

Návrh monitorování středně velké IT infrastruktury pro společnost Axians s.r.o.

Bc. Michal Owczarzy



Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav elektroniky a měření

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Bc. Michal Owczarzy
Osobní číslo:	A23514
Studijní program:	N1032A020003 Bezpečnostní technologie, systémy a management
Specializace:	Bezpečnostní technologie
Forma studia:	Kombinovaná
Téma práce:	Návrh monitorování středně velké IT infrastruktury pro společnost Axians s.r.o.
Téma práce anglicky:	Project of Monitoring of a Medium-Sized IT Infrastructure for Axians s.r.o.

Zásady pro vypracování

1. Specifikujte požadavky na systém dle potřeb společnosti Axians s.r.o.
2. Zpracujte přehled dostupných nástrojů pro monitorování IT infrastruktury.
3. Proveďte výběr vhodného nástroje.
4. Implementujte vybrané řešení v testovací infrastruktuře.
5. Ověřte funkčnost vybraného řešení a splnění požadavků zadavatele,

Seznam doporučené literatury:

1. TRAORÉ, Issa; AWAD, Ahmed a WOUNGANG, Isaac. Information security practices. 2017. ISBN 9783319489476.
2. Nathan Liefting, Brian Van Baekel. Zabbix 7 IT Infrastructure Monitoring. 2024. ISBN 9781801078979.
3. Zabbix: Enterprise Network Monitoring Made Easy Rihards Olups, Andrea Dalle Vacche, Patrik Uytterhoeven
4. VACCHE, Andrea Dalle a LEE, Stefano Kewan. Mastering Zabbix: monitor your large IT environment efficiently with Zabbix. Community experience distilled. Birmingham: Packt, 2013.
5. MUKHERJEE, Aditya. Network Security Strategies. Birmingham: Packt Publishing, Limited, 2020. ISBN 9781789801057.
6. MIŠUTKA, Tomáš; MALANÍK, David; UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ. FAKULTA APLIKOVANÉ INFORMATIKY a TOMAS BATA UNIVERSITY IN ZLÍN. FACULTY OF APPLIED INFORMATICS. Detekcia útočníkov a anomálií v sieti. 2022.
7. KINCL, Jan; MALANÍK, David; UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ. FAKULTA APLIKOVANÉ INFORMATIKY a TOMAS BATA UNIVERSITY IN ZLÍN. FACULTY OF APPLIED INFORMATICS. Zabezpečení a monitoring rozsáhlých IT infrastruktur. 2022.

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **29. listopadu 2024**

Termín odevzdání diplomové práce: **30. května 2025**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan



Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 29. listopadu 2024

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že

- odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení diplomové práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – diplomovou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na diplomové práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Diplomová práce se zaměřuje na návrh monitorování středně velké IT infrastruktury pro společnost Axians s.r.o. Cílem je specifikovat požadavky na monitorovací systém dle potřeb společnosti, zpracovat přehled dostupných nástrojů pro monitorování IT infrastruktury a vybrat nejvhodnější z nich. Následně je vybrané řešení implementováno v testovací infrastruktuře a ověřena jeho funkčnost a splnění požadavků zadavatele. Výsledkem práce je návrh efektivního monitorovacího systému, který pomůže s doručováním IT služeb společnosti Axians s.r.o.

Klíčová slova: Axians, Zabbix, Síťový monitoring

ABSTRACT

The thesis focuses on designing the monitoring of a medium-sized IT infrastructure for the company Axians s.r.o. The aim is to specify the requirements for a monitoring system according to the company's needs, to compile an overview of available tools for monitoring IT infrastructure, and to select the most suitable one among them. Subsequently, the chosen solution is implemented in a test infrastructure, and its functionality and fulfillment of the client's requirements are verified. The result of the work is a proposal for an effective monitoring system that will help in delivering IT services by Axians s.r.o.

Keywords: Axians, Zabbix, Network monitoring

Rád bych poděkoval své budoucí ženě Karolíně za dlouhodobou podporu nejen ve studiu, ale také v životě.

Chtěl bych také poděkovat Ing. Davidovi Malaníkovi Ph.D. za vedení této práce.

OBSAH

ÚVOD	13
CÍL PRÁCE.....	14
I TEORETICKÁ ČÁST.....	15
1 LITERÁRNÍ REŠERŠE	16
1.1 OBDOBNÉ PRÁCE	16
1.2 OFICIÁLNÍ DOKUMENTACE A ODBORNÁ LITERATURA.....	17
1.3 VÝZNAM ODBORNÝCH FÓR A KOMUNIT.....	18
1.4 ZÁVĚR LITERÁRNÍ REŠERŠE	18
2 PROSTŘEDÍ SPOLEČNOSTI AXIANS ICT CZ S.R.O	19
2.1 INFORMACE O SPOLEČNOSTI AXIANS ICT CZ S.R.O	19
2.2 IT PROSTŘEDÍ SPOLEČNOSTI AXIANS	19
3 POŽADAVKY SPOLEČNOSTI AXIANS.....	21
4 ANALÝZA MONITOROVACÍCH NÁSTROJŮ	24
4.1 PŘEHLED DOSTUPNÝCH NÁSTROJŮ	24
4.1.1 Nagios Core	24
4.1.2 Prometheus	26
4.1.3 ManageEngine OpManager.....	29
4.1.4 Site24x7	32
4.1.5 Icinga	34
4.1.6 SolarWinds Network Performance Monitor (NPM).....	37
4.1.7 PRTG Network Monitor	41
4.1.8 Datadog	44
4.1.9 Zabbix	47
4.2 ANALÝZA STÁVAJÍCÍCH ŘEŠENÍ	51
4.3 TABULKOVÉ SHRUTÍ ANALÝZY	53
4.4 SHRUTNÍ ANALÝZY	56
5 MONITOROVACÍ NÁSTROJ ZABBIX.....	58
5.1 ARCHITEKTURA ZABBIXU	58

II	PRAKTICKÁ ČÁST	60
6	VÝBĚR LABORATORNÍHO PROSTŘEDÍ	61
7	VIRTUÁLNÍ PROSTŘEDÍ	62
7.1	VYTVOŘENÍ VIRTUÁLNÍHO PROSTŘEDÍ	62
7.1.1	Vytvoření sítě ve virtuálním prostředí	62
8	INSTALACE NÁSTROJE ZABBIX	64
8.1	INSTALACE ZABBIX SERVERU	64
8.2	INSTALACE ZABBIX AGENTA NA OPERAČNÍM SYSTÉMU LINUX	66
8.3	PŘIDÁNÍ LINUXOVÉHO HOSTA NA ZABBIX SERVER	66
8.4	INSTALACE ZABBIX AGENTA NA OPERAČNÍM SYSTÉMU WINDOWS	67
9	AUTOMATICKÁ DETEKCE ZABBIX AGENTA V SÍTI	71
10	ZABEZPEČENÍ KOMUNIKACE MEZI AGENTEM A SERVEREM	73
11	VYTVÁŘENÍ METRIK	76
11.1	TVORBA POKROČILEJŠÍ METRIKY	78
12	SPOUŠTĚČE	79
12.1	UPOZORNĚNÍ POMOCÍ E-MAILU	81
13	BEZAGENTOVÉ MONITOROVÁNÍ	83
13.1	OCHRANA PŘED ÚTOKY DÍKY POUŽITÍ SNMPv3	84
13.2	NASTAVENÍ SNMPv3 NA AGENTOVÍ	85
13.3	MONITOROVÁNÍ HOSTA NA ZABBIX SERVERU POMOCÍ SNMP	86
14	NÁVRH ZABEZPEČENÍ DOPORUČENÉHO ŘEŠENÍ	88
14.1	RIZIKA	88
14.2	SÍŤOVÁ ARCHITEKTURA A PŘÍSTUPOVÁ POLITIKA	88
14.3	ZABEZPEČENÍ DATABÁZE	89
14.4	VYSOKÁ DOSTUPNOST	90
14.4.1	Předpoklady pro vysokou dostupnost	90
14.5	VYUŽITÍ PROXY SERVERŮ	91

15	OVĚŘENÍ FUNKČNOSTI VYBRANÉHO ŘEŠENÍ A SPLNĚNÍ POŽADAVKŮ	
	ZADAVATELE.....	93
	ZÁVĚR.....	94
	SEZNAM POUŽITÉ LITERATURY	95
	SEZNAM OBRÁZKŮ	102
	SEZNAM TABULEK	103
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	104
	SEZNAM PŘÍLOH.....	107

ÚVOD

Společně se společností Axians s.r.o. byla stanovena problematika této diplomové práce. Aktuálním problémem společnosti Axians s.r.o. je síťový monitoring pro středně velké infrastruktury. Prozatím společnost doručuje síťový monitoring jako službu pouze zákazníkům, kteří mají malé infrastruktury. Nástroj vybraný v této práci by měl společnosti Axians s.r.o. zjednodušit dodávání této služby. Tento nástroj by měl splňovat podmínky, které jsou uvedeny v sekci Cíl práce.

Práce bude zahrnovat aktuální situaci ohledně síťového monitoringu ve společnosti Axians s.r.o., a následně budou rozepsány jednotlivé požadavky na síťový monitoring u středně velkých zákazníků.

V této práci bude provedena také analýza trhu a porovnání nástrojů, které tyto požadavky mohou naplnit. Z těchto nástrojů bude vybrán jeden, který bude splňovat nejlépe tyto požadavky a bude pro společnost nejvýhodnější. Tento nástroj bude nasazen v laboratorních podmínkách a budou na něm otestovány jednotlivé funkce, které byly součástí požadavků.

CÍL PRÁCE

Cílem této práce je vytvořit návrh pro monitorování středně velké infrastruktury pro společnost Axians s.r.o. Tento návrh může zjednodušit monitoring u středně velkých zákazníků a otevřít tak nové možnosti spolupráce pro Axians s.r.o. Požadavky společnosti zahrnují: síťový monitoring, monitoring webových aplikací, vizualizaci metrik a alerting. Dále se společnost zaměří na finanční stránku produktu a na jednoduchost nasazení v zákaznickém prostředí.

Tato práce může rovněž sloužit jako návod pro síťové inženýry.

I TEORETICKÁ ČÁST

1 LITERÁRNÍ REŠERŠE

Ačkoliv je problematika monitorování středně velkých IT infrastruktur relativně nové téma, existuje řada dostupných zdrojů, které tuto oblast rozebírají z různých pohledů. Největší pozornost je v posledních letech věnována nástrojům s otevřeným zdrojovým kódem, jako jsou Zabbix, Nagios či Prometheus. Tyto nástroje nejen řeší komplexní problematiku monitoringu, ale také umožňují snadnou integraci a vysokou flexibilitu, což je klíčovým faktorem při jejich implementaci.

Kromě odborných článků a knih jsou důležitým zdrojem informací oficiální dokumentace a praktické zkušenosti publikované na odborných diskusních fórech. Díky tomu lze najít nejen teoretické informace, ale i reálné příklady nasazení jednotlivých nástrojů v praxi. Rešerše se proto zaměřuje na literaturu a zdroje, které se vztahují k metodám monitoringu, nástrojům a jejich aplikacím v různých typech infrastruktur.

1.1 Obdobné práce

Jednou z inspirativních prací je „Implementace monitoringu v podnikové infrastruktuře“ [1], která se zaměřuje na využití nástroje Nagios pro sledování stavu IT systémů. Autor v práci detailně popisuje způsoby konfigurace, nastavení upozornění a propojení s dalšími systémy, jako je Grafana pro vizualizaci dat. Tato práce přináší cenné poznatky, které budou významně využity při analýze potřeb monitoringu pro společnost Axians.

Další relevantní zdroj představuje kniha „Mastering Zabbix“ [2], která je zaměřena na hlubší pochopení tohoto nástroje. Kniha detailně popisuje jednotlivé komponenty Zabbixu, jejich konfiguraci a možnosti škálování. Tento zdroj bude užitečný při řešení otázek spojených s přizpůsobením monitoringu pro středně velkou infrastrukturu.

Inspirací mohou být také články, jako je „Comparative Study of Open-Source Monitoring Tools“ [3], které nabízejí porovnání nástrojů Prometheus, Zabbix a Nagios z hlediska jejich schopnosti zvládnout rozdílně komplexní infrastruktury. Autor zde klade důraz na výkonnostní metriky a schopnost škálování těchto nástrojů, což je klíčové při výběru vhodného řešení.

Dalším významným zdrojem je kniha „Practical Monitoring“ [4], která se zaměřuje na strategický přístup k monitoringu IT systémů. Autor zde zdůrazňuje důležitost definování

klíčových metrik a přizpůsobení monitorovacího systému specifickým potřebám organizace. Kniha je také cenným zdrojem doporučení, jak postupovat při zavádění monitoringu v prostředí s vysokou dostupností.

Relevantní jsou i publikace zaměřené na novější přístupy a technologie, například kniha „Cloud Monitoring: A Practical Approach“ [5], která popisuje monitorování distribuovaných cloudových infrastruktur a integraci s moderními nástroji pro analýzu dat. Tento zdroj přináší užitečné postřehy zejména v oblasti prediktivního monitorování a strojového učení.

Dále je vhodné zmínit knihu „Modern Monitoring: Real-Time Insights into IT Systems“ [6], která popisuje aktuální trendy v monitoringu a integraci moderních nástrojů, jako jsou Elastic Stack nebo Splunk. Tato kniha nabízí ucelený pohled na monitorování v komplexních prostředích.

1.2 Oficiální dokumentace a odborná literatura

Důležitým zdrojem bude oficiální dokumentace jednotlivých nástrojů. Například dokumentace k Prometheus [7] detailně popisuje, jak nastavit sběr metrik, vytvořit upozornění a propojit tento nástroj s Grafanou pro vizualizaci. Tento zdroj je nepostradatelný při pochopení, jak implementovat monitoring vhodný pro potřeby Axians s.r.o.

Podobně dokumentace Zabbixu [8] poskytuje podrobný pohled na konfiguraci a možnosti škálování. Obsahuje také příklady nasazení v různých typech infrastruktur, což je užitečné při vytváření vlastního návrhu. Například postupy pro nastavení distribuovaných agentů nebo detailní popisy integračních možností s jinými nástroji.

Dále byla využita kniha „Site Reliability Engineering: How Google Runs Production Systems“ [9], která nabízí pohled na best practices pro provoz kritických IT systémů. Tato publikace pomůže zejména v oblasti vysoké dostupnosti. Ačkoliv se kniha věnuje spíše softwarovému inženýrství, jsou zde popsány velmi detailně principy load balancingu, rozdělení provozu a celkově vysoké dostupnosti pro kriticky důležité systémy.

Další důležitou knihou je „The Art of Monitoring“ [10], která se věnuje praktickým aspektům monitoringu a vizualizace dat. Tento zdroj je užitečný zejména při návrhu metrik, vytvoření uživatelsky přívětivých dashboardů a integraci monitorovacích nástrojů do větších systémů. Autor zde také zdůrazňuje důležitost sledování trendů a predikce výkonových problémů.

1.3 Význam odborných fór a komunit

Velkou roli hrají fóra a online komunity, jako je Stack Overflow či Reddit, kde jsou sdíleny reálné zkušenosti s nasazením jednotlivých nástrojů. Tyto zdroje často obsahují řešení specifických problémů a mohou sloužit jako cenná inspirace pro navrhované řešení. Zejména komunity zaměřené na Prometheus a Grafanu poskytují bohatou databázi příkladů a praktických rad pro optimalizaci monitorování.

Dalším přínosným zdrojem jsou blogy a případové studie publikované na platformách, jako je Medium nebo DevOps.com. Tyto články často obsahují podrobné popisy implementačních kroků a reálných problémů, na které jejich autoři narazili během nasazování monitorovacích řešení.

1.4 Závěr literární rešerše

Tato literární rešerše přináší široký pohled na problematiku monitoringu IT infrastruktury a poskytuje relevantní informace, které budou využity při tvorbě návrhu pro společnost Axi-ans s.r.o. Kombinace odborných prací, knih, oficiální dokumentace a reálných zkušeností z praxe umožní vytvořit efektivní a prakticky použitelné řešení. Dodatečné zdroje, jako jsou online komunity, případové studie a nové publikace, mohou dále obohatit výsledný návrh monitorovacího systému. Široký záběr literatury zaručuje komplexní přístup k problematice a umožňuje identifikovat nejlepší dostupné postupy pro konkrétní potřeby společnosti.

2 PROSTŘEDÍ SPOLEČNOSTI AXIANS ICT CZ S.R.O

2.1 Informace o společnosti Axians ICT CZ s.r.o

Axians ICT CZ, s.r.o., je jedním z největších systémových integrátorů v České republice. V prosinci 2022 se společnost stala součástí nadnárodní skupiny VINCI Energies, která sdružuje společnosti z mnoha různých odvětví, zabývající se infrastrukturou a průmyslem. [11]

Axians ICT CZ poskytuje široké spektrum služeb v oblasti informačních a komunikačních technologií, mezi které patří:

- **Kybernetická bezpečnost:** Nabídka komplexních řešení pro ochranu dat a systémů před kybernetickými hrozbami.
- **Cloud and Data Center Infrastructure:** Poskytování služeb spojených s cloudovými technologiemi a datovými centry pro efektivní správu a ukládání dat.
- **Digital Workspace:** Řešení pro moderní digitální pracoviště, která podporují spolupráci a produktivitu zaměstnanců.
- **Managed Services:** Komplexní správa IT služeb, která umožňuje klientům soustředit se na jejich hlavní činnosti.

Společnost Axians ICT CZ zaměstnává více než 300 zkušených profesionálů, kteří navrhují, provozují a dodávají řešení v oblastech IT infrastruktury, podnikových informačních systémů, IT bezpečnosti, Průmyslu 4.0, vývoje softwaru, cloudových technologií a dalších.

Axians ICT CZ, s.r.o., je dceřinou společností skupiny VINCI Energies, která je součástí globálního koncernu VINCI. Tato struktura umožňuje společnosti čerpat z mezinárodního know-how a zdrojů, což jí umožňuje poskytovat špičková řešení přizpůsobená lokálním potřebám českého trhu [12].

2.2 IT prostředí společnosti Axians

Jak je již uvedeno výše, společnost Axians se primárně zaměřuje na poskytování IT služeb podle individuálních potřeb svých zákazníků. To znamená, že samostatně neprovozuje rozsáhlou infrastrukturu jako společnosti, které se zaměřují na provozování webových služeb nebo výrobu konkrétních produktů. Mezi takové společnosti lze zařadit například Škoda

Auto, Novartis nebo českou společnost Seznam.cz, která se specializuje na webové služby. Škoda Auto i Novartis jsou významnými zákazníky společnosti Axians, a proto jsou v tomto kontextu zmíněny.

Ačkoliv společnost Axians sama o sobě nevlastní rozsáhlou infrastrukturu, v její pobočce se nachází technická místnost vybavená třemi racky. Tyto racky slouží jak pro testovací prostředí, které umožňuje testování nových nástrojů pro zákazníky. Dále jsou zde umístěny části infrastruktury zákazníků, kteří z různých důvodů nemohou nebo nechtějí provozovat vlastní on-premise řešení. V těchto případech funguje Axians jako poskytovatel cloudových služeb. Toto řešení využívají především menší zákazníci, kteří nechtějí investovat do budování vlastní infrastruktury.

Z technického hlediska je v této infrastruktuře provozován rozsáhlý Zabbix server, který zajišťuje monitorování prostřednictvím více Zabbix proxy nasazených u zákazníků. Tyto proxy servery shromažďují data z jednotlivých zákaznických prostředí a přenášejí je do infrastruktury společnosti Axians. Následně zákazníci mohou prostřednictvím zabezpečeného připojení, například pomocí VPN, přistupovat ke svým datům a monitorovat stav své infrastruktury.

3 POŽADAVKY SPOLEČNOSTI AXIANS

Společnost Axians čelí výzvám při nabízení cloudových řešení středně velkým zákazníkům. Tyto firmy často preferují služby od významných poskytovatelů, známých jako "velká trojka" – Amazon Web Services, Microsoft Azure a Google Cloud. Důvodem je jejich pokročilá integrace a vysoká redundance, což zajišťuje spolehlivost a efektivitu jejich cloudových služeb.

Mnohé středně velké a velké společnosti provozují virtualizovaná řešení ve vlastních datových centrech nebo využívají cloudové služby zmíněných poskytovatelů. V tomto kontextu má Axians specifické požadavky na platformu pro monitorování IT infrastruktury těchto společností.

Požadavky na monitorovací platformu:

- **Komplexní monitoring:** Platforma by měla efektivně monitorovat všechny prvky IT infrastruktury, přičemž využití protokolu SNMP je preferováno díky odborným znalostem specialistů společnosti Axians.
- **Upozorňování na incidenty:** Systém by měl být schopen zasílat upozornění prostřednictvím e-mailu nebo SMS, aby bylo možné rychle reagovat na technické problémy v infrastruktuře. Součástí tohoto bodu je také přiřazování závažností jednotlivým událostem na síti. V tomto případě společnost Axians požaduje minimálně 5 kategorií závažností.
- **Vizualizace dat:** Platforma by měla nabízet přehledné a uživatelsky přívětivé vizualizace, které umožňují managementu snadno interpretovat monitorovaná data. Pokud samotný nástroj nedisponuje vizualizacemi, jako jsou grafy či řídicí panely (dashboards), musí alespoň umožňovat integraci s řešením, které tuto funkcionalitu poskytuje. Mezi vizualizačními nástroji společnost Axians preferuje Grafanu, Riverbed Portal nebo Splunk.
- **Open-source řešení:** Open-source řešení jsou preferována zejména kvůli své nákladové efektivitě, což výrazně přispívá ke zvýšení konkurenceschopnosti společnosti Axians. Použití nástrojů s otevřeným zdrojovým kódem umožňuje snížit pořizovací i provozní náklady, čímž se zvyšuje atraktivita těchto řešení pro zákazníky. Nicméně, sa-

motná nulová pořizovací cena není jediným faktorem; velký význam má také možnost profesionální podpory. Axians vyžaduje, aby vybraný nástroj poskytoval zákazníkům možnost přikoupení odborné podpory od vývojářů nebo oficiálních partnerů. Toto zajišťuje, že i při využití open-source řešení mohou zákazníci dosáhnout rychlého řešení problémů a mít k dispozici asistenci při implementaci či údržbě systému.

