ZABBIX

Boas práticas de segurança com Zabbix

Leonardo Southier - LinkedIn
Technical Support Engineer

O que é o Zabbix?

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

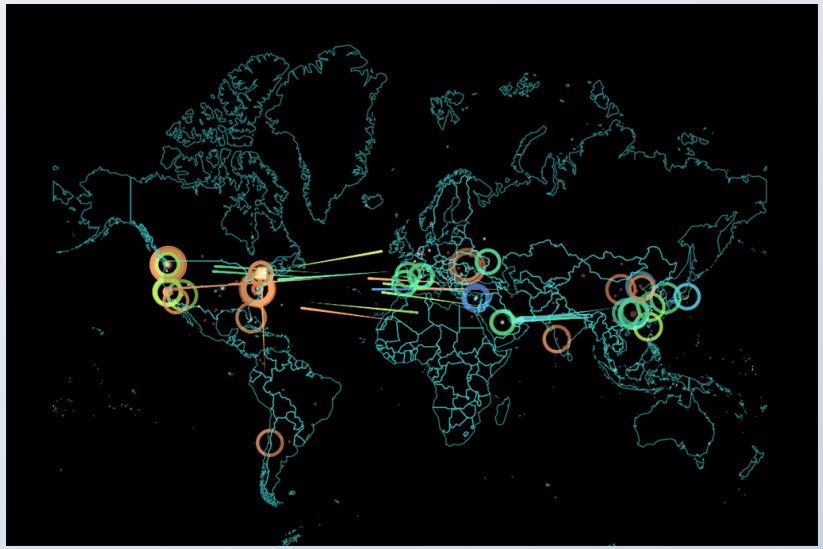
Por que devo me preocupar com segurança?

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).

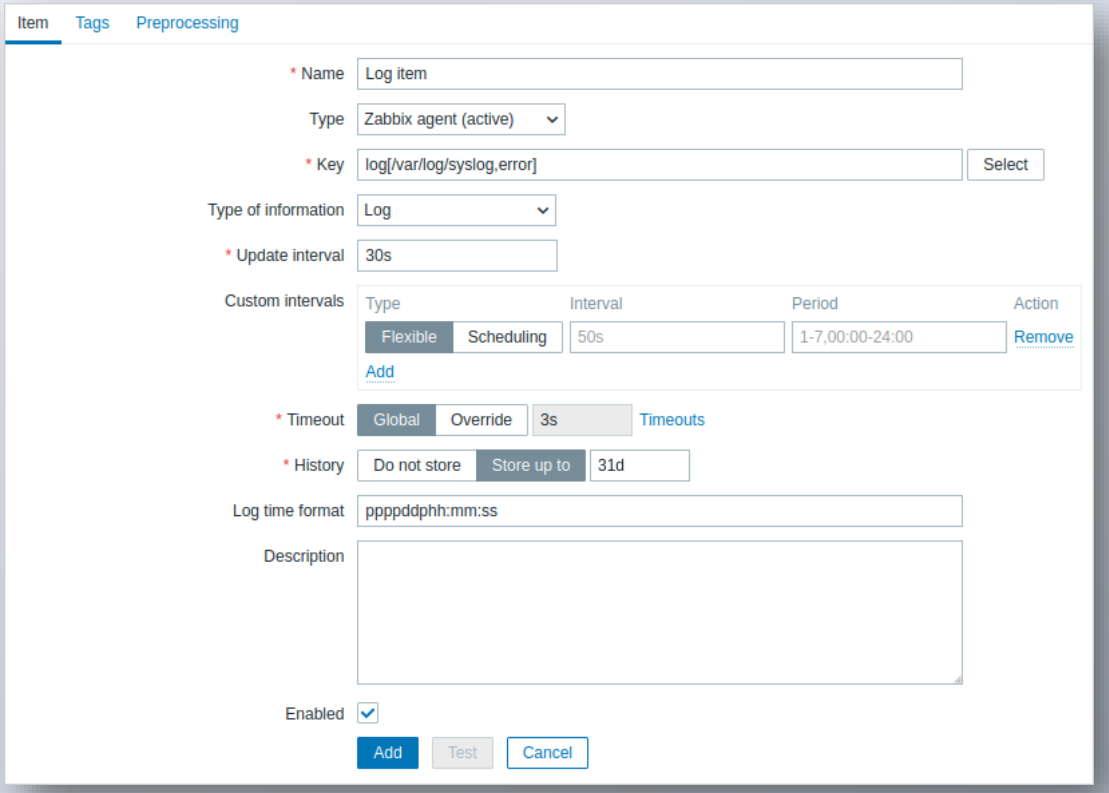
Algumas das principais ameaças cibernéticas

