>	6	{TEST_MACRO}	
2021-11-03 10:41:12	karlis	192.168.100.200	<u>Script</u>	<u>Execute</u>	2		script.execute_on: => 1 script.hostid: => 10084 script.command: => /usr/sbin/traceroute 192.168.7.203 2>&1 script.error: => sh: /usr/sbin/traceroute: No such file or directory
2021-11-03 10:41:05	karlis	192.168.100.200	<u>Script</u>	<u>Execute</u>	1		script.execute_on: => 1 script.hostid: => 10084 script.command: => /usr/bin/ping -c 3 192.168.7.203 2>&1 script.output: => PING 192.168.7.203 (192.168.7.203) 56(84) bytes of data. 64 bytes from 192.168.7.203: icmp_seq=2 ttl=64 time=0.073 ms 64 bytes from 192.168.7.203: icmp_seq=2 ttl=64 time=0.073 ms 64 bytes from 192.168.7.203: icmp_seq=2 ttl=64 time=0.073 ms 192.168.7.203 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 500 ms rtt min/avg/max/mdev = 0.073/0.081/0.088/0.012 ms
2021-11-03 10:40:56	karlis	192.168.100.200	<u>Script</u>	<u>Execute</u>	3		script.execute_on: => 1 script.hostid: => 10084 script.command: => nmap -O 192.168.7.203 2>&1 script.error: => TCP/IP fingerprinting (for OS scan) requires root privileges. QUITTING!

COMPLEX USER PASSWORDS

- ✓ Password no longer cannot be *password*
- ✓ Implemented password complexity and policy, encryption in bcrypt
- ✓ Implemented password requirements:
 - ✓ 8 characters long
 - ✓ Must not contain name/last name/username
 - ✓ Not easy to guess (~~abcd~~1234, ~~asdf~~1234)
 - ✓ ~1 million most common passwords cannot be used
- ✓ Fresh installation Admin password **does not** change



* Password ?

* Password (once again)

Password requirements:

- must be at least 8 characters long
- must not contain user's name, surname or username
- must not be one of common or context-specific passwords



Password = **qwerty1234**



Details ▲ Cannot update user

Incorrect value for field "/1/passwd": must not be one of common or context-specific passwords.

Name = **John**

Password= **John1234**



Details ▲ Cannot update user

Incorrect value for field "/1/passwd": must not contain user's name, surname or username.

MONITORING OF CERTIFICATE ATTRIBUTES

- ✓ Zabbix Agent 2 built-in plugin starting from **Zabbix Agent2 5.0.15**
- ✓ Displays information about certificate in a website
- ✓ Template available out of the box
- ✓ `web.certificate.get[<website_DNS_name>,port,ip]`



"GOOD" CERTIFICATE

```
zabbix_agent2 -t web.certificate.get[www.zabbix.com]
```

```
web.certificate.get[www.zabbix.com]          [s|{"x509":{"version":3,
"serial_number":"0f5bd7fa1129ddf854e2745a3e8dc788",
"signature_algorithm":"ECDSA-SHA256",
"issuer":"CN=Cloudflare Inc ECC CA-3,O=Cloudflare\\, Inc.,C=US",
"not_before":{"value":"Jun 08 00:00:00 2021 GMT","timestamp":1623110400},
"not_after":{"value":"Jun 07 23:59:59 2022 GMT",
"timestamp":1654646399},
"subject":"CN=zabbix.com,O=Cloudflare\\, Inc.,L=San Francisco,ST=California,C=US",
"public_key_algorithm":"ECDSA",
"alternative_names":["*.zabbix.com","zabbix.com"]}},
"result":{"value":"valid",
"message":"certificate verified successfully"},
"sha1_fingerprint":"e759419726b0599484d75977b5e0c8f6a4fa6728",
"sha256_fingerprint":"0ffeeef9b263219decf7db55c32ba65cd59bfe72b83841aa6fb720c830281fe71"}]]
```