- **Vysoká dostupnost:** Platforma musí podporovat vysoce dostupnou architekturu (high-availability), která zajišťuje nepřetržitý provoz a odolnost vůči výpadkům – to je zásadní zejména u primárních monitorovacích systémů, kde je klíčová kontinuita služeb. Co se týče technických specifikací, společnost Axians požaduje, aby bylo dosaženo úrovně SLA minimálně 99%.

SLA, neboli Service Level Agreement, je smlouva o úrovni poskytovaných služeb, ve které jsou explicitně vymezeny požadavky na dostupnost, výkonnost, reakční doby a další důležité metriky. Tato dohoda slouží jako záruka, že poskytovatel zajistí definovanou úroveň kvality a spolehlivosti provozu systému. V praxi to znamená, že systém musí být funkční a dostupný pro uživatele alespoň 99% času. V případě, že poskytovatel nedodrží sjednané parametry, mohou klienti mít nárok na kompenzace nebo jiné nápravné opatření podle podmínek SLA.

Z důvodu, že tento nástroj bude nasazovat a podporovat primárně společnost Axians, bude SLA uzavřeno s Axians jako poskytovatelem služeb. To znamená, že smlouva o úrovni poskytovaných služeb bude formulována tak, aby chránila zákazníka tím, že Axians přebírá odpovědnost za dodržení předem definované úrovně dostupnosti a kvality služeb. V případě, že by služba neodpovídala sjednaným parametrům (minimálně 99% dostupnosti), má zákazník možnost uplatnit nápravná opatření nebo kompenzace, jak je stanoveno ve smlouvě.

- **Kybernetická bezpečnost:** Řešení musí být navrženo s důrazem na bezpečnost a využívat moderní šifrovací metody a bezpečnostní architekturu, aby byla zajištěna ochrana citlivých dat. Z technických parametrů společnost Axians vyžaduje zabezpečenou komunikaci mezi jednotlivými uzly systému. Tuto bezpečnost lze dosáhnout buď pomocí digitálních certifikátů, které jsou nainstalovány na obou stranách komunikace, nebo pomocí předem sdíleného klíče (PSK). Oba přístupy poskytují ochranu přenášených

dat proti odposlechu a neoprávněným zásahům. Kromě toho Axians očekává, že bude navržen bezpečnostní koncept celého systému z pohledu sítě.

4 ANALÝZA MONITOROVACÍCH NÁSTROJŮ

4.1 Přehled dostupných nástrojů

Pro analýzu bylo vybráno devět monitorovacích nástrojů, které by mohly uspokojit požadavky Axians na monitoring středně velké IT infrastruktury. Nástroje byly vyhledány tak, aby představovaly konkurenci nejen z pohledu funkcionality, ale také z hlediska licenční politiky a provozních nákladů.

V následujících částech textu jsou podrobně popsány vlastnosti jednotlivých platform. Každý nástroj je analyzován s ohledem na jeho klíčové výhody a omezení, přičemž je kladen důraz na aspekty důležité pro Axians, které jsou zmíněny výše v této práci. Tyto informace budou následně použity jako základ pro porovnání a závěrečné doporučení.

4.1.1 Nagios Core

Nagios Core je modulární open-source nástroj s dlouhou historií (první vydání v roce 1999) sloužící k komplexnímu dohledu nad infrastrukturou [13]. Umožňuje monitorovat dostupnost a výkon různých služeb, serverů a síťových zařízení.

- **Komplexní monitoring:** Nagios Core umožňuje monitorovat servery, operační systémy i síťová zařízení a podporuje jak aktivní dotazování, tak pasivní příjem dat. Pomocí vestavěných pluginů a rozšíření lze Nagios Core monitorovat standardní metriky přes protokol SNMP (včetně SNMPv1, SNMPv2c i SNMPv3 s autentizací a šifrováním) [13]. Dále využívá protokoly pro out-of-band management jako je IPMI, aplikační rozhraní JMX pro Javu a Windows systémy se monitorují přes WMI – například prostřednictvím agentů jako NSClient++ [13]. Kromě toho lze sledovat síťový provoz (např. NetFlow a další flow protokoly, typicky s pomocí doplňku Nagios Network Analyzer) a využít bohatou knihovnu více než 4 000 komunitních pluginů, což zaručuje podporu širokého spektra zařízení a metrik [13].
- **Upozorňování na incidenty:** Notifikační systém v Nagios Core umožňuje vytvářet komplexní upozorňovací pravidla s možností definovat různé kategorie závažnosti. Administrátor definuje kontakty a eskalační matice, čímž lze specifikovat, zda se mají upozornění zasílat při stavu „WARNING“ (varování), „CRITICAL“ (kritický výpadek) nebo „RECOVERY“ (obnovení) [13]. Systém podporuje zasílání upozornění pro-

střednictvím e-mailu (např. pomocí lokálního MTA či SMTP) a lze využít i externí příkazy pro další kanály, jako jsou SMS přes SMS gateway nebo GSM modem, paging či instant messaging [13].

- **Vizualizace dat:** Tento nástroj také poskytuje webové rozhraní zaměřené zejména na aktuální status monitorovaných objektů – zobrazuje přehled hostů, jejich stavy, historii výpadků a notifikací. Nativně však nenabízí pokročilé grafické dashboardy. Pro tvorbu pokročilých grafů a vizualizaci výkonových dat se typicky nasazuje doplněk PNP4Nagios, který ukládá časové řady do RRD databází a generuje historické grafy CPU, paměti a dalších metrik (Nagios Enterprises, 2023). Alternativně lze Nagios integrovat s nástroji jako Grafana, kde se exportovaná data (např. do Graphite či InfluxDB) následně zobrazují pomocí moderních dashboardů. Komerční verze Nagios XI již obsahuje vestavěné dashboardy a reporty, což výrazně zjednodušuje vizualizaci dat a umožňuje vytváření vlastních přehledových panelů (Nagios Enterprises, 2023).
- **Open-source řešení:** Jelikož je Nagios Core distribuován pod licencí GPL, jsou pořizovací náklady minimální. Podpora vychází primárně z komunity, což pro některé firmy může znamenat nedostatek oficiální profesionální podpory, nicméně existují komerční verze či služby třetích stran, které tento nedostatek eliminují [13].
- **Vysoká dostupnost:** Nagios Core sám o sobě nemá vestavěný clustering a obvykle běží jako jedna instance. V praxi lze dosáhnout vysoké dostupnosti provozem dvou identických Nagios serverů v aktivně-pasivním režimu s využitím nástrojů jako DRBD a Pacemaker, kdy v případě výpadku primárního serveru převezme monitoring sekundární instance. K dosažení plného řešení pro HA se někdy využívá také rozdělené monitorování s více nezávislými instancemi spravovanými centrální nadstavbou, jako je například Nagios Fusion [14].
- **Kybernetická bezpečnost:** Z hlediska bezpečnosti standardní instalace Nagios Core komunikuje nezašifrovaně – webové rozhraní je dostupné přes HTTP a agenty (např. NRPE) používají nezabezpečené protokoly. Pro zvýšení bezpečnosti se doporučuje provozovat webové rozhraní na Apache nebo Nginx se zapnutým TLS (HTTPS) a omezit přístup pomocí souborů .htaccess. Pro sběr dat je třeba nastavit SNMPv3 místo SNMPv2c, což umožňuje využití autentizace a šifrování (například pomocí AES a

SHA). Novější verze NRPE (např. NRPE 3) podporují šifrování komunikace pomocí SSL/TLS a mohou využít X.509 certifikáty pro ověřování serveru i klienta, čímž se zabrání útokům typu man-in-the-middle [15]. Nicméně samotné zabezpečení v jádře Nagios Core není integrováno, a proto je nutné tuto funkcionalitu zajistit dodatečnými bezpečnostními opatřeními (VPN, tunelování) [14].

4.1.2 Prometheus

Prometheus je moderní monitorovací systém open-source, spravovaný Cloud Native Computing Foundation (CNCF). Je navržen zejména pro ukládání metrik jako časových řad (time-series data).



Obrázek 4.1 Logo monitorovacího nástroje Prometheus [7]

- **Komplexní monitoring:** Prometheus primárně pracuje na principu pull modelu – v pravidelných intervalech dotazuje tzv. exportéry či instrumentované aplikace a stahuje od nich metriky. Díky široké škále dostupných exportérů je Prometheus schopen pokrýt mnohé oblasti monitoringu, které jsou běžně poskytovány tradičními nástroji. Například pro síťové prvky a servery využívá oficiální SNMP Exporter, který umožňuje dotazovat se při použití protokolu SNMP a jednotlivých OID – přičemž podporuje jak standardní SNMP verze, tak i SNMPv3, jež zahrnuje autentizaci a šifrování dat [16]. Pro prostředí Java je k dispozici nativní JMX Exporter, který dokáže číst metriky přímo z JMX (Java Management Extensions) rozhraní JVM. JMX Exporter lze nainstalovat jako Java Agent nebo samostatný proces, což umožňuje monitorovat aplikace běžící na virtuálním stroji JVM. Pro Windows systémy existuje Windows Exporter (dříve WMI Exporter), který sbírá metriky pomocí Performance Counters a WMI dotazů a zpřístupňuje je Prometheusu. Pro hardware senzory pak slouží IPMI Exporter, jež umožňuje dotazovat IPMI rozhraní základních desek. Kromě těchto klíčových

exportérů má Prometheus k dispozici desítky dalších, které pokrývají databáze, fronty, kontejnery, cloudové služby a další prostředí – například Node Exporter pro OS Linux nebo Blackbox Exporter pro syntetické testy dostupnosti. Přestože Prometheus neumí nativně zpracovávat NetFlow, lze použít Flow Exporter nebo integraci s projektem Flowlogs-Pipeline, která transformuje NetFlow/IPFIX statistiky na metriky. Celkově je Prometheus optimalizován pro numericé time-series, což umožňuje detailní analýzu výkonu, počtů požadavků apod., i když není primárně určen pro zpracování logů či událostí (pro tento účel se v CNCF ekosystému často nasazuje Fluentd/Loki).

- **Upozorňování na incidenty:** Samotný Prometheus provádí sběr a vyhodnocení metrik, avšak upozorňovací mechanismus je realizován pomocí samostatné komponenty zvané Alertmanager. Uživatel definuje v nástroji alerting rules – tedy podmínky nad metrikami, například příliš vysoké zatížení CPU. Pokud tato pravidla vyhodnotí anomálii, Prometheus odešle alert do Alertmanageru, který dále zajišťuje doručení upozornění správným kanálem. Podporovány jsou různé integrační kanály: e-mail (prostřednictvím SMTP), služby pro on-call notifikace jako PagerDuty nebo OpsGenie, chatovací platformy (Slack, Microsoft Teams) a obecné web hooky. Alertmanager také umožňuje definovat šablony a skupiny alertů, díky čemuž lze související události aggregovat do jedné zprávy. Závažnost alertů se řeší pomocí labelů – například label severity může mít hodnotu critical či warning, podle čehož Alertmanager aplikuje specifická pravidla (například kritické alerty odeslat i formou SMS, méně závažné jen e-mailem). Alertmanager dále podporuje funkce silencing (dočasné potlačení známých alertů) a inhibici (např. pokud je celý uzel nedostupný, individuální alerty jeho služeb se potlačí). Pokud běží více instancí Prometheus paralelně, Alertmanager má vestavěnou deduplikaci – ze shromážděných alertů odešle notifikaci pouze jednou [16].
- **Vizualizace dat:** Samotný Prometheus obsahuje jednoduchý webový prohlížeč – tzv. Prometheus Expression Browser, který umožňuje základní zobrazení grafů pro ověření dotazů. Avšak v reálné produkci se téměř vždy využívá vizualizační nástroj Grafana. Prometheus je plně podporován v Grafaně jako datový zdroj, který umožňuje tvorbu interaktivních dashboardů, panely a přehledy s aktualizacemi v reálném čase. Existují dokonce hotové Grafana dashboardy pro populární exportéry, například Node Exporter, což usnadňuje nasazení. Kromě Grafany lze využít také Console templates

(jednoduché HTML šablony) v Prometheus, nicméně hlavním nástrojem vizualizace zůstává Grafana, nebo alternativně Chronograf či jiné nástroje podporující PromQL dotazy. Data v Prometheus jsou uložena jako časové řady s vysokým rozlišením, což je vhodné pro grafy trendů, heatmapy a analýzu historických dat. Prometheus sám však tradiční reporty (např. PDF sestavy) nemá – ty se obvykle realizují integrací s jinými reportovacími nástroji [17].

- **Open-source řešení:** Prometheus je zcela open-source, distribuovaný pod licencí Apache 2.0. Projekt má aktivní a rychle se rozvíjející komunitu přispěvatelů, spravovanou oficiálně v rámci CNCF. Pravidelné aktualizace a bohatá dokumentace [18] přispívají k velmi nízkým pořizovacím nákladům. K dispozici jsou také komerční podpůrné služby od specializovaných firem (např. Grafana Labs nebo managed služby jako Amazon Managed Prometheus), což umožňuje získat profesionální podporu při potřebě. Výhodou open-source charakteru je také nulová licenční cena a možnost přizpůsobení bez omezení počtu monitorovaných metrik – škálování je omezeno pouze výkonem hardwaru [18].
- **Vysoká dostupnost:** Prometheus se obvykle nasazuje v redundanci – doporučuje se spustit dvě nebo více identických instancí, které shromažďují stejná data nezávisle. Alerty se posílají do Alertmanageru, který má vestavěnou deduplikaci a je schopen běžet v režimu aktiv-aktiv pomocí gossip protokolu pro výměnu informací mezi uzly (Prometheus Authors, 2023). Protože každý Prometheus server vlastní svou lokální TSDB (Time Series Database), nedochází ke sdílení dat mezi instancemi. Pro horizontální škálování a dlouhodobou úschovu dat se však využívají projekty jako Thanos nebo Cortex, které umožňují distribuované ukládání metrik a dotazování napříč více Prometheus servery. To pomáhá eliminovat single point of failure a zvyšuje spolehlivost monitoringu [19].
- **Kybernetická bezpečnost:** Prometheus jako moderní nástroj podporuje zabezpečení komunikace pomocí TLS. Lze jej nasadit za reverzním proxy s HTTPS nebo přímo s TLS, což zajišťuje šifrovanou komunikaci jak pro webové UI, tak pro API. Exportéry obvykle naslouchají na lokálních portech a mohou být chráněny firewally. Pro sběr dat je vhodné používat SNMPv3, které umožňuje zabezpečenou autentizaci a šifrování, a v

případě potřeby je možné nastavit také základní autentizaci nebo TLS klientské certifikáty, aby se zabránilo neoprávněnému přístupu (Prometheus Authors, 2023). Přestože Prometheus nemá vestavěný detailní audit log, lze generované alerty a interakce přes Alertmanager sledovat, a existují doplňky (např. Prometheus Operator) pro auditovací účely. S ohledem na architekturu microservices je Prometheus často nasazován ve vysoce zabezpečených clusterových prostředích, například v Kubernetes, kde veškerá komunikace probíhá uvnitř chráněné sítě [20].

4.1.3 ManageEngine OpManager

ManageEngine OpManager (od společnosti Zoho Corporation) je uzavřený komerční nástroj určený pro jednotné monitorování sítí a serverů [21].

- **Komplexní monitoring:**

Pro monitoring síťového provozu OpManager integruje tzv. Flow collector, které dokážou přijímat a analyzovat data z různých protokolů – NetFlow, sFlow, jFlow nebo IPFIX. Tyto funkce jsou často dostupné v rozšířené verzi OpManager Plus nebo prostřednictvím propojení s produktem NetFlow Analyzer. Dále OpManager monitoruje aplikační dostupnost – pomocí pluginů lze ověřovat dostupnost webových stránek, databází, LDAP serverů apod. Všechny nasbírané metriky jsou ukládány do vestavěné databáze, přičemž novější verze využívají PostgreSQL jako interní databázi [21]. U hardwarových senzorů je možné pomocí SNMP rozhraní získávat informace o teplotách, stavu ventilátorů a napájecích stavech – například monitoring systémů Dell iDRAC či HPE iLO je oficiálně podporován [21]. Pro monitorování virtualizace jsou pak k dispozici integrace s VMware vCenter a Hyper-V, které prostřednictvím API sledují stav VM a hostitelů. Díky šablonám a discovery modulům dokáže OpManager rychle pokrýt heterogenní prostředí bez nutnosti manuální konfigurace každé metriky [21].

- **Upozorňování na incidenty:** OpManager obsahuje propracovaný systém alarmů a notifikací. Při překročení definovaných prahových hodnot (například využití CPU, ztrátovost linky apod.) nebo při výpadku zařízení generuje OpManager alarm, kterému je přiřazena závažnost – v terminologii OpManageru se často rozlišuje mezi stavy jako

"Trouble"(střední závažnost) a "Critical"(vysoká závažnost) [22]. Alarmy se zobrazují v konzoli a spouštějí tzv. Notification Profiles, které definují typ oznámení. Mezi podporované metody patří zaslání e-mailu, odeslání SMS (přes konfigurovatelné SMS brány nebo externí GSM modem), spuštění vlastního skriptu či příkazu (umožňující integraci do interních systémů, například vytvoření ticketu), odeslání SNMP trapu, vytvoření zprávy do chatových aplikací (např. Microsoft Teams, Slack) a vyvolání webhooku pro HTTP volání [22]. Uživatelé si mohou přiřadit notifikační profil k uživatelským skupinám tak, aby každý dostával upozornění odpovídající jeho zodpovědnosti – například síť aři obdrží pouze notifikace týkající se síťových incidentů, zatímco serveroví administrátoři budou informováni o problémech se servery [22].

- **Vizualizace dat:** OpManager poskytuje bohaté grafické rozhraní přístupné přes webový prohlížeč. Hlavní konzole nabízí dashboardy, které lze upravit metodou drag-and-drop, a obsahují grafy vytížení CPU, mapy sítě, seznamy top N vytížených linek apod. Nástroj obsahuje předdefinované šablony pro dashboardy (například pro datacentrum, síť, servery) a zároveň umožňuje vytváření vlastních panelů. Data jsou vizualizována v reálném čase – například každý monitorovaný objekt má graf s historií výkonových metrik, získaných pomocí SNMP a WMI. OpManager má také modul Network Maps, který automaticky generuje topologické mapy na základě LLDP/CDP, přičemž aktuální stav zařízení se zobrazuje pomocí barevného indikátoru (zelená pro normální stav, červená pro problém). Dále jsou k dispozici reporty – jak plánované, tak ad-hoc, které lze exportovat do formátů PDF nebo CSV a automaticky zasílat e-mailem. Pokud by bylo požadováno, lze data také exportovat prostřednictvím REST API do externích vizualizačních nástrojů, například Grafany [23].
- **Open-source řešení a podpora:** ManageEngine OpManager je proprietární software, který je nabízen formou licencí – typicky dle počtu monitorovaných zařízení nebo senzorů. Výhodou je, že dodavatel (Zoho/ManageEngine) poskytuje kompletní technickou podporu, pravidelné aktualizace a asistenci při implementaci. OpManager není open-source, což znamená vyšší pořizovací náklady, ale zároveň zaručuje stabilitu, konzistentní aktualizace a komplexní podporu, včetně různých úrovní SLA. Dokumentace je rozsáhlá a dostupná online, což usnadňuje nasazení a provoz. Pro organizace, které vyžadují plnou kontrolu nad kódem a otevřený vývoj, však není OpManager

vhodný – je to čistě komerční produkt [24].

- **Vysoká dostupnost:** Pro zajištění nepřetržitého provozu monitoringu disponuje OpManager vestavěnou funkcionalitou failover. Lze konfigurovat primární server a záložní (Standby server), přičemž primární server neustále replikuje potřebná data do záložního – včetně databáze, kterou OpManager podporuje jak v řešení PostgreSQL, tak i MS SQL Failover Clusteru. Pokud primární server selže (například kvůli hardwarové poruše nebo výpadku operačního systému), záložní server automaticky detekuje výpadek (prostřednictvím heartbeat monitoru) a převezme monitoring a odesílání alertů. Po obnovení primárního lze provést failback. Tato HA funkce je dostupná převážně v Enterprise edici OpManageru. Kromě failoveru lze nastavit i Distributed Monitoring – pomocí Remote Probe instalací lze sbírat data z oddělených sítí a posílat je do centrálního serveru, přičemž vzdálené komponenty dokážou dočasně cacheovat data v případě přerušení spojení [25].
- **Kybernetická bezpečnost:** OpManager běží jako webová aplikace, typicky na vestavěném servletovém serveru nebo IIS, a přístup do webového uživatelského rozhraní lze zabezpečit pomocí HTTPS (s možností nahrání vlastního SSL certifikátu). Správa přístupu je realizována prostřednictvím role-based access control (RBAC) – administrátor může definovat, kteří uživatelé mají přístup k jednotlivým zařízením a jaké akce mohou provádět. OpManager je možné integrovat s Active Directory pro centralizované ověřování a podporuje také SAML autentizaci pro Single Sign-On. Komunikace s monitorovanými zařízeními probíhá pomocí zabezpečených protokolů – SNMPv3 s AES/MD5 je preferován pro síťová zařízení, zatímco WMI komunikace využívá protokol DCOM/WinRM, což je zabezpečeno prostřednictvím Windows autentizace (NTLM/Kerberos). Pro SSH přístupy lze využít šifrované pověření, které je uloženo v aplikaci. Citlivá hesla a další přihlašovací údaje se ukládají šifrovaně v databázi, přičemž je možno nastavit Master Key pro ještě vyšší úroveň ochrany. OpManager rovněž loguje uživatelské akce pro účely auditu, což usnadňuje sledování změn a případných bezpečnostních incidentů. Celkově umožňuje OpManager dosáhnout vysoké úrovně zabezpečení monitoringu, pokud je správně nakonfigurován a pravidelně aktualizován [26].

