DELTA – Střední škola informatiky a ekonomie, s.r.o.

Ke Kamenci 151, Pardubice

Provozní a bezpečnostní dohled za využití Zabbix

Kolín, Vojtěch

4.B

Informační technologie 18-20-M/01

Školní rok 2024/25

Zadání maturitního projektu z informatických předmětů

Jméno a příjmení: *Vojtěch Kolín*

Pro školní rok: *2024/2025*

Třída: *4.*

Obor: *Informační technologie 18-20-M/01*

Téma práce: Provozní a bezpečností dohled za využití Zabbix

Vedoucí práce: Josef Horálek

Způsob zpracování, cíle práce, pokyny k obsahu a rozsahu práce:

Cílem práce je popsat principy fungování provozního a bezpečnostního dohledu a dále představit možnosti nástroje Zabbix. V praktické části autor nasadí systém Zabbix v laboratorním prostředí, navrhne a otestuje základní nastavení a získané výsledky.

Stručný časový harmonogram (s daty a konkretizovanými úkoly):

Principy provozního a bezpečnostního dohledu

Možnosti nástroje Zabbix

Návrh testovací topologie a její konfigurace

Implementace Zabbix

Testování a ověření výsledků

Prohlašuji, že jsem maturitní projekt vypracoval(a) samostatně, výhradně s použitím uvedené literatury.

V Pardubicích 31. 3. 2023

_____

Poděkování

Upřímně děkuji doc. Mgr. Josef Horálek, Ph.D. za studijní materiál a odborné vedení při zpracovávání maturitního projektu.

Resumé

Tato práce se zaměřuje na provozní a bezpečnostní dohled IT systémů s využitím monitorovací platformy Zabbix. Popisuje základní principy dohledových systémů, jejich význam v kybernetické bezpečnosti a související legislativní požadavky. Zabbix je představen jako výkonný nástroj umožňující nepřetržité monitorování, detekci anomálií a automatizovanou reakci na incidenty.

V praktické části byla provedena implementace Zabbixu v testovacím prostředí, zahrnující návrh topologie, konfiguraci systému a ověření jeho funkcionalit. Výsledky potvrzují, že Zabbix efektivně pomáhá minimalizovat bezpečnostní rizika, zajišťuje stabilitu IT infrastruktury a umožňuje optimalizaci jejího provozu.

Práce shrnuje klíčové výhody nasazení dohledových systémů a poskytuje doporučení pro jejich efektivní využití v praxi.

Klíčová slova

Zabbix, provozní dohled, kybernetická bezpečnost, monitorování IT, detekce hrozeb, automatizace, síťová infrastruktura, analýza dat

Annotation

This thesis focuses on operational and security monitoring of IT systems using the Zabbix monitoring platform. It describes the fundamental principles of monitoring systems, their significance in cybersecurity, and related legislative requirements. Zabbix is presented as a powerful tool enabling continuous monitoring, anomaly detection, and automated incident response.

The practical part includes the implementation of Zabbix in a test environment, covering topology design, system configuration, and functionality validation. The results confirm that Zabbix effectively minimizes security risks, ensures IT infrastructure stability, and optimizes its operation.

The thesis summarizes the key benefits of deploying monitoring systems and provides recommendations for their effective use in practice.

Keywords

Zabbix, operational monitoring, cybersecurity, IT monitoring, threat detection, automation, network infrastructure, data analysis

Obsah

1. Provozní dohled v oblasti kybernetické bezpečnosti

1.1 Úvod

Provozní dohled je klíčovým prvkem kybernetické bezpečnosti, který zajišťuje monitorování, detekci a reakci na bezpečnostní hrozby v reálném čase. Bez důkladného dohledu by organizace mohly čelit významným rizikům, včetně ztráty dat, finančních ztrát a poškození pověsti. Tento dokument popisuje význam provozního dohledu, příslušné normy a legislativu, zdroje informací a příklady jeho reálného využití v České republice.

1.2. Proč se používá provozní dohled

Provozní dohled je klíčovým nástrojem pro zajištění bezpečnosti, stability a efektivity IT systémů. Umožňuje nepřetržité sledování provozu, rychlou reakci na incidenty a minimalizaci výpadků.

Jedním z hlavních důvodů jeho využití je ochrana infrastruktury před kybernetickými hrozbami. Monitorování sítě pomáhá detekovat neoprávněné přístupy, šíření malwaru či jiné bezpečnostní incidenty, na které lze okamžitě reagovat. Důležitou roli hraje také prevence ztráty dat, kdy dohledové systémy včas upozorňují na selhání hardwaru či problémy se zálohováním.

Provozní dohled zajišťuje i soulad s legislativními normami, například GDPR, a poskytuje podklady pro audity. Současně pomáhá optimalizovat výkon IT infrastruktury sledováním vytížení zdrojů a umožňuje automatizaci některých zásahů, čímž snižuje potřebu ruční správy.

Díky těmto funkcím je provozní dohled nezbytný pro efektivní správu systémů, ochranu dat a předcházení nečekaným problémům, které by mohly narušit chod organizace.

1.3. Normy a legislativa

Provozní dohled v oblasti kybernetické bezpečnosti podléhá řadě právních předpisů a norem, které stanovují pravidla pro zabezpečení informačních systémů. Tyto regulace pomáhají organizacím chránit citlivé údaje, předcházet kybernetickým útokům a zajistit stabilní provoz jejich IT infrastruktury.

V České republice je klíčovým právním předpisem **zákon č. 181/2014 Sb. o kybernetické bezpečnosti**, který definuje povinnosti organizací spravujících kritickou infrastrukturu nebo významné informační systémy. Tento zákon doplňuje **vyhláška č. 82/2018 Sb.**, která podrobně specifikuje technické a organizační požadavky na

zabezpečení informačních systémů, včetně opatření proti neoprávněným přístupům a hrozbám.

Kromě národní legislativy existují i mezinárodní normy, které stanovují standardy pro správu a ochranu informací. Mezi nejvýznamnější patří **ISO/IEC 27001**, která poskytuje rámec pro řízení bezpečnosti informací a pomáhá organizacím zavést efektivní bezpečnostní politiky. V oblasti kybernetické bezpečnosti je rovněž uznávaný americký standard **NIST SP 800-53**, který obsahuje podrobný soubor bezpečnostních kontrol a doporučení pro ochranu informačních systémů, zejména ve veřejném sektoru.

Dodržování těchto předpisů a norem umožňuje organizacím nejen chránit své systémy a data, ale také splnit legislativní požadavky a získat důvěru svých uživatelů a partnerů.

1.4. Příklady reálného použití

Provozní dohled je klíčovým prvkem kybernetické bezpečnosti napříč různými odvětvími, kde pomáhá chránit citlivá data a zajišťovat stabilitu systémů.

V energetickém sektoru se využívá k monitorování elektráren, rozvodných sítí a dalších prvků kritické infrastruktury. Nepřetržité sledování umožňuje včasnou detekci podezřelých aktivit a minimalizaci rizika kybernetických útoků, které by mohly ohrozit dodávky energie a způsobit rozsáhlé výpadky.