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



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

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



ZABBIX

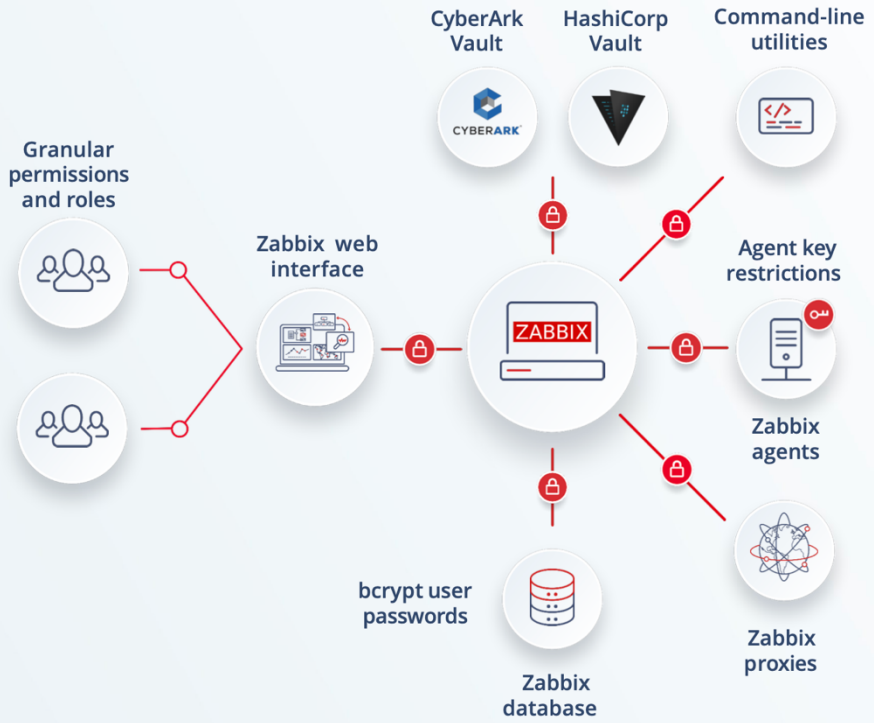
Utilizar o Zabbix para monitorar a segurança do ambiente é ótimo, mas e como vai a segurança do próprio Zabbix?

