

# ZABBIX 2022 Conference BRAZIL

## Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com a conformidade de Segurança da Informação  
(Security Information)



**PAULO R. DEOLINDO JUNIOR**  
Zabbix Trainer & DPO na Unirede  
Inteligência em TI



**PAULO R. DEOLINDO JUNIOR**  
Zabbix Trainer & DPO na Unirede  
Inteligência em TI



# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

O que é Security by Design?  
(What does mean Security by Design)

Aplicado à Engenharia de Software, **Security by Design** pode ser visto como um conceito de segurança ideal, se materializando na prática da entrega de um produto / serviço que aplica desde sua concepção, **Conceitos de Segurança da Informação e Segurança Cibernética, sem comprometer suas features!**

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

Definição por conceitos  
(Definition by concepts)

Integrações seguras de APIs com Tokens

Alta disponibilidade da solução

Retenção de dados em perda de conectividade

Critérios para senhas, uso de LDAPs e SAML

Criptografia entre principais componentes da solução

Prestação de contas de disponibilidade de serviços

Implementação em empresas + conservadoras

Acesso seguro de usuário

Confiabilidade no tráfego de informações do negócio

Monitoramento de escopo extraterritorial de informação

Análise de causa raiz de problemas

Registro de eventos de SI e de infraestrutura

Manutenção de sistemas e supressão de eventos

Trilha de auditoria de ações de usuários

Segurança na coleta e envio de dados remotos

Conformidade com leis de privacidade de dados

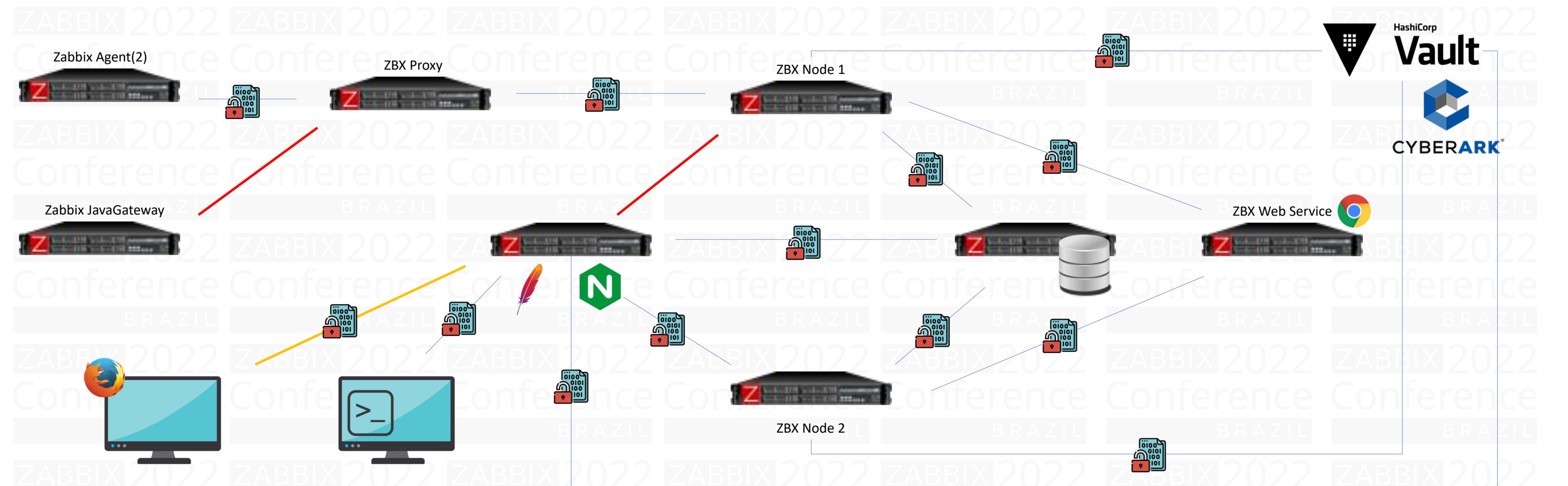
Diferentes usuários, papéis, permissões

Rígido controle de vulnerabilidades técnicas

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

Arquitetura da solução  
(Solution architecture)



# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

Comunicação entre os principais componentes  
(Main components communication)

ZBX Server Node 1 & Node 2



zabbix\_server.conf

DBHost=zbx-db-server  
DBName=zabbix

VaultToken=<my\_vault\_token>  
VaultURL=<my\_vault\_server:8200>  
VaultDBPath=zabbix/database

DBTLSConnect=  
DBTLSCAFile=  
DBTLSCertFile=  
DBTLSKeyFile=  
DBTLSCipher13=



ZBX Web Interface



Store credentials in  Plain text  HashiCorp Vault

Vault API endpoint

Vault secret path

Vault authentication token

Database TLS encryption

Verify database certificate

\* Database TLS CA file

Database TLS key file

Database TLS certificate file

Database host verification

Database TLS cipher list



# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

Alta Disponibilidade  
(High Availability)

