axians

ZABBIX PREMIUM PARTNER

ZABBIX TRAINING PARTNER

Budovanie bezpečného monitoringu v Zabbixe

23.10.2024

Marek Konečný

VINCI ENERGIES

axians
ZABBIX
PREMIUM PARTNER

axians

MAREK KONEČNÝ

CONSULTANT SENIOR

ZABBIX CERTIFIED TRAINER AND EXPERT

ZABBIX CERTIFIED TRAINER

ZABBIX CERTIFIED EXPERT

Mobil:	+421 905 618 324
E-mail:	marek.konecny@axians.sk
Web:	https://www.axians.sk/portfolio/monitorovanie-it/
Trainings and exams:	https://www.axians.sk/zabbix-training-center/
Consulting:	https://www.axians.sk/kontaktujte-nas/


axians
ZABBIX
PREMIUM PARTNER
Axians-Zabbix
partnership
VINCI
ENERGIES

Axians-Zabbix partnership

axians

ZABBIX
PREMIUM PARTNER

ZABBIX
TRAINING PARTNER

Axians Slovakia

Premium and Training partner

Jediná spoločnosť na Slovensku!

axians ZABBIX PREMIUM PARTNER

Webináre 2023/2024

- **08.11.2023** Zabbix 7.0 - 1.časť - Nové widgety Pie chart, Gauge...
- **15.11.2023** Zabbix 7.0 - 2.časť - GUI, komunikačný framework pre widgety
- **21.11.2023** Zabbix 7.0 - 3.časť - Akcie, LLD, triggery
- **06.12.2023** Zabbix 7.0 - 4.časť - Network discovery, zber údajov
- **24.01.2024** Zabbix 7.0 - 5.časť - Honeycomb widget, API history.push
- **07.02.2024** Zabbix 7.0 - 6.časť - Global scripts, timeouts, preprocessing
- **21.02.2024** Zabbix 7.0 - 7.časť - Plánované reporty
- **06.03.2024** Zabbix 7.0 - 8.časť - Maintenance, Host availability widget...
- **24.04.2024** Zabbix 7.0 - 9.časť - MF authentication, LLD…
- **22.05.2024** Zabbix 7.0 - 10.časť - Zabbix proxy load balancing, nové widgety

axians

axians ZABBIX PREMIUM PARTNER

Jeseň a zima 2024

- **18.9.2024** PostgreSQL databázový klaster inak
- **9.10.2024** Odporúčané postupy konfigurácie Zabbixu
- **23.10.2024** Budovanie bezpečného monitoringu v Zabbixe
- **20.11.2024** Monitoring cloudovej infraštruktúry
- **11.12.2024** Nasadenie Zabbixu v prostredí Kubernetes

axians

axians

axians

ZABBIX PREMIUM PARTNER

ZABBIX TRAINING PARTNER

Budovanie bezpečného monitoringu v Zabbixe

23.10.2024

Marek Konečný

VINCI ENERGIES

axians ZABBIX PREMIUM PARTNER

Agenda

1. Architektúra bezpečnosti v Zabbixe
2. Pripojenie na frontend
3. Pripojenie na databázu
4. Komunikácia medzi Zabbix komponentmi
5. Používateľské roly
6. Ochrana citlivých údajov
7. Reštrikcie pre Zabbix agenta
8. Autentifikácia používateľov
9. SELinux
10. Školenia a recertifikácie

