Zabbix a riešenie požiadaviek na bezpečný monitoring

Jún 2023

Stanislav Ťažiar

KONTAKTUJTE NÁS

STANISLAV ŤAŽIAR

CONSULTANT SENIOR

ZABBIX CERTIFIED PROFESSIONAL

Mobil: +421 905 210 301

E-mail: stanislav.taziar@snt.sk

Web: https://www.snt.sk/zabbix.html

Trainings and exams: https://www.snt.sk/zabbix.skolenia.html

Webinars: https://www.snt.sk/zabbix.webinare.html

S&T CEE HOLDING

ZABBIX premium partner

Zabbix premium partner since 2017

The only company in Slovakia

Zabbix a riešenie požiadaviek na bezpečný monitoring

Jún 2023

Stanislav Ťažiar

1 BEZPEČNOSŤ SIEŤOVEJ KOMUNIKÁCIE
Ako zabezpečiť komunikáciu medzi jednotlivými komponentmi Zabbixu

2 UŽÍVATEĽSKÉ ROLY
Ako granulovať prístupové práva užívateľom

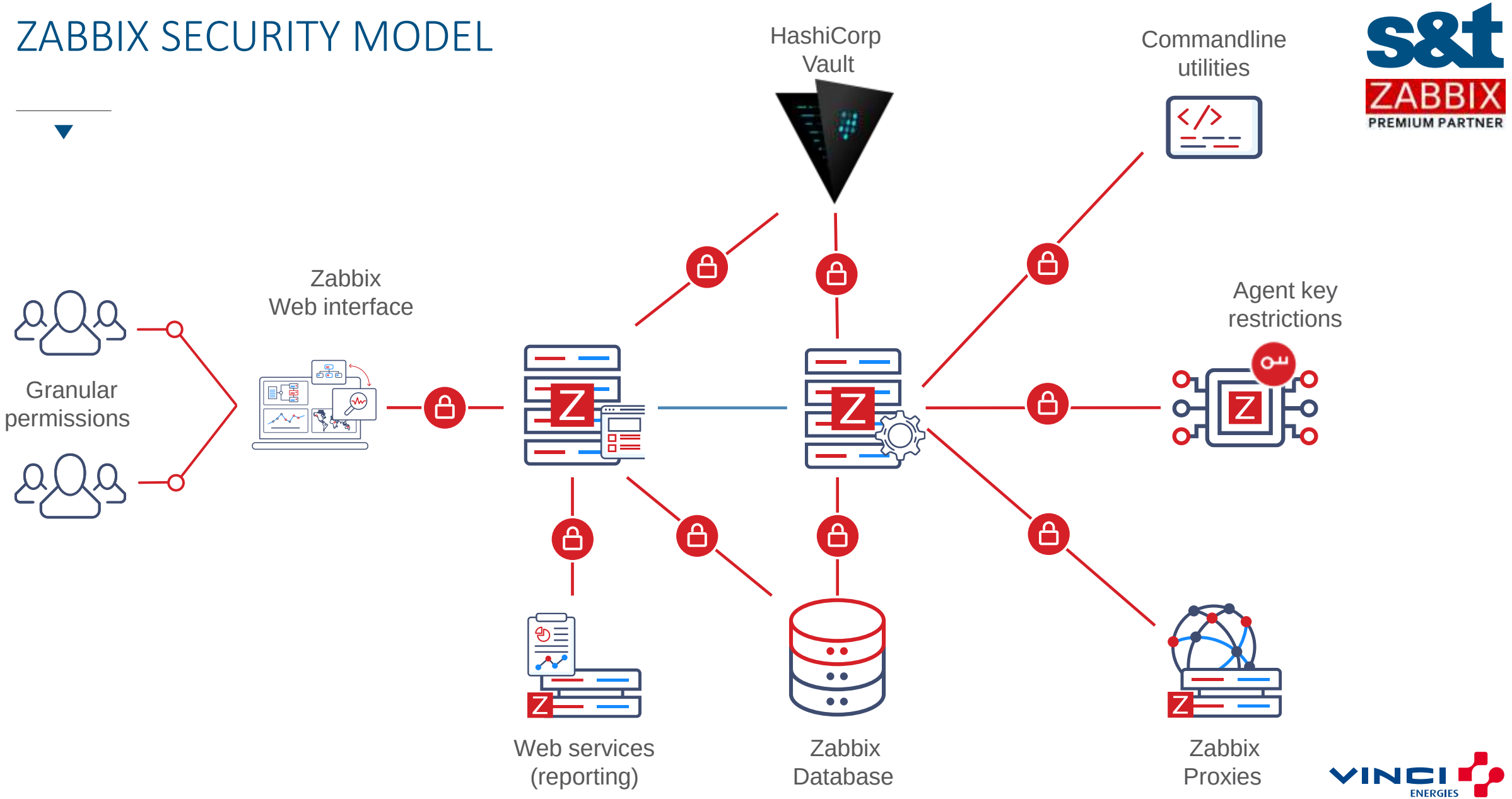
3 OCHRANA CITLIVÝCH ÚDAJOV
External vault a chránené užívateľské makrá