"BAD" CERTIFICATE

```
zabbix_agent2 -t web.certificate.get[self-signed.badssl.com]
```

```
web.certificate.get[self-signed.badssl.com]    [s|{"x509":{  
  "version":3,  
  "serial_number":"c9c0f0107cc53eb0",  
  "signature_algorithm":"SHA256-RSA",  
  "issuer":"CN=*.badssl.com,O=BadSSL,L=San Francisco,ST=California,C=US",  
  "not_before":{"value":"Oct 11 20:03:54 2021 GMT","timestamp":1633982634},  
  "not_after":{"value":"Oct 11 20:03:54 2023 GMT","timestamp":1697054634},  
  "subject":"CN=*.badssl.com,O=BadSSL,L=San Francisco,ST=California,C=US",  
  "public_key_algorithm":"RSA",  
  "alternative_names":["*.badssl.com","badssl.com"]},  
  "result":{"value":"valid-but-self-signed",  
  "message":"certificate verified successfully, but determined to be self signed"},  
  "sha1_fingerprint":"303eabd4efe3b129e56bb54132492777d57b7116",  
  "sha256_fingerprint":"fc31cc459fbfa26d95f4ba432b27275d2444a88a1c13b6d3bab99a71ac18b96c"}]
```

COMMON TRIGGER EXAMPLES

- Invalid certificate

```
{HOST:cert.validation.str("invalid")} = 1
```

- Certificate expires in 7 days

```
({HOST:cert.not_after.last()} -  
{HOST:cert.not_after.now()}) / 86400 < 7
```

- Certificate fingerprint has changed

```
{TEMPLATE_NAME:cert.sha1_fingerprint.diff()}=1
```



SERVICE TREE UPGRADES

- ✓ Reworked implementation
- ✓ Improved scalability
- ✓ Better API compatibility
- ✓ User permission improvements



MODIFYING ACCESS LEVELS

Access to services

Read-write access to services

NoneAllService list

service1 ×
type here to search

Select

Read-write access to services with tag

tagvalue

Read-only access to services

NoneAllService list

karlis ×
type here to search

Select

Read-only access to services with tag

tagvalue

PERMISSION VIEW

Services

Create service

View

Edit

All services / Read-only root service

Info



Filter



Read-only root service

Parent services:

Status: OK

SLA: 99.9000

Tags: City: Valmiera

<input type="checkbox"/>	Name	Status	Root cause	SLA	Tags	
<input type="checkbox"/>	Child service 1	OK				+ ↗ ✕
<input type="checkbox"/>	Child service 2	OK				+ ↗ ✕
<input type="checkbox"/>	Child service 3 with explicit read-write access	OK				+ ↗ ✕