Ve finančním sektoru pomáhá chránit banky a finanční instituce před podvody, neoprávněnými transakcemi a úniky citlivých údajů. Dohledové systémy analyzují transakční data v reálném čase, odhalují podezřelé aktivity a umožňují rychlou reakci na potenciální hrozby, čímž minimalizují finanční ztráty a zvyšují důvěryhodnost institucí.

Ve veřejném sektoru je provozní dohled nezbytný pro ochranu státních institucí a vládních agentur. Monitorovací systémy pomáhají předcházet únikům citlivých informací, chránit národní zájmy a odhalovat kybernetické útoky, které by mohly narušit chod státní správy nebo ohrozit bezpečnost obyvatelstva.

Díky těmto opatřením umožňuje provozní dohled organizacím rychle reagovat na bezpečnostní incidenty, zajistit ochranu klíčových systémů a předejít potenciálním škodám způsobeným kybernetickými hrozbami.

1.5. Doporučené postupy pro efektivní provozní dohled

Pro zajištění efektivního provozního dohledu je nezbytné dodržovat osvědčené postupy, které pomáhají minimalizovat bezpečnostní rizika a zvyšují stabilitu systémů. Klíčovým

prvkem je nepřetržité monitorování, které umožňuje průběžné sledování síťového provozu a okamžitou detekci podezřelých aktivit. Díky automatizovaným nástrojům lze odhalit anomálie, jež by mohly signalizovat kybernetický útok nebo technickou závadu.

Neméně důležitou součástí je existence jasně definovaného plánu reakce na incidenty. Tento plán stanovuje konkrétní kroky, které je nutné podniknout při detekci bezpečnostní hrozby, a zahrnuje postupy pro izolaci problému, jeho analýzu a nápravu. Rychlá a koordinovaná reakce minimalizuje dopady incidentu a zajišťuje kontinuitu provozu.

Dalším klíčovým opatřením jsou pravidelné audity, které hodnotí účinnost stávajících bezpečnostních opatření a pomáhají identifikovat možné slabiny v infrastruktuře. Na základě jejich výsledků lze přizpůsobit bezpečnostní strategii a implementovat nové ochranné mechanismy.

Nezbytnou součástí efektivního provozního dohledu je také průběžné školení zaměstnanců. Lidský faktor hraje zásadní roli v kybernetické bezpečnosti, a proto je důležité, aby zaměstnanci byli informováni o aktuálních hrozbách, správném zacházení s citlivými daty a postupech při podezřelých událostech. Zvýšení povědomí o bezpečnostních rizicích přispívá k celkovému posílení ochrany organizace.

Dodržování těchto doporučených postupů umožňuje organizacím nejen rychle a efektivně reagovat na bezpečnostní incidenty, ale také předcházet potenciálním hrozbám a zajistit dlouhodobou stabilitu a bezpečnost jejich IT infrastruktury.

1.6. Shrnutí

Provozní dohled hraje zásadní roli v oblasti kybernetické bezpečnosti a umožňuje organizacím efektivně monitorovat a chránit jejich informační systémy. Díky nepřetržitému sledování síťového provozu pomáhá odhalovat bezpečnostní hrozby, minimalizovat rizika a zajistit rychlou reakci na incidenty.

Jeho využití je klíčové v mnoha sektorech, od energetiky a financí až po veřejnou správu, kde přispívá k ochraně kritické infrastruktury a citlivých dat. Dodržování stanovených norem a legislativy umožňuje organizacím zajistit soulad s bezpečnostními požadavky a posílit ochranu před kybernetickými útoky.

Zavedením efektivních postupů, jako je pravidelné testování bezpečnostních opatření, školení zaměstnanců a jasně definované krizové plány, mohou organizace výrazně zvýšit úroveň své ochrany a zajistit spolehlivý provoz svých IT systémů.

2. Dohledové systémy

2.1 Definice

Dohledové systémy představují kombinaci softwarových a hardwarových řešení určených k monitorování, správě a analýze provozu IT infrastruktury, zařízení a služeb. Jejich hlavním cílem je zajistit vysokou dostupnost, optimalizovat výkon a včas odhalovat potenciální problémy, které by mohly ohrozit stabilitu systémů.

Fungují na principu sběru dat ze sledovaných komponent, která jsou následně analyzována a vyhodnocována podle předem definovaných parametrů. Na základě těchto analýz mohou systémy generovat upozornění na zjištěné problémy nebo automaticky provádět předem nastavené akce k jejich nápravě. Tím dochází k minimalizaci výpadků a zvýšení efektivity správy IT prostředí.

2.2 Příklady aplikací

Dohledové systémy nacházejí uplatnění v širokém spektru oblastí, kde pomáhají monitorovat provoz, zvyšovat bezpečnost a optimalizovat výkon technologií. Jejich využití sahá od správy IT infrastruktury přes průmyslovou výrobu až po zdravotnictví a dopravu.

2.2.1 IT infrastruktura

V oblasti správy IT se dohledové systémy využívají k nepřetržitému monitorování serverů, sítí a aplikací. Sledují datové toky, vytížení systémů a odhalují potenciální problémy dříve, než způsobí výpadek. Automatizovaná hlášení incidentů umožňují rychlou reakci a minimalizují dopady na provoz organizací.

2.2.2 Průmyslová automatizace

Ve výrobních závodech pomáhají dohledové systémy monitorovat činnost výrobních linek a provádět prediktivní údržbu strojů. Díky analýze provozních dat lze předcházet neplánovaným odstávkám a optimalizovat výrobní procesy, což vede k vyšší efektivitě a nižším nákladům.

2.2.3 Bezpečnostní systémy

V oblasti bezpečnosti se dohledové systémy používají ke správě kamerových systémů, detekci narušení a identifikaci kybernetických hrozeb. Moderní technologie, jako je biometrická autentizace nebo přístupové kontrolní systémy, umožňují efektivní správu oprávnění a zajištění fyzické i digitální bezpečnosti.

2.2.4 Zdravotnictví

Ve zdravotnictví se dohledové systémy využívají ke sledování provozu zdravotnických zařízení a zajištění jejich nepřetržité funkčnosti. Pokročilé monitorovací nástroje analyzují

data pacientů v reálném čase, čímž pomáhají lékařům rychle reagovat na změny zdravotního stavu. Správa nemocniční IT infrastruktury pak zajišťuje stabilní provoz informačních systémů a ochranu citlivých údajů.

2.2.5 Dopravní infrastruktura

V oblasti dopravy slouží dohledové systémy k monitorování dopravních toků a jejich efektivnímu řízení. Sledují stav vozidel, plánují jejich údržbu a umožňují automatickou detekci nehod či rizikových situací. Díky těmto funkcím přispívají k plynulejšímu provozu a vyšší bezpečnosti na silnicích.

2.3 Proč využíváme dohledové systémy?

Dohledové systémy jsou klíčovým nástrojem pro zajištění stability, efektivity a bezpečnosti IT i průmyslové infrastruktury. Jejich nasazení pomáhá organizacím předcházet problémům, optimalizovat provoz a splňovat legislativní požadavky.