4 REŠTRIKCIE PRE ZABBIX AGENTA
Obmedzenia Zabbix agenta ako ochrana pred zneužitím prístupu

5 ĎALŠIE MOŽNOSTI SPRÁVY BEZPEČNOSTI

1| Bezpečnosť sieťovej komunikácie

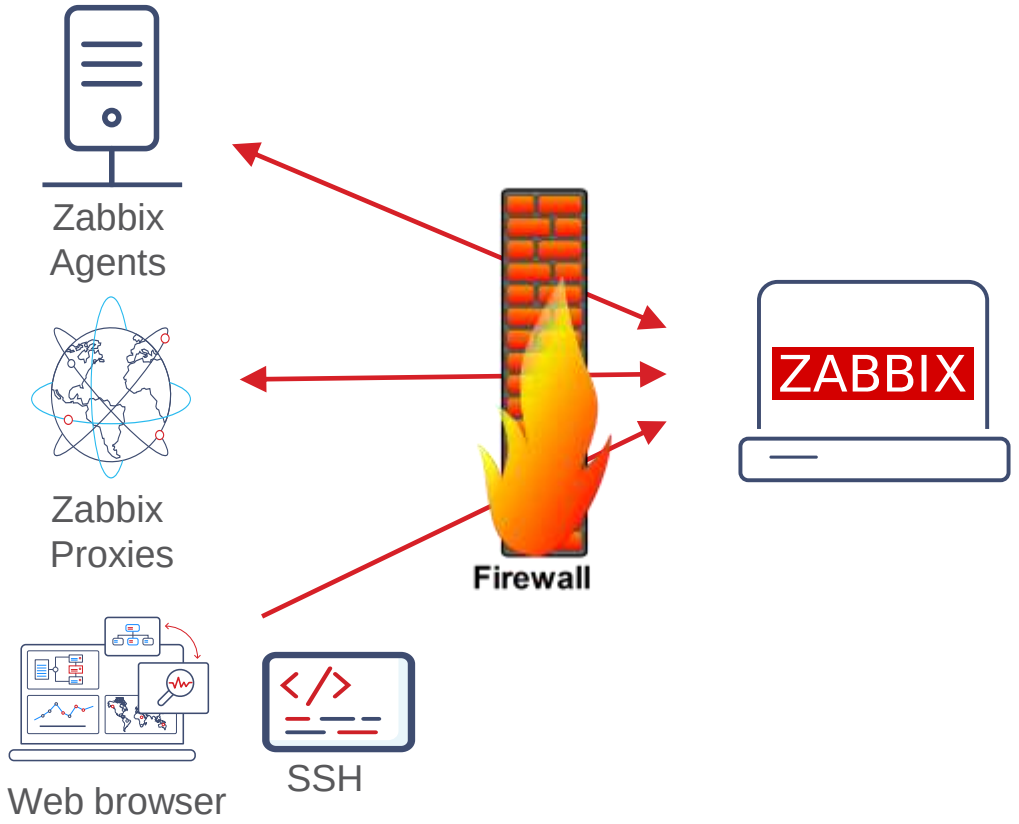
ZABBIX SECURITY MODEL



FIREWALL

Ochrana Zabbix servera proti sieťovým útokom

- Minimálne nastavenia pre príchodziu komunikáciu
  - HTTP (TCP 80) / HTTPS (TCP 443) pre Zabbix frontend
  - TCP 10051 pre Zabbix active agent a active proxy
- SSH potrebné pre prístup ku konzole
  - TCP 22
- Porty k samostatnému DB serveru
  - TCP 3306 pre MySQL DB
  - TCP 5432 pre PostgreSQL DB
  - TCP 1521 pre Oracle DB
- Ostatné porty
  - TCP 8200 pre HashiCorp vault
  - Všetky monitorované služby (SNMP, IPMI, HTTP, SSH, ...)



1.1| Pripojenie na Frontend

FRONTEND
HTTPS

- **HTTPS** (Hypertext Transfer Protocol Secure):
  - SSL (Secure Sockets Layer) je štandard pre bezpečnú komunikáciu
  - TLS (Transport Layer Security) je novšia, bezpečnejšia verzia SSL.

- Konfigurácia na podporovaných frontendoch Apache a Nginx

1.2| Pripojenie na databázu

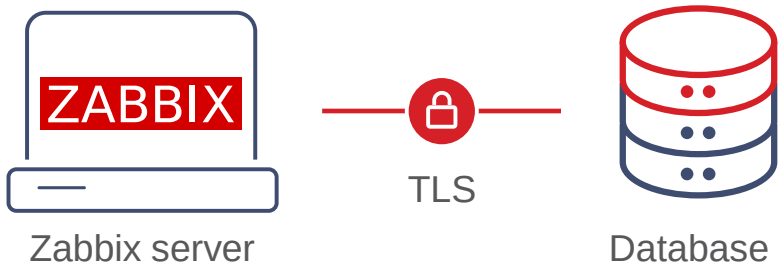
ZABBIX A DATABÁZA

- Komunikáciu medzi Zabbixom a databázou je možné zabezpečiť s využitím **TLS a certifikátov**
- Podporované pre databázy
  - MySQL
  - PostgreSQL
- Nepodporované pre databázu na lokálnom hoste
  - Socket connections can not be encrypted

ZABBIX A DATABÁZA

Zabbix server

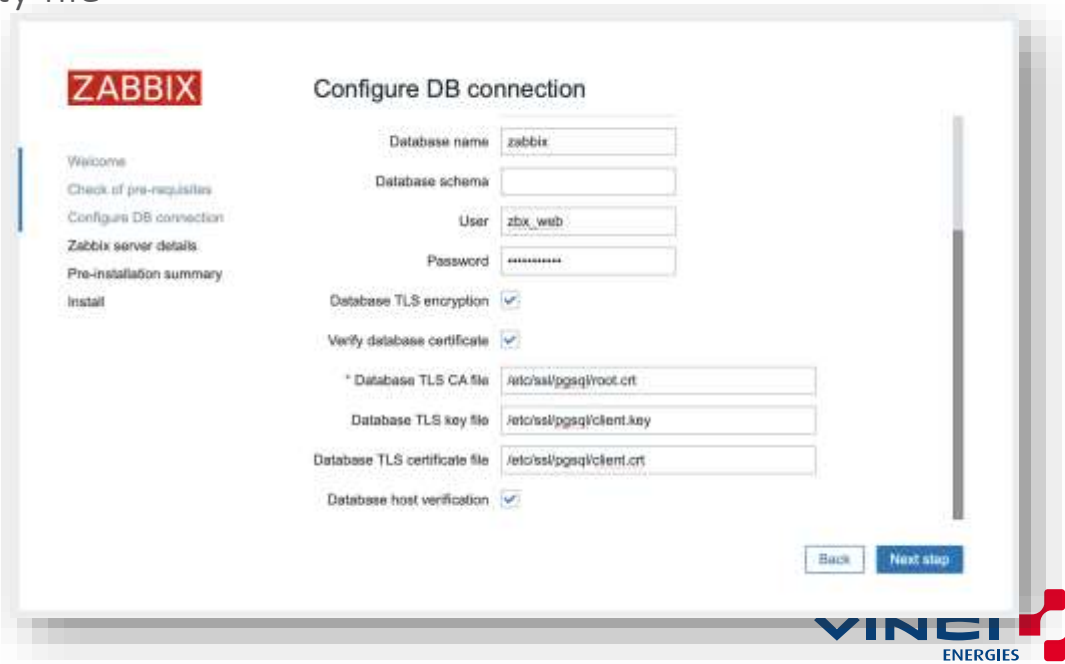
- Zabbix server podporuje viacero režimov – parameter **DBTLSConnect**:
  - **required** – pripojenie cez TLS bez kontroly identity
  - **verify_ca** - pripojenie cez TLS a overenie databázového certifikátu
    - DBTLSCAFile – súbor pre TLS certificate authority
  - **verify_full** – naviac overí, že DBHost je rovnaký ako je uvedený v poli CN v certifikáte databázy
- Je možné použiť aj klientsky certifikát pre Zabbix server
  - DBTLSCertFile – špecifikácia súboru s klientskym certifikátom
  - DBTLSKeyFile - špecifikácia súboru s privátnym kľúčom