Garantindo a segurança do Zabbix

SECURITY

PROTECT YOUR DATA

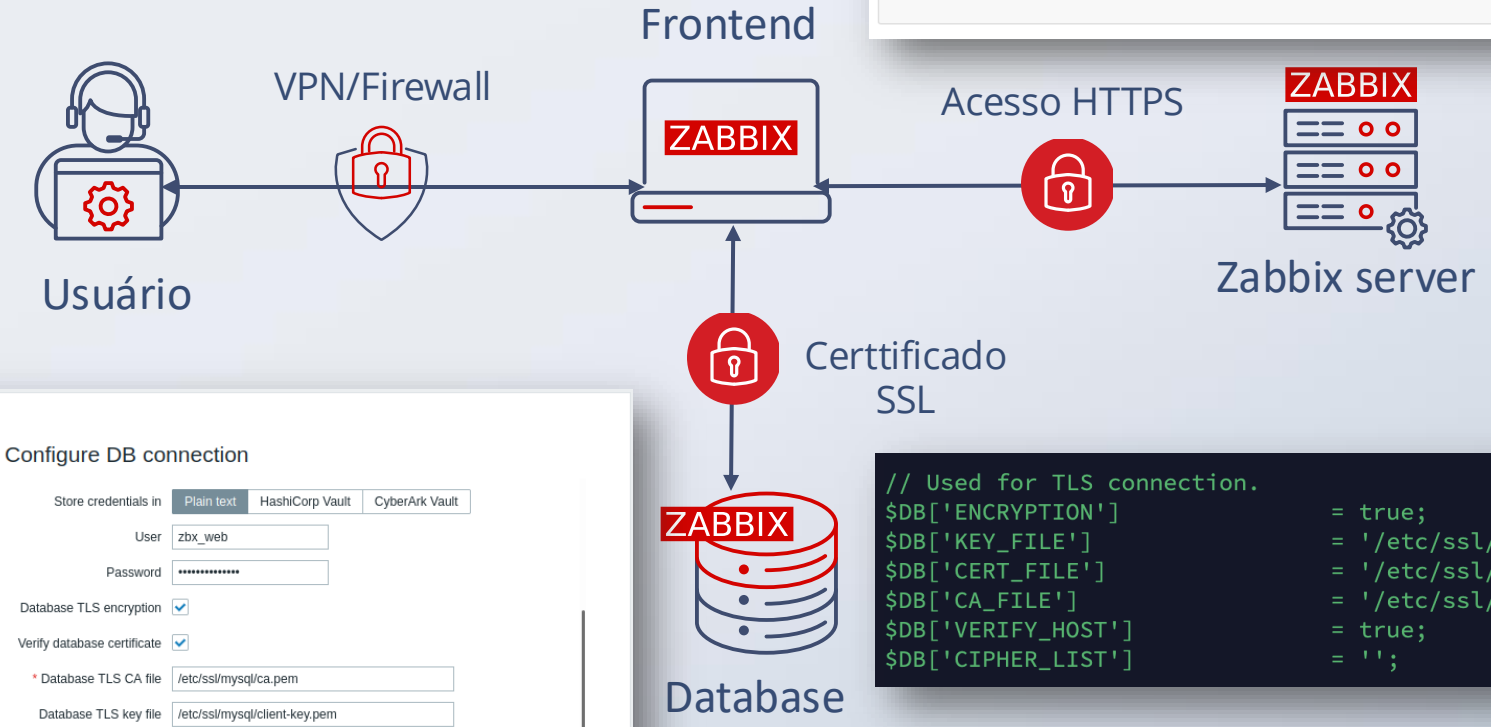
- Strong encryption between all Zabbix components
- PSK and certificate encryption support
- TLS v. 1.2 and 1.3 support
- Option to store all of your sensitive credentials in an external vault
- Multiple authentication methods: Open LDAP, Active Directory
- Flexible user permission and role schema
-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