Jedním z hlavních důvodů jejich využití je prevence výpadků. Neustálé monitorování umožňuje včasné odhalení potenciálních problémů, což minimalizuje riziko neplánovaných odstávek a snižuje finanční ztráty spojené s výpadky služeb. Kromě toho dohledové systémy přispívají ke zvyšování efektivity tím, že analyzují využití zdrojů a pomáhají optimalizovat výkon infrastruktury.

Důležitým aspektem je také bezpečnost. Monitorovací nástroje sledují síťový provoz, detekují anomálie a chrání systémy před kybernetickými hrozbami. Díky pokročilé analýze dat je možné včas identifikovat neoprávněné aktivity nebo pokusy o útoky a přijmout odpovídající opatření.

Dalším přínosem je automatizace a reporting. Dohledové systémy umožňují generování přehledných reportů, které poskytují cenné informace pro strategická rozhodnutí a optimalizaci provozu. Automatizované procesy zároveň snižují potřebu manuálních zásahů, což zefektivňuje správu systémů.

V neposlední řadě pomáhají organizacím zajistit shodu s právními a regulačními předpisy. V mnoha odvětvích, jako je zdravotnictví, finance nebo průmysl, existují přísné požadavky na bezpečnost a dostupnost dat. Dohledové systémy zajišťují, že organizace splňují tyto normy a mohou bez obav projít audity a kontrolami.

Nasazením dohledových systémů tak organizace získávají nejen vyšší stabilitu a bezpečnost, ale také lepší kontrolu nad svými technologickými prostředky a efektivnější řízení provozu.

3. Provozní dohled a role Zabbixu v kybernetické bezpečnosti

Zabbix je výkonná open-source platforma, která se v oblasti provozního dohledu stala jedním z nejpoužívanějších nástrojů pro monitorování a správu IT infrastruktury. Díky svým pokročilým funkcím umožňuje organizacím efektivně sledovat provoz systémů, detekovat anomálie a rychle reagovat na bezpečnostní incidenty. Jeho flexibilita a široké možnosti integrace z něj činí ideální nástroj pro zvýšení úrovně kybernetické bezpečnosti.

3.1. Široké možnosti monitorování

Jednou z klíčových výhod Zabbixu je schopnost monitorovat různé typy systémů a aplikací. Umožňuje sledování serverů, síťových zařízení, databází i koncových uživatelů, čímž poskytuje komplexní přehled o celém IT prostředí organizace.

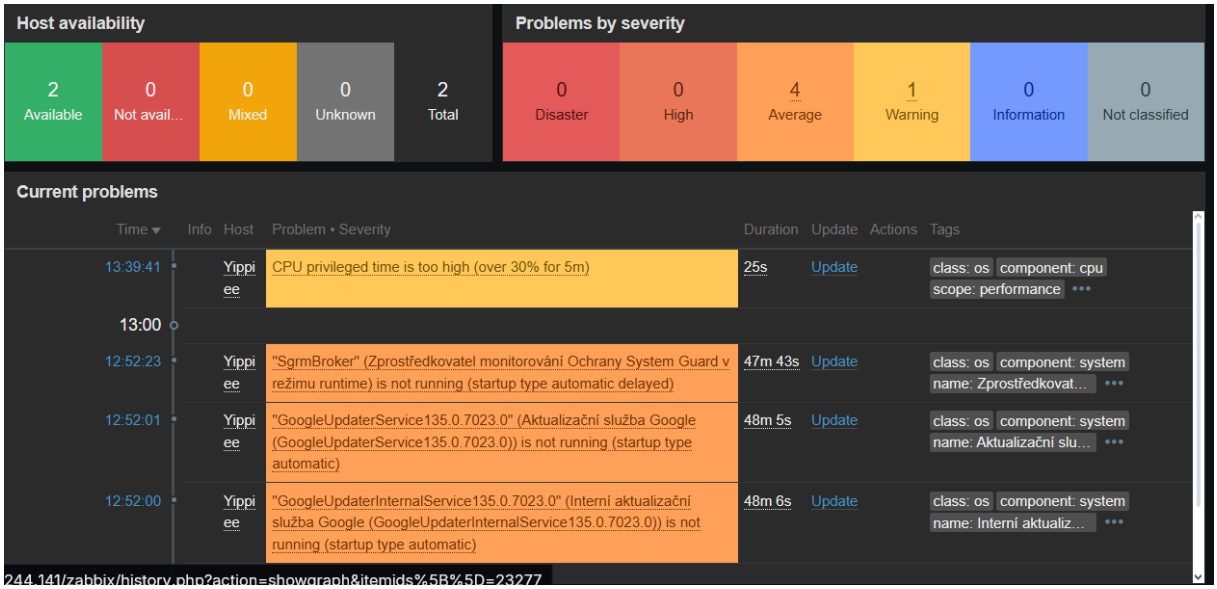
Další silnou stránkou Zabbixu je podpora různých protokolů a technologií. Díky kompatibilitě se standardy jako SNMP, IPMI, JMX nebo HTTP může monitorovat širokou škálu zařízení a služeb, což usnadňuje integraci s existující IT infrastrukturou. Tato univerzálnost umožňuje nasazení Zabbixu ve firmách různé velikosti i v organizacích s heterogenním prostředím.

3.2. Detekce anomálií a hrozeb v reálném čase

Zabbix umožňuje pokročilou detekci anomálií a bezpečnostních hrozeb díky nepřetržitému monitorování síťového provozu a systémových zdrojů. Dokáže identifikovat neobvyklé aktivity, jako jsou pokusy o neoprávněný přístup, prudké nárůsty síťového provozu nebo nestandardní zatížení serverů, a okamžitě na ně upozornit administrátory.

Jednou z klíčových funkcí je schopnost automatické reakce na incidenty. Při detekci podezřelé události může Zabbix automaticky spustit předdefinované skripty nebo provést konkrétní akce, například restartovat službu, blokovat podezřelou IP adresu nebo odeslat upozornění odpovědnému týmu. Díky tomu se minimalizuje doba potřebná k řešení bezpečnostních problémů a snižuje se riziko narušení provozu.