ZABBIX A DATABÁZA

Zabbix Frontend

- Konfigurácia Zabbix frontendu má podobné možnosti
  - $DB['ENCRYPTION'] = true;
  - $DB['KEY_FILE'] = specify the client private key file
  - $DB['CERT_FILE'] = specify the client certificate file
  - $DB['CA_FILE'] = specify the TLS certificate authority file
  - $DB['VERIFY_HOST'] = true;
  - $DB['CIPHER_LIST'] = '';
- Na nastavenie je možné použiť aj sprievodcu



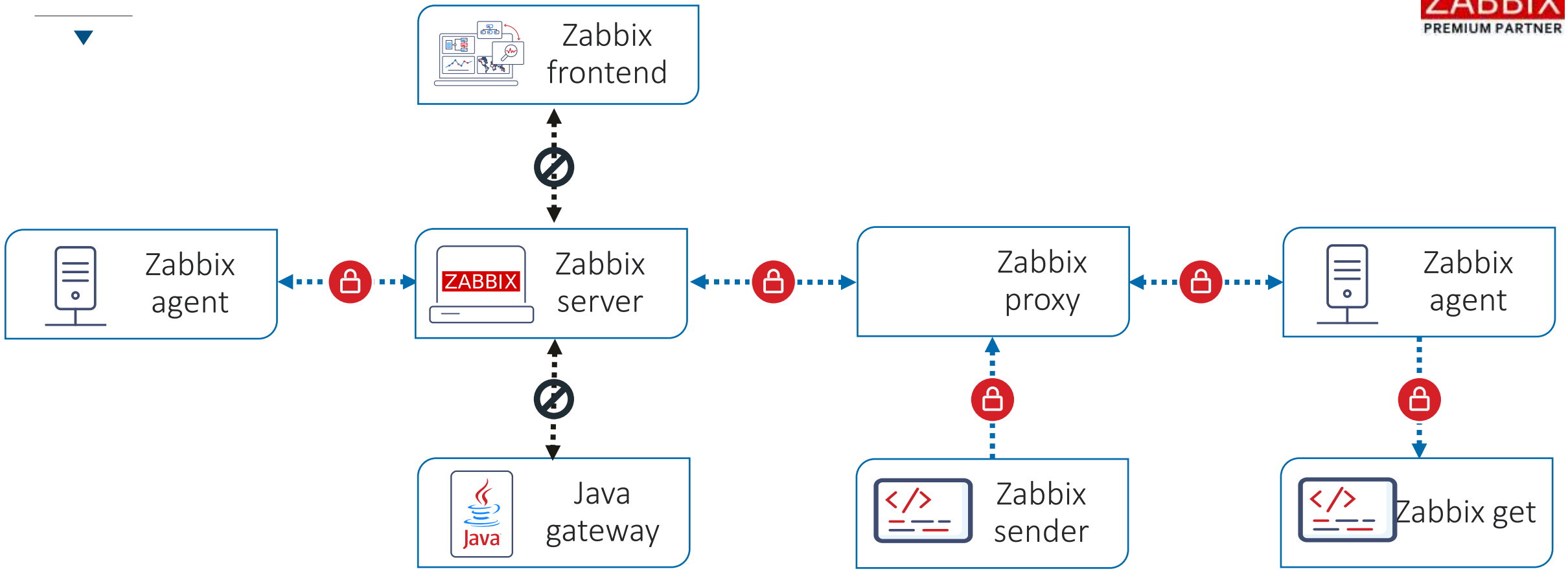
ZABBIX A DATABÁZA

- Použitie SSL má dopad na výkon databázy
  - Nové verzie DB bývajú väčšinou výkonnejšie než staré
  - Veľkosť kľúča x509 certifikátu priamo vplýva na rýchlosť šifrovania
  - TLS 1.3 je rýchlejší ako staršie protokoly
  - Šifry používané na enkrypciu majú dopad na výkon
- MySQL poskytuje nástroj **mysql_secure_installation** pre zvýšenie bezpečnosti
  - Nastavenie hesla pre root účty
  - Minimálna zložitosť hesla
  - Odstránenie root účtov, ktoré sú dostupné zvonku local hosta
  - Odstránenie anonymných účtov
  - Odstránenie test databázy

1.3| Interná komunikácia medzi Zabbix komponentmi

INTERNÁ KOMUNIKÁCIA

Architektúra



Šifrovanie momentálne nie je podporované medzi Zabbix Java gateway alebo frontendom na jednej strane a Zabbix Serverom na druhej

INTERNÁ KOMUNIKÁCIA

Protokoly a knižnice

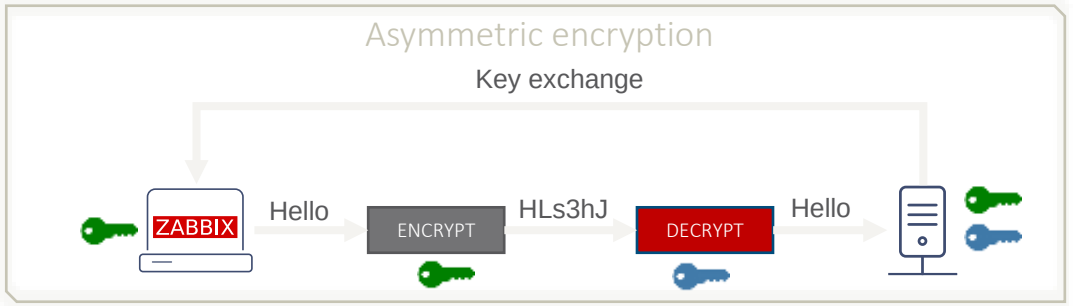
- Zabbix používa Transport Layer Security protocols **TLS 1.2** a **TLS v1.3**