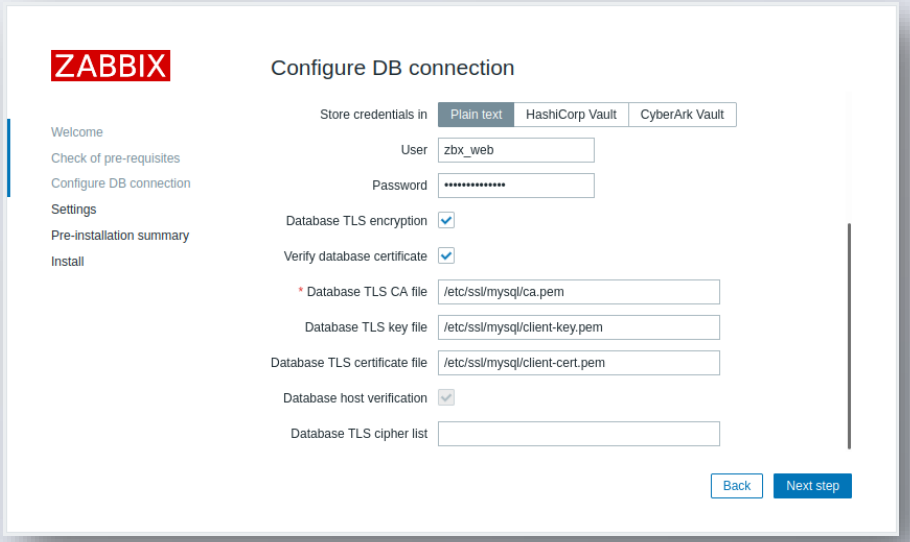


Garantindo a segurança do Zabbix

Criptografia entre componentes web – server e database

```
<VirtualHost *:443>
   Header set Strict-Transport-Security "max-age=31536000"
</VirtualHost>
```