Obr. 1: výstraha - zpomalení Wifi (zdroj: autor)



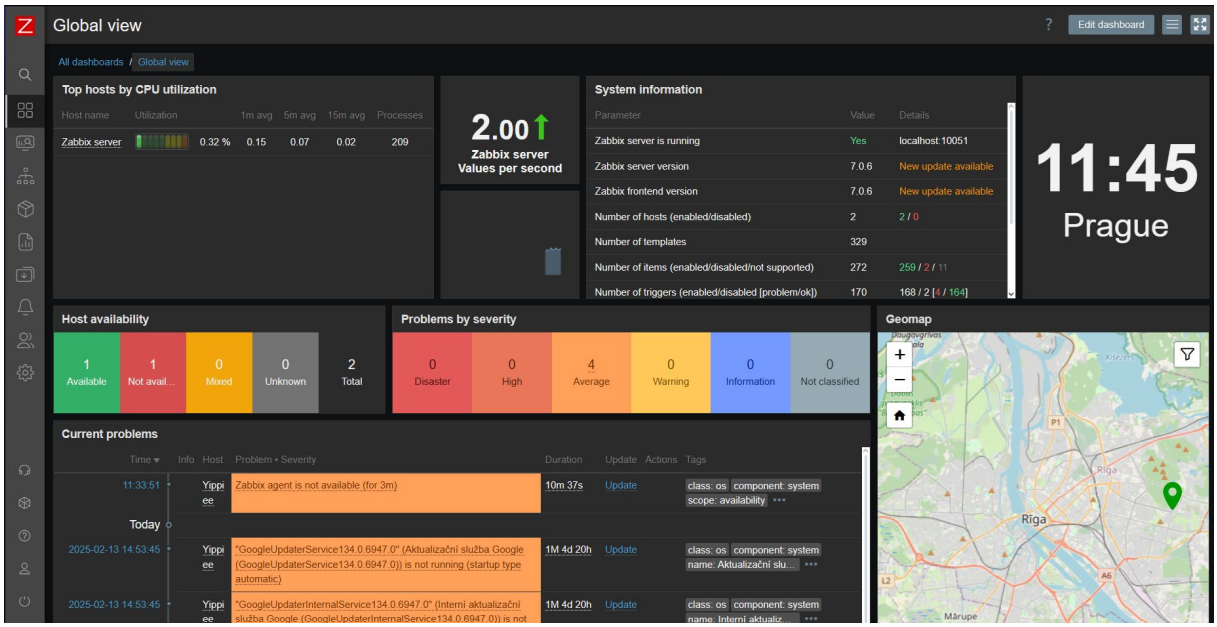
Obr. 2: výstraha - přetížení CPU (zdroj: autor)

3.3. Centrální dohled a škálovatelnost

Zabbix poskytuje centralizovaný přehled o všech monitorovaných prvcích prostřednictvím přehledného dashboardu, kde lze sledovat bezpečnostní události v reálném čase. Tento konsolidovaný pohled umožňuje rychlou identifikaci problémů a zefektivňuje správu rozsáhlých IT infrastruktur.

Velkou výhodou Zabbixu je jeho škálovatelnost, která mu umožňuje zpracovávat velké objemy dat i ve složitých síťových prostředích. Díky tomu je vhodný nejen pro menší

organizace, ale také pro velké podniky a kritickou infrastrukturu, kde je potřeba monitorovat tisíce zařízení a služeb současně.



Obr. 3: Náhled dashboard (zdroj: autor)

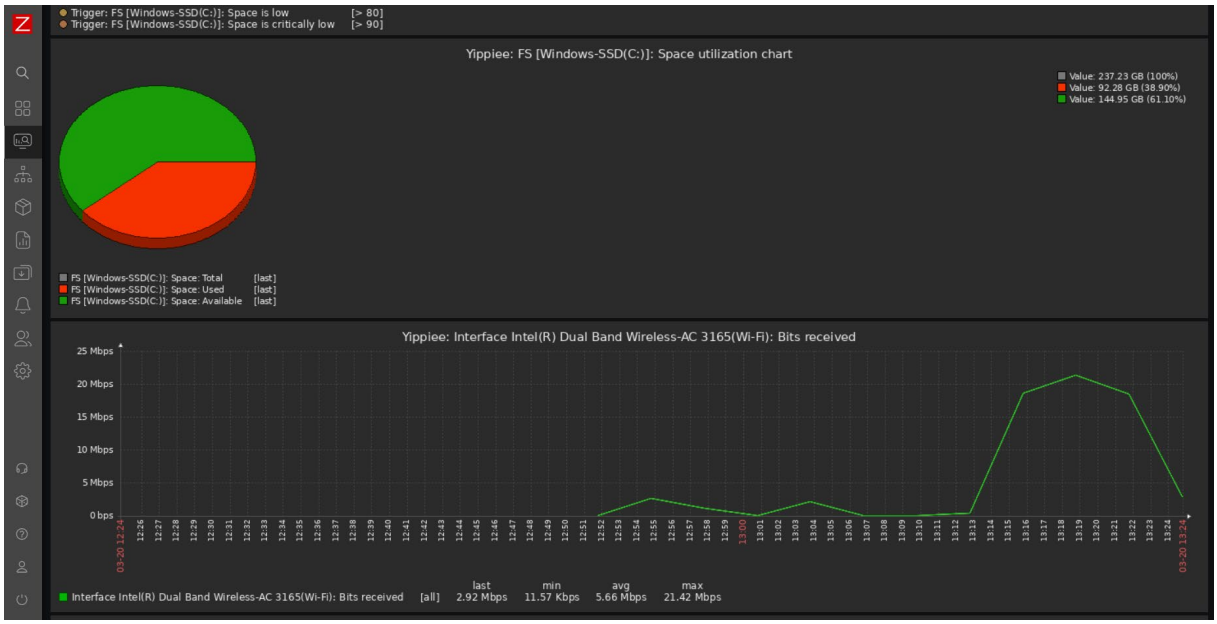
3.4. Podpora souladu s předpisy

Zabbix může významně pomoci organizacím splnit legislativní požadavky v oblasti kybernetické bezpečnosti. Jeho funkcionality podporují dodržování právních předpisů, jako je **Zákon č. 181/2014 Sb. o kybernetické bezpečnosti**, a mezinárodních norem, například **ISO/IEC 27001**. Díky možnosti detailního logování a uchovávání auditních záznamů poskytuje Zabbix důležité podklady pro interní i externí audity. To umožňuje organizacím nejen sledovat bezpečnostní události, ale také zpětně analyzovat incidenty a hodnotit účinnost přijatých opatření.

3.5 Vizualizace a analýza dat

Přehlednost a efektivní interpretace dat jsou zásadní pro správné rozhodování. Zabbix nabízí široké možnosti vizualizace, včetně interaktivních **dashboardů a reportů**, které umožňují rychlé vyhodnocení klíčových metrik a trendů. Díky **grafům a mapám** lze snadno identifikovat problémové oblasti, což pomáhá včas přijmout potřebná opatření a

zlepšit celkovou správu IT infrastruktury.



Obr. 4: Náhled grafu využití (zdroj: autor)

3.6. Snadná integrace a přizpůsobení

Zabbix je flexibilní a snadno integrovatelný s dalšími nástroji používanými v oblasti správy IT a kybernetické bezpečnosti. Podporuje propojení se **SIEM systémy**, které slouží k analýze bezpečnostních událostí, a může být integrován s **nástroji pro správu tiketů**, jako je **Jira**, pro efektivnější řízení incidentů. Pro pokročilou vizualizaci lze využít integraci s **platformami, jako je Grafana**.

Další výhodou je možnost vytváření **uživatelsky definovaných šablon**, které umožňují přizpůsobit monitorování specifickým potřebám organizace. Díky tomu lze Zabbix konfigurovat tak, aby poskytoval přesně ta data, která jsou pro dané prostředí nejdůležitější.