- Zabbix podporuje nasledovné knižnice SSL
  - **OpenSSL** 1.0.1, 1.0.2, 1.1.0 a 1.1.1 (default)
  - LibreSSL od 2.7
    - Podporovaná kompatibilná náhrada OpenSSL
    - Zabbix nebudú môcť používať PSK, iba certifikáty
  - GnuTLS od 3.1.18

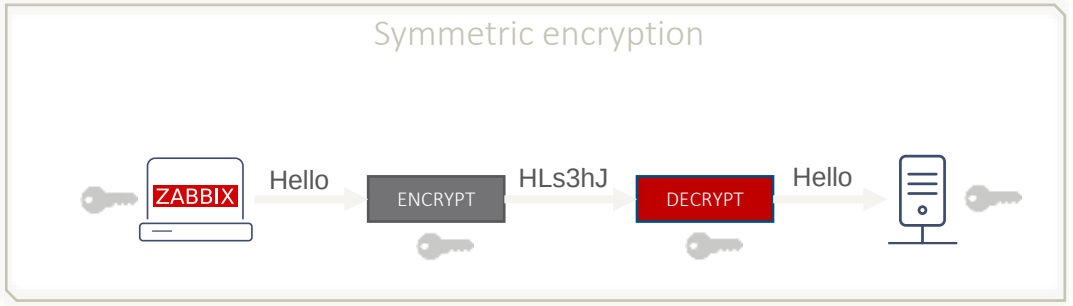
INTERNÁ KOMUNIKÁCIA

Typy šifrovania

- **Certifikáty**
  - Pre výmenu kľúčov sa použije asymetrické šifrovanie
  - Po výmene kľúčov sa už používa symetrické šifrovanie
  - Poskytuje overenie identity
  - Je možné obmedziť uvedením Issuer a Subject
  - Je možné použiť Certificate revocation lists (CRL)



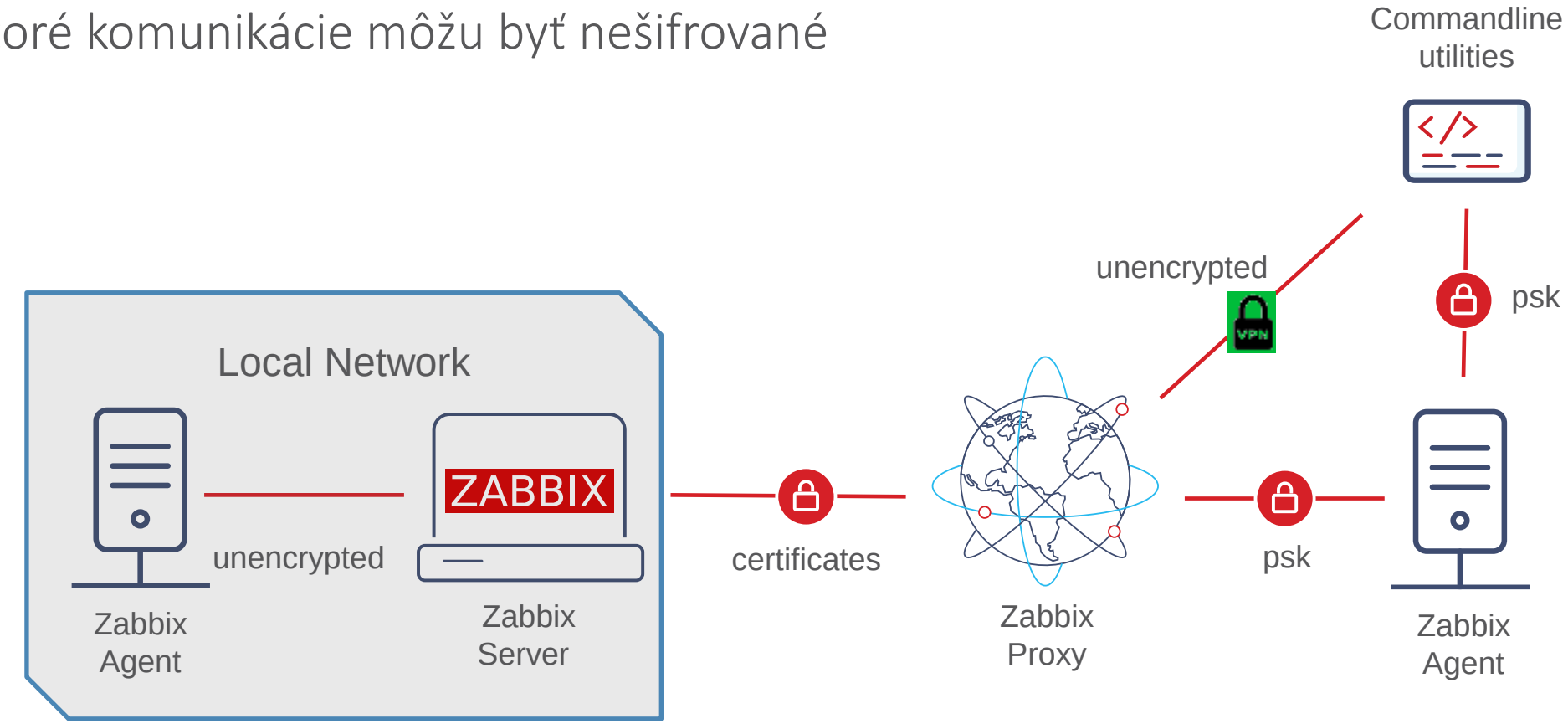
- **Pre-shared keys (PSK)**
  - Iba symetrické šifrovanie
  - Neposkytuje bezpečné overenie identity
  - Výmena kľúčov manuálna (vopred nasadené)
  - Ľahšie na nakonfigurovanie



INTERNÁ KOMUNIKÁCIA

Typy šifrovania

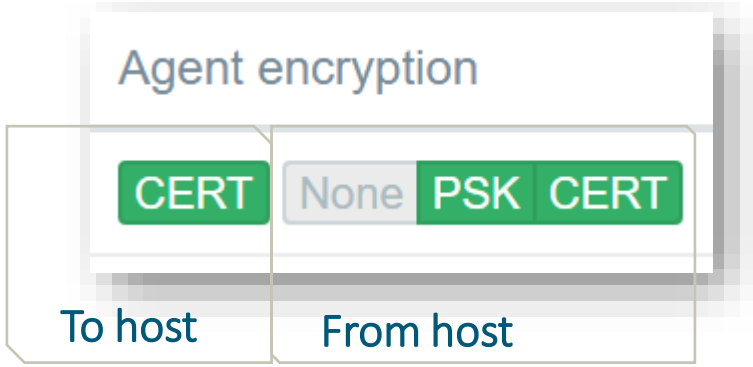
- Je možné skombinovať rôzne nástroje alebo typy komunikácie pre rôzne komponenty
- Niektoré komunikácie môžu byť nešifrované