ZBX Server Node 1



ZBX Server Node 2



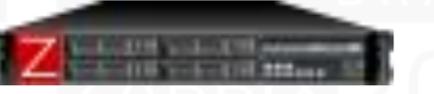
ZBX Web Interface



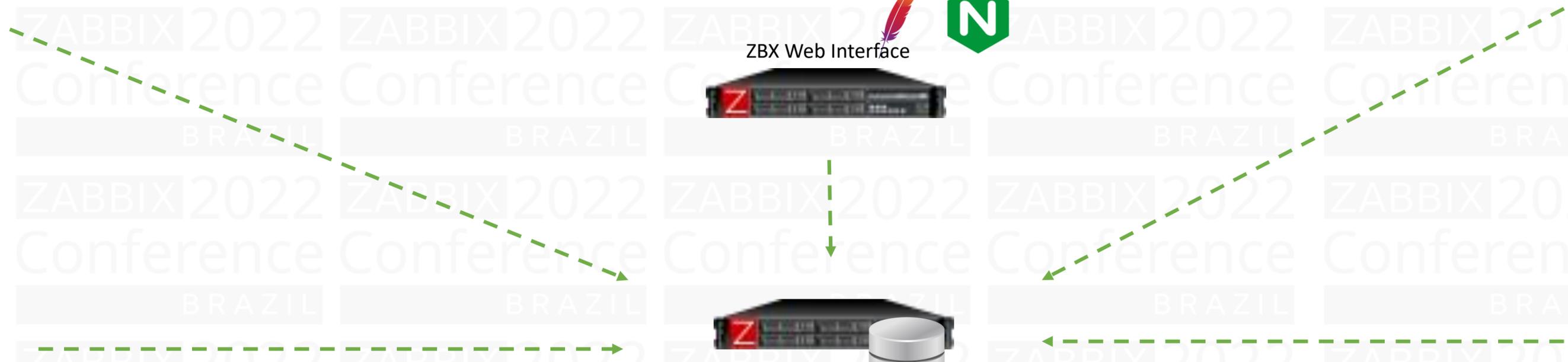
ZBX Server Node 3



ZBX Server Node 4



FailOver <> LoadBalance



# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

## Acesso seguro ao Frontend (Secure frontend access)



TLS/SSL

ZBX Web Interface



Zabbix DB



Bcrypt  
Hashing + Salt



\* 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

Zabbix DB



MD5SUM





<https://myzabbyx.com>

DNS round-robin

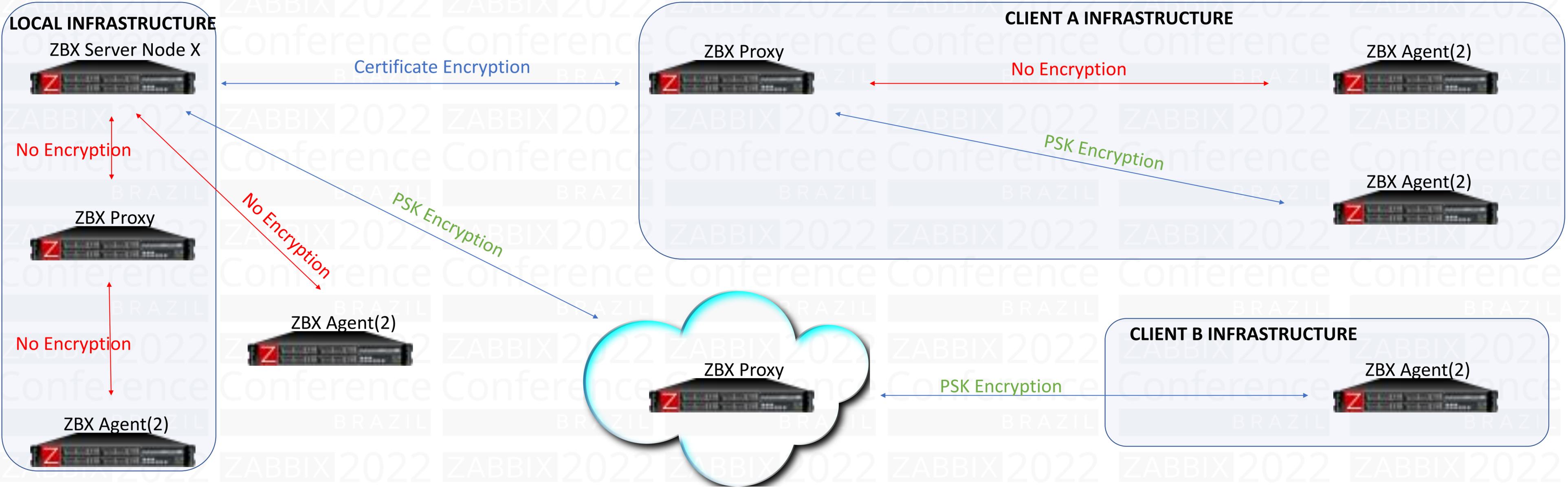


HTTP Server Technology  
Not Zabbix

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

## Zabbix Server x Zabbix Proxy x Zabbix Agent(2)



## Bibliotecas para suporte à Criptografia entre componentes Zabbix (exceto Zabbix Frontend e Zabbix JavaGateway)

- GnuTLS – a partir da versão 3.1.18
- OpenSSL - versões 1.0.1, 1.0.2, 1.1.0, 1.1.1, 3.0.x. **A versão 3.0.x é suportada desde o Zabbix 6.0.4**
- LibreSSL – testado com as versões 2.7.4, 2.8.2:
  - LibreSSL é suportado como compatibilidade ao OpenSSL e possui limitações de uso em alguns cenários.

## Gestão de Conexões Criptografadas

no encryption (default)