3.7. Efektivní incident response

Zabbix hraje klíčovou roli v rychlé detekci a řešení bezpečnostních incidentů. Díky automatickým upozorněním a definovaným akcím dokáže včas identifikovat problémy a minimalizovat jejich dopad na provoz organizace. Systém může být navíc integrován do existujícího **Incident Response Plánu**, což umožňuje koordinovanou reakci a efektivní řízení krizových situací. Díky propojení s dalšími bezpečnostními nástroji může Zabbix například automaticky eskalovat incidenty, spouštět obranné mechanismy nebo upozorňovat odpovědné týmy prostřednictvím různých komunikačních kanálů.

3.8. Nepřetržité monitorování (24/7)

Jednou z největších výhod Zabbixu je jeho schopnost nepřetržitého monitorování, což umožňuje **identifikaci a řešení problémů ještě předtím, než dojde k výpadku nebo narušení služeb**. Díky automatizovanému sběru dat a detekci odchylek od normálního stavu mohou administrátoři rychle reagovat a předcházet dlouhodobým výpadkům.

Nepřetržité sledování výkonu systémů navíc pomáhá s **optimalizací provozu**, protože umožňuje identifikovat přetížení zdrojů, neefektivní procesy a potenciální úzká místa infrastruktury. To vede nejen k vyšší stabilitě IT prostředí, ale i k lepšímu využití dostupných zdrojů a snížení provozních nákladů.

4. Zabbix: Úvod do monitorovací platformy

Zabbix je moderní open-source řešení určené pro monitorování IT infrastruktury, které poskytuje pokročilé nástroje pro detekci, analýzu a reakci na potenciální problémy v reálném čase. Díky své flexibilitě a škálovatelnosti nachází využití nejen v IT sektoru, ale také v průmyslu, zdravotnictví, finančních institucích a veřejné správě. Tato kapitola přináší přehled hlavních důvodů pro nasazení Zabbixu, jeho funkcí a výhod, stejně jako základní kroky pro jeho implementaci.

4.1 Klíčové vlastnosti Zabbixu

Zabbix je známý svou schopností integrovat různé technologie a poskytovat ucelený pohled na IT infrastrukturu. Mezi jeho nejdůležitější vlastnosti patří široká podpora monitorovaných prvků, flexibilní systém upozornění, pokročilé vizualizace a vysoká škálovatelnost.

4.1.1 Široká podpora monitorovaných prvků

Zabbix umožňuje sledovat servery, síťová zařízení, databáze, aplikace, kontejnery i cloudové služby. Díky podpoře standardních protokolů, jako jsou **SNMP, HTTP, JMX, IPMI** a další, lze Zabbix snadno integrovat s většinou moderních zařízení a služeb.

Flexibilní systém upozornění

Systém umožňuje nastavení **automatických notifikací** při detekci problémů prostřednictvím **e-mailu, SMS nebo integračního API**. Pro kritické incidenty je k dispozici funkce **eskalací**, která zajišťuje, že důležité události nezůstanou nepovšimnuty a budou včas řešeny odpovědnými osobami.

4.1.2 Vizualizace a analýza dat

Zabbix nabízí **přehledné dashboardy, grafy a mapy**, které umožňují snadnou interpretaci dat a identifikaci problémových oblastí. Automaticky generované **reporty** pomáhají zjednodušit pravidelné vyhodnocování výkonu systémů a podporují efektivní rozhodování.

4.1.3 Škálovatelnost a dostupnost

Zabbix je vhodný pro **malé podnikové sítě** i rozsáhlé infrastruktury s **tisíci zařízeními**. Díky podpoře **clusteringu a redundance** lze zajistit vysokou dostupnost systému a spolehlivost monitorování i v rozsáhlých IT prostředích.

4.2 Proč používat Zabbix?

Nasazení Zabbixu přináší organizacím řadu strategických výhod, které přispívají k efektivnější správě IT infrastruktury, zvýšení bezpečnosti a snížení provozních nákladů.

Jedním z hlavních přínosů je **zajištění dostupnosti a stability systémů**. Zabbix minimalizuje riziko výpadků díky včasné detekci problémů a pomáhá identifikovat úzká místa, která by mohla vést ke snížení výkonu nebo přetížení infrastruktury.

Další klíčovou výhodou je **podpora souladu s předpisy a audity**. Zabbix umožňuje vytvářet podrobné logy o provozu a bezpečnostních událostech, což je nezbytné pro auditní účely a splnění legislativních požadavků, například zákona o kybernetické bezpečnosti v České republice.

Díky **automatizaci monitorování** navíc dochází k významné **úspoře času a nákladů**. IT týmy jsou méně zatíženy ruční správou a mohou se soustředit na strategické úkoly. Otevřená licence Zabbixu eliminuje potřebu nákupu drahých komerčních řešení, přičemž poskytuje širokou škálu funkcí pro komplexní dohled nad IT prostředím.

4.3 Použití Zabbixu v praxi

Díky své flexibilitě nachází Zabbix využití v různých odvětvích, kde pomáhá zajišťovat stabilitu a bezpečnost klíčových systémů:

- **Energetika**: Monitorování kritické infrastruktury, jako jsou elektrárny, distribuční sítě nebo ropovody, k prevenci nečekaných poruch a optimalizaci výkonu.
- **Zdravotnictví**: Zajištění nepřetržitého provozu nemocničních informačních systémů a sledování funkčnosti lékařských přístrojů, kde je vysoká dostupnost zásadní.
- **Finanční sektor**: Ochrana bankovních systémů před kybernetickými útoky a monitorování jejich dostupnosti pro zajištění plynulého provozu finančních služeb.
- **Cloudové služby**: Dohled nad výkonností a dostupností cloudových platforem, detekce výpadků a optimalizace využití zdrojů pro maximální efektivitu.

4.4 Doporučené postupy pro implementaci Zabbixu

Pro úspěšné nasazení Zabbixu je důležité postupovat systematicky a přizpůsobit konfiguraci specifickým potřebám organizace.

Prvním krokem je **analýza požadavků**, která zahrnuje identifikaci klíčových metrik a služeb, jež mají být monitorovány. Je důležité definovat konkrétní cíle, jako je minimalizace výpadků nebo zlepšení výkonnosti infrastruktury.

Dalším krokem je **přizpůsobení šablon**, které umožňuje efektivnější správu různých typů zařízení a služeb. Vytvoření specifických šablon pomáhá standardizovat monitorování a usnadňuje správu velkého množství prvků. Nastavení automatických notifikací a reakcí na běžné incidenty pak zajišťuje rychlou detekci a minimalizaci dopadů problémů.

Pro maximální efektivitu by měl být Zabbix **integrován s dalšími nástroji**, jako jsou systémy pro správu tiketů (např. **Jira**) nebo analytické platformy (např. **Grafana**). Organizace využívající **SIEM** (Security Information and Event Management) mohou Zabbix propojit s těmito nástroji pro lepší správu bezpečnostních událostí.

Nezbytnou součástí úspěšného provozu je také **školení týmu**, které zajistí, že administrátoři plně rozumí konfiguraci a funkcím Zabbixu. Pravidelné aktualizace a školení pomáhají udržet systém v optimální kondici a umožňují využít nové funkce, které platforma přináší.