INTERNÁ KOMUNIKÁCIA

Typy šifrovania

- Typ komunikácie je zvýraznený vo frontende



- Zabbix agent a proxy používajú konfiguračné parametre
  - TLSConnect
  - TLSAccept

- Komunikácia môže byť nakonfigurovaná
  - **Pre-shared key (PSK)**

  - **Certificate**

  - **Mixed** (iba pre príchodzie pripojenia)

INTERNÁ KOMUNIKÁCIA

Certifikáty

- Certifikáty musia byť nasadené na oboch stranách spojenia

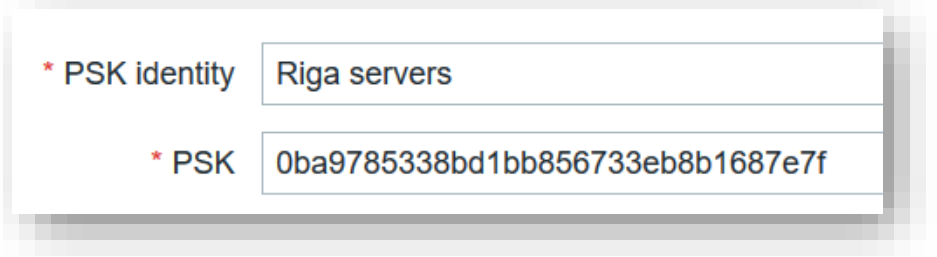
- Musia byť špecifikované aspoň tri parametre:
  - **TLSCAFile** CA certificate
  - **TLSCertFile** Server / Proxy / Agent certificate
  - **TLSKeyFile** Server / Proxy / Agent certificate private key

- Naviac môžu byť skontrolované polia certificate Issuer a Subject
  - TLSServerCertIssuer Certificate issuer
  - TLSServerCertSubject Certificate subject

INTERNÁ KOMUNIKÁCIA

PSK

- Každý PSK (pre-shared key) v Zabbixe je tvorený párom:
  - **PSK identity** - neutajený identifikačný reťazec, prenáša sa nezašifrovaný
  - **PSK value -** tajný reťazec použitý ako šifrovací kľúč
- Každá PSK identity musí byť spárovaná iba s jednou hodnotou PSK
- Obe strany musia mať rovnakú PSK identity a PSK value, aby spojenie mohlo pokračovať
- PSK identity a value sú zadané
  - Vo frontende Zabbix servera
  - V konfiguračnom súbore Zabbix agenta alebo proxy




```
TLSPSKIdentity=Riga servers
TLSPSKFile=/etc/zabbix/agent.psk
```

INTERNÁ KOMUNIKÁCIA

Upozornenia

- Každé TLS spojenie sa otvára s plným TLS handshake
  - Nepoužíva sa session caching ani tikety
  - Šifrovanie predlžuje čas kontroly itemov (v závislosti od sieť.oneskorenia)

- Súbory s privátnym kľúčom sú čitateľný text
  - Chrániť cez prístupové práva FS
  - Zabbix komponenty musia mať prístup

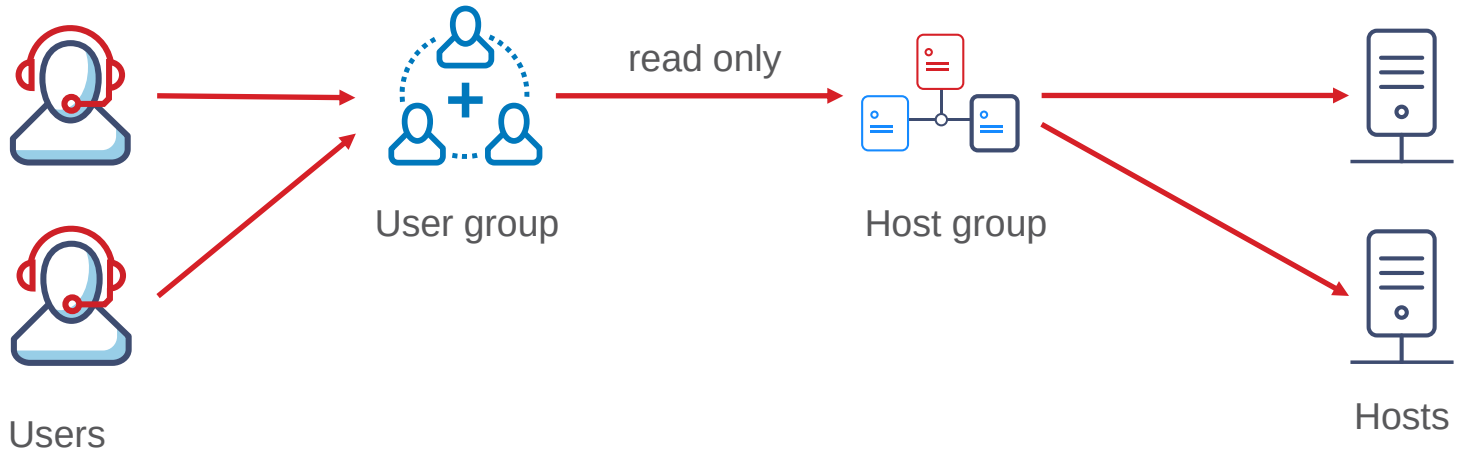
- PSK sú zadávané v Zabbix frontende
  - Nie sú viditeľné pre žiadneho užívateľa
  - V Zabbix databáze uložené ako nezašifrovaný text

- PSK môžu použiť aktívni agenti pri **autoregistrácii**
  - Všetci takíto agenti musia mať rovnaký pár