4.1.4 Site24x7

Site24x7 je cloudová SaaS platforma od Zoho Corporation (sesterský produkt ManageEngine) určená ke komplexnímu monitorování webových stránek, aplikačních výkonů i infrastruktury [27].

- **Komplexní monitoring:** Site24x7 kombinuje agentové i bezagentové monitorování. Pro fyzické i virtuální servery poskytuje Site24x7 vlastní agenty – malé demony instalované na operačním systému, které sbírají metriky jako jsou využití CPU, paměť, diskové operace nebo běžící procesy, a tyto údaje odesílají šifrovaně do cloudu. Pro síťová zařízení a případy, kdy není možné nebo vhodné instalovat agenta, používá Site24x7 tzv. On-Premise Poller. Jedná se o softwarovou sondu umístěnou v lokální síti zákazníka, která zajišťuje dotazování pomocí protokolů SNMP (včetně SNMPv1, SNMPv2c a SNMPv3) a WMI a předává nasbíraná data do cloudové služby (Site24x7, 2023). Díky tomuto přístupu je možné monitorovat širokou škálu zařízení, jako jsou switche, routery, tiskárny a další síťové prvky. Kromě toho nativně podporuje monitorování cloudových služeb (například AWS, Azure, GCP) prostřednictvím příslušných API, kdy například sleduje využití zdrojů v AWS pomocí CloudWatch metrik. Pro pokročilejší monitorování hardwarových senzorů jsou podporovány protokoly jako SNMP či REST API zařízení (Dell iDRAC, HPE iLO, IBM IMM), případně lze využít i Redfish API, se kterým tento On-Premise Poller komunikuje [28].
- **Upozorňování na incidenty:** Jako SaaS služba poskytuje Site24x7 robustní systém upozornění, který je plně hostovaný. Uživatelé definují pravidla notifikací (tzv. Notification Profiles) a seznam kontaktů. Platforma nabízí více kanálů upozornění, přičemž základním kanálem je e-mail. Dále podporuje SMS, hlasové volání, push notifikace zasílané prostřednictvím mobilní aplikace Site24x7 a integraci s IM systémy (např. Slack, Microsoft Teams, Jabber) [29]. Tyto kanály lze kombinovat – například při kritickém výpadku lze současně odeslat SMS, spustit hlasový alert a poslat e-mail. Notifikační systém umožňuje nastavení časových oken (například v noci zasílat pouze kritické alerty) a eskalačních pravidel, kdy pokud první upozornění není potvrzeno, dojde k odeslání dalšího upozornění na vyšší úroveň [29]. Kromě toho systém opakuje notifikace periodicky, dokud není incident vyřešen. V rámci webového portálu je k

dispozici přehled aktuálních alarmů, který zobrazuje jejich závažnost a stav. Site24x7 také nabízí možnost integrace se systémy ITSM, jako je ServiceNow nebo Zoho ServiceDesk, což umožňuje automatické vytváření tiketů při výpadcích [29].

- **Vizualizace dat:** Site24x7 disponuje moderním webovým portálem, kde po přihlášení uživatelé vidí centrální dashboard, zobrazující celkové zdraví monitorovaných skupin, například procentuální dostupnost (uptime) a aktuální stav alarmů. Uživatelé mohou vytvářet vlastní dashboardy kombinující různé widgety – například grafy vytížení CPU, interaktivní mapy světa s lokalitami monitoringu a latencí, tabulky dostupnosti či top N analýzy [30]. Grafy jsou interaktivní, lze v nich měnit časová období (například poslední hodiny, dny, měsíce) a zobrazovat podrobné statistiky (průměry, max hodnoty). Platforma také nabízí speciální Network Traffic Dashboard pro analýzu síťového provozu, kde jsou vizualizovány statistiky jako top talkers a top protokoly. Kromě toho umožňuje generovat reporty SLA, které lze automaticky distribuovat e-mailem. Pro mobilitu je k dispozici mobilní aplikace pro Android a iOS, která umožňuje v reálném čase sledovat dashboardy a grafy [30]. I když integrace s externími vizualizačními nástroji, jako je Grafana, není typicky nutná, existuje REST API, které umožňuje případné exportování dat do jiných systémů.
- **Open-source řešení a podpora:** Site24x7 je proprietární SaaS služba – její zdrojový kód není veřejně přístupný a licencování probíhá formou předplatného, typicky podle počtu monitorovaných jednotek nebo objemu zpracovávaných dat (Site24x7, 2023). Uživatel tedy nedisponuje možností software sám modifikovat nebo rozšiřovat, ale získává hotový produkt s minimální administrativní režijní zátěží. Podpora je poskytována přímo Zoho/ManageEngine v rámci předplatného, s možností online helpdesku 24/7 (v závislosti na zvolené úrovni služby). Jako cloudová služba má Site24x7 výhodu, že se stará o veškeré aktualizace, což znamená nižší náklady na interní správu. Nicméně zákazník musí počítat s tím, že data se fyzicky nacházejí u dodavatele, což může být významné z hlediska důvěry a souladu s firemními bezpečnostními politikami [31].
- **Vysoká dostupnost:** Jako cloudová platforma je Site24x7 navržena s vysokou dostupností v rámci své infrastruktury – Zoho provozuje službu ve více geografických oblastech a díky internímu clusteringu a load balancingu dosahuje SLA, která bývá

často deklarována jako 99,9%. On-Premise Poller, který sbírá data z lokálních sítí, dokáže pracovat i offline – dočasně ukládá data a po obnovení spojení je nahrává do cloudu. To zajišťuje, že krátké výpadky internetového připojení neznamenaají ztrátu dat [32]. Pro zvýšení redundance lze nasadit více pollerů v různých síťových segmentech, což minimalizuje riziko, že selže spojení ke všem zařízením. Celkově tedy Site24x7 poskytuje vysokou dostupnost jako službu, kdy Axians nemusí budovat vlastní HA cluster monitoringu [32].

- **Kybernetická bezpečnost:** Bezpečnost u Site24x7 je řešena dvouvrstevně – jak na straně klienta, tak na straně cloudu. Komunikace mezi On-Premise Pollerem, agenty a cloudovou platformou je šifrována pomocí TLS 1.2/1.3. Poller se autentizuje unikátním klíčem, aby se zabránilo neoprávněnému přístupu. Přístup do webového portálu je chráněn uživatelským účtem s možností dvoufaktorové autentizace, přičemž Zoho podporuje OTP či SAML integraci pro Single Sign-On. Každý uživatel může mít přiřazenu konkrétní roli (například „Read-only“ pro manažery nebo „Operator“ pro administrátory) a monitorované položky lze přiřadit k určitým byznysovým jednotkám, což umožňuje oddělení přístupu dle zodpovědnosti. Poller využívá SNMPv3 a WMI – SNMPv3 zabezpečuje komunikaci pomocí autentizačních údajů a šifrovacího klíče, zatímco WMI využívá Windows autentizaci (NTLMv2/Kerberos). Citlivé údaje, například hesla ke SNMP, jsou ukládány zašifrovaně v databázích Zoho, které splňují standardy ISO 27001 a SOC 2. Kromě toho Site24x7 obsahuje modul Audit Trail, který zaznamenává změny v konfiguracích a přístupech, což napomáhá při vyšetřování incidentů. Data v cloudu jsou navíc uložena v zašifrované podobě a integrita je zajištěna transakčními mechanismy v clusterech [33].

4.1.5 Icinga

Icinga vznikla jako odnož Nagiosu a především druhá generace, Icinga 2, přinesla modernizovanou architekturu. Díky svému původu podporuje široké spektrum monitorovacích metod a protokolů podobně jako Nagios[34].

- **Komplexní monitoring:** Icinga 2 využívá koncept pluginů, přičemž je plně kompatibilní s existujícími Nagios pluginy. Díky tomu lze monitorovat zařízení pomocí SNMP (podporuje verze SNMPv1, SNMPv2c i SNMPv3, kdy SNMPv3 umožňuje využít au-

tentizaci a šifrování), což pokrývá širokou škálu síťových zařízení i dalších SNMP prvků. Pro monitorování hardwarových senzorů lze použít specializované pluginy, jako je například `check_ipmi_sensor` pro IPMI senzory. Dále jsou k dispozici pluginy pro JMX, které umožňují spouštět kontroly přes příkaz `check_jmx` definovaný v konfiguračním jazyce. Pro Windows systémy pak Icinga umožňuje využít nativní Icinga agent, který dokáže spouštět PowerShell skripty a získávat potřebná data, případně lze využít externí plugin, například `check_wmi_plus`, který umožňuje vzdálené WMI dotazování [35].

Icinga 2 podporuje jak agentový monitoring (nativní Icinga agent je dostupný pro Linux i Windows), tak bezagentový monitoring, například prostřednictvím SNMP nebo SSH. Dále umožňuje i log monitoring – agent může sledovat log soubory a generovat upozornění na základě definovaných vzorků. Nativně však Icinga nemá vestavěnou podporu pro analyzování NetFlow, takže v tomto případě se předpokládá využití externích řešení pro zpracování síťového provozu. Icinga plně podporuje i definici byznys závislostí – umožňuje modelovat vztahy mezi nadřazenými a podřazenými objekty, což zabraňuje tomu, aby výpadek klíčového zařízení (například routeru) spustil nadměrné množství upozornění v připojených systémech. K monitorování se v Icinga sledují především stavové hodnoty (například OK, WARNING a CRITICAL) a výkonnostní data (numerické hodnoty získané z pluginů). Historická data lze ukládat do lokální RRD databáze nebo odesílat do externích TSDB systémů (například InfluxDB či Graphite) pomocí tzv. Writer modulu, který umožňuje přenos výkonových dat pro pozdější vizualizaci [35].

- **Upozorňování na incidenty:** Icinga 2 disponuje vlastním systémem notifikací, který je konfigurován pomocí deklarativního jazyka (DSL). Administrátor definuje tzv. Notification objekty, do kterých se přiřazují konkrétní hostitelé či služby, časová okna a uživatelé či skupiny, kterým se upozornění mají odesílat. Icinga standardně obsahuje šablony pro e-mailové notifikace (například skript „mail-service-notification.sh“ na Linuxu či PowerShell ekvivalent na Windows), a dále podporuje odesílání notifikací přes SMS – to se řeší přidáním vlastního příkazu (Notification Command), který může volat API SMS brány nebo spouštět skripty pro GSM modem. Kromě e-mailu lze přes webhook modul integrovat notifikace do chatovacích platforem, jako jsou Slack

nebo Microsoft Teams, případně do služeb pro on-call upozornění jako PagerDuty. Systém notifikací v Icinga podporuje nastavení period notifikací, opakování a tlumení, takže např. pokud nebyla odeslána první notifikace, lze definovat interval, po kterém se upozornění opakuje, nebo nastavit, aby se při potvrzení další notifikace neodesílaly. Všechny tyto možnosti umožňují detailní konfiguraci notifikačního systému, který lze tak přizpůsobit interním postupům firmy [36].

- **Vizualizace dat:** Icinga nabízí vlastní webové rozhraní zvané Icinga Web 2, které poskytuje aktuální přehled o stavu monitorované infrastruktury. Přes toto rozhraní jsou k dispozici dashboardy, které zobrazují seznam hostů a služeb, přehled aktuálních incidentů a detailní historii stavů. Pro vizualizaci výkonových dat lze Icinga integrovat s nástroji jako Grafana či Graphite – Icinga má Writer modul, který umožňuje odesílat výkonová data do těchto externích systémů a následně je zobrazit v interaktivních grafech. Alternativou je použití PNP4Nagios modulu, který funguje podobně jako v Nagios Core. Icinga Web 2 je responzivní a vhodná i pro NOC zobrazení – zobrazuje přehled všech aktuálních problémů, stav alarmů, a umožňuje uživatelům interaktivně filtrovat a třídit data. Kromě toho Icinga Web 2 podporuje topologické mapy, které ukazují závislosti mezi zařízeními, což umožňuje vizualizaci vztahů mezi nadřazenými a podřízenými systémy [37].
- **Open-source a podpora:** Icinga je open-source software, distribuovaný pod GNU GPL (v2 pro jádro a v3 pro webový frontend). Software vyvíjí společnost Icinga GmbH spolu s aktivní komunitou přispěvatelů. To znamená, že software je zdarma k použití a lze jej libovolně modifikovat. Pro firmy, které vyžadují profesionální podporu, Icinga GmbH nabízí komerční služby, jako jsou konzultace, školení a podpora. Díky tomu je možné, aby Axians uzavřel smlouvu s certifikovaným partnerem, což zajistí odbornou asistenci při nasazení a provozu systému [38].
- **Vysoká dostupnost:** Icinga 2 má vestavěnou podporu pro distribuované a vysokou dostupnost (HA) nasazení. Je možné provozovat dva Icinga 2 master servery, které běží paralelně a synchronizují si informace o stavu, konfiguraci a výsledcích. Tyto servery mohou fungovat v režimu aktivní-aktivní nebo aktivní-pasiví, v závislosti na nastavení zón. Icinga masters sdílejí databázové backendy (např. IDO nebo nově IcingaDB, které pracují s MySQL či PostgreSQL a Redis), které lze také spojit do clusteru, aby

nebyl jeden jediný bod selhání. Navíc Icinga umožňuje nasazení distribuovaného monitoringu pomocí Satellite uzlů, které jsou umístěny blíže monitorovaným systémům a v případě výpadku hlavního serveru mohou dočasně sbírat data [39].

- **Kybernetická bezpečnost:** Icinga 2 byla navržena s důrazem na bezpečnou komunikaci mezi všemi komponentami. Všechny nody (masters, satellites, agenti) komunikují pomocí vlastního protokolu nad TLS, přičemž Icinga při instalaci generuje TLS certifikáty, které lze podepisovat vlastní CA nebo využít automatizované podepisování mezi masterem a agenty. Podporovány jsou moderní TLS verze (1.2 a 1.3) a Icinga umožňuje jak šifrování pomocí certifikátů, tak i využití pre-shared keys (PSK), přičemž v praxi se většinou spoléhá na certifikáty. Tím se výrazně zvyšuje bezpečnost, protože agent přijme příkazy ke kontrole pouze od ověřeného masteru. Webové rozhraní Icinga Web 2 lze zabezpečit pomocí HTTPS a lze jej integrovat s Active Directory nebo SAML SSO moduly pro centralizovanou autentizaci. Icinga také implementuje audit log, který zaznamenává všechny přihlášení a konfigurace, což zajišťuje možnost sledovat bezpečnostní události. Celkově Icinga poskytuje robustní zabezpečení komunikace a integrity dat v clusteru, avšak správné nastavení (např. pravidelná obměna certifikátů) vyžaduje určitou disciplínu administrátorů [40].



Obrázek 4.2 Logo monitorovacího nástroje Icinga [34]

4.1.6 SolarWinds Network Performance Monitor (NPM)

SolarWinds NPM je zavedené komerční řešení určené primárně pro monitorování sítí a síťových zařízení, které je možné rozšířit i na monitorování serverů. Nástroj je bezagentový, což znamená, že při sběru dat se nespolečá na instalaci speciálních agentů na cílová zařízení, ale využívá standardní protokoly jako SNMP a WMI [41].

- **Komplexní monitoring:** SolarWinds NPM automaticky skenuje síť a detekuje zařízení pomocí ICMP (ping) a SNMP, čímž rychle identifikuje routery, switche, přístupové body a další síťová zařízení v různých podsítích [42]. Pro každé nalezené zařízení provádí SNMP dotazování ke čtení MIB hodnot, například propustnosti rozhraní, využití CPU u switchů či stavu hardwarových zdrojů. Kromě toho podporuje SNMPv3 a umožňuje nastavit různé přihlašovací údaje pro různá zařízení, kdy při skenování využívá SNMPv3 credentials a případně fallback na SNMPv2c [42]. Pro Windows servery je preferovanou metodou sběru dat WMI – Orion platforma umožňuje volit, zda pro daný uzel použít SNMP nebo WMI, přičemž WMI je typicky vyhrazeno pro doménové Windows systémy, zatímco SNMP se využívá u síťových prvků (SolarWinds, 2023). SolarWinds NPM umožňuje také sběr dat pomocí volitelných agentů – například Orion Agent pro Windows nebo Linux, který může výrazně zvýšit spolehlivost sběru dat přes firewally. Dále NPM integruje modul NetFlow Traffic Analyzer (NTA) pro zachytávání a analýzu síťových toků, pokud je nasazen tento modul, NPM může přijímat data z NetFlow v5/v9, sFlow, J-Flow či IPFIX a zobrazovat detailní statistiky o provozu, například nejvytíženější IP adresy či aplikace [42]. SolarWinds rovněž monitoruje hardwarové zdraví serverů – například prostřednictvím SNMP se získávají informace z iLO/DRAC či CIM, což umožňuje čtení teplot, stav ventilátorů, napájecích stavů a RAID konfigurací. Výhodou NPM je také široká podpora různých vendor MIB díky vestavěným Universal Device Pollerům, kde si administrátor může ručně nakonfigurovat SNMP OID pro monitorování specifických parametrů konkrétního zařízení [42].
- **Upozorňování na incidenty:** SolarWinds Orion platforma, jejíž součástí je NPM, disponuje robustním systémem pro upozornění. Administrátoři definují upozornění na základě podmínek – například pokud využití CPU překročí 90% po dobu 5 minut, nebo pokud zařízení přejde do stavu „Down“. NPM obsahuje řadu předdefinovaných upozornění pro běžné scénáře a umožňuje každému upozornění přiřadit jednu či více akcí. Podporované akce zahrnují odesílání e-mailů s detailním popisem, zasílání SMS (buď přes e-mail-to-SMS bránu, nebo integrací s poskytovateli jako Twilio či Clickatell), zápisy do Windows Event Log, spuštění externích skriptů, odesílání SNMP trapů nebo volání REST API (například pro integraci se ServiceNow) [43]. Novější verze Orionu

podporují také webhook volání a integraci s chatovými aplikacemi, jako jsou Microsoft Teams nebo Slack. Nástroj umožňuje definovat eskalační řetězce – pokud upozornění není vyřešeno do stanoveného času, odesílá se upozornění na další úroveň. Kromě toho lze nastavit opakování notifikací, aby se kritické stavy nepřehlédly [43].

- **Vizualizace dat:** SolarWinds NPM běží na platformě Orion, která poskytuje bohaté webové rozhraní postavené na ASP.NET. Uživatelé mají přístup k přizpůsobitelným dashboardům, například k výchozímu Network Summary, který zobrazuje grafy zatížení sítě, seznam nejvytíženějších rozhraní, mapu sítě a aktuální upozornění. Moderní dashboardy v Orionu (Modern Dashboards) umožňují tvorbu interaktivních pohledů pomocí dotazů SWQL a různých widgetů, zatímco starší dashboardy se upravují přímo přes webový konfigurační mód. NPM má také modul Network Atlas, který umožňuje vytvořit vlastní mapu s ikonami zařízení a zobrazením jejich stavů barevným indikátorem. Dále jsou k dispozici heat mapy pro bezdrátové sítě a modul Report Writer, který umožňuje generovat detailní tabulkové a grafické reporty, jako například průměrnou dostupnost či top 10 rozhraní podle propustnosti, a tyto reporty lze plánovaně zasílat e-mailem. Data jsou ukládána v databázi MS SQL a jsou přístupná přes REST API, což umožňuje integraci s externími nástroji, například s Grafanou, i když Orion Web poskytuje velmi komplexní vizuální prostředí [44].
- **Open-source a podpora:** SolarWinds NPM je komerční software vyvíjený firmou SolarWinds. Není open-source, tudíž zákazník získává binární instalaci a licenci. S licencí je k dispozici oficiální technická podpora, která zahrnuje možnost kontaktovat inženýry e-mailem nebo telefonicky v rámci sjednané úrovně SLA. SolarWinds provozuje také aktivní komunitní fórum THWACK, kde si uživatelé vyměňují dotazy a vlastní řešení. Produkt má rozsáhlou dokumentaci, která zahrnuje administrátorské průvodce a osvědčené postupy. Na druhou stranu, reputace SolarWinds byla v minulosti narušena kvůli bezpečnostní kauze Sunburst (2020), což vedlo k zavedení dodatečných opatření jako digitální podpis aktualizací a izolace prostředí. Licencování produktu se obvykle provádí dle počtu monitorovaných prvků, rozhraní a objemu dat [45].
- **Vysoká dostupnost:** SolarWinds NPM běží na Windows serveru s databází MS SQL Server. K zajištění vysoké dostupnosti je k dispozici volitelný modul Orion High Avail-

lability, který umožňuje nasazení dvou Orion serverů (primárního a záložního) v režimu aktivního-pasivního clusteru. Tyto servery sdílejí virtuální IP adresu, takže v případě výpadku primárního serveru záložní automaticky převezme jeho funkce během několika desítek sekund. Databázová vrstva se doporučuje provozovat pomocí MS SQL clusteru (např. AlwaysOn Availability Groups) pro zajištění redundance. Dále lze nasadit více polling serverů pro rozložení zátěže a zvýšení redundance sběru dat. Orion tedy nabízí komplexní HA řešení, které umožňuje zajištění vysoké dostupnosti monitorovací služby i při selhání jednotlivých komponent [46].

