

ZABBIX

Boas práticas de segurança com Zabbix



Leonardo Southier - LinkedIn
Technical Support Engineer



O que é o Zabbix?



ZABBIX

O Zabbix é uma ferramenta de classe empresarial e de código aberto para monitoramento de dispositivos, serviços aplicações etc.



Por que devo me preocupar com segurança?



ZABBIX

A segurança no ambiente de TI pode:

- ⚡ Prevenir o acesso não autorizado à informações confidenciais.
- ⚡ Reduzir interrupções causadas por ataques cibernéticos.
- ⚡ Proteger sistemas críticos contra falhas ou invasões.
- ⚡ Minimizar custos com recuperação e mitigação de incidentes.
- ⚡ Garantir a privacidade e conformidade com legislações (ex.: LGPD, GDPR).

Algumas das principais ameaças cibernéticas



ZABBIX

- Ransomware
- DDoS
- Phishing
- DNS Tunneling
- Spoofing
- Ataques Impulsionados por IA



Como o Zabbix pode ajudar na segurança e prevenção de ataques?



ZABBIX

- ⚡ Monitorar padrões de comportamento
- ⚡ Analisar LOGs
- ⚡ Integração com ferramentas SIEM
- ⚡ Automatizar ações de resposta
- ⚡ Monitorar processos críticos
- ⚡ Monitorar DNS

Item Tags Preprocessing

* Name

Type

* Key

Type of information

* Update interval

Custom intervals

Type	Interval	Period	Action
<input checked="" type="checkbox"/> Flexible <input type="checkbox"/> Scheduling	<input type="text" value="50s"/>	<input type="text" value="1-7,00:00-24:00"/>	<input type="button" value="Remove"/>

[Add](#)

* Timeout Global Override [Timeouts](#)

* History Store up to

Log time format

Description

Enabled



Utilizar o Zabbix para monitorar a segurança do ambiente é ótimo, mas e como vai a segurança do próprio Zabbix?

Garantindo a segurança do Zabbix

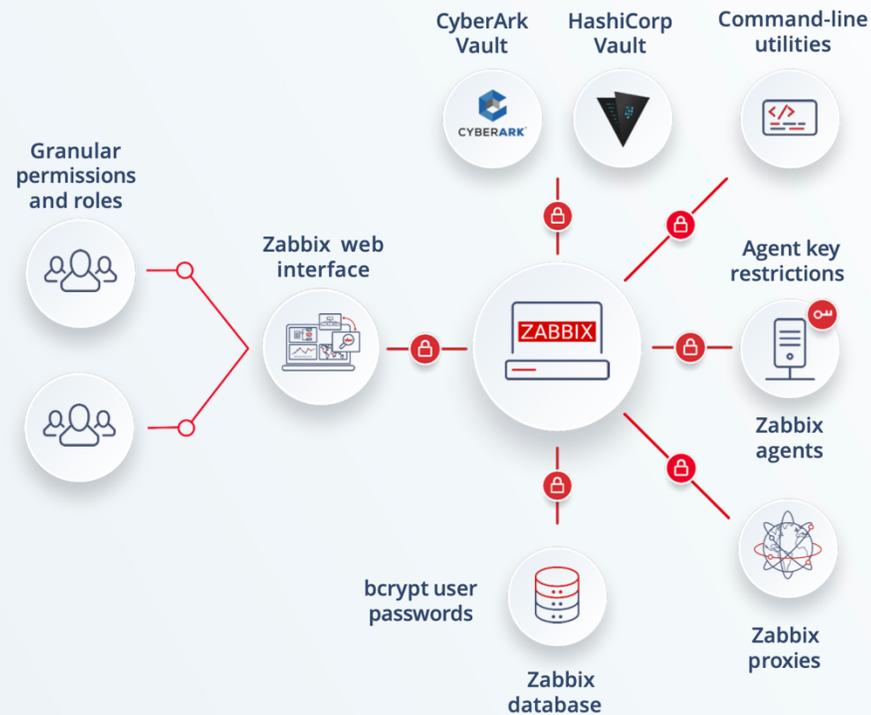


ZABBIX

SECURITY

PROTECT YOUR DATA

- ✓ Strong encryption between all Zabbix components
- ✓ PSK and certificate encryption support
- ✓ TLS v. 1.2 and 1.3 support
- ✓ Option to store all of your sensitive credentials in an external vault
- ✓ Multiple authentication methods:
 - Open LDAP, Active Directory
- ✓ Flexible user permission and role schema
- ✓ Full isolation between user groups and host groups for multi-tenant deployments
- ✓ Zabbix code is open for security audits