2| Užívateľské roly

PRIDEĽOVANIE PRÁV

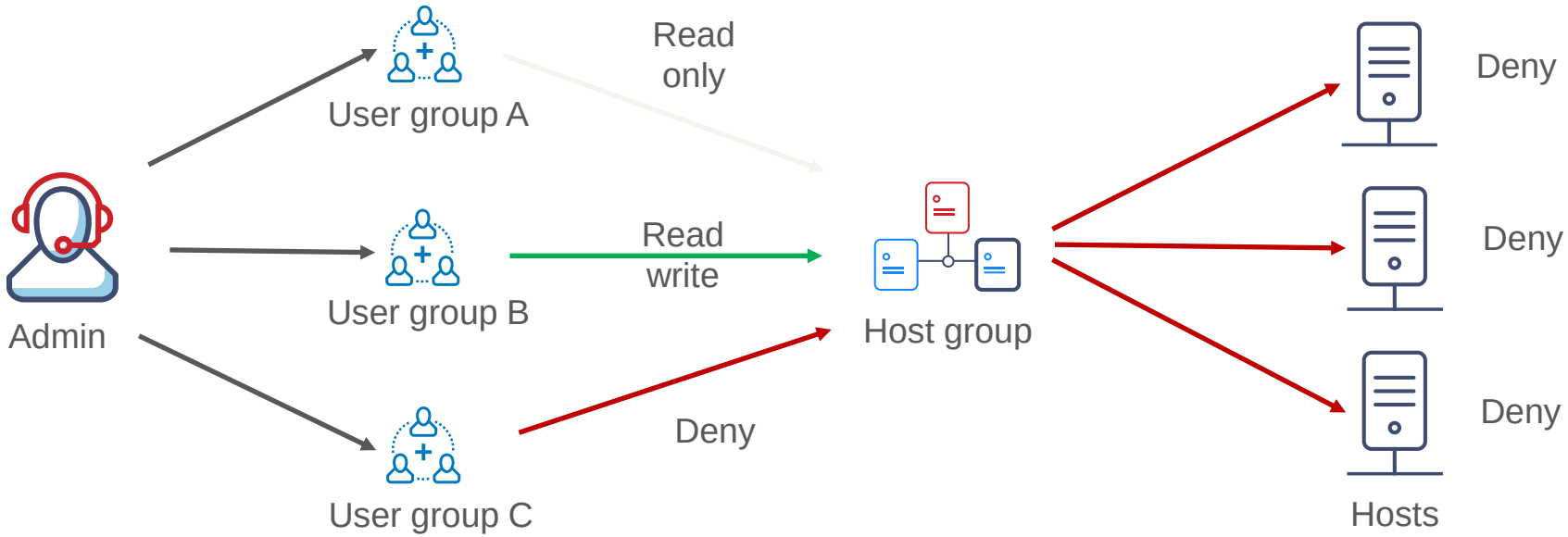
› V Zabbixe sa prístupové práva prideľujú na základe **user groups a host groups**



› Použijeme aj keď chceme jednému užívateľovi dať prístup k jednému hostovi

PRIDEĽOVANIE PRÁV

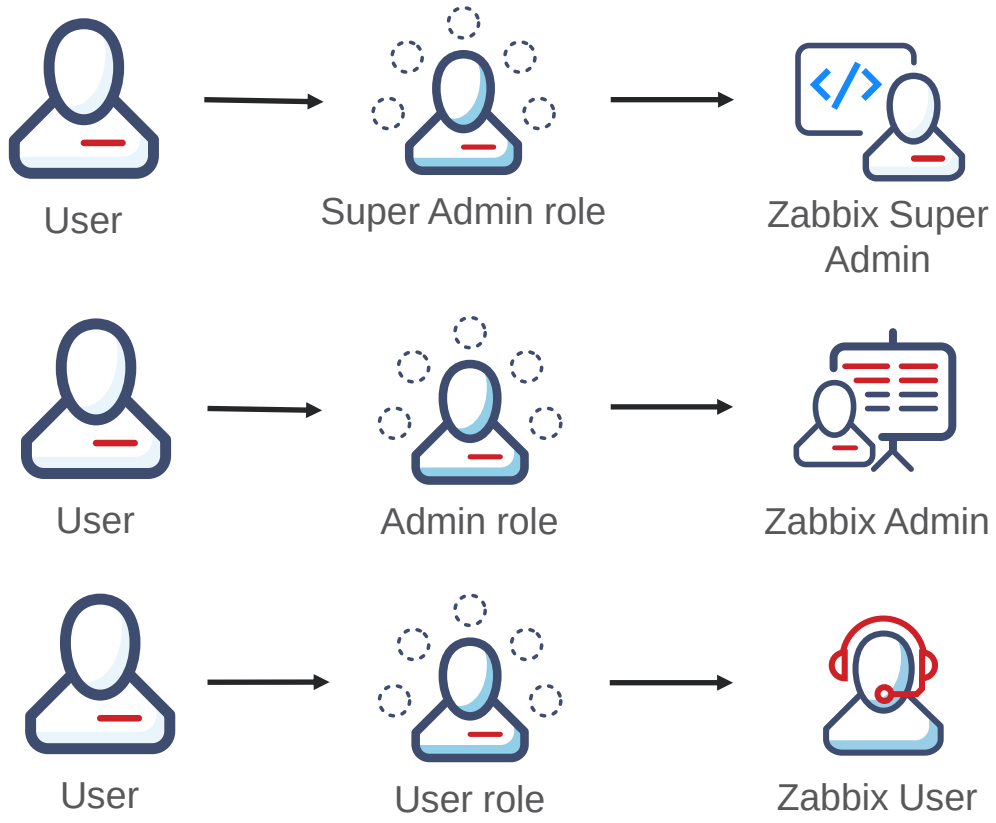
- **Host** môže patriť do viacerých host groups
- **Užívateľ** môže patriť do viacerých user groups
- Platí priorita práv: **Deny > Read Write > Read only**



PRIDEĽOVANIE PRÁV

User roles

- Zabbix 6.0 priniesol **užívateľské roly**:
  - **Super admin, Admin, User a Guest** roly sú preddefinované
  - Super admin rola sa nedá modifikovať
- Je možné vytvárať nové roly s prístupom obmedzeným iba na vybrané časti prostredia
  - Napr. Super admin iba pre správu proxín



PRIDEĽOVANIE PRÁV

User roles

Nastavuje sa prístup roly pre položky v rôznych častiach:

- **Acces to UI elements**
- **Acces to services**
  - Read vs. Read-write
  - None, All, Service list
- **Access to modules**
- **Access to API can be limited**
  - Môže byť zakázaný úplne, zakázaný pre vybrané metódy alebo povolený pre vybrané metódy
- **Access to actions**
  - Možné zakázať napr. vytváranie dashboardov, zatváranie problémov atď.