- **Kybernetická bezpečnost:** SolarWinds Orion poskytuje robustní bezpečnostní mechanismy. Přístup do webového rozhraní je chráněn pomocí autentizace uživatelů – Orion podporuje interní účty a integraci s Active Directory, přičemž lze nastavit také dvoufaktorovou autentizaci (např. prostřednictvím SSO řešení). Komunikace mezi Orion servery a jejich webovými klienty je šifrována pomocí HTTPS, přičemž uživatelé instalují vlastní SSL certifikáty. Pro sběr dat se využívají zabezpečené metody. WMI komunikace probíhá přes DCOM/WinRM s Windows autentizací (NTLM, Kerberos) a SNMP komunikace je zajištěna pomocí SNMPv3, který podporuje šifrování a autentizaci. Citlivé údaje, jako jsou SNMP komunitní řetězce či hesla, jsou ukládány šifrovaně v databázi Orion. SolarWinds také implementuje řízení přístupu pomocí modulů Account Limitations a User Rights, které umožňují přesně definovat, která zařízení mohou být spravována jednotlivými uživateli. Po incidentu Sunburst (2020) SolarWinds výrazně zlepšil své bezpečnostní procesy, například zavedením digitálního podepisování aktualizací a izolací prostředí. Orion rovněž podporuje příjem SNMP trapů i syslogů, přičemž u syslogů je implementováno TLS šifrování. Celkově Orion NPM vyhovuje firemním bezpečnostním standardům – zabezpečuje komunikaci, omezuje přístup a pravidelně vydává bezpečnostní aktualizace [47].

4.1.7 PRTG Network Monitor

PRTG Network Monitor je monitorovací nástroj, který umožňuje sledovat dostupnost a výkon síťových zařízení, serverů a aplikací. Nabízí předdefinované senzory pro různé typy monitorování a poskytuje real-time data prostřednictvím přehledných dashboardů [48].



Obrázek 4.3 Logo monitorovacího nástroje PRTG Network Monitor [48]

- **Komplexní monitoring:** PRTG Network Monitor od společnosti Paessler je známý jako „vše-v-jednom“ monitorovací nástroj s bezagentním přístupem. Jeho architektura je založena na tzv. senzorech – předkonfigurovaných kontrolních jednotkách určených pro konkrétní typy metrik. PRTG disponuje širokou paletou senzorů pro monitorování síťových prvků, serverů, aplikací a dalších zařízení. Například pro síťová zařízení je k dispozici senzor SNMP Traffic, který sleduje provoz na rozhraní, senzor SNMP Up-time pro monitorování dostupnosti a senzor SNMP Hardware Status pro stav hardwarových zařízení. PRTG podporuje protokoly SNMP verze 1, 2c i 3, přičemž SNMPv3 poskytuje možnost zabezpečeného přenosu dat pomocí autentizace a šifrování [49].

V prostředí Windows využívá PRTG bohatě WMI – má senzory jako WMI CPU Load, WMI Memory nebo WMI Disk Health, které přímo dotazují Windows Management Instrumentation a získávají systémové údaje. Alternativně lze na Windows využít Performance Counters senzor, který komunikuje přes protokol PerfMon. Pro Linux/Unix servery PRTG preferuje monitorování přes SNMP nebo SSH – senzory jako SSH Load Average využívají přihlášení přes SSH a spuštění příkazů (Paessler AG, 2023). Kromě toho PRTG nabízí speciální senzory pro prostředí VMware, Hyper-V a cloudové služby (například Azure a AWS), které komunikují s API hypervizorů či cloudových služeb a získávají data o využití zdrojů. Pro monitorování hardwaru je k dispozici i senzor IPMI System Health, který sleduje hardware serverů přes IPMI rozhraní

– například měří teploty, stav ventilátorů a napětí (Paessler AG, 2023). Unikátní vlastností PRTG je vestavěný modul pro Flow monitoring, kdy PRTG obsahuje senzory pro zachycení NetFlow (v5/v9), sFlow a IPFIX dat. Stačí nasměrovat export síťového provozu z routeru na PRTG server a ten zobrazí statistiky jako největší komunikátoři nebo přehled protokolů, čímž kombinuje funkce NMS a NTA v jednom produktu. Data PRTG ukládá do vlastní interní (souborové) databáze, aniž by potřeboval externí SQL řešení [50].

- **Upozorňování na incidenty:** PRTG má vestavěný systém notifikací, který je snadno konfigurovatelný prostřednictvím grafického uživatelského rozhraní. Uživatelé definují tzv. Notification Triggers – například když senzor přejde do stavu Down, nebo když překročí definovaný práh pro stav Warning. PRTG podporuje současné zasílání upozornění více kanály. Mezi podporované metody patří odesílání e-mailů (přímo přes SMTP nebo vlastní e-mailový server), SMS (prostřednictvím integrace s externími SMS bránami nebo e-mail-to-SMS službami), push notifikace do mobilní aplikace PRTG (která je k dispozici pro iOS a Android), HTTP request (webhook) a spuštění externího programu či skriptu na serveru [51]. Konfigurace notifikačních spouštěčů umožňuje definovat různé způsoby zasílání v závislosti na závažnosti – například pro stav upozornění se odesílá pouze přes e-mail, zatímco pro stav Down se odesílá SMS i e-mail. Systém rovněž podporuje eskalaci upozornění, kdy při delším a opakovaném výpadku může dojít k odeslání další notifikace na jiného příjemce. Podle doporučení výrobce se doporučuje vždy nastavit aspoň dvě metody zasílání, aby nedošlo k selhání jedné cesty [51].
- **Vizualizace dat:** PRTG Network Monitor má vlastní webové rozhraní, které zobrazuje centrální dashboard (PRTG Home) s globálním přehledem stavu – např. počet aktuálních výpadků, varování, poslední upozornění a vytížení sondy. Každé zařízení má své specifické zobrazení se seznamem senzorů a jejich aktuálních hodnot. Uživatelé si mohou zobrazovat grafy (tzv. Live Graph) pro jednotlivé senzory, přičemž PRTG automaticky zobrazuje data za posledních 2 hodiny, 2 dny, 30 dní či 365 dní s vhodnou granularitou. Grafy jsou interaktivní a lze je exportovat jako obrázky. Dále PRTG obsahuje Map Designer, který umožňuje sestavit vlastní mapy infrastruktury s umístěním objektů, stavovými ikonami, grafy a tabulkami, což je vhodné například

pro NOC panely nebo manažerské přehledy. Uživatelé mohou rovněž generovat reporty, například PDF reporty dostupnosti a průměrů za určité období, které mohou být automaticky zasílány e-mailem. Přestože je možné data exportovat pomocí REST API pro integraci s externími nástroji, většina uživatelů využívá vestavěné grafy a mapy, které poskytují solidní, i když poněkud tradičnější grafickou prezentaci [52].

- **Open-source a podpora:** PRTG je komerční software, nikoliv open-source, a licencuje se podle počtu senzorů, které se monitorují. Menší prostředí mohou využít bezplatnou edici (do 100 senzorů), zatímco pro větší infrastruktury jsou dostupné placené licence odstupňované podle počtu senzorů (např. 500, 1000, 2500 atd.). V ceně licence je zpravidla zahrnuta roční podpora (aktualizace a technická podpora), po jejímž uplynutí lze doplácet za další údržbu. Společnost Paessler poskytuje kvalitní podporu, zpravidla prostřednictvím e-mailu v angličtině s krátkou dobou odezvy. Existuje také komunita uživatelů, která doplňuje oficiální dokumentaci, i když ta není tak rozsáhlá jako u některých open-source řešení. Výhodou proprietárního modelu je, že software je připraven k použití a integrace mezi jeho komponentami jsou již přednastavené, což minimalizuje nutnost ladění. Na druhou stranu, uzavřenost řešení omezuje možnost úprav vnitřního fungování systému, ale PRTG umožňuje vytvoření vlastních senzorů a využití REST API pro rozšíření, což poskytuje určitou flexibilitu. Paessler je středně velká německá firma specializovaná na monitorovací řešení, což zaručuje kontinuitu vývoje a pravidelné aktualizace [48].
- **Vysoká dostupnost:** PRTG lze provozovat v HA clusteru. Software umožňuje konfiguraci failover clusteru, kdy se jeden PRTG server označí jako Primary Master a druhý jako Failover Node. Primární instance neustále replikuje svou konfiguraci a data na failover server v reálném čase. V režimu aktivní-aktivní oba servery monitorují senzory, takže při selhání primární instance failover okamžitě převzme funkce, což zajišťuje kontinuitu bez přerušení přístupu uživatelů [53]. Pro vyšší redundanci může být nasazeno více failover instancí, a také PRTG podporuje Remote Probes, které umožňují monitorování vzdálených lokalit s lokálním ukládáním dat v případě přerušení spojení s hlavním serverem. Tím se minimalizuje riziko ztráty dat a zajišťuje se nepřetržitý monitoring [53].
- **Kybernetická bezpečnost:** PRTG je typicky nasazen v interní síti organizace a jeho

webové uživatelské rozhraní běží na TCP portech 80/443. Po instalaci software výchozí používá HTTP, ale administrátor může povolit SSL/TLS, přičemž PRTG je schopen vygenerovat certifikát nebo importovat vlastní. Podporováno je TLS 1.2, přičemž starší protokoly, jako SSLv3, nejsou podporovány. Uživatelé se autentizují jménem a heslem, přičemž PRTG umožňuje integraci s Active Directory, což umožňuje používání doménových účtů a případně i SSO mechanismus Windows. Lze definovat uživatelská práva tak, aby každý uživatel měl přístup pouze k určitým sekcím monitorovací struktury. Komunikace mezi PRTG serverem a Remote Probe sondami je šifrována pomocí TLS a chráněna vzájemným autentizačním klíčem. PRTG ukládá citlivé údaje, jako jsou hesla k SNMP nebo WMI účtům, v konfiguraci šifrované pomocí uživatelského hesla, což vyžaduje re-autentizaci při přístupu do nastavení. Dále PRTG umožňuje nastavit pravidla pro IP Access Control, která definují, které IP adresy mají povolený přístup k webovému rozhraní a API. PRTG také vede logy událostí, do kterých jsou zaznamenávány přihlášení, změny nastavení a výpadky senzorů, což pomáhá při auditu bezpečnosti [54].

4.1.8 Datadog

Datadog je cloudová monitorovací platforma navržená pro sledování výkonu a zdraví různých IT komponent, včetně serverů, databází, nástrojů pro automatizaci a instrumentaci, aplikací a dalších. Nabízí centralizovaný pohled na metriky, logy a trasování v reálném čase, což usnadňuje správu složitých IT infrastruktur.



Obrázek 4.4 Logo monitorovacího nástroje Datadog [55]

- **Komplexní monitoring:** Datadog je cloudová monitorovací a analytická platforma (Monitoring as a Service), která dokáže pokrýt metriky, logy i sledování provozu na aplikační vrstvě. V kontextu monitorování infrastruktury funguje především na bázi agentů. Na monitorované servery – ať už jde o fyzické stroje, virtuální servery nebo kontejnery – je instalován Datadog Agent, který sbírá metriky operačního systému (CPU, paměť, IO a další) a umožňuje také provádět kontroly například ověření odezvy webových serverů nebo sledování stavu front v systémech, jako je RabbitMQ. Datadog disponuje přes 500 předpřipravenými integracemi, jež pokrývají většinu běžně používaných technologií. Pro síťová zařízení například existuje integrace SNMP, kdy agent může fungovat jako SNMP poller a sbírat metriky z kompatibilních zařízení, přičemž podporuje i SNMPv3 s bezpečnostními mechanismy [55].

Dále Datadog nabízí modul Network Device Monitoring (NDM), který v kombinaci s agentem dokáže přijímat data ze síťových zařízení pomocí NetFlow, sFlow, J-Flow a IPFIX. Vestavěný Flow Collector, který naslouchá například na UDP portu 2055 pro NetFlow v9, umožňuje provádět analýzu síťového provozu. Pro Windows servery agent sbírá metriky z Performance Counters. Performance Counters jsou speciální metriky, které poskytují informace o výkonu systému, typicky ve Windows prostředí. WMI není explicitně využíváno, a pro aplikační prostředí jsou k dispozici integrace, jako je JMX integrace (agentový modul JMXFetch), integrace pro databáze (Oracle, MSSQL, MySQL), fronty (Kafka, RabbitMQ), kontejnery (Kubernetes, Docker) a cloudové služby (AWS CloudWatch, Azure Monitor, GCP) [56]. Datadog tak sbírá nejen infrastrukturní metriky (hardware, operační systém), ale i aplikační (např. počet dotazů, latence) a umožňuje agregaci vlastních metrik prostřednictvím API.

- **Upozorňování na incidenty:** Koncept „Monitorů“ v Datadogu umožňuje definovat pravidla pro generování upozornění nad příchozími daty – například lze nastavit monitor, který bude sledovat hodnoty CPU u skupiny serverů, nebo detekovat opakované chyby v logech. Když nastane definovaná podmínka, Datadog aktivuje spouštěč. Notifikační ekosystém je velmi bohatý a podporuje kanály jako e-mail, SMS (přes integraci s Twilio), anonymní telefonní hovory a také integraci s nástroji jako Slack, Microsoft Teams, PagerDuty, OpsGenie, Jira, ServiceNow a dalšími. Systém také umožňuje konfiguraci throttlingu (potlačení příliš častých notifikací) a více úrovněvé upozornění

(Alert Priority). Každý monitor může mít definovány výchozí zprávy včetně šablon, do kterých lze vložit poslední hodnoty, malé grafy apod. Notifikace jsou odesílány z cloudové platformy, čímž se minimalizuje závislost na vnitřních e-mail serverech uživatele. Pro případ kritických situací je možné nastavit, aby určité upozornění byly eskalovány například do PagerDuty, což zajistí 24/7 dostupnost on-call podpory [57].

- **Vizualizace dat:** Datadog se zaměřuje na vizualizaci prostřednictvím interaktivních webových dashboardů. Uživatelé mohou snadno sestavit vlastní panely, přičemž platforma nabízí řadu předpřipravených dashboardů pro běžné integrace – například po aktivaci integrace pro Apache se automaticky objeví dashboard se všemi klíčovými metrikami (požadavky za sekundu, chybovost, zatížení atd.). Dashboardy lze klonovat, upravovat a přizpůsobovat dle potřeb. K dispozici jsou různé typy grafů, včetně časových řad, heatmap, top-N analýz, map infrastruktury a vztahových map aplikací (service maps). Pro síťové prostředí generuje Datadog Network Map, která zobrazuje síťová zařízení a spoje mezi nimi s indikací vytížení. Unikátní jsou také screenboardy (volné uspořádání prvků) a timeboardy (uspořádání podle času) spolu s notebook stylem, který kombinuje grafy a text – vhodné pro reporty s komentářem. Datadog podporuje také geografické mapy a KPI panely pro byznys, a umožňuje konfiguraci SLO (Service Level Objectives), kdy platforma automaticky počítá plnění služeb. Dashboardy jsou přístupné prostřednictvím veřejného URL v režimu pouze pro čtení a existuje mobilní aplikace pro iOS a Android, která umožňuje sledovat panely v reálném čase [58].
- **Open-source a podpora:** Datadog je proprietární SaaS platforma, což znamená, že zákazník nemá přístup k internímu zdrojovému kódu. Na rozdíl od toho je však Datadog Agent open-source – zveřejněný na GitHubu, což umožňuje nezávislou auditaci agentů. Klient na oplátku získává plně hostovanou službu s garancí dostupnosti, přičemž Datadog uvádí SLA dostupnosti 99,9%. Podpora je součástí předplatného – standardně se poskytuje 24/5, případně 24/7 s rychlou dobou odezvy pro kritické incidenty. Platformu vyvíjí americká firma Datadog, Inc. a nabízí také bohatou komunitu, dokumentaci, blogy a konference, což značně usnadňuje implementaci a provoz. Cenový model Datadog je založen na monitorovaných hostech a objemech dat (např. logy dle GB), což může znamenat vyšší náklady v případě velmi rozsáhlého nasazení, ale

zároveň šetří investice do vlastního hardwaru a administrace [59].

- **Vysoká dostupnost:** Jelikož jde o cloudovou službu, Datadog je z podstaty vysoce dostupný – běží v redundantních clusterech, přičemž poskytovatel se stará o replikaci dat a failover. Datadog deklaruje, že v případě výpadku celého regionu dokáže přesměrovat službu do záložního regionu, což znamená pouze krátké omezení viditelnosti dat. Agenti lokálně akumulují data v případě výpadku připojení a po obnovení linky je do cloudu odesílají, takže krátké přerušení nezpůsobí ztrátu metrik. Notifikace jsou odesílány z cloudu, což zajišťuje, že i při výpadku lokální infrastruktury zákazníka jsou všechna upozornění doručena [60].
- **Kybernetická bezpečnost:** Datadog klade velký důraz na bezpečnost, protože zpracovává citlivá provozní data zákazníků v cloudovém prostředí. Veškerá komunikace mezi agenty a cloudovou platformou je šifrována pomocí TLS (aktuálně TLS 1.2 a novější verze). Agenti se autentizují pomocí unikátního API tokenu, což zajišťuje, že data mohou posílat pouze důvěryhodné instance. Platforma je certifikována podle standardů, jako jsou ISO 27001 a SOC 2, a podporuje role-based access control, což umožňuje nastavit, kdo má přístup k jakým dashboardům a monitorům. Datadog také podporuje SAML SSO, čímž lze integrovat firemní Identity Provider (např. Azure AD) a zajistit dvoufaktorovou autentizaci. Každá akce v systému je auditována pomocí modulu Audit Trail, což umožňuje sledovat, kdo a kdy provedl změny. Ze sítě komunikují agenti přes standardní port 443 HTTPS, což minimalizuje riziko neautorizovaného přístupu, a případné exportované metriky lze také dále zabezpečit pomocí dodatečných šifrovacích opatření [61].

4.1.9 Zabbix

Zabbix je robustní open-source platforma, která umožňuje komplexní monitorování IT infrastruktury v reálném čase. Nástroj podporuje monitorování serverů, sítí, aplikací a cloudových služeb. Nabízí pokročilé možnosti vizualizace dat, přizpůsobitelné dashboardy a systém upozornění na incidenty [8].

- **Komplexní monitoring:** Zabbix představuje špičkové open-source řešení pro monitoring celé infrastruktury. Kombinuje podporu pro agentové i bezagentové monitorování



Obrázek 4.5 Logo monitorovacího nástroje Zabbix [8]

a pokrývá síťové prvky, servery, aplikační prostředí i cloud. Nativní Zabbix agent, dostupný pro Linux, Windows či Unix, je vysoce efektivní a umí sbírat stovky metrik, jako například údaje o CPU [8]. Agent může data posílat aktivně nebo se server sám dotazuje. Pro zařízení, u nichž nelze agenta nainstalovat, Zabbix nabízí podporu SNMP (verze SNMPv1, SNMPv2c i zabezpečený SNMPv3) a umožňuje pravidelné dotazování pomocí OID, stejně jako naslouchání SNMP trapům prostřednictvím speciálního Trap daemonu. Díky těmto funkcím je možné monitorovat například switche, routery, tiskárny nebo UPS srovnatelně s dedikovanými NMS nástroji. Dále Zabbix integruje IPMI monitoring, který umožňuje přímo číst hardware senzory serverů (včetně IPMI 2.0) a detekovat tak hardwarové poruchy. Pro Java aplikace je k dispozici Zabbix Java Gateway, který umožňuje JMX monitoring (přes RMI a podporu autentizace). Windows lze monitorovat pomocí agenta nebo alternativně pomocí WinRM skriptů, kdy Zabbix volá externí skripty. Zabbix rovněž podporuje log monitoring a event trapping – agent může sledovat log soubory a pomocí filtrů posílat pouze relevantní řádky, čímž pokrývá základní požadavky SIEM. Pro síťový provoz Zabbix integruje také Network Discovery, které prohledá IP rozsahy a automaticky přidá nalezená zařízení podle definovaných profilů (například pomocí ping nebo SNMP). Kromě toho umožňuje přijímání externích skriptů a webhooků, což umožňuje integraci s cloudovými API (např. AWS, Azure) pro stahování metrik z externích monitorovacích služeb. Metriky v Zabbixu jsou primárně uchovávány jako časové řady (číselné hodnoty) a také jako stavy datového typu boolean (OK/PROBLEM). Navíc může monitorovat dostupnost služeb pomocí web scénářů, kdy dokáže provést vícezkrokové HTTP testy s ověřením obsahu. Celkově je Zabbix velmi všestranný – existuje rozsáhlá šablonová databáze (Zabbix Share) s předpřipravenými šablonami pro různé typy zařízení a aplikací (např. Cisco, HP iLO, Oracle DB, Docker). Pro společnost Axians by Zabbix pokryl monitorování

serverů (detailní metriky s historickými daty), sítě (SNMPv3, SNMP trap, IPMI) a aplikačních služeb (agent, JMX, skripty), včetně monitoringu virtualizačních platforem (nativní VMware modul využívající VMware API) [62].