axians

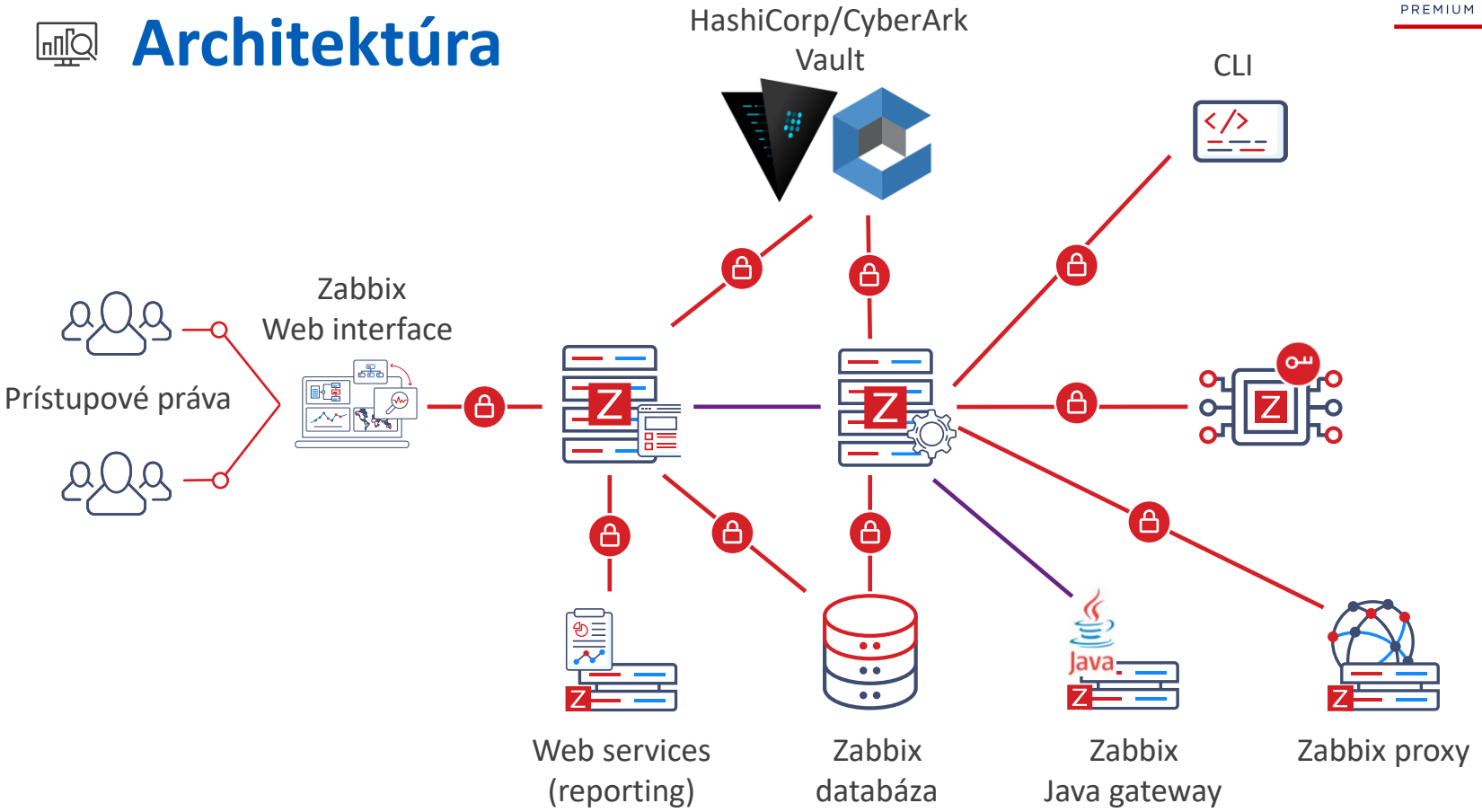
ZABBIX

PREMIUM PARTNER

Architektúra bezpečnosti v Zabbixe

VINCI ENERGIES

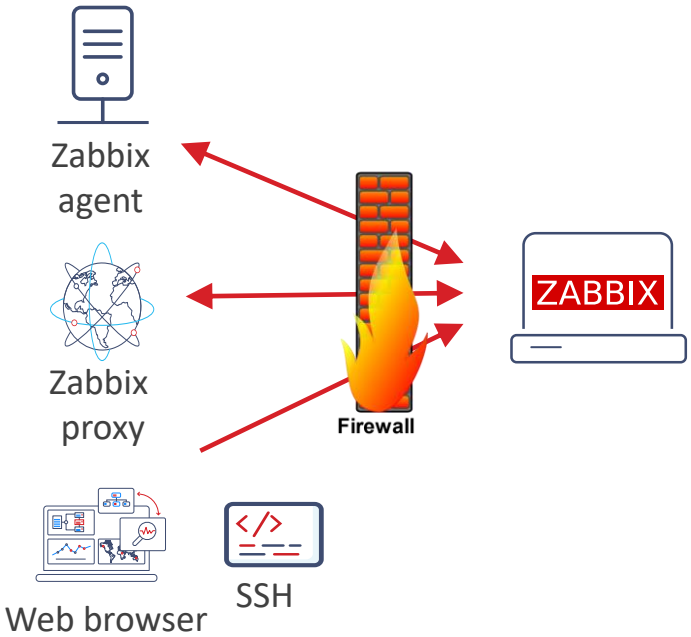
Architektúra



Konfigurácia firewallu

Ochrana Zabbix infraštruktúry 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
  - RCP 1858 pre CyberArk vault
  - Všetky monitorované služby (SNMP, IPMI, HTTP, SSH, ...)



axians

ZABBIX

PREMIUM PARTNER

Pripojenie na frontend

VINCI ENERGIES

axians ZABBIX PREMIUM PARTNER

Pripojenie na frontend

HTTPS (Hypertext Transfer Protocol Secure)

- SSL (Secure Sockets Layer) je štandard pre bezpečnú komunikáciu
- TLS (Transport Layer Security) je novšia, bezpečnejšia verzia SSL

Systém certifikátov

- Pomáha používateľom overovať identitu stránok, ku ktorým sa pripájajú
- Detaily certifikátu je možné zobraziť kliknutím na symbol v lište prehliadača

Typy SSL certifikátov

- SSL certifikáty s vlastným podpisom (self-signed)
- Certifikáty SSL podpísané dôveryhodnou certifikačnou autoritou - odporúčané pre produkčné prostredie


axians
ZABBIX
PREMIUM PARTNER
Pripojenie na databázu
VINCI ENERGIES

Pripojenie na databázu

Komunikáciu medzi Zabbix serverom (Zabbix proxy) a databázou je možné zabezpečiť s využitím TLS protokolu a certifikátov

Podporované pre databázy

- MySQL
- PostgreSQL

Nepodporované pre databázu na lokálnom hoste

- Socket spojenie nemôže byť šifrované

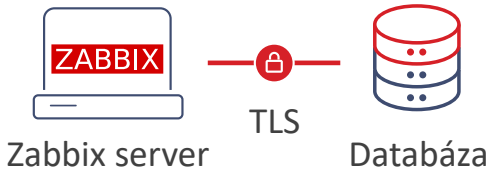
Pripojenie na databázu

Zabbix server (proxy) 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 klientský certifikát pre Zabbix server (proxy):

- **DBTLSCertFile** – špecifikácia súboru s klientskym certifikátom
- **DBTLSKeyFile** - špecifikácia súboru s privátnym kľúčom