RSA certificate-based encryption

PSK-based encryption

→ por padrão, a comunicação ocorre sem criptografia

→ criptografia com base em certificados digitais

→ criptografia simétrica, com chaves compartilhadas

## Conexões de entrada x saída

TLSConnect=psk

TLSAccept=psk,cert

→ para conexões de saída (monitoramento ativo)

→ para conexões de entrada (monitoramento passivo)

## Exemplo de biblioteca Openssl, versão e implementação de cifras

	Certificate ciphersuites	PSK ciphersuites
<i>OpenSSL 1.1.1d</i>	TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA AES128-GCM-SHA256 AES128-CCM8 AES128-CCM AES128-SHA256 AES128-SHA	TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256 ECDHE-PSK-AES128-CBC-SHA256 ECDHE-PSK-AES128-CBC-SHA PSK-AES128-GCM-SHA256 PSK-AES128-CCM8 PSK-AES128-CCM PSK-AES128-CBC-SHA256 PSK-AES128-CBC-SHA

For Zabbix agent:

Agent connection setup	Cipher configuration
TLSCipherCert	TLSCipherCert, TLSCipherCert13
TLSCipherPSK	TLSCipherPSK, TLSCipherPSK13
TLSCipherAll	TLSCipherCert, TLSCipherCert13
TLSCipherAll13	TLSCipherPSK, TLSCipherPSK13
TLSCipherAll, TLSCipherAll13	TLSCipherAll, TLSCipherAll13

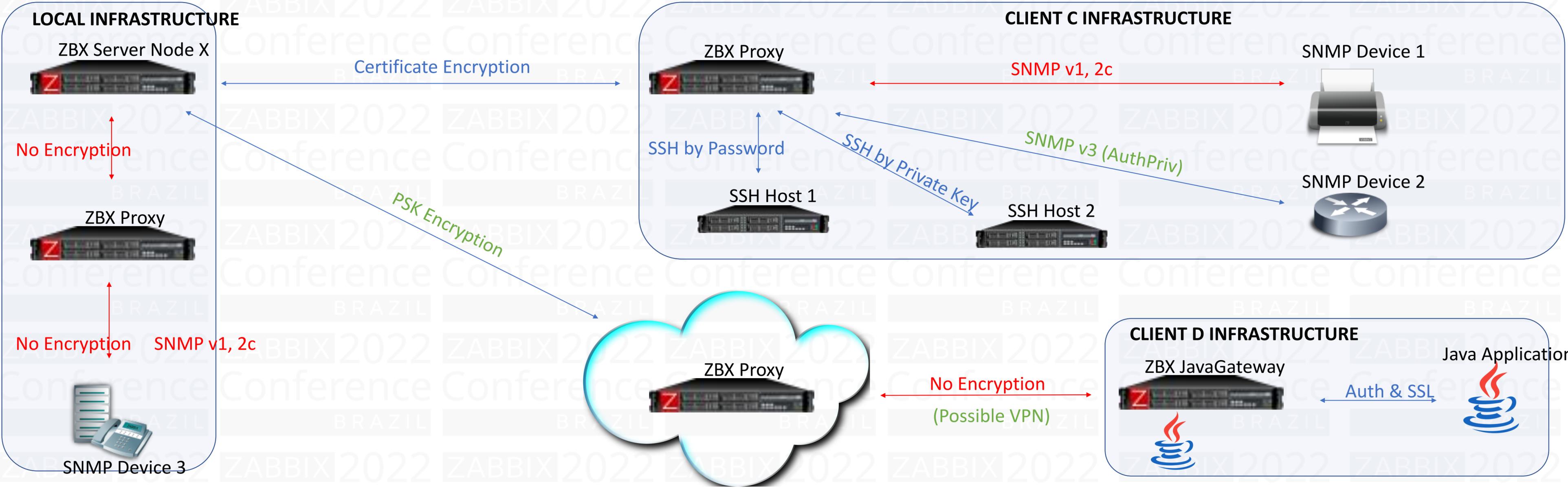
For Zabbix server and \*\* proxy\*\*:

Connection setup	Cipher configuration
Outgoing connections using PSK	TLSCipherPSK, TLSCipherPSK13
Incoming connections using certificates	TLSCipherAll, TLSCipherAll13
Incoming connections using PSK if server has no certificate	TLSCipherPSK, TLSCipherPSK13
Incoming connections using PSK if server has certificate	TLSCipherAll, TLSCipherAll13

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

## SSH, SNMP v3 & SNMPTRAP (v3)



LOCAL INFRASTRUCTURE

ZBX Server Node X



SSH Host 1



\* Name A SSH Item 1

Type SSH agent

\* Key ssh.run[key1]

Type of information Numeric (unsigned)

\* Host interface 127.0.0.1:10050

Authentication method Password

\* User name {SMY\_SSH\_USER}

Password {SMY\_SSH\_PASSWORD}

Host

Host macros Inherited and host macros

Macro	Value	Description
{SMY_SSH_USER}	user	description
{SMY_SSH_PASSWORD}	121314	description

Add

- T Text
- Secret text
- Vault secret

USING CREDENTIALS



\* Name

Type

\* Key

Type of information

\* Host interface

Authentication method

\* User name

\* Public key file

\* Private key file

Password

\* Executed script



USING PUBLIC KEY



ZBX Server Node X



SNMP v3 Device



### SNMP Interface (v3)

SNMP 127.0.0.1   IP DNS 161  Remove

\* SNMP version

Context name

Security name

Security level

Authentication protocol

Authentication passphrase

Privacy protocol

Privacy passphrase

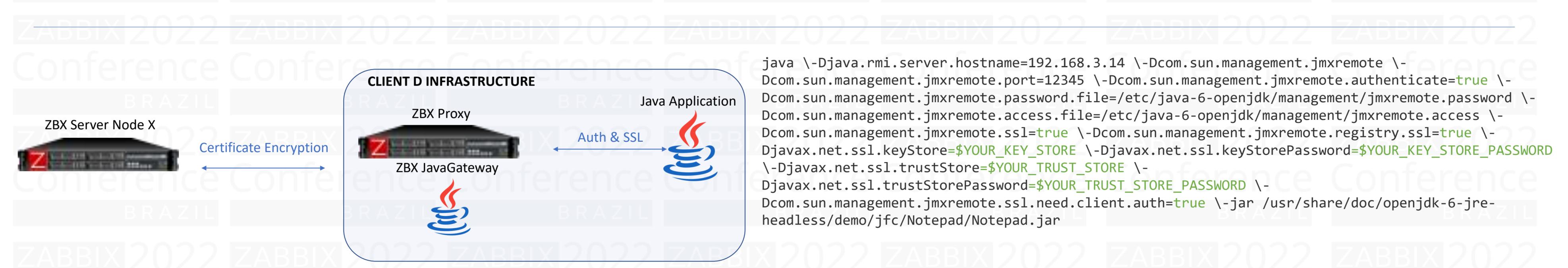
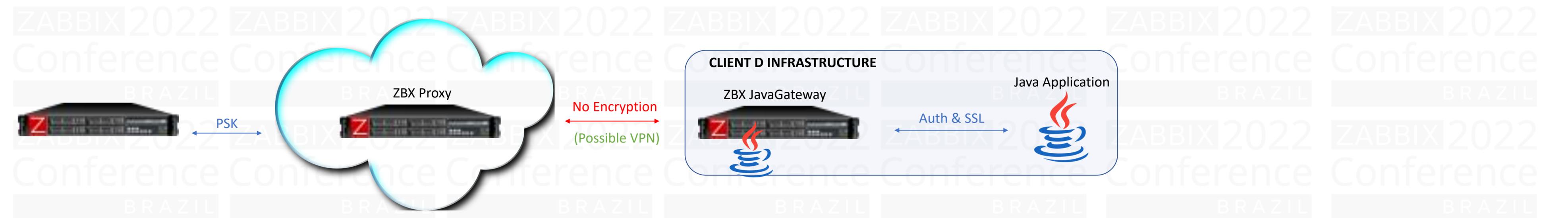
**SNMP v1, v2c = Community information**  
No auth, no encryption

**SNMP v3 = Auth + Encryption**

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

## Zabbix JavaGateway



```
java \-Djava.rmi.server.hostname=192.168.3.14 \-Dcom.sun.management.jmxremote \-
Dcom.sun.management.jmxremote.port=12345 \-Dcom.sun.management.jmxremote.authenticate=true \-
Dcom.sun.management.jmxremote.password.file=/etc/java-6-openjdk/management/jmxremote.password \-
Dcom.sun.management.jmxremote.access.file=/etc/java-6-openjdk/management/jmxremote.access \-
Dcom.sun.management.jmxremote.ssl=true \-Dcom.sun.management.jmxremote.registry.ssl=true \-
Djavax.net.ssl.keyStore=$YOUR_KEY_STORE \-Djavax.net.ssl.keyStorePassword=$YOUR_KEY_STORE_PASSWORD
\ -Djavax.net.ssl.trustStore=$YOUR_TRUST_STORE \-
Djavax.net.ssl.trustStorePassword=$YOUR_TRUST_STORE_PASSWORD \-
Dcom.sun.management.jmxremote.ssl.need.client.auth=true \-jar /usr/share/doc/openjdk-6-jre-
headless/demo/jfc/Notepad/Notepad.jar
```