- **Upozorňování na incidenty:** Systém spouštěčů a notifikací v Zabbixu je jedním z jeho klíčových prvků. Uživatelé definují spouštěče jako logické podmínky nad jednou či více metrikami – podporovány jsou sofistikované výrazy a funkce jako průměr za 5 minut nebo opakované výskyty chyby. Jakmile spouštěč přejde do stavu PROBLEM, Zabbix vygeneruje událost. Každému spouštěči lze přiřadit úroveň závažnosti (od Not classified až po Disaster), která se poté využívá při řízení alarmů. Ke každému spouštěči je možné přidělit akci – tato akce určuje, jaké notifikace se odešlou (např. e-mail, SMS, Jabber, webhook). Výchozí druhy komunikace zahrnují e-mail, Jabber (XMPP) a SMS (např. využitím Ez Texting gateway), přičemž novější verze podporují také webhooky pro integraci se Slack, PagerDuty, Microsoft Teams a dalšími službami. Administrátor může jednotlivým uživatelům či skupinám přiřadit preferované kanály notifikací. Když dojde k incidentu, je generována notifikace, která obsahuje podrobné informace, případně i grafické výstupy. Zabbix dále podporuje eskalaci notifikací – pokud spouštěč zůstane ve stavu PROBLEM příliš dlouho, odešle se upozornění i na další kontakty (např. manažerovi). Systém také zabráňuje duplicitnímu odesílání upozornění – opakovaná měření, která potvrzují již vyhlášený problém, nevedou ke generování nových upozornění, a zpráva o vyřešení problému je odeslána pouze při návratu do normálu. Uživatelé mohou v UI potvrdit (acknowledge) problém a tím zastavit další eskalace. Z toho důvodu je možné detailně nastavit, jaké notifikace bude který tým přijímat (např. DB administrátoři dostanou pouze upozornění týkající se Oracle, zatímco síť aři pouze síťová upozornění) [63].
- **Vizualizace dat:** Zabbix disponuje vestavěným webovým rozhraním (frontend napsaný v PHP), které nabízí různé možnosti vizualizace monitorovaných metrik. Historická data jsou uchovávána v databázi (obvykle v časové databázi, například TimescaleDB nad PostgreSQL), a uživatelé mohou generovat grafy libovolných metrik za zvolené časové období. Zabbix umožňuje ruční vytváření grafických prototypů na úrovni šablon a také ad hoc vykreslovat interaktivní grafy v rámci uživatelského rozhraní (s možností zoomování). Verze Zabbix 6 představila moderní dashboardy, ve kterých lze

sestavit vlastní panely s widgety, jako jsou grafy, statistiky (např. počet aktuálních problémů, procentuální dostupnost), mapy infrastruktury či top-N tabulky. Dále je možné vytvářet geografické mapy, kde se na mapě světa zobrazují lokace monitorovaných zařízení se stavovými indikátory, a Network Maps, které umožňují vizualizaci vztahů mezi zařízeními pomocí dynamicky měnících se barev. Pro management je k dispozici modul Reporting/SLA, který slouží k definici a počítání SLA na základě doby provozu služeb a umožňuje exportovat dashboardy do PDF. Alternativně lze data integrovat s externími nástroji, například pomocí oficiálního Zabbix pluginu pro Grafanu [64].

- **Open-source a podpora:** Zabbix je plně open-source řešení (distribuováno pod licencí GPL v2) a lze jej stáhnout bez jakýchkoliv licenčních poplatků. Je vyvíjen společností Zabbix LLC (SIA) a má velmi aktivní komunitu. Každoročně vychází hlavní verze s novými funkcemi a pravidelně jsou vydávány menší aktualizace a opravné aktualizace. Pro firmy, které potřebují profesionální podporu, Zabbix LLC nabízí placené podpůrné balíčky, konzultace, školení a dokonce vzdálenou správu. Díky otevřenosti dat je možné, aby Axians interně přizpůsobil a rozšířil monitorovací skripty a integrace, a tím získal plnou kontrolu nad vlastním řešením. Celkové TCO je obvykle nižší než u komerčních produktů, i když je třeba počítat s náklady na hardware a správu [65].
- **Vysoká dostupnost:** Zabbix ve verzi 6 podporuje high-availability cluster pro Zabbix server. Lze provozovat dva nebo více Zabbix serverů v HA uzlu – jeden aktivní a zbylé v pasivním režimu, kdy se aktivní server v případě výpadku automaticky nahrazuje. Všechny servery sdílejí centrální databázi, která musí být sama vysoko dostupná (například PostgreSQL provozovaná v clusteru pomocí Patroni). Při selhání aktivního uzlu se pasivní stane aktivním během několika sekund díky heartbeat mechanismu. Heartbeat mechanismus je metoda pro pravidelnou kontrolu dostupnosti nebo funkčnosti systému, zařízení nebo služby. Agentům a proxy lze nastavit více adres serveru, což umožňuje automatické přepnutí. Kromě toho Zabbix podporuje Distributed monitoring pomocí proxy serverů, které mohou fungovat i offline a postupně předávat data po obnovení spojení. Tento přístup eliminuje jediný bod selhání a zajišťuje kontinuální monitoring i v případě výpadků některých komponent. Pro Axians by to znamenalo možnost nasadit dva redundantní Zabbix servery ve dvou datacentrech, přičemž databáze bude provozována v HA clusteru, což zajistí provoz monitoringu i při vý-

padku celého datacentra. Zabbix také podporuje Master-Child hierarchii pro sloučení více nezávislých serverů do jednotného pohledu, což dodatečně zvyšuje odolnost celého systému [66].

- **Kybernetická bezpečnost:** Zabbix je navržen s ohledem na bezpečnost distribuovaných komponent. Od verze 3.0 podporuje šifrovanou komunikaci pomocí TLS (1.2 a 1.3, dle použitých knihoven OpenSSL/NSS) mezi Zabbix serverem, proxy a agenty. K šifrování lze využít buď pre-shared key (PSK) nebo X.509 certifikáty, což zajišťuje, že data, například přenos hesel a log souborů, jsou důvěrná a integrita je chráněna. Webové rozhraní Zabbix se provozuje přes HTTPS, což zajišťuje bezpečný přístup; autentizace uživatelů může být nastavena jak interně (s hashovanými hesly), tak prostřednictvím integrace s LDAP/AD nebo SAML SSO. Lze také využít dvoufaktorové ověření. Zabbix agent běží s minimálními právy a při potřebě lze nastavit povolený seznam příkazů. Citlivá data v konfiguraci (například hesla k SNMPv3 či API klíče) jsou ukládána šifrovaně a přístup k nim by měl mít pouze administrátor. Zabbix také podporuje audit log, který zaznamenává všechny uživatelské akce (přihlášení, změny konfigurace, úpravy spouštěčů) a umožňuje integraci s externími SIEM systémy. Díky těmto bezpečnostním opatřením je Zabbix schopen zajistit ochranu monitorovacích dat, což je pro Axians klíčové, zejména pokud se jedná o monitorování citlivých systémů [67].

4.2 Analýza stávajících řešení

Hodnocení bylo provedeno na základě šesti klíčových kritérií, která byla vybrána s ohledem na specifické potřeby společnosti Axians. Následuje podrobné technické vysvětlení bodování a hodnocení jednotlivých parametrů včetně silných a slabých stránek:

Nagios Core je nástroj s jednoduchým jádrem a rozsáhlými možnostmi rozšíření prostřednictvím pluginů. Jeho předností je flexibilita – lze jej libovolně konfigurovat a rozšiřovat o vlastní skripty. Na druhou stranu však vyžaduje značné manuální zásahy a postrádá moderní funkce, jako jsou vestavěné GUI či nativní šifrování komunikace, které musí být řešeny dodatečnými doplňky [13].

Prometheus exceluje především ve škálování a sběru časových řad, což ho činí ideálním nástrojem pro cloud-native prostředí. Díky své architektuře je schopen efektivně pracovat

s metrikami aplikací a serverů. Ovšem jako samostatné řešení není kompletní – je třeba doplnit Alertmanager pro notifikace a vizualizační nástroj, například Grafanu, a monitoring síťových zařízení zde není zcela ideálně pokryt [16].

ManageEngine OpManager a SolarWinds NPM jsou robustní komerční systémy, které nabízejí rozsáhlou funkcionalitu a moderní, přívětivé uživatelské rozhraní. Oba nástroje se pyšní automatickým objevováním zařízení, pokročilým systémem upozornění a širokou podporou protokolů (SNMP, WMI, IPMI, NetFlow). Nicméně, jejich nevýhodou jsou vysoké licenční náklady a nižší flexibilita v integraci a úpravách (vendor lock-in), což znamená, že organizace jsou do značné míry závislé na dodavateli a náklady se zvyšují s rostoucím rozsahem infrastruktury [21] [68].

PRTG Network Monitor je „vše-v-jednom“ monitorovací řešení s bezagentním přístupem, založené na senzorech. Díky široké nabídce předpřipravených senzorů dokáže efektivně monitorovat sítě, servery, aplikace a další prvky infrastruktury. Výhodou PRTG je jednoduchost nasazení a centrální správa přes jednotné webové rozhraní, avšak při velmi velkém měřítku (tisíce senzorů) může být řešení méně efektivní a jeho uzavřenost omezuje možnosti přizpůsobení [48].

Datadog jako SaaS platforma nabízí špičkové technologie v oblasti sběru metrik, APM a logů, přičemž agenti monitorují široké spektrum prostředí (Linux, Windows, kontejnery, cloud). Datadog výrazně odbourává starosti s provozem monitorovací infrastruktury, jelikož všechny komponenty běží v cloudu, což přináší vysokou dostupnost a škálovatelnost. Na druhou stranu cena služby při dlouhodobém a rozsáhlém využití může být vyšší a některé firmy mohou mít obavy z hostování citlivých dat mimo svou síť [55].

Icinga 2 je open-source řešení, které si zachovává výhody kompatibility s Nagios ekosystémem, ale zároveň přináší modernizovanou architekturu a nativní podporu pro šifrovanou komunikaci, HA a distribuované nasazení. Icinga 2 je velmi robustní, avšak pro komplexní vizualizační řešení je třeba často využít externích nástrojů, jako je Grafana. Komunita Icingy je aktivní, avšak méně rozšířená ve srovnání se Zabbixem, což může ovlivnit podporu v některých regionech [34].

Kritérium	Zabbix	Datadog	Prometheus	Nagios	PRTG	SolarWinds	Icinga	Site24x7
Komplexní monitoring	5	5	4	4	5	5	4	4
Upozorňování na incidenty	5	5	3	4	5	5	4	4
Vizualizace dat	5	5	3	2	5	5	4	4
Open-source řešení	5	0	5	5	2	0	5	0
Vysoká dostupnost	3	5	3	2	4	4	3	5
Kybernetická bezpečnost	5	5	3	3	5	2	4	5
Celkové skóre	33	30	21	20	26	21	24	22

Tabulka 4.1 Porovnání monitorovacích nástrojů

4.3 Tabulkové shrnutí analýzy

Komplexní monitoring: Nejlépe byly hodnoceny nástroje s širokým záběrem monitoringu napříč celou infrastrukturou i aplikacemi. Datadog a PRTG získaly nejvyšší bodové ohodnocení díky komplexnímu záběru – nabízejí jednotnou platformu pro infrastrukturu, síť, cloud i aplikační výkon (APM). Zabbix a SolarWinds NPM obdržely také nejvyšší hodnocení za široké pokrytí zejména v oblasti sítí a serverů. Icinga a Prometheus byla udělena druhá nejvyšší hodnota – Icinga rozšiřuje možnosti Nagiosu pro infrastrukturu, ale neobsahuje integrované APM, a Prometheus exceluje v monitorování cloudových a kontejnerových prostředí (časové řady metrik), avšak bez doplnění (Grafana, další nástroje) nepokrývá plné spektrum (např. uživatelskou zkušenost či logy). Nagios Core také získal 4 body v oblasti kompletního monitoringu. Jeho silnou stránkou je robustnost a flexibilita díky rozsáhlé knihovně pluginů, avšak postrádá moderní, intuitivní uživatelské rozhraní a vestavěnou podporu pokročilých vizualizačních a bezpečnostních funkcí, které by mu umožnily získat plných 5 bodů.

Upozorňování na incidenty: Nejvyšší počet bodů získaly nástroje s bohatými možnostmi notifikací a eskalací. Zabbix vyniká pokročilým systémem upozorňování – umožňuje definovat prahové podmínky, vícestupňové eskalační scénáře a různé kanály oznámení (e-mail, SMS, skripty). Podobně Datadog a PRTG dosáhly špičkového hodnocení díky notifikacím v reálném čase a široké škále podporovaných kanálů (včetně integrací do týmových chatů a ticketing systémů). Prometheus obdržel 3 body, ačkoliv s nasazeným Alertmanagerem poskytuje robustní notifikace, vyžaduje dodatečnou instalaci a konfiguraci. Nagios získal 4 body – podporuje základní notifikace, avšak postrádá uživatelsky přívětivé rozhraní pro jejich správu. Icinga a Site24x7, rovněž ohodnocené 4 body, nabízejí flexibilní a vysoce konfigurovatelná upozorňovací řešení, která umožňují administrátorům nastavovat individuální eskalační řetězce a notifikační kanály podle specifických potřeb organizace.

Vizualizace dat: V vizualizaci monitorovacích dat byly nejvýše hodnoceny nástroje s bohatými vestavěnými dashboardy a grafy. Datadog a PRTG získaly plný počet bodů – poskytují interaktivní, přehledné řídicí panely pro metriky infrastruktury i aplikací v reálném čase. Zabbix také obdržel nejvyšší hodnocení. Nabízí detailní grafy, mapy a přizpůsobitelné dashboardy přímo v základu, což jej staví nad ostatní open-source nástroje v této oblasti. SolarWinds NPM získal plný počet bodů za vizualizaci – jeho intuitivní a upravitelné dashboardy poskytují detailní a real-time přehled síťových dat, zatímco Site24x7, ohodnocený 4 body, nabízí funkční, ale méně sofistikovaná vizuální řešení. Icinga získala tři body, protože její webové rozhraní nabízí přehledný pohled na infrastrukturu, avšak rozsah vestavěných grafů a vizualizací není tak bohatý jako u Zabbixu či komerčních řešení. Prometheus byl hodnocen nejhůře. Prometheus samotný umožňuje jen základní graf výrazu a pro plnohodnotné dashboardy vyžaduje integraci s Grafanou. Nagios nemá vestavěnou vizualizaci vůbec a spoléhá na doplňky typu NagVis, což vedlo k nejnižšímu počtu bodů v této kategorii.

Open-source řešení: V této kategorii získaly plný počet bodů nástroje, které jsou otevřené a zdarma přístupné, protože umožňují organizaci nezávislost na dodavateli a žádné licenční poplatky. Zabbix, Prometheus, Nagios i Icinga jsou open-source projekty, a proto obdržely maximální hodnocení. Tyto nástroje poskytují zdrojový kód, aktivní komunity a možnost přizpůsobení na míru (např. Zabbix i Nagios jsou zcela zdarma a škálovatelné dle potřeby). PRTG byl hodnocen výrazně níže – ačkoli nabízí bezplatnou verzi s omezeným počtem senzorů, samotný produkt je proprietární a rozšíření nad limit vyžaduje placenou licenci. SolarWinds, Datadog a Site24x7 získaly nejnižší možné hodnocení v kategorii open-source, neboť jde o uzavřená komerční řešení. Tato proprietární řešení sice mohou být robustní, ale organizace (např. Axians) musí počítat s náklady na licence a omezenou možností úprav systému.

Vysoká dostupnost: Nejlépe byly hodnoceny nástroje, které zajišťují spolehlivý provoz monitoringu i při výpadcích komponent. Datadog a Site24x7 získaly plný počet bodů díky architektuře SaaS – vysokou dostupnost zajišťuje poskytovatel automaticky v rámci cloudové služby (distribuované datové centrum, SLA). PRTG a SolarWinds obdržely vysoké hodnocení, neboť umožňují nasazení v clusteru/failover režimu pro redundantní monitoring: PRTG podporuje klastrování a rezervní uzly pro převzetí služeb při výpadku, SolarWinds nabízí failover engine a škálování na více pollerů pro velké podniky. Zabbix a Icinga dosáhly střed-

ního hodnocení – oba open-source nástroje lze provozovat v distribuovaném režimu (Zabbix Proxy, clusterová architektura Icinga) pro zvýšení odolnosti, avšak implementace vysoké dostupnosti vyžaduje pokročilejší nastavení (např. databázový clustering, redundantní servery). Prometheus byl hodnocen taktéž průměrně, protože v základní verzi běží jako samostatná instance, ale v praxi může běžet ve dvojicích pro redundanci a podporuje federaci dat – plná HA řešení však vyžadují doplňkové projekty (Thanos/Cortex pro dlouhodobé ukládání a škálování). Nagios získal nejnižší počet bodů v této kategorii, protože jeho open-source verze nenabízí vestavěný high-availability režim – zajištění redundance monitoringu vyžaduje buď komerční verzi (Nagios XI) či komplikovanou ruční synchronizaci konfigurací mezi více servery.

Kybernetická bezpečnost: V oblasti bezpečnosti byly nejlépe hodnoceny nástroje, které disponují robustním zabezpečením komunikace, přístupu a případně integrací bezpečnostních monitorovacích funkcí. Datadog a Site24x7 získaly maximální počet bodů – jako cloudové služby podnikové třídy dodržují vysoké standardy zabezpečení (šifrovaná komunikace agentů, certifikace SOC2/ISO27001, role-based access kontrola uživatelů). Navíc nabízejí i moduly pro monitorování bezpečnostních událostí (integrace logů, detekce anomálií), což je pro organizaci bonus. Avšak data jsou ukládána v cloudovém prostředí poskytovatele, což může být pro některé podniky problém z hlediska jejich interních politik. Z hlediska technologického zabezpečení jsou tyto nástroje však vybaveny velmi dobře. Zabbix byl hodnocen velmi dobře díky podpoře šifrování mezi všemi komponentami a možností autentizace uživatelů přes externí adresáře (LDAP, Active Directory). Icinga také obdržela vysoké hodnocení – navazuje na Nagios, ale přináší moderní zabezpečení (šifrovaná komunikace mezi master/satelity, detailní řízení přístupů v Icinga Web). PRTG a SolarWinds dosáhly také vyšších hodnot. PRTG umožňuje zabezpečený přístup (SSL na web rozhraní, integrace s AD pro ověřování uživatelů) a šifrované senzory, nicméně jako uzavřený systém vyžaduje důvěru v dodavatele ohledně rychlé záplaty případných zranitelností. U SolarWinds se v hodnocení zohlednilo, že po známém bezpečnostním incidentu z roku 2020 firma zavedla přísnější bezpečnostní procesy, ale některé organizace mohou stále vnímat jisté riziko; jinak SolarWinds NPM nabízí pokročilé řízení uživatelských rolí a šifrování dat, což mu zajistilo solidní, i když ne nejvyšší skóre. Prometheus a Nagios získaly průměrné hodnocení v kategorii kybernetické bezpečnosti. Prometheus postrádá v základní verzi autentizaci a spoléhá

na zabezpečení na úrovni sítě nebo externí proxy – podpora TLS/basic auth je pouze experimentální, což snižuje jeho bezpečnostní hodnocení pro podnikové nasazení. Nagios (Core) má limitované vestavěné zabezpečení, webové rozhraní lze sice chránit HTTP autentizací a komunikaci pluginů šifrovat dodatečně, avšak chybí komplexnější bezpečnostní funkce a rychlost reakcí na nové zranitelnosti závisí na komunitě. To vše vedlo k nižším bodům pro Nagios v této oblasti.

4.4 Shrnutí analýzy

Zabbix se v této analýze jeví jako nejvhodnější volba pro společnost Axians z několika klíčových důvodů:

Nejširší pokrytí monitorovacích scénářů: Zabbix nabízí podporu pro agentové monitorování na serverech (Linux, Windows, Unix) a zároveň umožňuje monitorování síťových zařízení prostřednictvím SNMP (včetně zabezpečeného SNMPv3), IPMI a trapů. Navíc disponuje bohatou šablonovou databází (Zabbix Share) s předpřipravenými šablonami pro různé typy zařízení – od Cisco a HP až po Oracle DB či Docker kontejnery. Tímto způsobem lze konsolidovat monitorování celé infrastruktury do jednoho systému (Zabbix LLC, 2023).

Robustní systém upozornění a eskalací: Systém spouštěčů v Zabbixu umožňuje definovat složité logické podmínky a přiřazovat jim úroveň závažnosti. Spolehlivé doručení notifikací přes různé kanály (e-mail, SMS, webhooky) a možnost eskalace v případě neřešeného incidentu zajišťují, že odpovědné osoby obdrží včas varování. Takové možnosti přizpůsobení upozornění jsou kritické pro velké organizace (Zabbix LLC, 2023).

Silná bezpečnost: Zabbix podporuje kompletní šifrování komunikace pomocí TLS (s možností použití pre-shared key nebo X.509 certifikátů) mezi servery, agenty a proxy. Kombinace pokročilé autentizace, kontroly přístupu a audit logů zabezpečuje monitorovací data i v kriticky citlivých prostředích. Tato úroveň zabezpečení je nezbytná zejména tam, kde jsou monitorovány klíčové systémy a data [67].