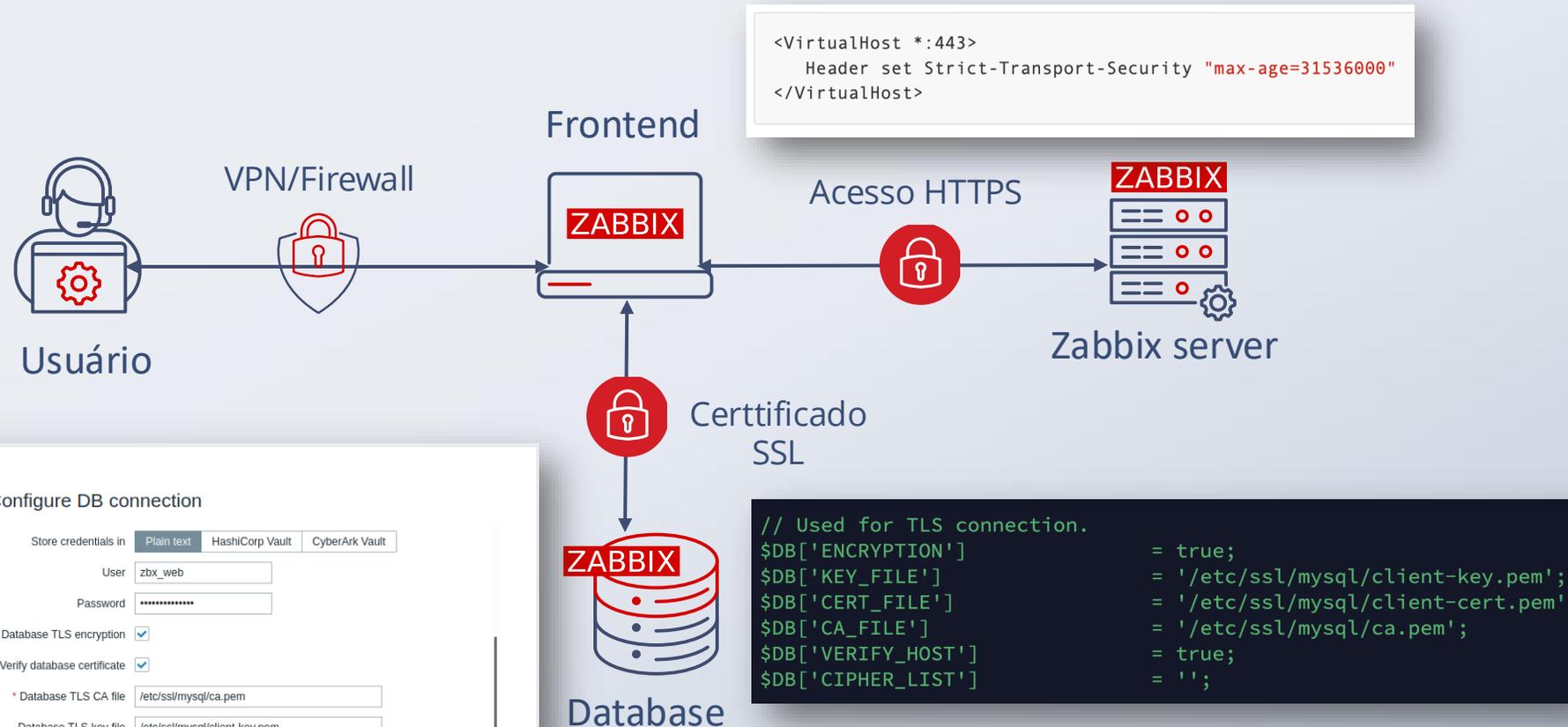


Garantindo a segurança do Zabbix



ZABBIX

Criptografia entre componentes web – server e database



ZABBIX

Welcome
Check of pre-requisites
Configure DB connection
Settings
Pre-installation summary
Install