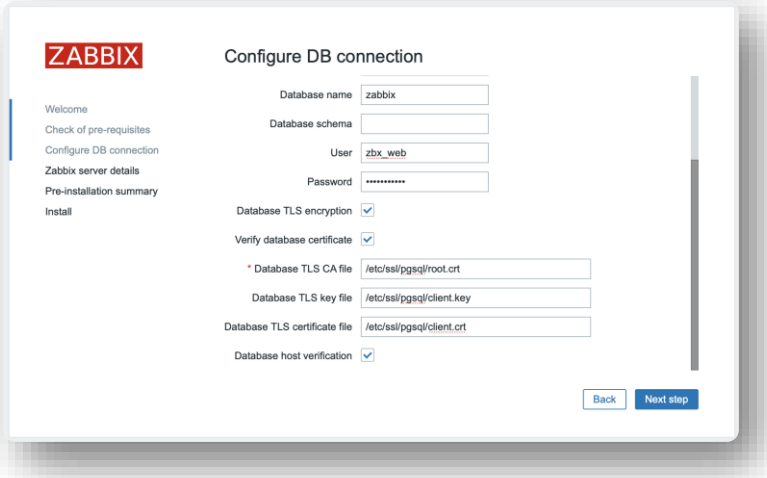
axians ZABBIX PREMIUM PARTNER

Pripojenie na databázu

Konfigurácia Zabbix frontendu má podobné možnosti (zabbix.conf.php)

```
$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



axians ZABBIX PREMIUM PARTNER

Pripojenie na databázu

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

Na testovanie výkonu SSL možno použiť diagnostické nástroje na generovanie záťaže

- **mysqlslap**
- **pgslap**

axians
ZABBIX
PREMIUM PARTNER

Pripojenie na databázu

MySQL poskytuje nástroj **mysql_secure_installation** pre zvýšenie bezpečnosti

- Nastavenie hesla pre root účty
- Minimálna zložitosť hesla
- Odstránenie root účtov, ktoré sú dostupné zvonku
- Odstránenie anonymných účtov
- Odstránenie test databázy

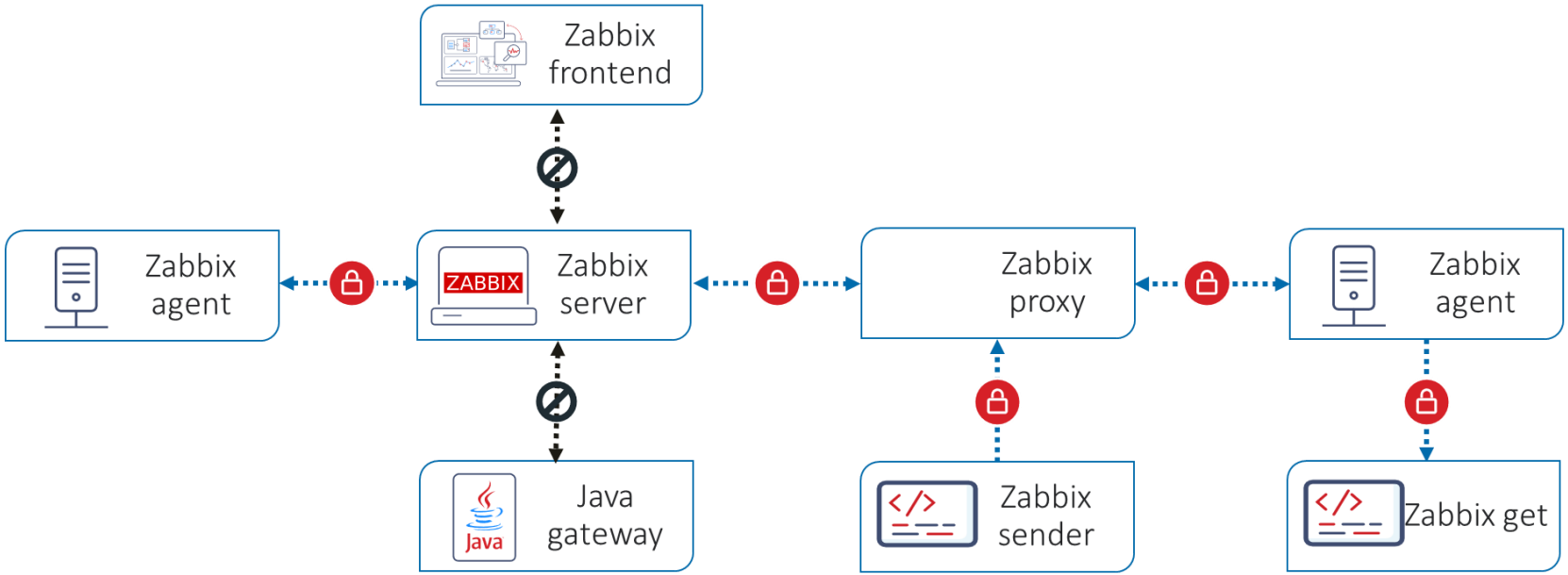
Pripojenie na databázu

Zabezpečenie databázy Zabbixu pred akýmkoľvek neoprávneným prístupom je základom bezpečnej implementácie monitoringu!

- Obsahuje prihlasovacie údaje používané na prístup k monitorovaným systémom
- Môže byť upravená tak, aby sa zmenila konfigurácia itemu


axians
ZABBIX
PREMIUM PARTNER
Komunikácia medzi
Zabbix komponentmi
VINCI
ENERGIES

Komunikácia medzi Zabbix komponentmi



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

axians ZABBIX PREMIUM PARTNER

Komunikácia medzi Zabbix komponentmi