Open-source a nákladová efektivita: Zabbix je zdarma k použití a díky své otevřenosti není uživatel vázán na jednoho dodavatele. To umožňuje snadnou úpravu a rozšíření řešení interním týmem, což je výhodné z hlediska kontroly a dlouhodobých nákladů, zejména při monitorování rozsáhlé infrastruktury [65].

Možnost profesionální podpory: Pro firmy, které vyžadují vyšší úroveň podpory, Zabbix

LLC nabízí placené podpůrné balíčky, školení a konzultace. Tím je možné dosáhnout podobného komfortu jako u komerčních produktů, aniž by byly ohroženy výhody open-source modelu.

Škálovatelnost a vysoká dostupnost: Díky vestavěné podpoře high-availability clusteru, distribuovaným proxy serverům a možnosti provozovat Zabbix ve dvou datacentrech lze teoreticky dosáhnout nepřetržitého monitoringu. Ve skutečnosti však tento model výrazně závisí na přesné a pečlivé konfiguraci, a jakékoli nedostatky v nastavení HA řešení či synchronizaci mezi servery mohou vést k neplánovaným výpadkům či ztrátě dat. Tato složitost a závislost na infrastrukturních podmínkách vedla k ohodnocení pouze 3 body v tabulkové analýze, což naznačuje, že i když má Zabbix silné teoretické HA možnosti, jeho praktická implementace může představovat významné riziko při provozu kritických systémů. [66].

Komplexní vizualizace a reporting: Vestavěné webové rozhraní Zabbixu umožňuje vytváření detailních technických grafů i přehledných dashboardů pro management. Data lze snadno exportovat a integrovat s dalšími BI nástroji, jako je Grafana nebo PowerBI, což poskytuje odborně přesný a přehledný pohled na monitorovanou infrastrukturu [64].

Reference a osvědčení: Zabbix je nasazen v řadě firem, včetně kritických infrastruktur, a má dlouholetou tradici. Například společnosti jako Škoda Auto, České dráhy či významné telekomunikační společnosti využívají Zabbix, což potvrzuje jeho spolehlivost a funkčnost [69].

S ohledem na výše uvedené aspekty, zejména nejširší pokrytí monitorovacích scénářů, robustní upozorňovací systém, silnou bezpečnost a bezlicenční otevřenost, se Zabbix jeví jako nejvhodnější monitorovací nástroj pro potřeby společnosti Axians. Zabbix umožní centralizaci monitoringu, snadnou integraci do stávající infrastruktury a poskytne vysokou škálovatelnost a dostupnost monitorovací služby, což jsou kritické požadavky pro středně velké organizace.

5 MONITOROVACÍ NÁSTROJ ZABBIX

Zabbix je robustní open-source platforma pro monitorování IT infrastruktury, navržená tak, aby poskytovala komplexní přehled o výkonu a dostupnosti různých systémů a aplikací. Jeho modulární architektura umožňuje škálovatelnost od malých instalací až po rozsáhlá podniková prostředí. Primárně z důvodu škálovatelnosti je Zabbix vhodný i pro malé, střední i velké zákaznické společnosti Axians.

5.1 Architektura Zabbixu

Architektura Zabbixu je tvořena několika klíčovými komponentami, které spolupracují na sběru, zpracování a prezentaci monitorovacích dat. Tato modulární struktura zajišťuje flexibilitu a škálovatelnost systému.

Hlavní komponenty Zabbixu:

- **Zabbix Server:** Zabbix server je centrální součástí monitorovacího systému Zabbix, která zajišťuje sběr, zpracování a ukládání dat o dostupnosti, integritě a výkonu monitorovaných systémů. Komunikuje s agenty a proxy servery, přijímá od nich data, vyhodnocuje je a ukládá do databáze. Na základě předem definovaných podmínek (triggerů) server generuje upozornění a může provádět aktivní kontroly síťových služeb, jako jsou webové nebo e-mailové servery, pomocí jednoduchých kontrol služeb [70].

Server ukládá veškerá konfigurační, statistická a provozní data v databázi, která slouží jako centrální úložiště pro celý systém. Tato data jsou přístupná prostřednictvím webového rozhraní, které umožňuje správu konfigurace, sledování aktuálního stavu infrastruktury, analýzu historických dat a generování reportů [70].

Zabbix server je navržen tak, aby byl vysoce škálovatelný a dokázal monitorovat tisíce zařízení a služeb v reálném čase. Pro zajištění vysoké dostupnosti a odolnosti proti výpadkům lze server konfigurovat v redundantních architekturách, například pomocí clusterových řešení nebo replikace databáze. To je zvláště důležité v kritických prostředích, kde je nepřetržitý monitoring klíčový pro provoz organizace [70].

- **Zabbix Agent:** Lehký software nainstalovaný na monitorovaných zařízeních, který sbírá data o lokálních zdrojích a aplikacích, jako je využití CPU, paměti, stav disků

nebo běh konkrétních procesů. Agenti mohou pracovat ve dvou režimech: Pasivní režim: Server iniciuje spojení s agentem a požaduje data. Aktivní režim: Agent sám iniciuje spojení se serverem a odesílá data. Tento přístup zajišťuje flexibilitu v různých síťových prostředích a umožňuje optimalizovat zatížení sítě [70].

- **Zabbix Proxy:** Volitelná komponenta, která funguje jako prostředník mezi agenty a serverem. Proxy shromažďuje data od agentů v vzdálených nebo oddělených sítích a předává je serveru. Je užitečná v situacích, kdy je potřeba: Snížit zatížení hlavního serveru. Monitorovat vzdálené lokality s omezeným připojením. Překonat síťové bariéry, jako jsou firewally nebo NAT. Proxy může také dočasně ukládat data v případě dočasné nedostupnosti hlavního serveru, čímž zajišťuje kontinuitu sběru dat [70].
- **Databáze:** Všechna konfigurační data a nasbírané metriky jsou ukládány v relační databázi. Zabbix podporuje různé databázové systémy, jako jsou MySQL, PostgreSQL, Oracle nebo SQLite. Výběr vhodného databázového systému závisí na velikosti a požadavcích monitorovaného prostředí [70].
- **Webové rozhraní (Frontend):** Zabbix poskytuje webové uživatelské rozhraní, které umožňuje správu konfigurace, sledování aktuálního stavu infrastruktury, analýzu historických dat a generování reportů. Frontend je obvykle hostován na stejném serveru jako Zabbix Server, ale může být nasazen i na samostatném webovém serveru [70].

II PRAKTICKÁ ČÁST

6 VÝBĚR LABORATORNÍHO PROSTŘEDÍ

Z důvodu zjednodušení testování všech funkcionalit platformy Zabbix bylo pro tuto práci vybráno virtuální prostředí. Díky virtualizaci je totiž nejjednodušší nainstalovat operační systém jak pro Zabbix server, tak i pro Zabbix agenty. Dalším významným benefitem je segmentace na úrovni síťové vrstvy – v tomto případě budou všechna zařízení ve stejné síti.

7 VIRTUÁLNÍ PROSTŘEDÍ

Pro účely testování všech funkcionalit nástroje Zabbix bylo zvoleno virtuální prostředí Oracle VirtualBox, které umožňuje snadnou instalaci virtuálních strojů na hostitelský počítač. V tomto případě se jedná o herní počítač vybavený procesorem AMD Ryzen 7 2700X, 32 GB operační paměti, grafickou kartou Nvidia RTX 3070 a úložiště s kapacitou 2 TB typu m2 NVMe SSD. Tento hostitelský stroj bude s přehledem dostávat požadavkům pro praktickou část této diplomové práce.

7.1 Vytvoření virtuálního prostředí

V této sekci je popsán postup, jak vytvořit virtuální stroj pomocí nástroje Oracle VirtualBox. Prvním a velmi důležitým krokem je povolení virtualizace v BIOSu hostitelského počítače. V našem případě se jedná o základní desku od společnosti AMD, jejíž výchozí konfigurace BIOSu má tuto možnost zablokovanou, takže je nutné ji ručně povolit. Dalším krokem je stažení a instalace programu Oracle VirtualBox.

Dále byly staženy instalační soubory jednotlivých operačních systémů, konkrétně Windows 11 Pro a Ubuntu 24.04.2 LTS. Po stažení těchto souborů byly vytvořeny virtuální stroje pro každou komponentu. V laboratorním prostředí vzniknou tři virtuální stroje: jeden pro Zabbix Server, jeden pro Zabbix Agent pro operační systémy založené na Linuxu a jeden virtuální stroj pro komponentu Zabbix Agent 2, která běží na operačním systému Windows 11 Pro.

Po vytvoření všech tří virtuálních strojů byla provedena instalace jednotlivých operačních systémů. Zatímco operační systém Ubuntu je open-source, Windows vyžaduje aktivaci licence. Pro účely této diplomové práce je však dostačující i verze bez licence.

7.1.1 Vytvoření sítě ve virtuálním prostředí

K tomu, aby mezi sebou jednotlivé komponenty řádně komunikovaly, je nutné zajistit plnou konektivitu. V laboratorním prostředí proto byla vytvořena síť s IP adresou 192.168.10.0/24. V prostředí Oracle VirtualBox byla nastavena možnost dynamického přidělování adres z tohoto rozsahu. Přidělené adresy jsou neměnné – VirtualBox je přiřadí jednou a následně již nemění, což činí tento přístup ideálním pro testovací účely v prostředí s více virtuálními stroji.

Síťovou konfiguraci ověříme pomocí příkazu „ifconfig“ na všech komponentech. V tomto případě získal Zabbix Server adresu 192.168.10.6, linuxový Zabbix Agent adresu 192.168.10.4 a windowsový agent adresu 192.168.10.5.

Dále tuto konfiguraci otestujeme pomocí příkazu „ping“ na jednotlivé IP adresy. Úspěšný ping potvrdí výsledná hláška, kdy byly poslány čtyři pakety a všechny čtyři se vrátily s odpověďmi: „4 packets transmitted, 4 packets received.“ Viz obrázek.

8 INSTALACE NÁSTROJE ZABBIX

8.1 Instalace Zabbix serveru

Zabbix server lze nainstalovat několika způsoby. Na oficiálních webových stránkách nástroje Zabbix nalezneme různé varianty instalace a nasazení. Mezi ně patří klasické nasazení přímo na operační systém, například na Linux nebo Raspberry PI OS, či nasazení v cloudovém prostředí. Je však třeba poznamenat, že Zabbix server nelze nainstalovat na operační systém Windows.

Zabbix také nabízí možnost nasazení v Zabbix cloudu, což uživateli velmi usnadní práci, protože většina komponent a také síť je již předem nakonfigurována. Stačí tak jen nasadit řešení dle předem definovaného architektonického návrhu.

Další možností je instalace Zabbix serveru pomocí kontejnerů. Tato varianta je v dnešní době velmi populární, neboť mnoho společností upřednostňuje kontejnerizovanou infrastrukturu. Nejčastěji se k tomuto účelu používá nástroj Docker, případně systémy pro orchestraci jako Kubernetes.

Nicméně nejčastějším způsobem zůstává instalace Zabbix serveru přímo na operační systém, což byla i volba této praktické části.

Na hlavní webové stránce Zabbix byla vybrána předpřipravenou konfiguraci s nejnovější aktuální verzí serveru, tedy verzi 7.2. Dále byla zvolena instalace na Ubuntu ve verzi 24.04. a byly zahrnuty komponenty server, frontend, agent, databáze typu MySQL a webový server Apache.

Je třeba poznamenat, že konfigurace se může lišit dle potřeb zákazníka. Například pokud má zákazník vyškolené zaměstnance pro správu databáze PostgreSQL, nedává smysl instalovat MySQL. Totéž platí i pro výběr webového serveru.

V dalších krocích provedeme příkazy uvedené v dokumentaci. Samotná instalace je velmi jednoduchá a vyžaduje minimální zásahy uživatele.

Složitější úkol nastává při instalaci a hlavně konfiguraci databáze. Příkazy jsou náročnější a vzhledem k nutnosti vytvořit databázový účet s heslem je zde prostor pro chyby minimální. Po správném vytvoření databázového účtu je nutné tento účet definovat v konfiguračním souboru Zabbix serveru.

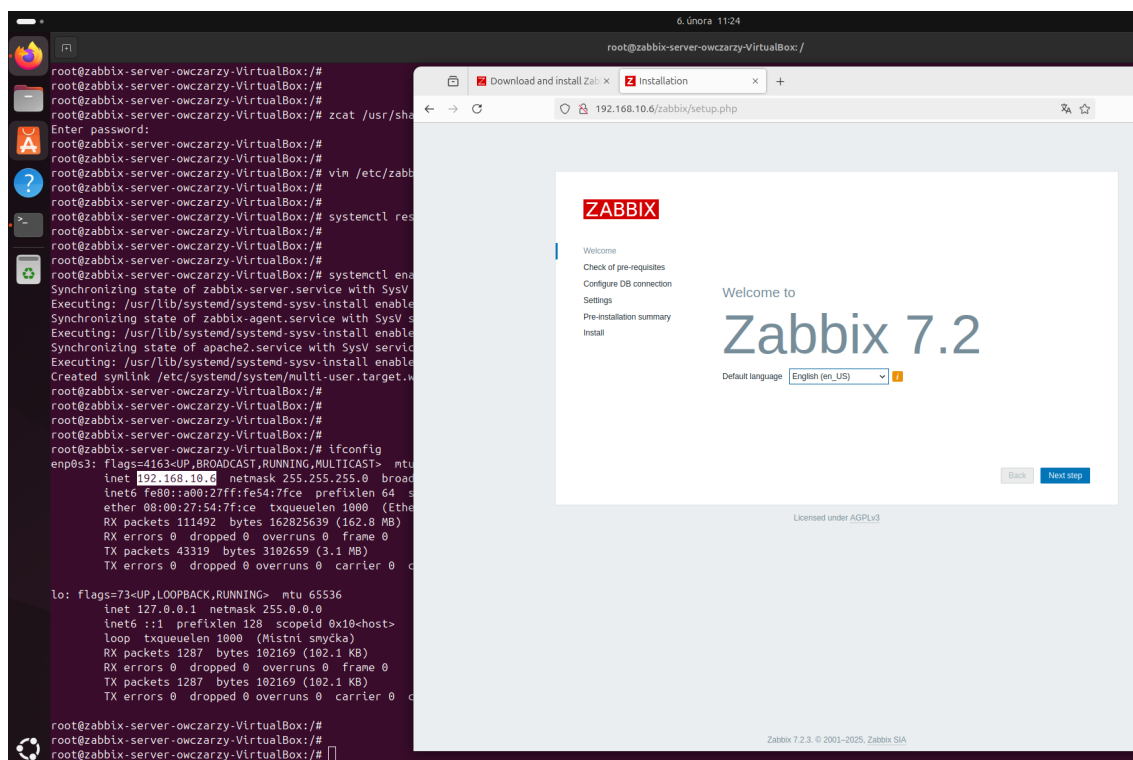
Výchozí lokace konfiguračního souboru pro Zabbix se nachází v adresáři `/etc/zabbix/`

zabbix_server.conf. Pro úpravu tohoto souboru lze použít řadu nástrojů, avšak z personálních důvodů byl zvolen editor vim. Úprava se provádí zadáním příkazu „vim“ následovného cestou k souboru – nebo, pokud se již nacházíme v adresáři, pouze názvem souboru.

V tomto souboru je nutné změnit parametry DBname, DBuser a DBpassword na hodnoty, které jsme vytvořili v databázi. V našem případě se jedná o DBname=zabbix, DBuser=zabbix a heslo, které z bezpečnostních důvodů nebude zveřejněno.

Následně je nutné restartovat Zabbix Server z důvodů propsání změn v konfiguračním souboru.

Po restartu bude uživatelské rozhraní Zabbix serveru dostupné na URL: <IP>/zabbix/setup.php. V tomto případě IP adresa odpovídá adrese našeho rozhraní, které získalo dynamicky přidělenou adresu 192.168.10.6 prostřednictvím Oracle VirtualBox.



Obrázek 8.1 Vystavení Zabbix frontendu, zdroj: vlastní

V uživatelském rozhraní je nutné přidat databázový účet, který byl vytvořen při instalaci. Další možnosti, jako je nastavení jazyka rozhraní nebo další konfigurace, lze upravit podle potřeb a preferencí.

8.2 Instalace Zabbix agenta na operačním systému Linux

V této sekci je popsán postup, jak nainstalovat klasického Zabbix agenta na linuxovém hostitelském počítači. Instalace je velmi podobná té u Zabbix serveru – Zabbix agent lze stáhnout jako balíček pomocí příkazové řádky nebo jako desktopovou aplikaci pomocí uživatelského rozhraní.

Společnost Axians, která se zaměřuje na řešení pro středně velké a velké zákazníky, využije obě možnosti nasazení. Instalace agenta přes příkazovou řádku je nejčastější, protože se jím monitorují linuxové servery. Na druhou stranu je pro velké společnosti, kde má každý zaměstnanec svůj laptop, rovněž velmi důležitá instalace Zabbix agenta jako desktopové aplikace. Pro monitoring těchto zařízení by mohl být ideálním řešením Zabbix Agent 2, který je dále podrobně popsán v následující sekci této praktické části.

Na oficiálních webových stránkách Zabbixu jsou k dispozici dva způsoby, jak nainstalovat Zabbix agenta na linuxovém hostitelském počítači. Pro linuxového agenta byla v této sekci vybrána instalace klasického Zabbix agenta pomocí balíčku.

V sekci Zabbix packages jsme zvolili instalaci nejnovější verze 7.2, dále distribuci pro Ubuntu verzi 24.04 a variantu Agent. Je zde také možnost instalace Zabbix Agent 2, o jehož rozdílech bude věnována samostatná sekce této praktické části.

Po úspěšné instalaci Zabbix agenta je nutné agenta nakonfigurovat tak, aby správně reagoval na požadavky Zabbix serveru. V konfiguračním souboru proto uvedeme IP adresu Zabbix serveru a také jméno Zabbix agenta. V tomto případě se jedná o IP adresu Zabbix serveru 192.168.10.6 a jméno agenta bylo nakonfigurováno jako `Zabbix_agent_0wczarzy`.

8.3 Přidání linuxového hosta na Zabbix Server

Seznam hostů je v uživatelském rozhraní v sekci Sběr dat a následně v záložce Hosté. V této záložce se nachází tlačítko Přidat hosta. Po kliknutí se zobrazí vyskakovací okno. V tomto okně je nutné zadat stejné jméno agenta, jaké jsme zadali v konfiguračním souboru na agentovi. Dále se zde nachází výběr šablony.

Šablona na Zabbix serveru představuje předdefinovanou sadu konfigurací, která obsahuje položky monitorování, spouštěče, grafy a další parametry potřebné k monitorování zařízení nebo služeb. Díky šablonám je možné snadno aplikovat jednotné monitorovací nastavení

na více hostitelů, což výrazně zjednodušuje správu a údržbu monitorovací infrastruktury. Například při monitorování serverů se stejným operačním systémem můžete vytvořit jednu šablonu, která definuje všechny relevantní metriky a upozornění, a tuto šablonu následně přiřadit ke všem daným serverům. V tomto případě byla použita výchozí šablona Linux by Zabbix agent.

Dále je třeba přidat IP adresu Zabbix agenta. V tomto případě se jedná o adresu 192.168.10.4, na kterou budou ze strany Zabbix serveru odesílány požadavky o data. Tento agent pracuje v pasivním režimu.

V Zabbixu existují dva základní typy agentů – pasivní a aktivní, které se liší způsobem komunikace se Zabbix serverem. Pasivní agent čeká na dotazy ze strany serveru nebo proxy; server se tak periodicky dotazuje na konkrétní metriky a agent na ně odpovídá. Tento způsob vyžaduje, aby byl agent vždy dostupný a aby síťová konfigurace či firewall neblokovaly příchozí požadavky. Naopak aktivní agent sám iniciuje komunikaci se Zabbix serverem nebo proxy a pravidelně odesílá nasbíraná data bez toho, aby byl server aktivně dotazován. Tento model je vhodný zejména v prostředích, kde je omezený příchozí provoz nebo kde jsou stanovena přísná bezpečnostní pravidla.

Jakmile Zabbix server odešle požadavek na IP adresu agenta a obdrží jeho odpověď, zobrazí se data v uživatelském rozhraní. Hodnoty jsou pak k vidění v sekci „Sledování“ pod záložkou „Poslední hodnoty“, kde je přehledně uvedeno, jaká metrika byla zaznamenána, jaká hodnota byla obdržena a kdy proběhla poslední kontrola. Obdržená data se rovněž automaticky zobrazují v sekci „Sledování“ v záložce „Hosté“, kde Zabbix server generuje grafy z naměřených hodnot.

8.4 Instalace Zabbix agenta na operačním systému Windows

V této sekci bude už výše zmíněná instalace Zabbix agenta pro desktopovou verzi hostitele. V této sekci bude nainstalována verze Zabbix Agent 2. Dále zde také bude nainstalována verze aktivního agenta.

Zabbix agent a Zabbix agent 2 se liší především ve své architektuře a implementaci. Zabbix agent, který je starší, je napsán v jazyce C a využívá synchronní metody pro sběr dat. Naopak Zabbix agent 2 představuje modernější variantu, která je vyvíjena s modulární architekturou a podporou dynamicky načítaných modulů. Díky této modulárnosti lze snadno



Obrázek 8.2 Grafy po přidání Zabbix agenta, zdroj: vlastní

přidávat nové funkce bez zásahu do základního kódu, což usnadňuje rozšiřování a přizpůsobení monitorovacího řešení specifickým potřebám. Další výhodou Zabbix agent 2 je podpora asynchronního zpracování dat, což může vést k vyšší výkonnosti a lepší škálovatelnosti zejména v náročnějších monitorovacích prostředích.