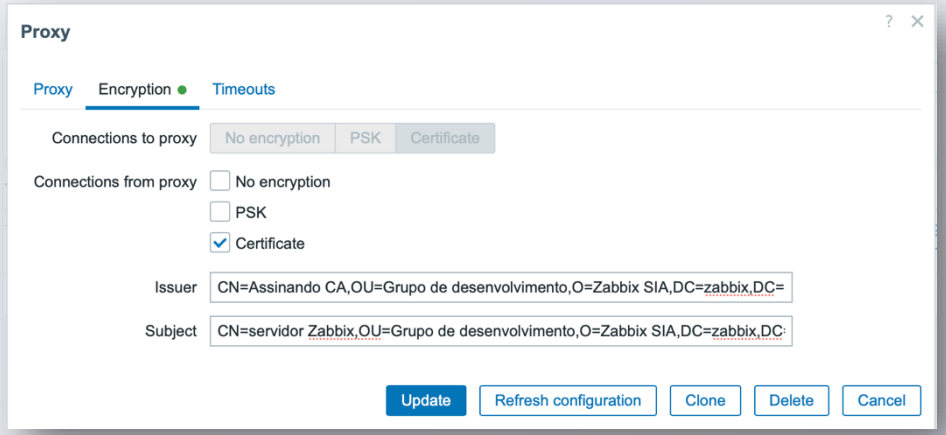


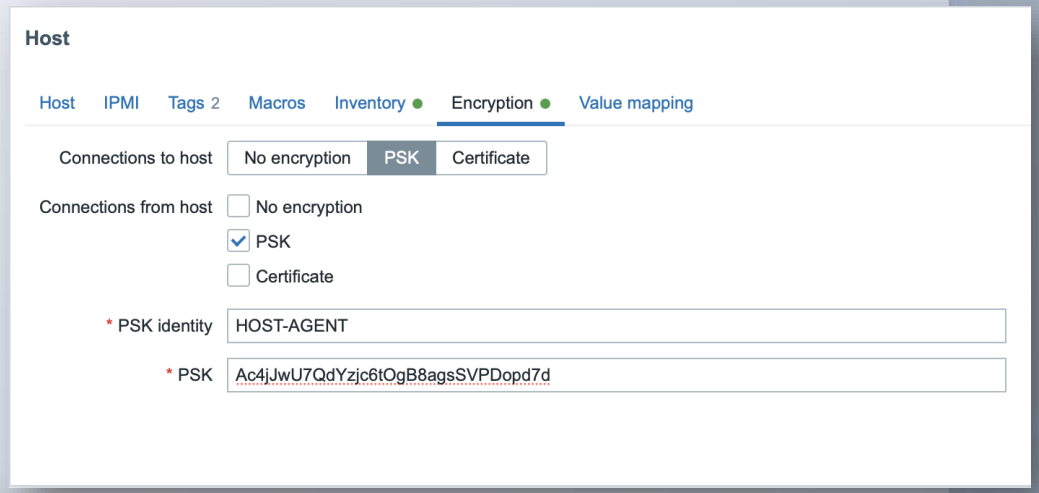


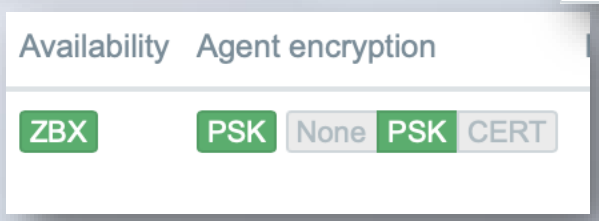

```
// Used for TLS connection.
$DB['ENCRYPTION']               = true;
$DB['KEY_FILE']                 = '/etc/ssl/mysql/client-key.pem';
$DB['CERT_FILE']                = '/etc/ssl/mysql/client-cert.pem';
$DB['CA_FILE']                  = '/etc/ssl/mysql/ca.pem';
$DB['VERIFY_HOST']              = true;
$DB['CIPHER_LIST']              = '';
```