4.5 Přínosy Zabbixu při monitorování

Zabbix přináší řadu výhod nejen IT administrátorům, ale i manažerům odpovědným za strategické řízení IT infrastruktury.

Jedním z nejvýznamnějších přínosů je **centralizovaný přehled o infrastruktuře**. Všechny důležité informace jsou dostupné na jediném dashboardu, což usnadňuje sledování klíčových metrik, jako je využití procesoru, síťový provoz nebo dostupnost aplikací. Díky tomu lze rychle identifikovat a řešit problémy dříve, než ovlivní koncové uživatele.

Dalším důležitým aspektem je **automatizace a efektivita**. Zabbix umožňuje automatizovanou detekci problémů i reakci na incidenty, čímž snižuje potřebu manuálních zásahů a šetří čas IT týmu. Funkce **automatického škálování** navíc umožňuje dynamické přizpůsobení monitorovací infrastruktury aktuálním požadavkům bez nutnosti ručních úprav.

Zabbix rovněž **podporuje strategická rozhodnutí** tím, že poskytuje detailní analýzy trendů a prediktivní funkce. To umožňuje efektivní plánování kapacity IT prostředků a optimalizaci provozních nákladů. Data shromážděná prostřednictvím Zabbixu mohou

sloužit jako cenný podklad pro investiční rozhodování a dlouhodobé plánování rozvoje infrastruktury.

4.6 Jak Zabbix pomáhá v kybernetické bezpečnosti?

Nasazení monitorovacího nástroje Zabbix přináší mnoho výhod v oblasti kybernetické bezpečnosti. Tento nástroj umožňuje nejen sledování stavu IT infrastruktury, ale také pomáhá předcházet bezpečnostním hrozbám a minimalizovat jejich dopady.

Jednou z hlavních funkcí Zabbixu je detekce bezpečnostních hrozeb. Systém dokáže monitorovat podezřelé aktivity, jako jsou pokusy o neautorizovaný přístup, neobvyklé vzorce v síťovém provozu či anomálie ve výkonu serverů. Jakmile Zabbix zaznamená neobvyklé chování, automaticky upozorní správce systému, což umožňuje rychlou reakci a minimalizaci potenciálních škod.

Další významnou výhodou je možnost integrace Zabbixu s jinými bezpečnostními nástroji. Pomocí API lze Zabbix propojit s firewally, SIEM platformami a dalšími systémy, což poskytuje komplexní přehled o bezpečnostních událostech a urychluje jejich řešení. Tato integrace usnadňuje správcům IT efektivněji analyzovat hrozby a reagovat na ně.

V oblasti souladu s legislativou Zabbix nabízí nástroje pro audity a sledování shody s normami, jako jsou GDPR nebo ISO/IEC 27001. Umožňuje detailní logování a uchovává záznamy o změnách v systému, což je klíčové při kontrolách a auditech kybernetické bezpečnosti.

4.7 Implementace Zabbixu: Praktické kroky

Aby byla implementace Zabbixu úspěšná, je vhodné dodržet několik klíčových kroků. Prvotní fáze zahrnuje přípravu infrastruktury, kde je důležité zajistit dostatečný výkon serveru, obzvláště pokud se plánuje monitorování velkého počtu prvků. Součástí příprav je také nastavení zálohovacích mechanismů pro uchování důležitých dat.

Po technické přípravě následuje vytvoření testovacího prostředí, kde lze ověřit konfiguraci a funkčnost monitorovacích šablon. Doporučuje se provést zátěžové testy, které pomohou zhodnotit, zda systém zvládne očekávanou zátěž a bude schopný efektivně reagovat na všechny požadavky.

Důležitou součástí implementace je konfigurace notifikací a reakcí. V této fázi se definují specifické události, při kterých se spustí automatizované reakce, jako je odeslání notifikací

nebo aktivace opravných skriptů. Správci systému by měli také nastavit eskalace incidentů, které vyžadují zásah vyšší úrovně podpory.

Závěrečnou fázi tvoří pravidelná údržba a aktualizace Zabbixu. Pravidelná aktualizace softwaru zajistí dostupnost nejnovějších funkcí a bezpečnostních záplat. Stejně tak je důležité provádět periodickou revizi konfigurace a analyzovat efektivitu monitorovacího systému, aby byla zajištěna optimální ochrana a stabilita IT infrastruktury.

5. Principy a architektura Zabbix

5.1 Základní principy Zabbixu

Zabbix je open-source monitorovací systém, který umožňuje sledování široké škály IT prostředků, včetně serverů, síťových zařízení, databází a aplikací. Jeho hlavní principy spočívají ve sběru, analýze a vizualizaci dat v reálném čase, což umožňuje efektivní dohled nad výkonností a stabilitou IT infrastruktury.

Mezi klíčové vlastnosti Zabbixu patří podpora agentového i bezagentového monitorování, což znamená, že systém může získávat data buď prostřednictvím speciálních agentů nainstalovaných na sledovaných zařízeních, nebo pomocí standardních protokolů jako SNMP, IPMI či HTTP. Další důležitou funkcí je flexibilní systém notifikací a eskalací, který umožňuje automatické upozornění na detekované problémy prostřednictvím e-mailu, SMS nebo API. Zabbix je navržen jako škálovatelný systém, takže jej lze využít jak v malých podnicích, tak i ve velkých korporacích s rozsáhlou infrastrukturou. Rovněž podporuje integraci s ITSM a DevOps nástroji, což umožňuje lepší správu incidentů a automatizaci reakcí na zjištěné problémy.

5.2 Architektura Zabbixu

Architektura Zabbixu je navržena tak, aby umožňovala efektivní monitorování a škálování podle potřeb uživatelů. Systém se skládá z několika klíčových komponent, které spolupracují na zajištění sběru, ukládání a analýzy monitorovacích dat.