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

HTTP checks, Web Scenarios



API

HTTP check

ZBX Server Node X



HTTP proxy

HTTP authentication

SSL verify peer

SSL verify host

SSL certificate file

SSL key file

SSL key password

HTTP authentication

SSL verify peer

SSL verify host

SSL certificate file

SSL key file

SSL key password



Web Scenario

ZBX Server Node X

Variables

Name	Value	
{password}	⇒ {SAPP_PASSWORD}	<a href="#">Remove</a>
{user}	⇒ {SAPP_USER}	<a href="#">Remove</a>

T ^ description

- T Text
- 👁 Secret text
- 🔒 Vault secret

HTTP proxy

HTTP authentication

SSL verify peer

SSL verify host

SSL certificate file

SSL key file

SSL key password



**ZABBIX** 2022  
Conference  
BRAZIL

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

## Zabbix Trapper

ZBX Server Node X



ZBX Trapper



Example(s):

`zabbix_sender -z 127.0.0.1 -s "Linux DB3" -k db.connections -o 43` → # No secure

`zabbix_sender -z 127.0.0.1 -s "Linux DB3" -k db.connections -o 43 \`  
`--tls-connect cert --tls-ca-file /home/zabbix/zabbix_ca_file \`  
`--tls-server-cert-issuer \`  
`"CN=Signing CA,OU=IT operations,O=Example Corp,DC=example,DC=com" \`  
`--tls-server-cert-subject \`  
`"CN=Zabbix proxy,OU=IT operations,O=Example Corp,DC=example,DC=com" \`  
`--tls-cert-file /home/zabbix/zabbix_agentd.crt \`  
`--tls-key-file /home/zabbix/zabbix_agentd.key` → # Secure

`zabbix_sender -z 127.0.0.1 -s "Linux DB3" -k db.connections -o 43 \`  
`--tls-connect psk --tls-psk-identity "PSK ID Zabbix agentd" \`  
`--tls-psk-file /home/zabbix/zabbix_agentd.psk` → # Secure

Item Tags Preprocessing

\* Name

Type

\* Key

Type of information

Units

\* History storage period

\* Trend storage period

Value mapping

Allowed hosts

# Zabbix 6.0: Security by Design

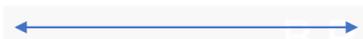
Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

## Zabbix Agent(2)

ZBX Server Node X



ZBX Agent(2)



### Zabbix System User

Zabbix run as a "zabbix system user"  
Zabbix user **need no shell**

### AllowKey x DenyKey

AllowKey=system.run[systemctl restart service1]  
AllowKey=system.run[systemctl restart service2]  
AllowKey=system.run[systemctl restart service3]  
DenyKey=system.run[\*]

### Specific security Keys

vfs.file.md5sum[file]  
vfs.file.owner[file,<ownertype>,<resulttype>]  
vfs.file.permissions[file]  
vfs.file.time[file,<mode>]

### Item → Log File Monitoring

Name: Monitoring Failed Authentications  
Type: Zabbix agente (active)  
Key: log[/var/log/auth.log,(Failed | Accepted)]  
Type of information: Log  
Update interval: 1s  
Log time format: <yyyy-MM-ddphh:mm:ss>

Tag  
Name: Service  
Value: Auth

### Trigger to Log File Monitoring

Name: Authentication Failed for {{ITEM.VALUE}.regsub("[^:](Failed | Accepted)(\s)password for (.\*)\s)from\s)(\d+\.\d+\.\d+\.\d+)",\3}}

Problem expression.: find(/Zabbix server/log[/var/log/auth.log,(Failed | Accepted)],,"Failed")=1

Ok event Generation: Recovery expression: find(/Zabbix server/log[/var/log/auth.log,(Failed | Accepted)],,"Accepted")=1

PROBLEM event Generation mode: Multiple

OK event closes: all problems if tag values match

Tag for matching: User

Allow manual close: Checked

### Tags

Name: User  
Value: {{ITEM.VALUE}.regsub("[^03:00]+(\s)+(.\*):(\s)(Started | Stopped)+(\s)+(.\*)[.]",\6)}

Name: From  
Value: {{ITEM.VALUE}.regsub("[^:](Failed | Accepted)(\s)password for (.\*)\s)from\s)(\d+\.\d+\.\d+\.\d+)",\3}}

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

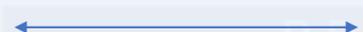
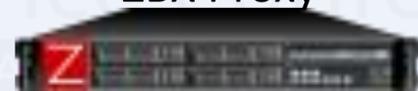
Monitoramento via ODBC  
(ODBC monitoring)

## ODBC Monitoring

ZBX Server Node X



ZBX Proxy



Oracle  
PostgreSQL  
Mysql

Another DB Engines (not for Zabbix)

Chave não segura (precisa acesso ao odbc.ini)

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

Chave segura (versão 5+):

`db.odbc.select[<unique short description>,<dsn>,<connection string>]`

“Connection string” aceita “User macros” com “Secret text”.