Garantindo a segurança do Zabbix

Criptografia entre Server – Proxy - Agente

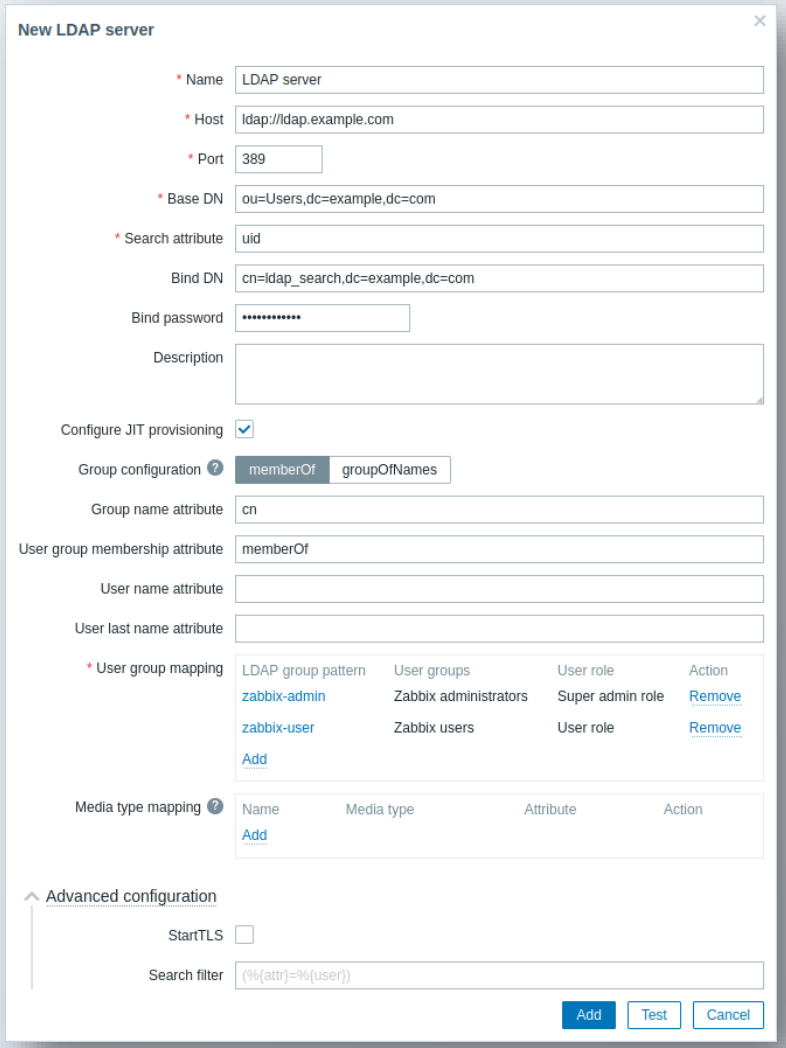


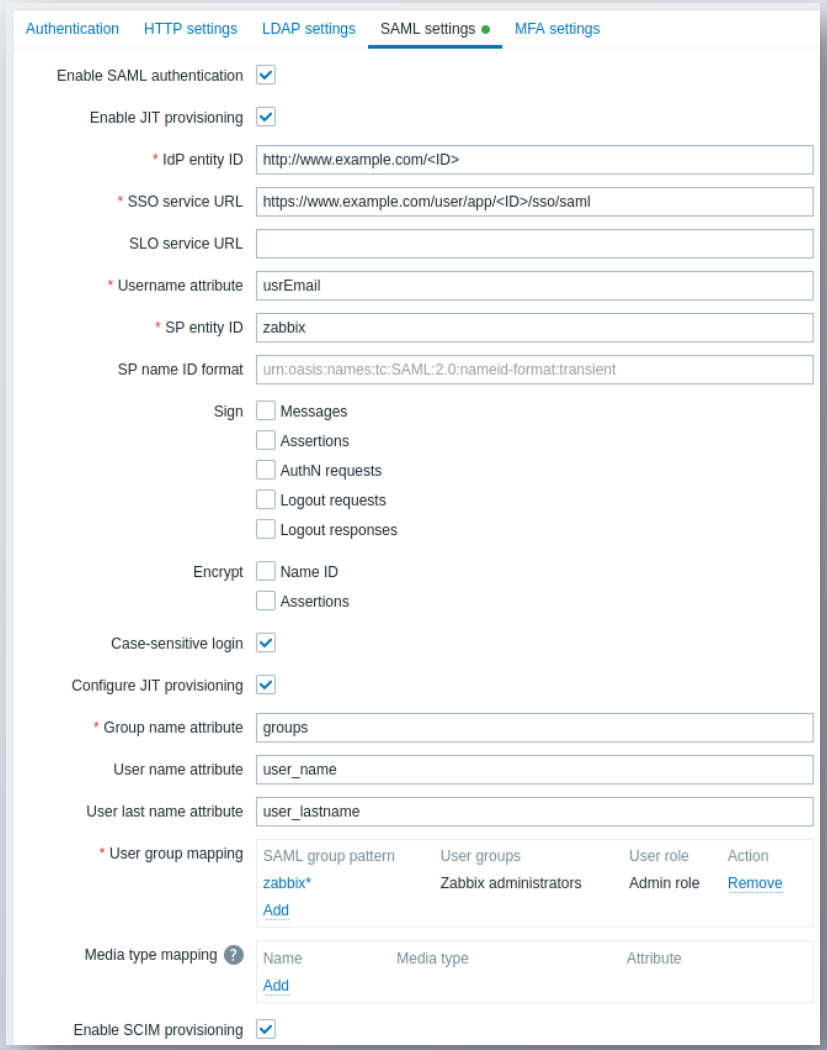




Garantindo a segurança do Zabbix

Autenticação segura LDAP ou SAML

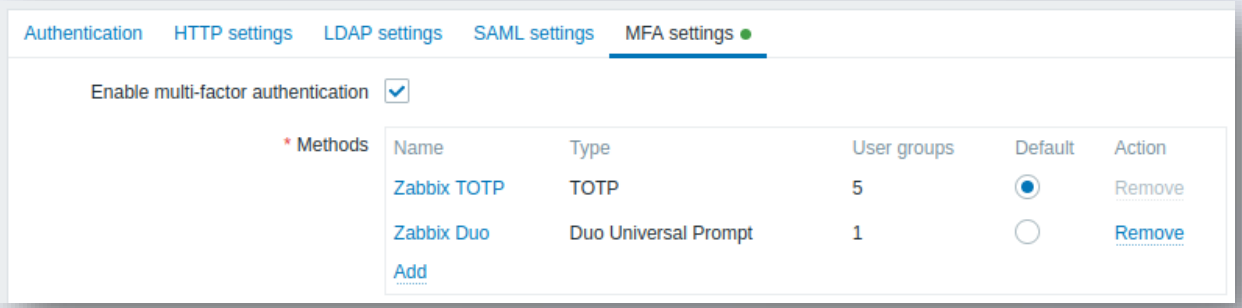


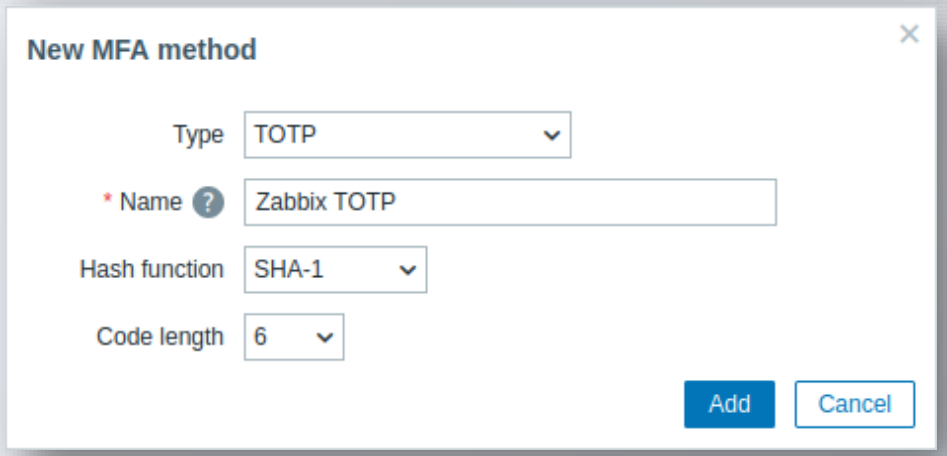