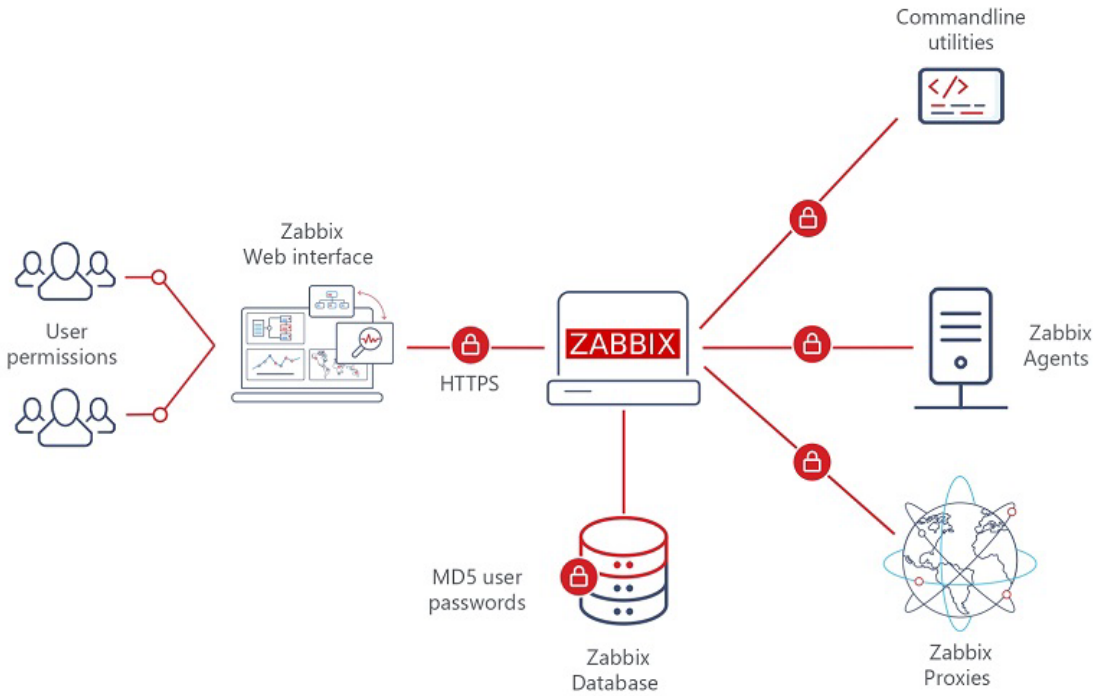
Základem je **Zabbix Server**, který funguje jako centrální bod monitorovacího systému. Zpracovává a ukládá data získaná od monitorovaných zařízení a uživatelům poskytuje přehled o stavu infrastruktury. Zabbix Server lze provozovat na různých linuxových distribucích, včetně Ubuntu, Debianu, CentOS a Red Hatu.

Další klíčovou komponentou je **Zabbix Proxy**, který usnadňuje distribuci monitorovacích úloh v rozsáhlých sítích. Proxy umožňuje efektivní správu dat ze vzdálených lokalit a snižuje zatížení hlavního serveru.

Pro sběr dat ze zařízení slouží **Zabbix Agent**, který je nainstalován přímo na sledovaných systémech. Tento agent je dostupný pro operační systémy jako Windows, Linux a macOS a umožňuje získávat detailní informace o výkonu a stavu monitorovaných zařízení.

Monitorovací data se ukládají do **databázového serveru**, který zajišťuje dlouhodobé uchování informací. Zabbix podporuje různé databázové systémy, například MySQL, PostgreSQL a Oracle.

Poslední důležitou součástí je **webové rozhraní**, které poskytuje uživatelům přístup k monitorovacím datům prostřednictvím přehledného a intuitivního prostředí. Díky němu mohou administrátoři snadno sledovat aktuální stav systémů, analyzovat historická data a nastavovat monitorovací politiky.



Obr. 5: Architektura Zabbix (zdroj: https://www.scmgalaxy.com/tutorials/what-is-zabbix/)

5.2.2 Tok dat v Zabbixu

Tok dat v Zabbixu začíná u monitorovaných zařízení, ze kterých jsou sbírána data pomocí agentů nebo síťových protokolů. Tato data jsou následně přenášena na Zabbix Server nebo Proxy, kde dochází k jejich analýze a vyhodnocení stavů. Pokud je zjištěn problém, systém automaticky generuje upozornění, které je odesláno administrátorům nebo dalším připojeným systémům. Výsledky monitorování jsou zobrazovány ve webovém rozhraní, kde je možné provádět další analýzu a konfiguraci systému.

5.3 Implementace a použití Zabbixu

Příklad nasazení Zabbixu v podniku zahrnuje několik klíčových scénářů. Mezi nejčastější případy použití patří **monitorování serverů**, kdy systém sleduje využití procesoru, operační paměti a síťového provozu. Dále je možné **analyzovat dostupnost služeb**, což umožňuje detekovat výpadky a reagovat na ně dříve, než ovlivní běžný provoz organizace. Výhodou Zabbixu je také možnost **automatizace reakcí**, kdy lze nastavit spuštění skriptů

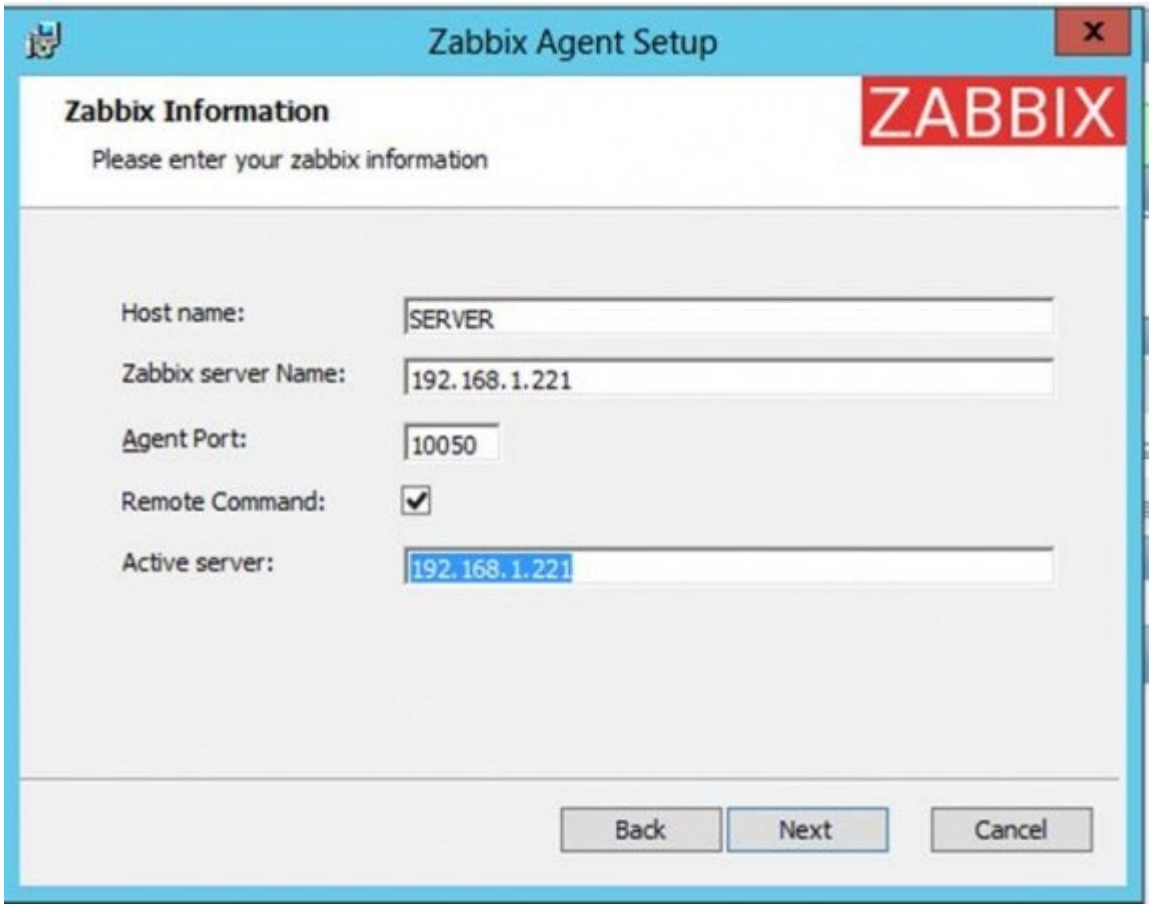
při dosažení určitých podmínek, což pomáhá rychle řešit běžné problémy bez nutnosti manuálního zásahu administrátorů.