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

## Registro Automático de Hosts (Autoregistration)

Encryption level  No encryption

PSK

\* PSK identity

\* PSK

```
Hostname=My Host
Metadata=Linux,PRD,Client A
TLSConnect=psk
TLSPSKIdentity=My Identity
TLSPSKFile=/home/zabbix/agentd.psk # PSK content
```

Audit log

Details

```
host.groups[548]: Added
host.groups[548].groupid: 5
host.groups[548].hostid: 10517
host.groups[549]: Added
host.groups[549].groupid: 2
host.groups[549].hostid: 10517
host.host: My Host
host.hostid: 10517
host.interfaces[13]: Added
host.interfaces[13].dns: zabbix-server
host.interfaces[13].ip: 192.168.100.30
host.interfaces[13].main: 1
host.inventory_mode: -1
host.tls_accept: 2
host.tls_connect: 2
host.tls_psk: *****
host.tls_psk_identity: *****
```

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

## Métodos de Autenticação (Authentication Methods)

User Group B

User Group A

User Group D

## Authentication

Authentication HTTP settings LDAP settings SAML settings

Default authentication

Internal

LDAP

### Password policy

Minimum password length

Password must contain ?  an uppercase and a lowercase Latin letter  
 a digit  
 a special character

Avoid easy-to-guess passwords ?

Update

User Group C

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

## API Tokens

API tokens ▾

- Support
- Integrations
- Help
- User settings**
  - Profile
  - API tokens

**\* Name**

Description

Set expiration date and time

**\* Expires at**

Enabled

API tokens ▾

API token added

Name: My first token

Auth token: a23d5a1a80cc7c056516888bb6c40403b782ffbd49eea7e789cedee7e897fac

Expires at: 2022-12-31 00:00:00

Description: OTRS Integration

Enabled:

Zabbix Super Admin view

API tokens ▾

<input type="checkbox"/>	Name ▲	User	Expires at	Created at	Created by user	Last accessed at	Status
<input type="checkbox"/>	My first token	Joao	2022-12-31 00:00:00	2022-05-29 22:35:46	Joao	Never	Enabled

0 selected



# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

## Papéis de Usuários (User Roles)

## User roles

\* Name

User type

### Access to UI elements

- |            |   |  |   |
|------------|---|--|---|
| Monitoring | <input checked="" type="checkbox"/> Dashboard   | <input checked="" type="checkbox"/> Problems | <input checked="" type="checkbox"/> Hosts |
|            | <input checked="" type="checkbox"/> Latest data | <input checked="" type="checkbox"/> Maps     | <input type="checkbox"/> Discovery        |
| Services   | <input type="checkbox"/> Services               | <input type="checkbox"/> Service actions     | <input type="checkbox"/> SLA              |
|            | <input type="checkbox"/> SLA report             |  |   |
| Inventory  | <input checked="" type="checkbox"/> Overview    | <input checked="" type="checkbox"/> Hosts    |   |
| Reports    | <input type="checkbox"/> System information     | <input type="checkbox"/> Availability report | <input type="checkbox"/> Triggers top 100 |
|            | <input type="checkbox"/> Audit                  | <input type="checkbox"/> Action log          | <input type="checkbox"/> Notifications    |

API methods

### Access to actions

- Create and edit dashboards
- Create and edit maps
- Create and edit maintenance
- Add problem comments
- Change severity
- Acknowledge problems
- Close problems
- Execute scripts
- Manage API tokens
- Manage scheduled reports
- Manage SLA

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

## Permissões (Permissions)



Admins



Admins



Users

RW

RW

RO

RW

RO

RO

Host group A

Host group B

Host group C

Host group D

FULL

FULL

FULL

FULL

FULL



Super Admin

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

## Trilha de Auditoria (Audit Tracking)

# Audit log

< Zoom out > **Last 15 minutes** ⌚ Filter ▾

Users

Resource  ▾

Resource ID

Action  ▾

Recordset ID

Time	User	IP	Resource	ID	Action	Recordset ID	Details
2022-05-29 21:51:30	Admin	192.168.15.110	User	1	Failed login	cl3s0mdjv000008df760i519q	
2022-05-29 21:51:30	Admin	192.168.15.110	User	1	Update	cl3s0mdjv000008df760i519q	Description: Admin user.attempt_failed: 0 => 1
2022-05-29 21:51:29	guest	192.168.15.110	User	2	Failed login	cl3s0mdjv000008df760i519q	
2022-05-29 21:51:26	guest	192.168.15.110	User	2	Failed login	cl3s0majv000008dfvj2c30ht	
2022-05-29 21:51:25	System		Item	42697	Update	cl3s0m9vd010rjdf7wmmozi6	Description: Cluster node []: Last access age <a href="#">Details</a>