Zabbix Agent 2 přináší také možnost zabezpečení přenosu pomocí PSK. PSK je zkratka pro "Pre-Shared Key", tedy předem sdílený klíč. V Zabbix Agent 2 se tento klíč používá pro zabezpečenou komunikaci mezi agentem a serverem. Obě strany – server i agent – mají předem nastavenou stejnou hodnotu PSK, což umožňuje ověření identity a šifrování dat, aniž by bylo potřeba využívat certifikáty. Tím se zvyšuje bezpečnost přenášených informací a zabráňuje se neautorizovanému přístupu k monitorovaným datům. Zabezpečení pomocí PSK bude věnována samostatná kapitola v této praktické části.

Z oficiálního webu monitorovacího nástroje Zabbix je potřeba najít desktopovou verzi v záložce Zabbix Agent. Zde je možné si stáhnout všechny dostupné Zabbix Agent desktopové distribuce. Je zde na výběr mezi Windows, Linux desktopovými distribucemi, ale třeba i macOS nebo třeba operační systém Solaris.

Zde byla vybrána verze agenta 7.2 pro hardware amd64, zabezpečení OpenSSL a balíček jako MSI. Hardware "amd64" označuje 64bitovou architekturu procesoru, což znamená, že software je optimalizován pro systémy s 64bitovým operačním systémem a odpovídajícím hardwarem. "Zabezpečení OpenSSL" pak znamená, že pro šifrování a bezpečnou komunikaci mezi komponentami Zabbix agenta 2 a serverem se využívá knihovna OpenSSL, která poskytuje implementaci šifrovacích protokolů a zajišťuje bezpečnost dat. Balíček ve formátu MSI je instalační balíček pro operační systém Windows, který umožňuje snadnou a standardizovanou instalaci Zabbix agenta 2 prostřednictvím Windows Installeru.

Po stažení verze Zabbix Agent 2 a otevření instalačního souboru se zobrazí konfigurační okno, ve kterém zadáme potřebné informace pro Windows agenta. Jako název hosta bylo zvoleno jméno ZABBIX_AGENT. Tento název je klíčový, protože při přidávání hosta do Zabbix serveru musí být zadán přesně, aby server dokázal správně identifikovat zařízení v síti. Dále byla nastavena IP adresa Zabbix serveru a port, na kterém agent naslouchá požadavkům serveru – v tomto případě byl ponechán výchozí port 10050. Rovněž jsme zadali IP adresu serveru pro aktivní kontrolu.

V tomto případě byla u Windows agenta otestována funkce aktivních kontrol.

Rozdíl mezi aktivními a pasivními kontrolami spočívá v tom, že u pasivních kontrol Zabbix server iniciuje dotazy přímo na agenta, který následně reaguje a poskytuje požadovaná data. Naopak u aktivních kontrol agent sám navazuje spojení se serverem a pravidelně odesílá nasbíraná data, aniž by byl server přímo vyzván. Aktivní kontroly jsou zvláště vhodné v situacích, kdy je agent chráněn firewallem nebo se nachází v prostředí s omezeným příchozím provozem, protože umožňují flexibilnější a spolehlivější monitorování.

Po dokončení konfigurace se Zabbix Agent 2 automaticky spustí, což lze ověřit ve Správci úloh v záložce Procesy – zde bude proces Zabbix Agent 2 zobrazen jako spuštěný. Následně je nutné přidat Zabbix agenta i na straně Zabbix serveru. Tento krok probíhá obdobně jako při přidávání Linuxového Zabbix agenta, avšak s tím rozdílem, že v tomto procesu je vybrána šablona „Windows by Zabbix agent active“. Tato šablona umožňuje zobrazovat metriky odesílané agentem na server. Poté daného hosta přiřadíme do příslušné skupiny – v tomto případě byla vytvořena nová skupina s názvem „Windows Servers“.

Nové zařízení

Hostitel IPMI Značky Makra Inventář Šifrování Mapování hodnot

* Název hosta ZABBIX_AGENT

Zobrazované jméno ZABBIX_AGENT

Šablony Windows by Zabbix agent active X Vybrat
pište zde pro vyhledávání

* Skupina hostů Windows Servers (nový) X Vybrat
pište zde pro vyhledávání

Rozhraní Nejsou definována žádná rozhraní.
[Přidat](#)

Popis

Monitorováno Server Proxy Skupina proxy

Povoleno ☒

[Přidat](#) [Zrušit](#)

Obrázek 8.3 Přidávání Windows agenta s aktivními kontrolami, zdroj: vlastní

Po přibližně třech minutách se začnou zobrazovat příchozí metriky na Zabbix serveru. Tyto metriky lze následně zkontrolovat přímo u hosta nebo pomocí grafů, kde jsou data přehledně vizualizována.

9 AUTOMATICKÁ DETEKCE ZABBIX AGENTA V SÍTI

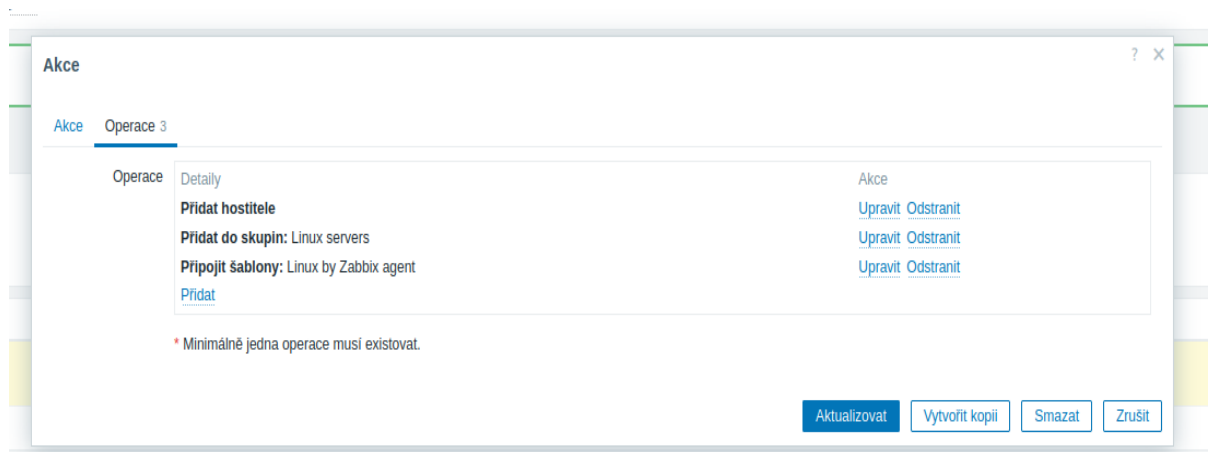
Automatická detekce v Zabbixu umožňuje dynamické přidávání nových hostitelů do monitorovacího systému bez nutnosti manuálního zásahu. Tento proces vychází z pravidel, která definují, jaké zařízení nebo služby mají být automaticky objeveny, a následně automaticky přidány do Zabbixu. V rámci automatické detekce se nejčastěji využívá tzv. network discovery, kdy Zabbix pravidelně prohledává síť a identifikuje nové hostitele podle zadaných kritérií, například pomocí IP rozsahu nebo jiných identifikačních parametrů [71].

V této práci bude využita možnost přidávání hostitelů pomocí metadat, konkrétně s využitím určitého řetězce (stringu). Tento přístup umožňuje definovat metadata, která jsou přiřazena ke každému nově objevenému zařízení. Pokud metadata obsahují specifikovaný řetězec, Zabbix automaticky přiřadí danému hostiteli příslušnou šablonu, skupinu nebo další konfigurační parametry. Tímto způsobem lze snadno a rychle rozšířit monitorovací infrastrukturu a zajistit, že všechny nové hostitele splňující definovaná kritéria budou správně monitorovány bez nutnosti ručního zásahu.

Celkově proces automatické detekce nejen zjednodušuje správu monitorovaného prostředí, ale také zvyšuje efektivitu, jelikož zajišťuje, že nové prvky v síti jsou okamžitě začleněny do systému a monitorovány podle předem definovaných pravidel.

V této praktické části bylo demonstrováno, jak přidat linuxového agenta pomocí automatické detekce za využití metadat obsahujících řetězec „linux“.

Nejprve byl na Zabbix serveru odebrán linuxový host, aby bylo možné později využít automatické detekce. Následně v záložce Upozornění v sekci Akce nalezneme volbu „Akce autoregistrace“. V pravém horním rohu se nachází tlačítko pro vytvoření nové akce. Po jeho stisknutí se zobrazí vyskakovací okno, ve kterém je třeba zadat název akce a přidat podmínku. V tomto případě byla použita podmínka, že pokud metadata agenta obsahují řetězec „linux“, přidej agenta. Byla tedy vybrána podmínka „Host metadata“ s hodnotou „linux“. Následně byly přidány operace, které se spustí, pokud bude tato podmínka splněna. Konkrétně bude host automaticky přidán a přiřazen do skupiny „Linux servers“ a bude mu rovněž přiřazena šablona „Linux by Zabbix agent“.



Obrázek 9.1 Pravidlo pro automatickou detekci linuxového agenta, zdroj: vlastní

Na straně Zabbix agenta je třeba v jeho konfiguračním souboru uvést příslušný řetězec metadat. Proměnná tedy bude vypadat následovně: `HostMetadata=linux`. Je důležité poznamenat, že proměnná `HostMetadata` je ve výchozím nastavení zakomentována, proto je nutné odstranit mřížku před touto proměnnou. Po uložení a ukončení souboru je nutné restartovat Zabbix agenta, aby se změny v konfiguraci projeví. Toho docílíme zadáním příkazu: `service zabbix-agent restart`. Následně můžeme ověřit stav agenta příkazem: `service zabbix-agent status`.

Po přibližně třech minutách bude automatická registrace úspěšně provedena a nový host bude přidán na Zabbix server. Zabbix server automaticky zařadí tohoto hosta do skupiny „Discovered hosts“, což umožní snadné rozlišení mezi automaticky přidanými a ručně konfigurovanými hosty.

10 ZABEZPEČENÍ KOMUNIKACE MEZI AGENTEM A SERVEREM

Zabezpečení komunikace mezi Zabbix agentem a serverem je nezbytné pro ochranu citlivých dat a zajištění integrity monitorovací infrastruktury. Monitorovací data mohou obsahovat informace o výkonu, konfiguraci a potenciálních zranitelnostech systémů, a proto je klíčové zajistit, aby tato data nebyla zachycena nebo pozměněna neautorizovanými subjekty. Zabezpečení také pomáhá předcházet útokům typu „man-in-the-middle“, kdy by útočník mohl narušit komunikaci a vložit škodlivé informace.

V rámci této diplomové práce bude pro zabezpečení komunikace využit mechanismus pre-shared key (PSK). PSK představuje předem sdílený klíč, který je nakonfigurován jak na Zabbix agentu, tak i na Zabbix serveru. Při navázání spojení se obě strany vzájemně ověří pomocí tohoto klíče. Pokud se klíče shodují, naváže se šifrované spojení, které zaručuje integritu a důvěrnost přenášených dat. Pokud by došlo k nesouladu, spojení je okamžitě odmítnuto, čímž se zamezí případným útokům.

Použití PSK má několik výhod. Za prvé, jeho implementace je relativně jednoduchá, protože stačí nastavit stejnou hodnotu klíče na všech zařízeních, která mají komunikaci zabezpečit. Za druhé, PSK poskytuje efektivní ochranu v kontrolovaných prostředích, jako jsou interní monitorovací systémy, kde jsou zařízení umístěna za důvěryhodnými firewally a dalšími bezpečnostními opatřeními.

Implementace PSK v Zabbix agentu 2 využívá šifrovací knihovnu OpenSSL, která zajišťuje moderní šifrovací protokoly. Díky tomu je zajištěna bezpečná výměna dat mezi agentem a serverem, což přispívá k celkové stabilitě a bezpečnosti monitorovaného prostředí.

Celkově lze říci, že zabezpečení komunikace pomocí pre-shared key je klíčovým prvkem pro ochranu monitorovacích dat v Zabbixu. Díky němu je možné minimalizovat riziko úniku citlivých informací a narušení provozu, což je v dnešním digitálním prostředí naprosto nezbytné.

V této praktické části bude generován 256bitový klíč.

Tento klíč byl vygenerován pomocí příkazu OpenSSL:

```
openssl rand -hex 32
```

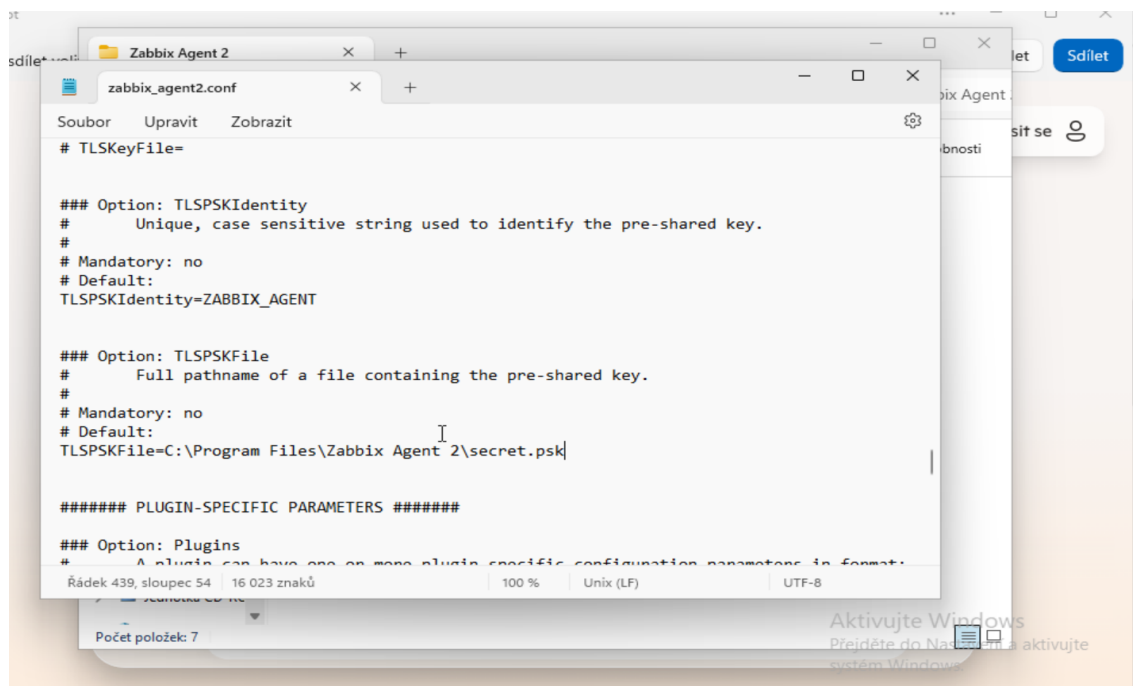
OpenSSL je open-source knihovna pro implementaci kryptografických funkcí a protokolů, která umožňuje generovat šifry a další bezpečnostní prvky, používaná zejména pro

zabezpečenou komunikaci. V uvedeném příkazu OpenSSL vygeneruje 32 bajtů (tedy 256 bitů) náhodných dat ve formě hexadecimálního řetězce.

PSK komunikace je možná pouze s využitím Zabbix agenta 2. V tomto případě se jedná o Windows agenta. I když byl klíč původně vygenerován pomocí OpenSSL na linuxovém systému, byl následně zkopírován a uložen na Windows agenta. Klíč byl uložen do adresáře `C:\Program Files\Zabbix Agent 2\secret.psk`. Při této operaci je nutné spustit Poznámkový blok jako administrátor, vložit dříve vygenerovanou hodnotu a uložit soubor jako typ „všechny soubory“. Pokud by nebyla vybrána správná volba typu souboru, systém by soubor uložil s příponou `.txt`.

Dalším krokem bylo upravit konfiguraci Zabbix agenta 2. Pro tento účel byl opět spuštěn Poznámkový blok jako administrátor a otevřen konfigurační soubor Zabbix Agent 2. V sekci `TLS-RELATED PARAMETERS` bylo nutné provést následující změny:

- `TLSConnect=psk` – tato proměnná určuje, že agent se při navazování spojení bude připojovat pomocí předem sdíleného klíče.
- `TLSAccept=psk` – touto proměnnou se specifikuje, že agent bude akceptovat příchozí spojení, pokud jsou zabezpečena pomocí PSK.
- `TLSPSKIdentity=ZABBIX_AGENT` – tato proměnná definuje identitu agenta. Musí být totožná jak na straně agenta, tak na straně serveru, aby bylo možné správné ověření.
- `TLSPSKFile=C:\Program Files\Zabbix Agent 2\secret.psk` – touto proměnnou je specifikována cesta k souboru obsahujícímu PSK klíč. U operačního systému Windows mohou být v cestě mezery, což je třeba respektovat. Na Linuxu naopak systém mezery v názvech souborů neřeší stejným způsobem.



Obrázek 10.1 Konfigurace PSK na straně Windows agenta, zdroj: vlastní

Po uložení konfiguračního souboru je nutné restartovat Zabbix agenta 2. Tuto akci provedeme ve Správci úloh v záložce Služby – stačí pravým tlačítkem kliknout na službu Zabbix Agent 2 a zvolit možnost restartovat.

Po této konfiguraci na straně Zabbix serveru může dojít ke zpozorování problému s komunikací, pokud server ještě neobsahuje odpovídající PSK klíč. V takovém případě bude Zabbix server veškerý příchozí provoz od tohoto Windows agenta okamžitě odmítat, protože se klíče neshodují.

K přidání PSK klíče k danému agentovi byla na straně Zabbix serveru rozkliknuta konfigurace hostitele. V záložce Šifrování byla vybrána volba „Připojení k agentovi jako PSK“ i „Připojení od agenta jako PSK“. Poté se zobrazila pole pro zadání PSK Identity, která musí být shodná s hodnotou uvedenou v konfiguračním souboru (`TLSPSKIdentity=ZABBIX_AGENT`), a pole pro zadání PSK hodnoty. Tato hodnota musí přesně odpovídat hodnotě uložené v souboru `secret.psk`. Po kontrole všech údajů se klikne na tlačítko Aktualizovat.

V přehledu agentů se poté zobrazí Zabbix Agent 2, spuštěný na operačním systému Windows, s označením zabezpečení PSK – v sloupci Agent Encryption bude viditelná zelená ikonka, která signalizuje, že komunikace probíhá pomocí PSK.

11 VYTVÁŘENÍ METRIK

Manuální přidávání metrik (items) v Zabbixu poskytuje řadu výhod, zejména ve středně velkém IT prostředí, kde je nutné precizně konfigurovat monitorovací parametry podle specifických provozních požadavků. Tento přístup umožňuje detailní úpravu sběru dat – definovat přesné intervaly měření, nastavovat prahové hodnoty, či parametrizovat upozornění na události – a poskytuje tak vyšší míru kontroly nad monitorovanou infrastrukturou. Manuální konfigurace je ideální v situacích, kdy předdefinované šablony nedostačují k zachycení unikátních charakteristik sledovaných systémů nebo aplikací, což umožňuje efektivně identifikovat abnormality a reagovat na specifické provozní podmínky.

V této kapitole praktické části bude otestováno, zda Zabbix server umožňuje vytváření metrik podle údajů uvedených v dokumentaci.

Nejprve je nutné odstranit šablonu z daného hosta. Toho bylo dosaženo tak, že po rozkliknutí hosta v sekci šablon se zobrazila možnost „odpojit“ (unlink) a poté byla smazána příslušná šablona.

Následně, po zavření okna, byla v pravém horním rohu zvolena možnost „nový item“. Pro účely testování této funkce bylo rozhodnuto vytvořit položku představující ping pro Zabbix agenta. Nejprve je nutné položku pojmenovat. Zde byl zvolen název „Zabbix Agent ping“. Dále se jako typ položky vybere „Zabbix agent“ a jako klíč (tedy metrika), kterou budeme monitorovat, se uvede „agent.ping“. Zabbix server nabízí velké množství metrik, z nichž každá obsahuje informace o vrácených hodnotách a jejich významu. Tyto informace jsou důležité, protože správná interpretace hodnot monitorovaných metrik je klíčová pro správnou diagnostiku a vyhodnocení stavu sledovaného zařízení.