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

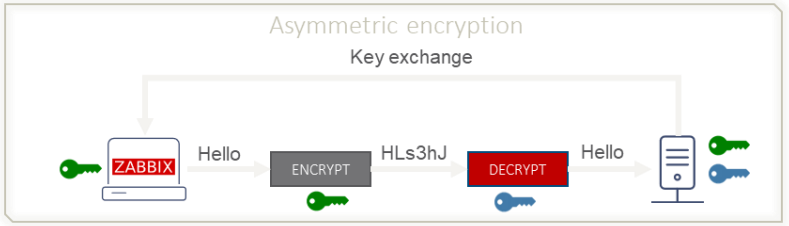
Zabbix podporuje nasledovné knižnice SSL

- OpenSSL
- LibreSSL od 2.7
  - Podporovaná kompatibilná náhrada OpenSSL
  - Nie je možné používať PSK, iba certifikáty
- GnuTLS od 3.1.18

Komunikácia medzi Zabbix komponentmi

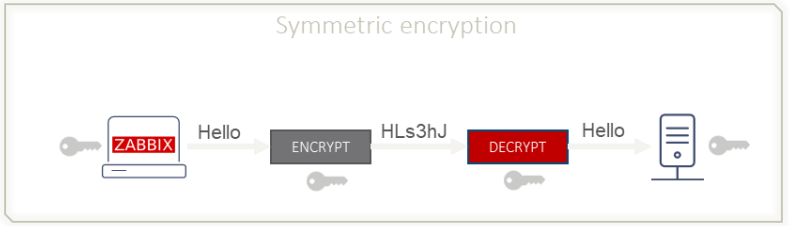
Certifikáty

- 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)

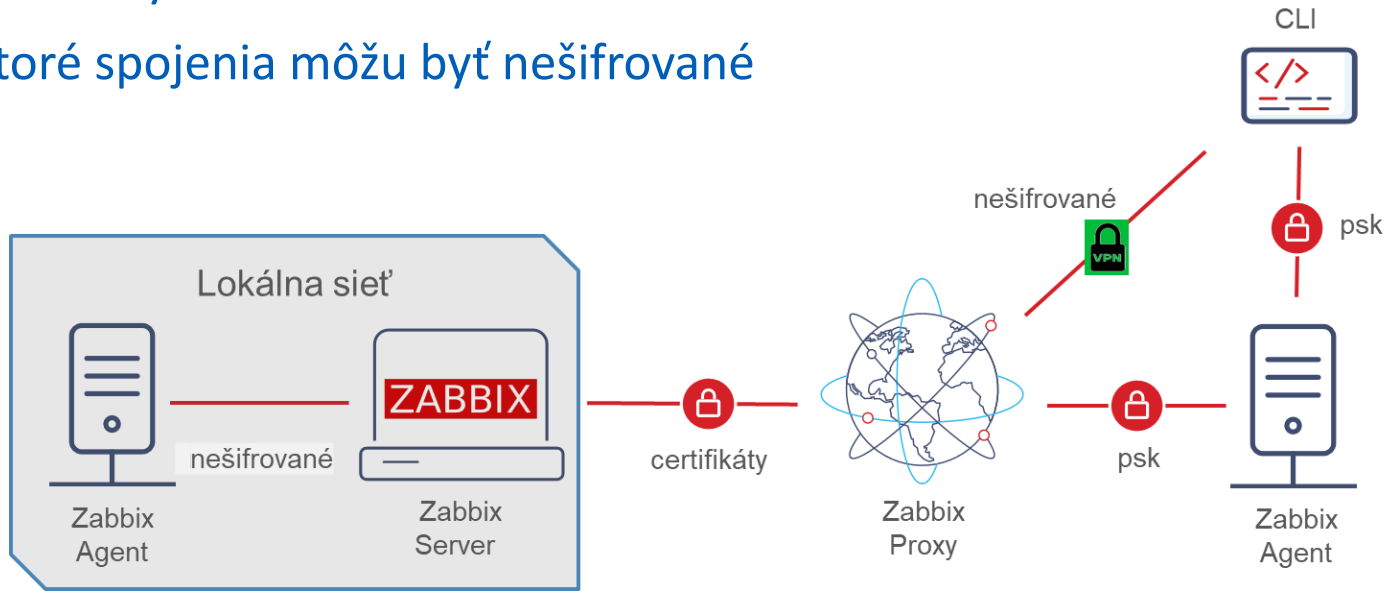
- Iba symetrické šifrovanie
- Neposkytuje bezpečné overenie identity
- Výmena kľúčov manuálna (vopred nasadené)
- Ľahšie na nakonfigurovanie



Komunikácia medzi Zabbix komponentmi

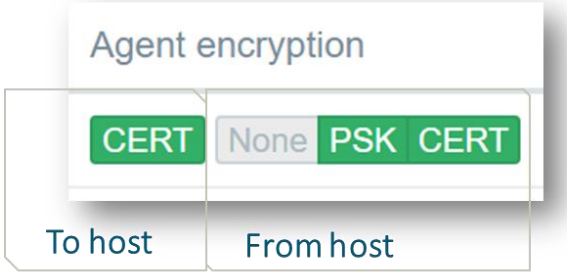
Je možné skombinovať rôzne nástroje alebo typy komunikácie pre rôzne komponenty

Niektoré spojenia môžu byť nešifrované



Komunikácia medzi Zabbix komponentmi

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)

axians ZABBIX PREMIUM PARTNER

Komunikácia medzi Zabbix komponentmi

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

Komunikácia medzi Zabbix komponentmi

Každý PSK (pre-shared key) v Zabbixe je tvorený párom

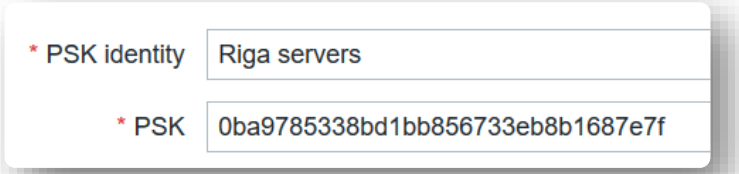
- PSK identity - neutajený identifikačný reťazec, prenáša sa nezašifrovaný
- PSK value - tajný reťazec použitý ako šifrovací kľúč

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
```