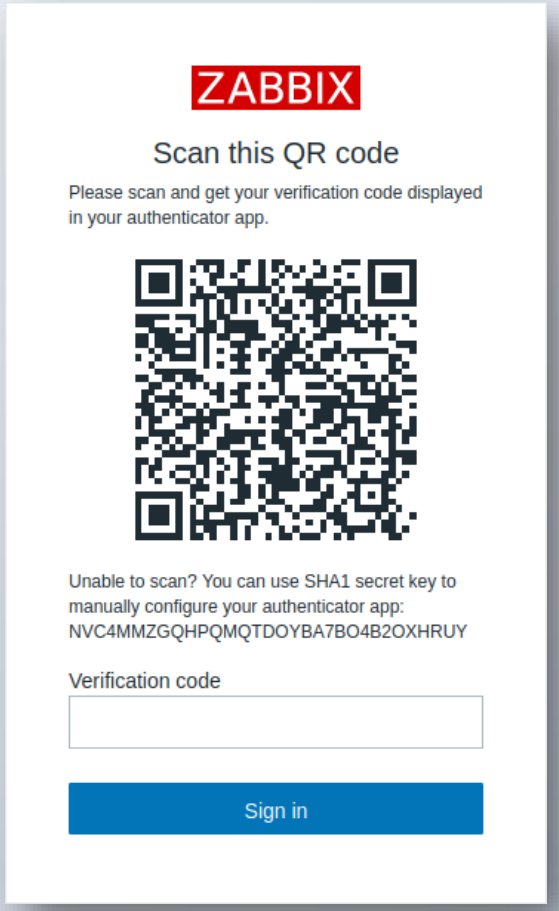
Utilizando comunicação criptografada

Garantindo a segurança do Zabbix

Autenticação com MFA (Multi-factor Authentication)







Garantindo a segurança do Zabbix

Armazenamento seguro de credenciais

HashiCorp Vault

CYBERARK

ZABBIX

Obrigado!