PRIDEĽOVANIE PRÁV

Poznámky

- Každý užívateľ má pridelenú iba jednu rolu

- Super admin môže vykonávať operácie rýchlejšie ako Admin alebo User
  - Nekontrolujú sa tabuľky súvisiace s právami
  - Pamätať na to pri API skriptoch

- Super admin user type may perform faster then User or Admin types
  - Tables related to permissions are not checked
  - This may be beneficial in API scripts (API methods can be limited using user roles)

- Super admin s právami na role administration môže modifikovať vlastnú rolu!

3| Ochrana citlivých údajov

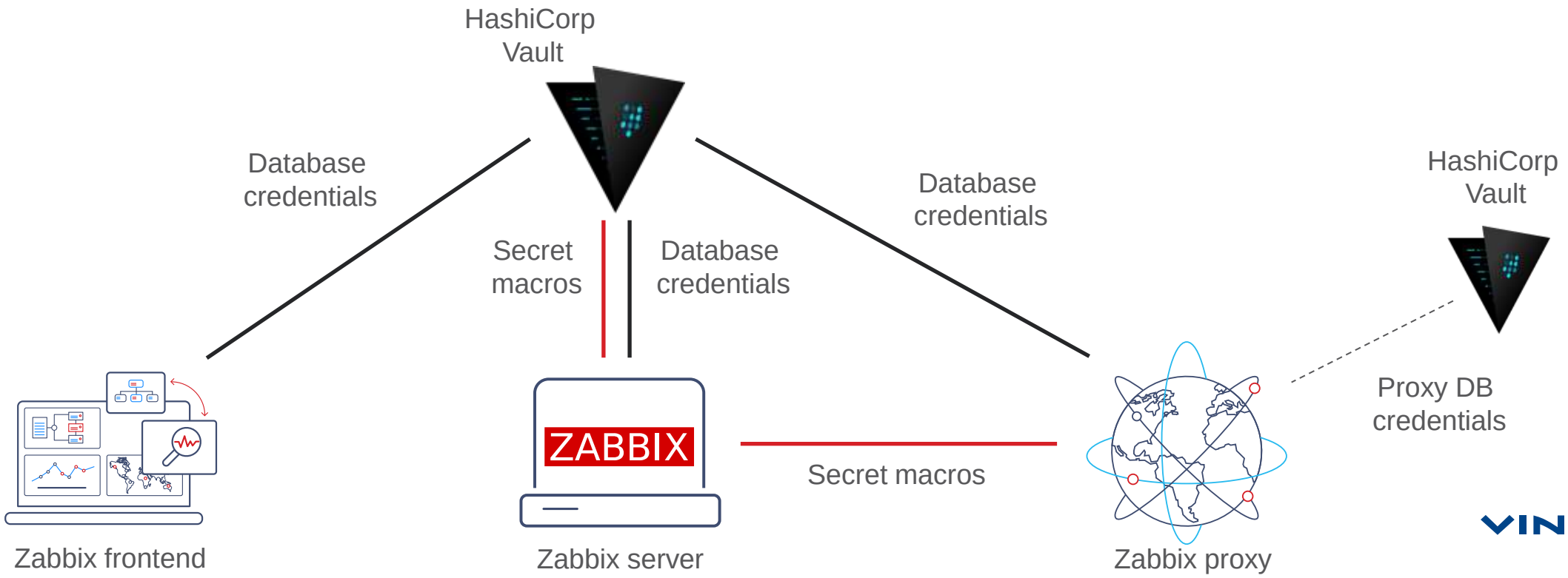
EXTERNAL VAULT

- Zabbix používa **HashiCorp Vault (**od verzie 6.2 aj **CyberArk Vault)** na ukladanie citlivých údajov ako
  - Oprávnenia na **prístup k databáze** pre Zabbix server, frontend a proxy
  - Hodnoty **užívateľských makier**
- Môže byť nainštalovaný na tom istom alebo inom serveri
- Pripojenie musí byť zabezpečené TLS

EXTERNAL VAULT

HashiCorp Vault

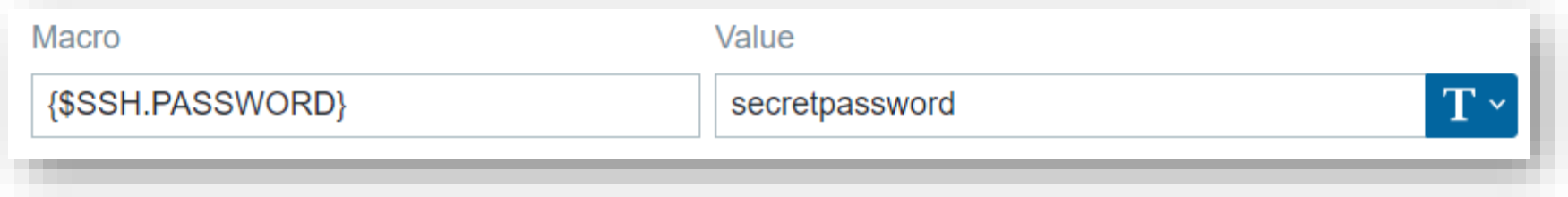
- Iba Zabbix server potrebuje pristupovať k tajným hodnotám makier
- V prípade potreby odošle server hodnoty na proxy cez internú komunikáciu
- Každá proxy môže mať vlastný trezor pre uloženie prístupu k DB