axians ZABBIX PREMIUM PARTNER

Komunikácia medzi Zabbix komponentmi

Každé TLS spojenie sa otvára s plným TLS handshake

- Nepoužíva sa session caching ani tikety
- Šifrovanie predlžuje čas kontroly itemov (v závislosti od oneskorenia na sieti)

Súbory so zdieľaným 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 kľúč-identita

axians

ZABBIX

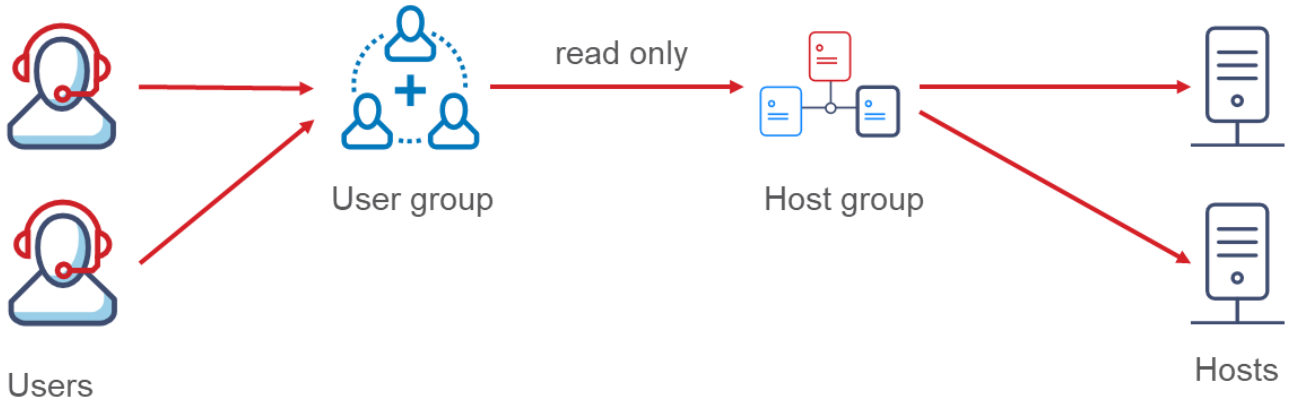
PREMIUM PARTNER

Používateľské roly

VINCI ENERGIES

Používateľské roly

V Zabbixe sa prístupové práva prideľujú na základe používateľských skupín (user groups), skupín hostov (host groups) a skupín šablón (template groups)



Nutné použiť aj keď chceme jednému používateľovi dať prístup k jednému hostovi alebo šablóne

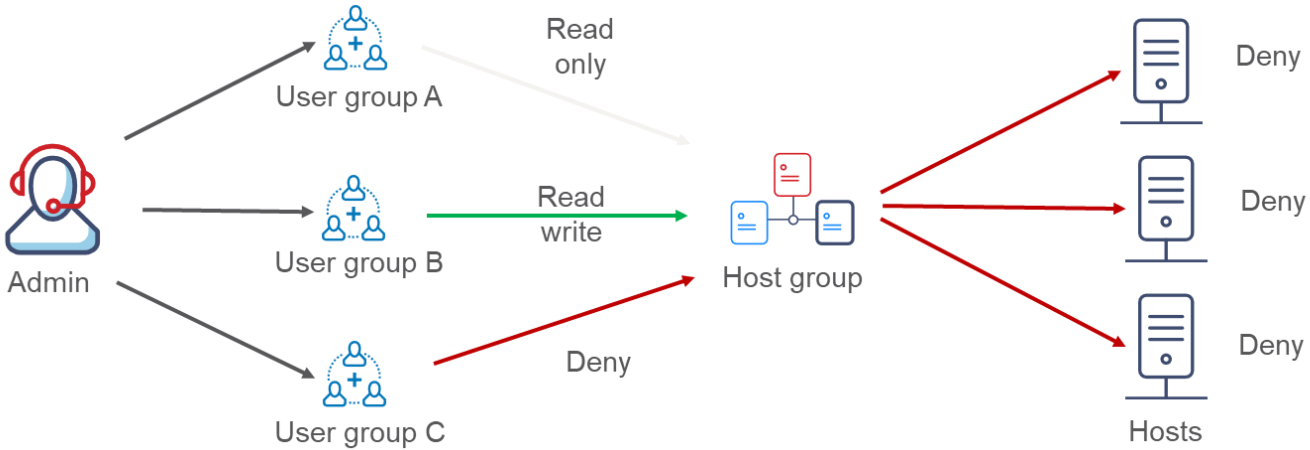
Používateľské roly

Host môže patriť do viacerých host groups

Šablóna môže patriť do viacerých template groups

Používateľ môže patriť do viacerých user groups

Platí priorita práv: **Deny > Read Write > Read only**



Používateľské roly

Zabbix 6.0 priniesol používateľské roly

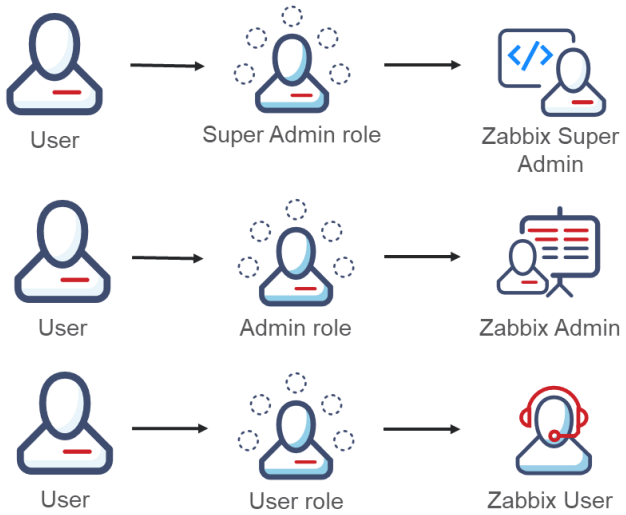
- **Super admin**, **Admin**, **User** a **Guest** roly sú preddefinované
- Super admin rola sa nedá modifikovať

Rola je spojená s jedným troch typov používateľov (User type)

- **User**
- **Admin**
- **Super admin**

Je možné vytvárať nové roly s prístupom obmedzeným iba na vybrané časti prostredia

- Napr. Super admin iba pre správu Zabbix proxy



axians
ZABBIX
PREMIUM PARTNER

Používateľské roly

Nastavuje sa prístup roly pre položky v rôznych oblastiach Zabbixu:

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

axians
ZABBIX
PREMIUM PARTNER

Používateľské roly

Dôležité poznámky

- Každý používateľ môže mať priradenú iba jednu rolu
- Používatelia typu **User** alebo **Administrátor** nemôžu meniť svoje vlastné nastavenia roly
- Používatelia akéhokoľvek typu nemôžu zmeniť svoju rolu
- Super administrátor môže upravovať nastavenia vlastnej roly

axians

ZABBIX

PREMIUM PARTNER

Ochrana citlivých údajov

VINCI ENERGIES

axians ZABBIX PREMIUM PARTNER

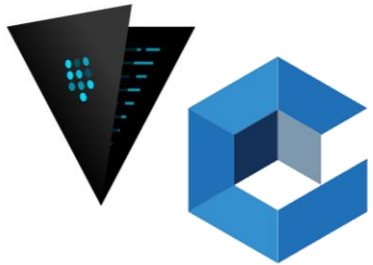
Ochrana citlivých údajov

Zabbix umožňuje využitie **HashiCorp Vault** a **CyberArk Vault** na ukladanie dvoch typov citlivých údajov:

- **Oprávnenia na prístup k databáze** pre Zabbix server, frontend a proxy
- **Hodnoty používateľských makier**

Trezor môže byť nainštalovaný na Zabbix server, Zabbix proxy alebo na samostatnom serveri

Pripojenie musí byť zabezpečené pomocou TLS protokolu

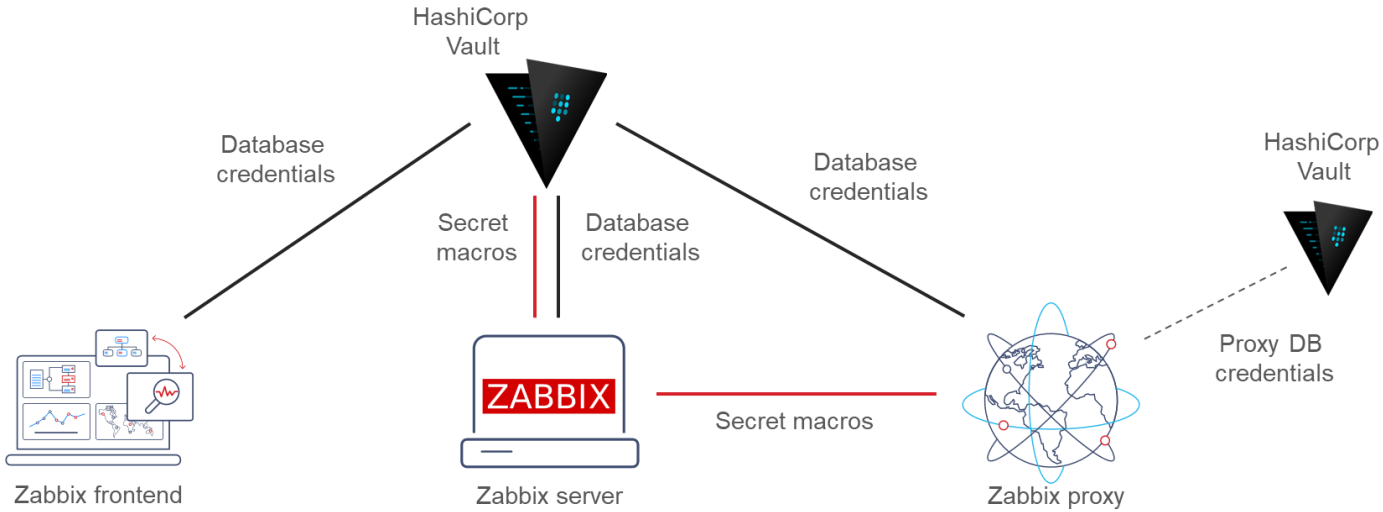


Ochrana citlivých údajov

Iba Zabbix server potrebuje pristupovať k utajeným hodnotám makier (**Vault secret User macro**)

V prípade potreby odošle Zabbix server hodnoty na proxy cez internú komunikáciu

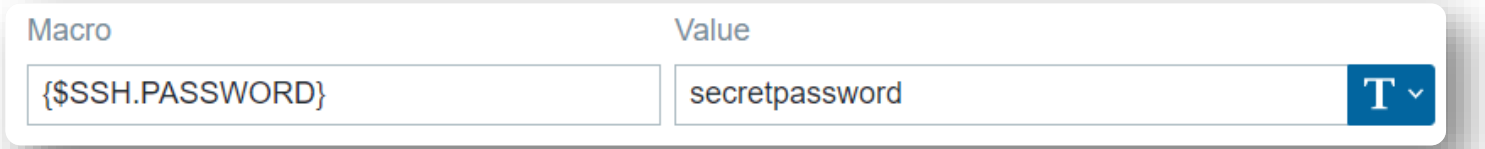
Každá proxy môže mať vlastný trezor pre uloženie prístupu k DB