Store credentials in: Plain text HashiCorp Vault CyberArk Vault

User:

Password:

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:

Garantindo a segurança do Zabbix



ZABBIX

Criptografia entre Server – Proxy - Agente



Proxy

Proxy Encryption Timeouts

Connections to proxy: No encryption PSK Certificate

Connections from proxy: No encryption PSK Certificate

Issuer: CN=Assinando CA,OU=Grupo de desenvolvimento,O=Zabbix SIA,DC=zabbix,DC=

Subject: CN=servidor Zabbix,OU=Grupo de desenvolvimento,O=Zabbix SIA,DC=zabbix,DC=

Update Refresh configuration Clone Delete Cancel

Host

Host IPMI Tags 2 Macros Inventory Encryption Value mapping

Connections to host: No encryption PSK Certificate

Connections from host: No encryption PSK Certificate

* PSK identity: HOST-AGENT

* PSK: Ac4jJwU7QdYzjc6tOgB8agsSVPDopd7d

Availability Agent encryption

ZBX PSK None PSK CERT

Garantindo a segurança do Zabbix



ZABBIX

Autenticação segura LDAP ou SAML

New LDAP server

* Name: LDAP server
* Host: ldap://ldap.example.com
* Port: 389
* Base DN: ou=Users,dc=example,dc=com
* Search attribute: uid
Bind DN: cn=ldap_search,dc=example,dc=com
Bind password: *****
Description:
Configure JIT provisioning:
Group configuration: memberOf groupOfNames
Group name attribute: cn
User group membership attribute: memberOf
User name attribute:
User last name attribute:
* User group mapping

LDAP group pattern	User groups	User role	Action
zabbix-admin	Zabbix administrators	Super admin role	Remove
zabbix-user	Zabbix users	User role	Remove

[Add](#)

Media type mapping

Name	Media type	Attribute	Action
			Add

Advanced configuration

StartTLS:
Search filter: (%{attr}=%{user})

[Add](#) [Test](#) [Cancel](#)

Authentication HTTP settings LDAP settings **SAML settings** MFA settings

Enable SAML authentication:
Enable JIT provisioning:
* IdP entity ID: http://www.example.com/<ID>
* SSO service URL: https://www.example.com/user/app/<ID>/sso/saml
SLO service URL:
* Username attribute: usrEmail
* SP entity ID: zabbix
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:
Configure JIT provisioning:
* Group name attribute: groups
User name attribute: user_name
User last name attribute: user_lastname
* User group mapping

SAML group pattern	User groups	User role	Action
zabbix*	Zabbix administrators	Admin role	Remove

[Add](#)

Media type mapping

Name	Media type	Attribute
		Add

Enable SCIM provisioning:

Utilizando comunicação criptografada

Garantindo a segurança do Zabbix



ZABBIX

Autenticação com MFA (Multi-factor Authentication)

Authentication HTTP settings LDAP settings SAML settings **MFA settings**

Enable multi-factor authentication

* Methods

Name	Type	User groups	Default	Action
Zabbix TOTP	TOTP	5	<input checked="" type="radio"/>	Remove
Zabbix Duo	Duo Universal Prompt	1	<input type="radio"/>	Remove

[Add](#)

New MFA method ✕

Type

* Name ?

Hash function

Code length

ZABBIX

Scan this QR code

Please scan and get your verification code displayed in your authenticator app.



Unable to scan? You can use SHA1 secret key to manually configure your authenticator app:
NVC4MMZGQHPQMOTDOYBA7BO4B2OXHRUY

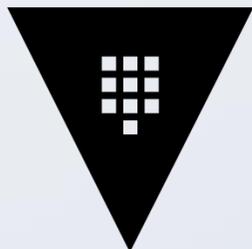
Verification code

Garantindo a segurança do Zabbix



ZABBIX

Armazenamento seguro de credenciais



HashiCorp
Vault



CYBERARK[®]

ZABBIX

Obrigado!