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

HTTPProxy

HTTPProxy permite que as verificações Web como [HTTP checks](#) e [Web Scenarios](#), além de [Webhooks](#), possam utilizar um canal seguro de conexão com a Internet ou outros locais, centralizando logs de acesso e garantindo permissões

**HTTP proxy**

```
[protocol://][user[:password]@]proxy.example.com[:port]
```

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

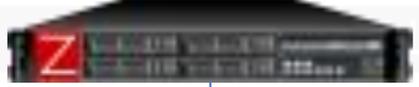
Auxiliando a obrigação de conformidade  
(Compliance)

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

OfflineBuffer  
(Proxy & Zabbix Agent2 (Active))

ZBX Server Node X



ZBX Proxy



ZBX Agent(2)



### Option: ProxyOfflineBuffer  
 # Proxy will keep data for N hours in case if no connectivity with Zabbix Server.  
 ProxyOfflineBuffer=24

EnablePersistentBuffer=1  
 PersistentBufferPeriod=120d  
 PersistentBufferFile=/var/lib/sqlite3/zabbix.db

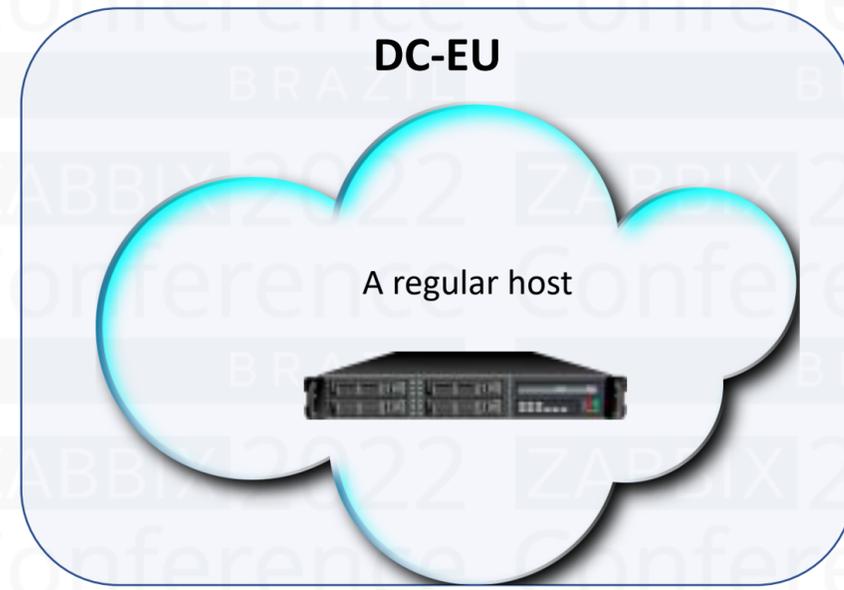
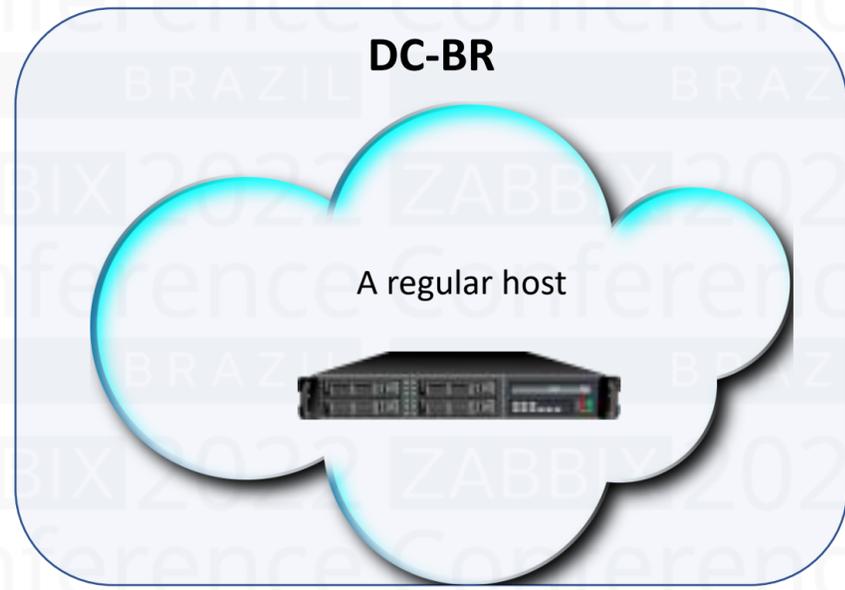
SSH checks, HTTP checks, SNMP checks, IPMI checks, ODBC checks, ...



# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

## Inventário de Host (Host Inventory)



Overview Details

Location latitude -22.966699851210  
Location longitude -43.414106427167

Cancel

Mudança de escopo para extraterritorial

Overview Details

Location latitude 52.3667  
Location longitude 4.89454

Cancel

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

Descoberta de Rede  
-Serviços não seguros-  
(Network Discovery: No secure services)

# Discovery rules

\* Name

Discovery by proxy

\* IP range

\* Update interval

## \* Checks

Type	Actions
FTP	<a href="#">Edit</a> <a href="#">Remove</a>
HTTP (80,8080)	<a href="#">Edit</a> <a href="#">Remove</a>
ICMP ping	<a href="#">Edit</a> <a href="#">Remove</a>
IMAP	<a href="#">Edit</a> <a href="#">Remove</a>
LDAP	<a href="#">Edit</a> <a href="#">Remove</a>
POP	<a href="#">Edit</a> <a href="#">Remove</a>
SMTP	<a href="#">Edit</a> <a href="#">Remove</a>
Telnet	<a href="#">Edit</a> <a href="#">Remove</a>
<a href="#">Add</a>	

Uma busca por serviços sem protocolos de segurança implementados!

## Actions

Action Operations 1

\* Name

## Conditions

Label	Name	Action
A	Discovery rule equals Finding No Secure Services	<a href="#">Remove</a>
<a href="#">Add</a>		

## Actions

Action Operations 1

## Operations

Details	Action
Send message to users: Admin (Zabbix Administrator) via Email	<a href="#">Edit</a> <a href="#">Remove</a>
<a href="#">Add</a>	

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

Serviços de Dados Pessoais  
Prestando contas com Leis de Privacidade  
(Privacy Laws AccountAbility)

## Services

All services / Personal Data Breach - LGPD (GD...

### Personal Data Breach - LGPD (GDPR)

Parent services:

Status: OK

SLA: Personal Data SLA: N/A <sup>?</sup>

Tags: Databreach LGPD PersonalData

Name	Status	Root cause	Created at
<a href="#">DB Services</a>	OK		2022-05-29
<a href="#">Data Subject Rights</a>	OK		2022-05-29
<a href="#">Personal Data App 1</a>	OK		2022-05-29
<a href="#">Personal Data App 2</a>	OK		2022-05-29

Gestão de sistemas com DADOS PESSOAIS!

Visão de Disponibilidade, Integridade e Confidencialidade de DADOS PESSOAIS!

Relatórios para prestação de contas com órgãos reguladores!

Informações gerenciais para tomada de decisões!

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

## Controle de Vulnerabilidades Técnicas (Security Advisories)

# Zabbix Security Advisories and CVE database

[How to report a security issue?](#)

Zabbix ID	CVE number	CVSS score	Zabbix severity <span>?</span>	Synopsis	Component/s	Affected version/s	Published
ZBA-2022-04-1	-	-		Zabbix products are not affected by vulnerabilities in Spring Framework (CVE-2022-22965 - Spring4Shell) and Spring Cloud Function (CVE-2022-22963)	-	-	2022 Apr 04
ZBA-2022-03-1	-	-		Zabbix products are not affected by CVE-2018-25032 vulnerability in zlib 1.2.11	-	-	2022 Mar 28
ZBV-2022-01-2	CVE-2022-24917	3.7	Low	Reflected XSS in service configuration window of Zabbix Frontend	Frontend	4.0.0-4.0.38 5.0.0-5.0.20 5.4.0-5.4.10	2022 Feb 02

## TAG VALUES

Frontend: version 1

<input type="checkbox"/> Host	Name ▲	Last check	Last value	Change	Tags
<input type="checkbox"/> Zabbix server	<u>Vulnerable frontend</u>	59s	6.0.4		Frontend: version

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

## Limitações (Limitations)

- Zabbix Servers e Zabbix Frontend → Sem criptografia
- Zabbix Serveres e Zabbix JavaGateway → Sem criptografia
- PSK → Armazenado em texto puro no DB
- Frontend não possui 2FA ou MFA nativos
- Nem todos os campos no Zabbix aceitam “User macros”
- Nem todas as bibliotecas de criptografia implementam o TLS 1.3
- Frontend não possui criptografia nativa; é necessário usar certificado digital para a comunicação com usuário
- Network Discovery não suporta criptografia
- O arquivo contendo o valor da PSK é guardado em texto puro no FileSystem

# Zabbix 6.0: Security by Design

Como o Zabbix 6.0 colabora com o Compliance de Segurança da Informação

Muito não existia! Muito foi feito! O que vem agora?  
(What is next?)

# ZABBIX 2022 Conference BRAZIL

Obrigado  
(Thank you)