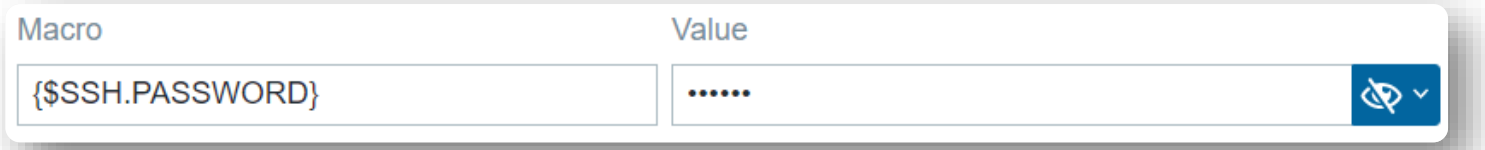
Ochrana citlivých údajov

Od verzie 5.2 má Zabbix 3 typy uloženia používateľských makier

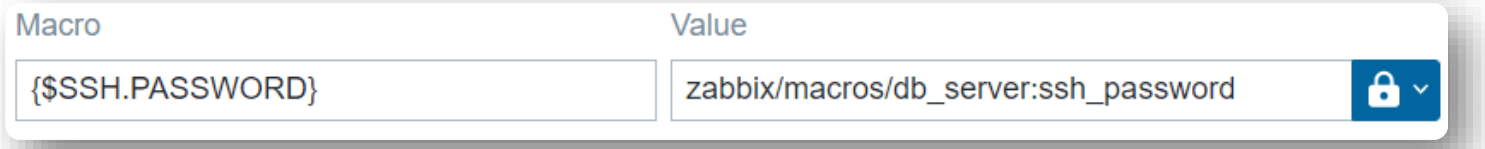
- Text



- Secret text



- Vault secrets



axians ZABBIX PREMIUM PARTNER

Ochrana citlivých údajov

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

axians ZABBIX PREMIUM PARTNER

Ochrana citlivých údajov

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 protokol

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

axians

ZABBIX

PREMIUM PARTNER

Reštrikcie pre Zabbix agenta

VINCI ENERGIES

axians
ZABBIX
PREMIUM PARTNER

Reštrikcie pre Zabbix agenta

Zabbix agent môže prostredníctvom itemov (ich kľúčov) zbierať citlivé údaje z

- Konfiguračných súborov
- Log súborov
- Súborov s heslami

Zabbix agent môže na hostoch vykonávať príkazy (pomocou kľúča **system.run[*]**)

- Na Linuxe beží Zabbix pod obmedzeným účtom
- Na Windows beží Zabbix agent (default) ako Local System!

axians ZABBIX PREMIUM PARTNER

Reštrikcie pre Zabbix agenta

Zabbix 5.0 zaviedol konfiguračné parametre **AllowKey/DenyKey** pre povolenie alebo zamietnutie konkrétneho kľúča (item key) na úrovni Zabbix Agenta

- Pre odmietnutý kľúč je item hlásený ako **unsupported**

Je možné špecifikovať neobmedzený počet AllowKey/DenyKey parametrov v konfiguračnom súbore Zabbix agenta

Platia nesledovné východzie pravidlá

- **system.run[*]** kľúč je zakázaný (ak nie je povolený pravidlom)
- Ostatné kľúče sú povolené pre spätnú kompatibilitu

Je možné používať wildcard (*) pri názve kľúča aj parametroch

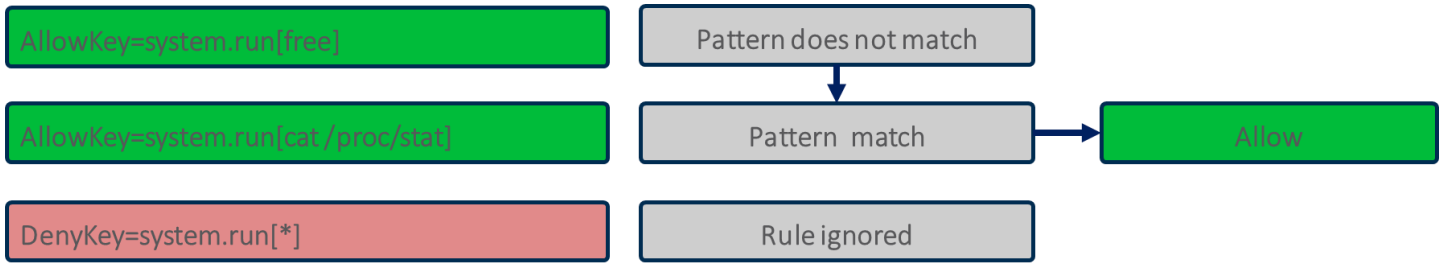
- system.cpu.* neplatí pre kľúč **system.cpu.load[]**
- system.cpu.*[*] neplatí pre kľúč **system.cpu.load**

Reštrikcie pre Zabbix agenta

Pravidlá sa vyhodnocujú v poradí, ako sú zadané

- Prvé pravidlo, pre ktoré vyhovuje item key, platí
- Ostatné sa nevyhodnocujú

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



axians

ZABBIX

PREMIUM PARTNER

Autentifikácia používateľov

VINCI ENERGIES

Externá autentifikácia používateľov

Externá autentifikácia pre správu používateľov

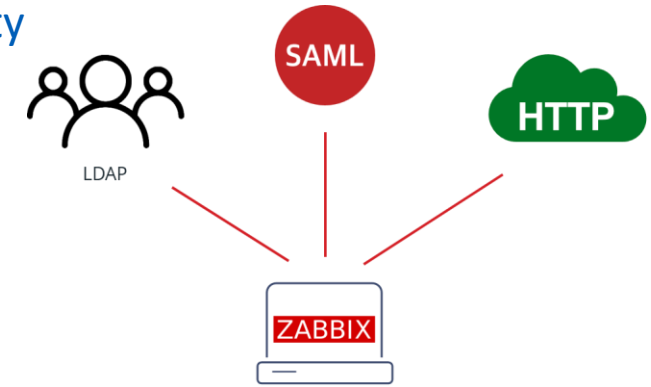
- Je možné kombinovať rôzne metódy overovania
- Odporúča sa ponechať si jedného Super administrátora s interným overením

Nastavenie spôsobu autentifikácie na úrovni skupiny používateľov (User group)