6. Doporučené kroky pro implementaci Zabbixu

Implementace Zabbixu na serveru s distribucí Debian vyžaduje specifické kroky k zajištění stabilního a efektivního provozu monitorovacího systému.

- **Příprava serveru** – Nejprve je nutné zajistit, že server běží na aktuální verzi Debianu a jsou nainstalovány všechny potřebné aktualizace. Doporučuje se také nakonfigurovat firewall a zabezpečit SSH přístup.
- **Instalace databázového serveru** – Zabbix vyžaduje databázi pro ukládání dat. Nejčastěji se používá MySQL/MariaDB nebo PostgreSQL. Po instalaci je nutné vytvořit databázi a přidělit oprávnění.
- **Instalace Zabbix serveru a agentů** – Pomocí oficiálních repozitářů Zabbixu lze jednoduše nainstalovat Zabbix Server, Web Interface a Zabbix Agenty.

```
# wget https://repo.zabbix.com/zabbix/7.2/release/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.2+debian12_all.deb
# dpkg -i zabbix-release_latest_7.2+debian12_all.deb
# apt update
# apt install zabbix-server-pgsql zabbix-frontend-php php8.2-pgsql zabbix-apache-conf zabbix-sql-scripts zabbix-agent
# sudo -u postgres createuser --pwprompt zabbix
# sudo -u postgres createdb -O zabbix zabbix
# zcat /usr/share/zabbix/sql-scripts/postgresql/server.sql.gz | sudo -u zabbix psql zabbix
# systemctl restart zabbix-server zabbix-agent apache2
# systemctl enable zabbix-server zabbix-agent apache2
```



Obr. 6: Instalace Zabbix Agenta (zdroj: https://tamlx.wordpress.com/2016/01/21/how-to-install-zabbix-agent-and-add-windows-host-to-zabbix-monitoring-part-3/)

- **Konfigurace Zabbixu** – Po instalaci je třeba upravit konfiguraci souboru zabbix_server.conf, nastavit připojení k databázi a nakonfigurovat webové rozhraní.
- **Nastavení monitorovacích šablon** – Vytvoření a přizpůsobení šablon pro sledovaná zařízení zajistí efektivní monitorování.
- **Pravidelná údržba a aktualizace** – Aktualizace Zabbixu, databáze a operačního systému jsou klíčové pro zajištění bezpečnosti a stability.

7. Budoucí rozvoj a trendy

Zabbix se neustále vyvíjí, aby reflektoval moderní technologické požadavky a poskytoval pokročilé monitorovací funkce. Mezi nejvýznamnější trendy, které ovlivní budoucnost Zabbixu, patří:

- **Integrace s umělou inteligencí (AI)** – Prediktivní analýza využívající AI umožní přesnější detekci anomálií, predikci poruch a lepší řízení výkonu IT infrastruktury.
- **Rozšířená podpora pro IoT zařízení** – S nárůstem internetu věcí (IoT) se očekává, že Zabbix bude stále více využíván pro sledování těchto zařízení a jejich bezpečnostní kontrolu.
- **Vylepšená kybernetická bezpečnost** – Rostoucí počet kybernetických hrozeb vede k neustálému zlepšování bezpečnostních funkcí Zabbixu, jako jsou pokročilé metody detekce hrozeb a integrace s bezpečnostními platformami.
- **Zlepšená škálovatelnost a výkon** – S rozvojem velkých datových center a cloudových řešení je kladen důraz na optimalizaci výkonu a škálovatelnosti Zabbixu, aby mohl efektivně fungovat i v rozsáhlých IT infrastrukturách.

Díky těmto inovacím bude Zabbix i nadále jedním z klíčových nástrojů pro monitorování IT prostředí a zajištění jeho stability a bezpečnosti.

8. Závěr

Tato práce se zaměřila na problematiku provozního a bezpečnostního dohledu s využitím monitorovacího systému Zabbix. V teoretické části byly popsány základní principy dohledových systémů, jejich význam pro kybernetickou bezpečnost a legislativní požadavky, které musí organizace v této oblasti splňovat. Dále byly analyzovány různé možnosti monitorování, přínosy nepřetržitého dohledu a způsoby, jakými Zabbix umožňuje efektivní detekci a řešení incidentů.

V praktické části byl Zabbix testován na dvou noteboocích, kde byla provedena konfigurace systému, monitorovacích prvků a nastavení upozornění na incidenty. Testování ukázalo, že Zabbix umožňuje detailní sledování výkonu IT infrastruktury, detekci bezpečnostních hrozeb a automatizaci reakce na incidenty. Výsledky potvrdily, že správné nastavení monitorovacího systému může významně přispět k vyšší stabilitě a bezpečnosti IT prostředí.

Práce rovněž ukázala, že efektivní provozní dohled vyžaduje nejen vhodné technologické nástroje, ale také dobře definované postupy, pravidelné audity a průběžné vzdělávání administrátorů. Zabbix se ukázal jako výkonné a flexibilní řešení, které je vhodné jak pro malé podnikové sítě, tak i pro rozsáhlejší IT infrastruktury.

Nasazení dohledového systému, jako je Zabbix, umožňuje organizacím minimalizovat rizika spojená s kybernetickými hrozbami, zvýšit provozní efektivitu a zajistit soulad s legislativními požadavky. Vzhledem k neustále se vyvíjejícím bezpečnostním výzvám je důležité monitorovací systémy průběžně aktualizovat a přizpůsobovat novým hrozbám.

Z výsledků této práce vyplývá, že provozní a bezpečnostní dohled je klíčovým prvkem správy IT prostředí, který pomáhá organizacím zajistit stabilitu, bezpečnost a optimální výkon jejich systémů.

9. Literatura

Zabbix Documentation 6.0 [online]. Zabbix LLC, 2024. Dostupné z: https://www.zabbix.com/documentation

ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti. In: Sbírka zákonů České republiky. 2014. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

ČESKO. Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti. In: Sbírka zákonů České republiky. 2018. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection. Geneva: ISO, 2022.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST Special Publication 800-53 Rev. 5 – Security and Privacy Controls for Federal Information Systems and Organizations. Gaithersburg: NIST, 2020. Dostupné z: https://csrc.nist.gov/publications

BARTH, Rihards. Mastering Zabbix 6.0 – Professional Monitoring to Secure IT Infrastructure. Birmingham: Packt Publishing, 2023. ISBN 978-1803238567.

KOVÁŘ, Jan. Monitorovací nástroje v IT bezpečnosti [online]. Brno: VUT, 2021. Diplomová práce. Dostupné z: https://dspace.vutbr.cz/

Seznam Obrázků