Displaying 3 of 3 found

0 selected

Mass update

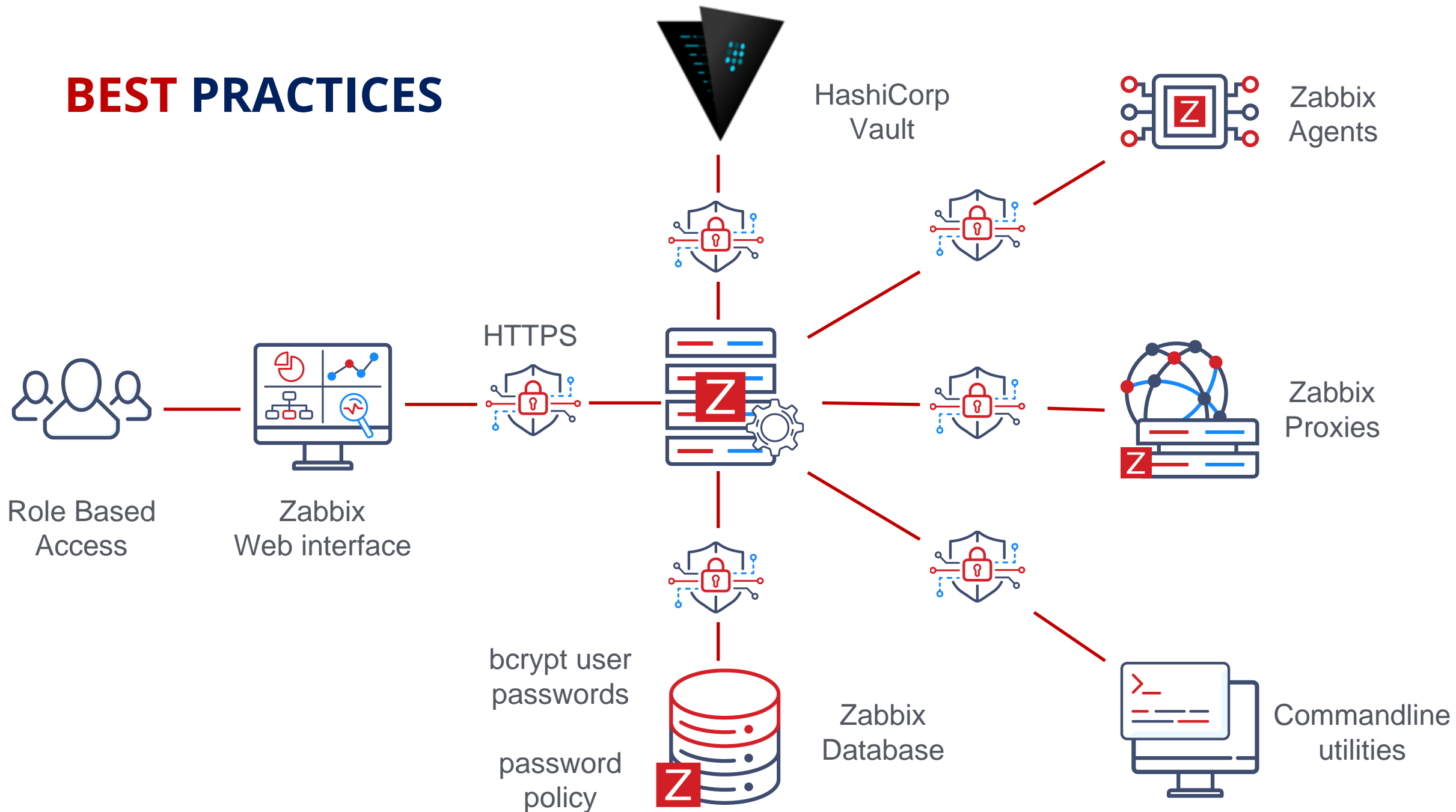
Delete

04

BEST PRACTICES

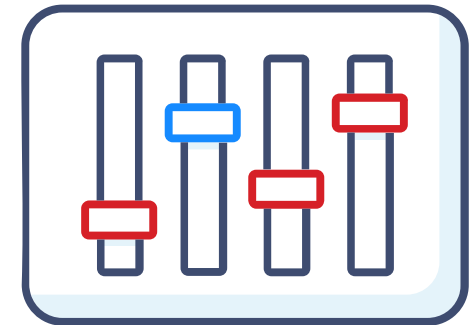


BEST PRACTICES



IS YOUR ZABBIX SECURE?

- ✓ Are you using encryption on ALL Zabbix components?
- ✓ Are you using HTTPS to access frontend?
- ✓ Is Zabbix Agent2 database connections secured?
- ✓ Is the connection to database secure?
- ✓ Are there agent key restrictions in place?
- ✓ Are user permissions configured correctly?
- ✓ Have important or possibly vulnerable macros been made secret?
- ✓ Are most valuable secrets stored in vault?
- ✓ Is the newest minor release installed?(4.0.**35**, 5.0.**17**, 5.4.**7**)



LEARN IN-DEPTH SECURITY FEATURES OF ZABBIX

- ✓ One day course
- ✓ Securing Zabbix components
- ✓ Using key vault
- ✓ Securing database connections
- ✓ RBAC system
- ✓ Zabbix Agent key restrictions



Advanced Zabbix Security Administration

The course will cover how to protect Zabbix internal communications and secure sensitive information like user credentials or encryption keys.

1 day

Requirements

No requirements

Price in EUR

Price in USD

€ 490

Price does not include VAT

Apply for course



SUMMIT
ONLINE/2021

Thank you!

www.zabbix.com