JIT – automatizované vytváranie účtov v Zabbixe

Zabbix podporuje nasledovných poskytovateľov identity

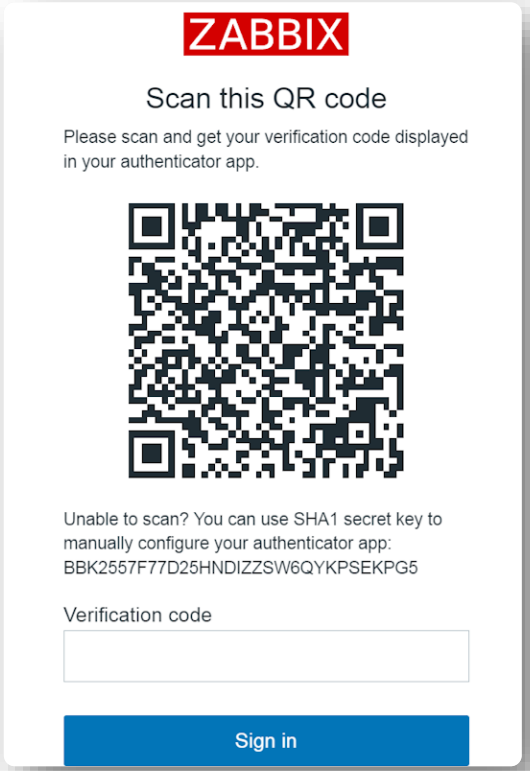
- **LDAP** (aj režim JIT)
- **SAML** (aj režim JIT)
- **HTTP**



Multi-factor autentifikácia

Out-of-the-box podpora pre multi-factor autentifikáciu (MFA):

- Time-Based One-Time Password (TOTP) autentifikácia
- Duo Universal Prompt autentifikácia



axians

ZABBIX

PREMIUM PARTNER

SELinux

VINCI ENERGIES

axians ZABBIX PREMIUM PARTNER

SELinux

SELinux (Security-Enhanced Linux)

- Umožňuje správcom mať väčšiu kontrolu nad tým, kto môže pristupovať do systému
- Definuje riadenie prístupu pre aplikácie, procesy a súbory v systéme
- Používa množinu politík, ktoré hovoria, k čomu sa dá alebo nedá pristupovať

Ak je prístup odmietnutý, do logu /var/log/audit sa zapíše správa „denied“

SELinux má 3 režimy

- **Disabled** SELINUX je úplne vypnutý
- **Enforcing** SELINUX vynucuje plnenie pravidiel
- **Permissive** SELINUX zaznamenáva správy „denied“, ale nič neblokuje

axians ZABBIX PREMIUM PARTNER

SELinux

SELinux je založený na politikách

- Zabbix poskytuje balíček **zabbix-selinux-policy** s politikami pre Zabbix
- Konkrétna implementácia si môže vyžiadať vytvorenie nových politík

Tvorba nových pravidiel

- Manuálne vytvorením súborov pravidiel z auditlogu
- Automaticky

Je vhodné najprv povoliť režim Permissive, vytvoriť politiky, skontrolovať výsledky a potom prepnúť na režim Enforcing

axians ZABBIX PREMIUM PARTNER

SELinux

audit2allow - nástroj umožňuje čítať auditlog a vytvárať politiku

SELinux musí byť v permisívnom režime – tvorba „denied” záznamov

```
# dnf -y install policycoreutils-python-utils
# grep "denied.*zabbix" /var/log/audit/audit.log | audit2allow -M zabbix_policy
# semodule -i zabbix_policy.pp
```

axians

ZABBIX

PREMIUM PARTNER

Bezpečnosť v Zabbixe - sumarizácia

VINCI ENERGIES

Bezpečnosť v Zabbixe – sumarizácia

Pripojenie používateľov na Zabbix frontend

Pripojenie Zabbix servera a Zabbix proxy na databázu

Komunikácia medzi Zabbix komponentmi (Zabbix server/proxy/agent)

Používateľské roly

Ochrana citlivých údajov – využitie trezorov

Reštrikcie pre Zabbix agenta – limitovanie zberu konkrétnych typov itemov

Autentifikácia používateľov

SELinux – ochrana na úrovni OS


axians
ZABBIX
PREMIUM PARTNER
Školenia a recertifikácie
VINCI
ENERGIES

axians ZABBIX PREMIUM PARTNER

Axians - Zabbix Training Center

Zabbix 7.0 – školenia a certifikácie

axians
ZABBIX
PREMIUM PARTNER

Recertifikácie na verziu 7.0

Pre certifikovaných špecialistov (ZCS) alebo profesionálov (ZCP) na verziu 6.0 ponuka Upgrade školení na verziu 7.0

axians

ZABBIX

ZCS Upgrade

ZCP Upgrade

Ste majiteľmi certifikátov na verziu 5.0? Kontaktujte nás.

axians ZABBIX PREMIUM PARTNER

Garantované termíny školení 2024

Možnosť prihlásiť sa na najbližšie školenia s garantovanými termínmi konania

axians

ZABBIX

- Zabbix Certified User - **30.10.2024**
- Zabbix Certified User - **31.10.2024**
- Zabbix Certified Specialist - **18.11.2024 – 22.11.2024**

Tieto termíny nie sú v ponuke na našej webstránke, preto nás v prípade záujmu kontaktujte priamo na adrese **zabbix@axians.sk**

Pripravujete sa na upgrade?

Zabbix konzultácia zdarma

Kontaktujte nás, sme pripravení vám kedykoľvek pomôcť. Navyše, prvú konzultáciu poskytujeme zdarma. Cez platformu MS Teams nám môžete predstaviť váš problém a spoločne sa pokúsime nájsť riešenie. Vyplňte formulár a my vás budeme kontaktovať, aby sme si dohodli termín vašej konzultácie zdarma.

* Polia označené hviezdičkou sú povinné.

OSLOVENIE

MENO


axians
ZABBIX
PREMIUM PARTNER
Otázky
???
VINCI
ENERGIES

axians
ZABBIX
PREMIUM PARTNER

axians

MAREK KONEČNÝ

CONSULTANT SENIOR

ZABBIX CERTIFIED TRAINER AND EXPERT

ZABBIX CERTIFIED TRAINER

ZABBIX CERTIFIED EXPERT

Mobil:	+421 905 618 324
E-mail:	marek.konecny@axians.sk
Web:	https://www.axians.sk/portfolio/monitorovanie-it/zabbix/
Trainings and exams:	https://www.axians.sk/zabbix-training-center/
Consulting:	https://www.axians.sk/kontaktujte-nas/