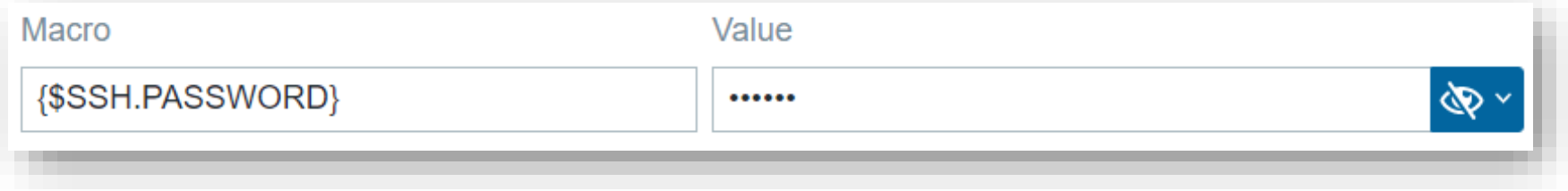
CHRÁNENÉ UŽÍVATEĽSKÉ MAKRÁ

Typy užívateľských makier

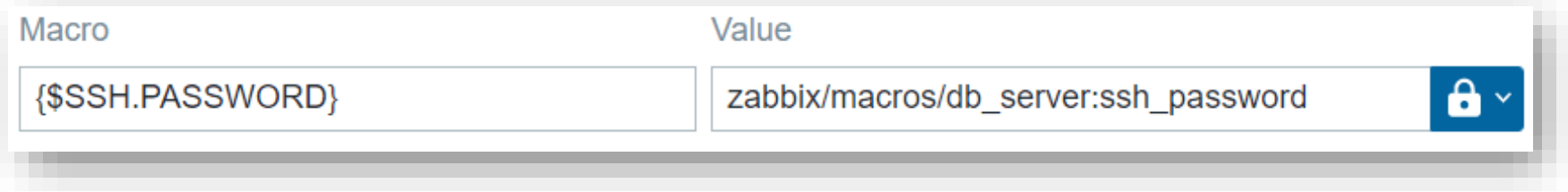
- Od verzie 5.2 má Zabbix 3 typy uloženia užívateľských makier
  - Text



  - Secret text



  - Vault secrets



CHRÁNENÉ UŽÍVATEĽSKÉ MAKRÁ

Správanie

- Hodnoty makier **Secret text** sú zobrazené hviezdičkami (******)
  - Sú nedostupné cez frontendové API volania
  - Formulár pre testovanie itemov nemá k nim prístup
  - Klonovanie hostov nenaklonuje ich hodnotu

- V makrách **Vault secret** sa používa ako hodnota cesta do trezoru
  - Frontend nemá prístup k hodnote
  - Formulár pre testovanie itemov nemá k nim prístup
  - Klonovanie hostov naklonuje názov a cestu

CHRÁNENÉ UŽÍVATEĽSKÉ MAKRÁ

Vlastnosti

- Potenciálne slabé stránky Secret text makier
  - Makrá sú uložené v DB ako text
  - Chrániť username a heslo k DB
  - Chrániť zálohy DB
  - Chrániť komunikáciu medzi Zabbix serverom / frontendom a databázou
  - Chrániť privátny kľúč DB ak používame TLS

- Potenciálne slabé stránky Vault secret makier
  - Chrániť trezorový token Zabbix servera
  - Nepoužívať rovnaký token pre Zabbix server a frontend
  - Chrániť privátny kľúč trezorového SSL certifikátu

4| Reštrikcie pre Zabbix agenta

ZABBIX AGENT

Bezpečnostné riziká

- Zabbix môže zbierať citlivé údaje z
  - Konfiguračných súborov
  - Log súborov
  - Súborov s heslami

- Zabbix agent môže na hostoch vykonávať príkazy
  - Na Linuxe beží Zabbix pod obmedzeným účtom
  - Na Windows beží Zabbix agent (default) ako Local System!

ALLOW / DENY KEY

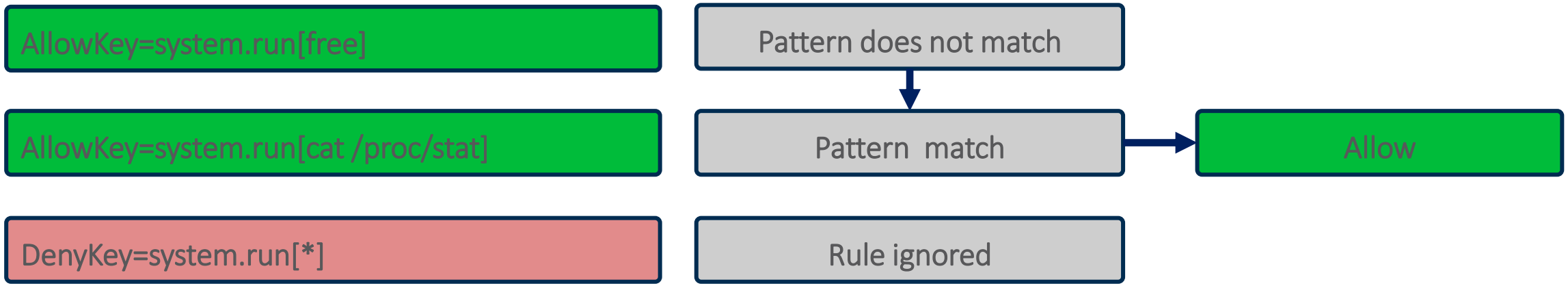
- Zabbix 5.0 zaviedol konfiguračné parametre **AllowKey/DenyKey**
  - Pre odmietnutý kľúč je item hlásený ako unsupported
- Je možné špecifikovať neobmedzený počet AllowKey/DenyKey
- Platia nesledovné východzie pravidlá
  - **system.run[*]** je zakázaný (ak nie je povolený pravidlom)
  - Ostatné kľúče sú povolené pre spätnú kompatibilitu
- Je možné používať wildcard (*) pri názve kľúča aj parametroch
  - system.cpu.* will not match system.cpu.load[] item key
  - system.cpu.*[*] will not match system.cpu.load item key

ALLOW / DENY KEY

Poradie pravidiel

- Pravidlá sa vyhodnocujú v poradí, ako sú zadané
  - Prvé pravidlo, pre ktoré sedí item key, platí
  - Ostatné sa nevyhodnocujú

- Napr pre `system.run[cat /proc/stat]`:



5| Ďalšie možnosti správy bezpečnosti

EXTERNÁ AUTENTIFIKÁCIA A SELINUX

- **Externá autentifikácia** pre správu užívateľov
  - Zabbix podporuje nasledovných poskytovateľov
    - LDAP
    - SAML
    - HTTP

- SELinux
  - Zabbix poskytuje balíček zabbix-selinux-policy s potrebnými politikami pre Zabbix
  - Po inštalácii môžu byť Zabbix binárky spustené s default nastaveniami


Otázky
???

KONTAKTUJTE NÁS

STANISLAV ŤAŽIAR

CONSULTANT SENIOR

ZABBIX CERTIFIED PROFESSIONAL

Mobil: +421 905 210 301

E-mail: stanislav.taziar@snt.sk

Web: https://www.snt.sk/zabbix.html

Trainings and exams: https://www.snt.sk/zabbix.skolenia.html

Webinars: https://www.snt.sk/zabbix.webinare.html