Typ informace byl v tomto případě nastaven na „Číslo (unsigned)“. Mezi další dostupné typy informací v Zabbixu patří například:

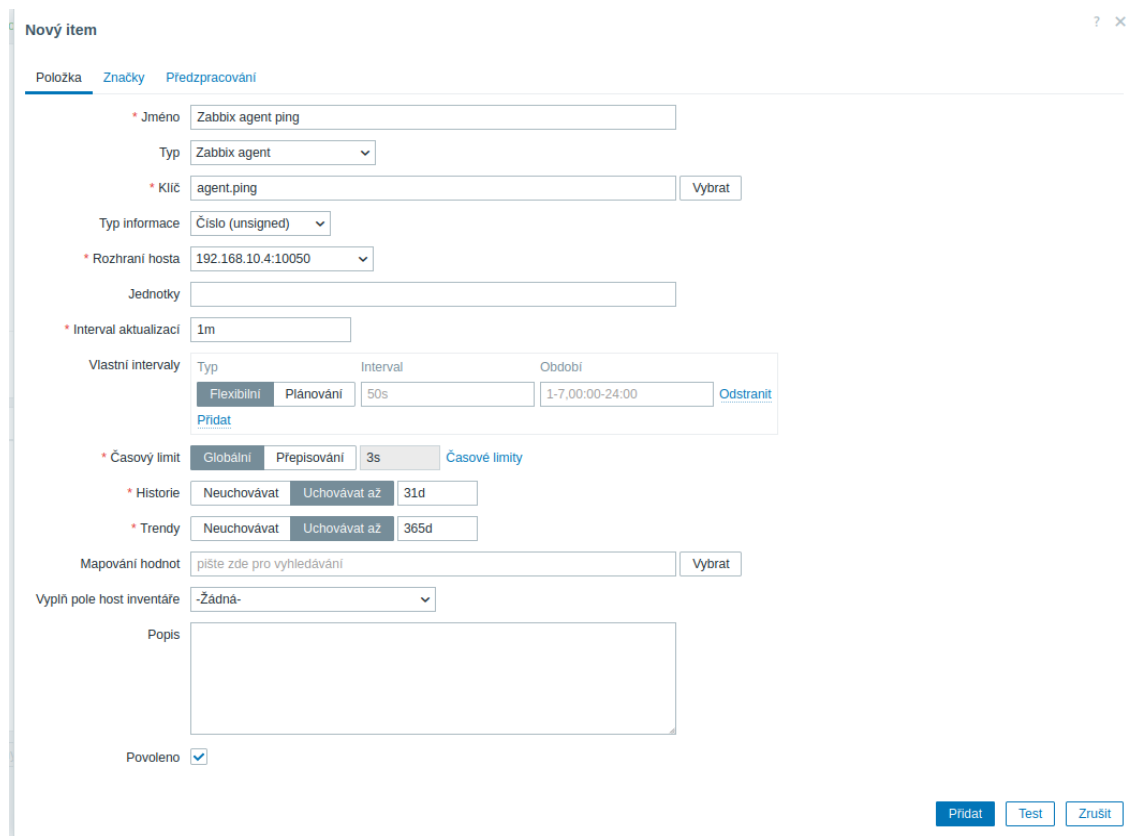
- Numerické (float): Umožňuje zadat desetinné hodnoty.
- Textové (Character): Slouží pro monitorování textových řetězců.
- Log: Určeno pro sledování logovacích dat.
- Text: Pro zadávání delších textových informací či poznámek.

Protože agenti použití v této praktické části mají pouze jedno síťové rozhraní s přiřazenou IP adresou, byla v sekci „Rozhraní hosta“ vybrána právě tato jediná možnost.

Dále je nutné nastavit následující parametry:

- Update interval: Udává, jak často bude položka monitorována. V této konfiguraci bude nastaven na 1 minutu.
- Timeout: Určuje maximální dobu čekání na odezvu, po jejímž uplynutí je vyhlášena chyba. Nastaveno bude na 3 sekundy.
- History: Určuje dobu, po kterou budou uchovávány detailní historické záznamy hodnot položky. Zde bude nastavena na 31 dní.
- Trends: Udává dobu, po kterou budou uchovávány agregované historické hodnoty pro účely trendové analýzy. V této konfiguraci bude nastavena na 365 dní.

Po uložení položky se zobrazí možnost jejího testování, která se nachází v pravém dolním rohu. Po kliknutí se otevře další okno, kde bude možné ověřit, jakou hodnotu ping vrátí – a zároveň, že typ informace odpovídá nastavení („unsigned“). Pokud by byl zvolen například typ informace „float“ a vrácená hodnota by s tímto typem neodpovídala, Zabbix server by vyhlásil chybovou hlášku o nesouladu typu informace s hodnotou uvedenou v klíči.



Obrázek 11.1 Zabbix agent ping, zdroj: vlastní

11.1 Tvorba pokročilejší metriky

Dále byla demonstrována pokročilejší metrika, konkrétně zjištění, kolik procent výkonu procesoru využívá daný uživatel. Toto bylo dosaženo velmi podobným způsobem jako u metriky ping. Jméno položky bylo zvoleno „CPU Util (User)“, přičemž typ položky zůstává nastaven na Zabbix agent, protože monitorovaným subjektem je opět Zabbix agent.

Jako klíč byl vybrán „system.cpu.util“. Tato metrika nabízí možnost sledovat různé parametry, například „user“, „system“, „idle“ a další, které určují rozložení využití CPU. V této konfiguraci byl vybrán pouze parametr „user“ a ostatní možnosti byly odstraněny.

Jako jednotka byla nastavena hodnota v procentech, což odpovídá názvu položky, jelikož se jedná o využití procesoru, které se běžně udává právě v procentech. Použité rozhraní hosta je stejné jako v předchozí demonstraci, interval aktualizací je rovněž stejný. Parametry pro uchovávání Historie a Trendů zůstaly také nezměněny.

Vzhledem k tomu, že se jedná o pasivní kontroly, budou hodnoty na straně Zabbix serveru viditelné po přibližně třech minutách.

12 SPOUŠTĚČE

Spouštěče (Triggers) v Zabbixu jsou mechanismus, který automaticky vyhodnocuje získaná data a signalizuje potenciální problémy v monitorovaném prostředí. Každý spouštěč je definován pomocí logické podmínky, která vychází z hodnot metrik. Pokud podmínka splní stanovené kritérium (například, když vytížení CPU přesáhne určitou hranici nebo dojde k nedostupnosti služby), spouštěč aktivuje upozornění.

Tento nástroj má v praxi řadu užitečných využití ve středně velkých firmách. Například:

- **Automatizované upozornění:** Spouštěče okamžitě informují administrátory o výskytu problémů, což umožňuje rychlou reakci a minimalizaci výpadků nebo degradace služeb.
- **Prevence a optimalizace:** Díky pravidelnému monitorování kritických parametrů mohou firmy dříve identifikovat potenciální problémy, optimalizovat provoz a plánovat kapacity s ohledem na růst.
- **Sledování trendů:** Spouštěče lze konfigurovat tak, aby sledovaly dlouhodobé trendy v chování systémů, což pomáhá při strategickém rozhodování a plánování údržby infrastruktury.
- **Centralizované řízení incidentů:** Ve středně velkých firmách, kde je často více systémů a aplikací, umožňují spouštěče centralizované monitorování a správu incidentů, čímž se zjednodušuje práce IT oddělení.

Celkově jsou spouštěče klíčovým prvkem monitorovacího systému Zabbix, neboť zajišťují, že správci jsou okamžitě upozorněni na neobvyklé a potenciálně kritické situace, což přispívá k efektivnější správě a udržení kontinuity provozu firmy.

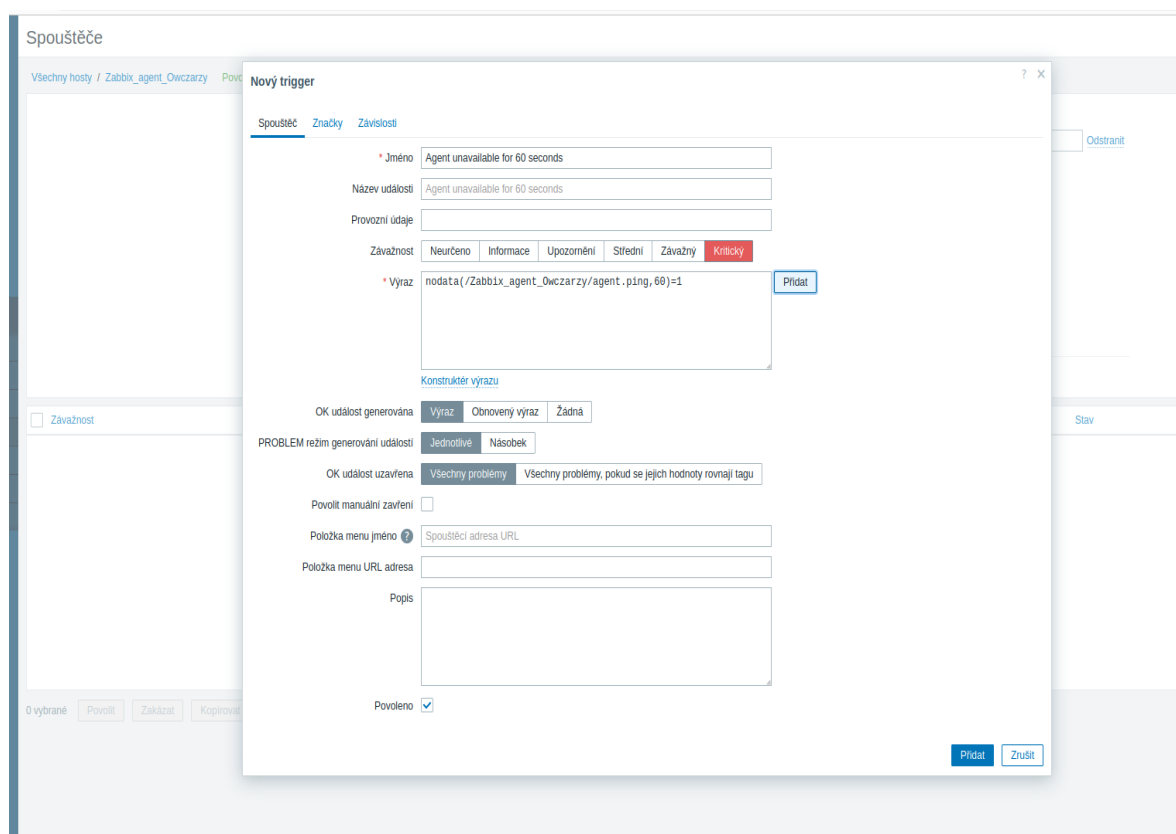
V této sekci praktické části je demonstrováno, jak vytvořit spouštěče (triggers) v Zabbixu. Konkrétně byl nastaven spouštěč, který vytvoří kritickou situaci, pokud agent nebude mít data po dobu 60 sekund. V Zabbixu existuje šest kategorií závažnosti: neurčeno, informace, upozornění, střední, závažný a kritický.

V sekci sběru dat v záložce „Hosté“ je zobrazen přehled všech dostupných i nedostupných hostů. V některém sloupci je možné kliknout na spouštěč konkrétního agenta. Po prokliku se objeví okno, ve kterém, v pravém horním rohu, najdeme tlačítko na přidání hosta.

Pro chybějící data po dobu 60 sekund byl vytvořen spouštěč s názvem „Agent unavailable for 60 seconds“ a jako závažnost byla nastavena hodnota kritická. Klíčovým prvkem spouštěče je podmínka, kdy se má aktivovat. V tomto případě byl jako položka zvolen „Zabbix Agent ping“ (dříve vytvořený item). Jako funkce byla použita funkce `nodata()`, tedy "No data received during period T"(1 – pravda, 0 – nepravda). Pokud agent neodpoví na ping požadavek, výsledná hodnota funkce je 1. Časový úsek byl nastaven na 60 sekund, takže výsledná podmínka zní: pokud agent nebude mít data po dobu 60 sekund, funkce `nodata()` vrátí hodnotu 1. V Zabbixu se tato podmínka zobrazí jako:

```
nodata(/Zabbix_agent_0wczarzy/agent.ping,60)=1
```

Na závěr konfigurace spouštěče je nutné zaškrtnout políčko pro aktivaci, aby byl spouštěč funkční.



Obrázek 12.1 Spouštěč pro nedostupnost hosta, zdroj: vlastní

Dalším pokročilejším spouštěčem, který byl vytvořen v rámci této diplomové práce, je spouštěč aktivující se, pokud kterýkoliv uživatel na agentovi využívá více než 75% procesového výkonu po dobu 2 minut. Při tvorbě tohoto spouštěče byl použit stejný postup jako u předchozího. Při tvorbě výrazu byla využita funkce `avg()` – tedy průměrná hodnota v daném

časovém intervalu T, přičemž byla zvolena hodnota 120 (což odpovídá 120 sekundám; ve výchozím nastavení jsou hodnoty udávány ve vteřinách, případně lze přidat jednotky, například 5m). Výsledek této podmínky byl nastaven na $> 0,75$.

Celkový výraz pro tento spouštěč zní:

```
avg(/Zabbix_agent_0wczarzy/system.cpu.util,[,user],120) > 0.75
```

To znamená, že pokud daný uživatel v průměru využívá více než 75% procesorového výkonu po dobu 2 minut, spouštěč se aktivuje. Následně lze tento spouštěč otestovat pomocí tlačítka umístěného v pravém dolním rohu, po jehož stisknutí se zobrazí okno, ve kterém Zabbix provede testování spouštěče na základě zadaných hodnot.

12.1 Upozornění pomocí e-mailu

K tomu, aby Zabbix mohl posílat emailová upozornění, je třeba nejprve nastavit SMTP server. Konfigurace SMTP serveru v Zabbixu se provádí prostřednictvím webového administračního rozhraní. Uživatel s odpovídajícími právy přistoupí do sekce pro správu typů médií, kde je možné buď upravit přednastavený e-mailový kanál, nebo si vytvořit nový, vlastní typ. Při vytváření tohoto typu se určuje název, který by měl reflektovat poskytovatele nebo charakter spojení, dále je nutné vyplnit adresu SMTP serveru a port, na kterém komunikuje. Typicky se využívá port 587 v kombinaci s šifrováním STARTTLS, případně port 465 pro spojení typu SSL/TLS. Dále je třeba zadat tzv. HELO identifikátor, což je zpravidla doména, ze které je komunikace vedena, a e-mailovou adresu, která bude používána jako odesílatel notifikací.

Pokud SMTP server vyžaduje ověření identity, což je u moderních poskytovatelů e-mailových služeb běžné, zadává se také uživatelské jméno a heslo k danému účtu. Po uložení této konfigurace je nový typ média připraven k použití a Zabbix jej může využívat pro odesílání zpráv.

Druhým krokem, který je nezbytný pro to, aby upozornění fungovalo, je přiřazení média konkrétním uživatelům systému Zabbix. Každý uživatel, který má být o událostech informován, musí mít v rámci svého profilu definován typ média, kterým chce notifikace přijímat, a adresu, na kterou mu mají být zprávy doručeny. Zároveň je třeba specifikovat časový rozsah, kdy jsou notifikace aktivní, a úroveň závažnosti událostí, na které má systém reagovat. To umožňuje zacílit upozornění pouze na relevantní incidenty a snížit tak množství rušivých

zpráv.

Jakmile je SMTP server nastaven a typ média přidělen konkrétním uživatelům, přichází na řadu propojení s logikou systému upozorňování, které se v Zabbixu realizuje pomocí tzv. akcí. Akce představují reakce na určité události vyvolané spouštěči. Trigger je definice stavu, který je považován za abnormální – například situace, kdy nedojde k odpovědi z monitorovaného serveru po stanovený časový interval, nebo kdy dojde k překročení prahové hodnoty zátěže procesoru.

Pro každou takovou událost lze definovat jednu nebo více akcí, které specifikují, jaký typ reakce má být proveden. V případě e-mailového upozornění se tedy vytvoří akce, která reaguje na aktivaci daného triggeru a odešle zprávu uživateli nebo skupině uživatelů, jejichž profily obsahují námi nakonfigurovaný typ média. Při definici akce je možné přesně určit, pro jaké typy událostí se má aktivovat – lze ji například omezit pouze na vybrané hosty, host groupy nebo konkrétní závažnosti problémů. V rámci jedné akce je rovněž možné nastavit více úrovní notifikace, tzv. eskalace. Ty slouží například k tomu, aby v případě přetrvávajícího problému systém po určitém čase kontaktoval další osobu nebo změnil způsob upozornění.

Po zavedení těchto kroků je vhodné provést testování správnosti nastavení. K tomu lze využít buď simulaci události, nebo vytvoření testovacího triggeru, který vyvolá notifikaci. Pokud se upozornění neodešle, je nutné zkontrolovat logy Zabbix serveru, které často obsahují detailní popis problému – například odmítnuté připojení, špatnou autentizaci nebo problémy s TLS handshake.

13 BEZAGENTOVÉ MONITOROVÁNÍ

Pro uspokojení potřeb společnosti Axians bylo v této diplomové práci také odzkoušeno bez-agentové monitorování pomocí Zabbixu.

Ne všechna zařízení umožňují instalaci monitorovacího agenta přímo na svůj operační systém, což platí například pro síťové prvky, tiskárny, IoT zařízení či některé uzavřené aplikační servery. V těchto případech je nutné najít alternativní způsob sběru dat. Ideálním řešením je využití protokolu SNMP (Simple Network Management Protocol).

SNMP je standardizovaný protokol používaný pro dohled a správu zařízení v síti. Umožňuje sběr informací o výkonu, stavu a konfiguraci bez nutnosti instalace speciálního softwaru na samotném zařízení. SNMP pracuje na modelu management station (řídící server) a agents (spravovaná zařízení), přičemž zařízení odpovídají na dotazy [72].

Pro účely společnosti Axians bylo jako preferované řešení vybráno a otestováno bez-agentové monitorování prostřednictvím protokolu SNMPv3, tudíž nejvyšší a nejvíce bezpečná dostupná verze.

SNMPv3 oproti starším verzím (SNMPv1 a SNMPv2c) přináší zásadní výhody v oblasti bezpečnosti. Podporuje:

- Autentizaci – ověřování identity uživatele, který se pokouší o přístup k monitorovaným datům.
- Šifrování – ochranu přenášených dat před odposlechem a manipulací.
- Kontrolu přístupu – detailní řízení oprávnění pro jednotlivé uživatele.

V rámci tohoto řešení bylo pro Axians použito zabezpečení na bázi SHA (Secure Hash Algorithm) pro autentizaci a AES128 (Advanced Encryption Standard, 128bitový klíč) pro šifrování přenášených dat.

Konkrétně v SNMPv3 se zabezpečení opírá o dvě hlavní bezpečnostní hesla:

- Authorization password (heslo pro autentizaci) — toto heslo je použito k ověření identity monitorovací stanice (například Zabbix serveru) vůči zařízení. Za pomoci algoritmu SHA je ze zadaného hesla vytvořen kontrolní otisk (hash), který zařízení ově-

řuje. Díky tomu je možné zajistit, že data přijímá nebo odesílá skutečně oprávněný uživatel.

- Privacy password (heslo pro šifrování) — toto heslo je využito k zašifrování samotných datových přenosů mezi monitorovacím serverem a zařízením. Použitím algoritmu AES128 jsou přenášené SNMP zprávy šifrovány tak, aby nebyly čitelné při případném odposlechu na síti.

Tato kombinace bezpečnostních mechanismů umožňuje zajistit jak důvěrnost, tak integritu dat v prostředí, kde je vyžadována vysoká úroveň zabezpečení. Zároveň zůstává kompatibilní s většinou moderních síťových zařízení. Společnost Axians klade důraz na bezpečnost svých řešení, proto v tomto případě byl protokol verze 3 jasnou volbou.

13.1 Ochrana před útoky díky použití SNMPv3

Jak již bylo zmíněno, v této práci byly použity zabezpečovací algoritmy AES a SHA. Toto zabezpečení předchází hned několika útokům :

- Ochrana proti odposlechu dat (Eavesdropping) Šifrování pomocí AES-128 zajišťuje, že přenášená SNMP data (například konfigurace zařízení nebo provozní statistiky) jsou zašifrována.

Pokud by útočník zachytil SNMP zprávy na síti, bez příslušného dešifrovacího klíče nebude schopen obsah zpráv přečíst.

To je zásadní například při monitorování citlivých zařízení, jako jsou firewally, servery nebo přístupové body.

- Ochrana proti manipulaci se zprávami (Message tampering) Autentizace pomocí SHA (Secure Hash Algorithm) ověřuje integritu SNMP zpráv.

SNMPv3 přidává ke každé zprávě digitální podpis. Pokud se zpráva během přenosu jakýmkoliv způsobem změní, příjemce to okamžitě detekuje a zprávu odmítne.

Tím se zabrání situaci, kdy by útočník pozměnil obsah SNMP zprávy, například aby falešně změnil stav zařízení.

- Ochrana proti útokům typu "Replay"(Opakování zpráv)

SNMPv3 implementuje časová razítka a počítadla zpráv.

Pokud útočník zachytí platnou SNMP zprávu a pokusí se ji později znovu přehrát, zařízení zprávu rozpozná jako duplicitní a zamítne ji.

Tím se zamezuje opakovanému odeslání starých zpráv, které by mohly například znovu vyvolat změnu konfigurace.

- Ochrana proti neoprávněnému přístupu Pomocí kombinace authorization password (autentizační heslo) a privacy password (šifrovací heslo) je v SNMPv3 vyžadována autentifikace každého připojení.

Authorization password ověřuje, že uživatel je skutečně tím, za koho se vydává (ověření identity pomocí HMAC-SHA).

Privacy password šifruje obsah zprávy, aby byl čitelný pouze pro oprávněného příjemce.

Pokud nejsou obě hesla správná, zařízení komunikaci odmítne.

Tento mechanismus výrazně omezuje možnost, že by se neautorizovaný subjekt pokusil o čtení nebo změnu SNMP dat.

13.2 Nastavení SNMPv3 na agentovi

V této kapitole je popsána instalace SNMP démona na operační systém Ubuntu 22.04 a jeho následná konfigurace pro použití protokolu SNMPv3.

Nejprve byl nainstalován samotný SNMP démon. Tento balíček není ve výchozí instalaci Ubuntu přítomen, proto je nutné jej nejdříve doinstalovat pomocí následujících příkazů:

```
sudo apt install snmp snmpd sudo apt install libsnmp-dev
```

Po úspěšné instalaci je třeba nakonfigurovat SNMP agenta tak, aby byl připraven reagovat na požadavky prostřednictvím protokolu SNMP verze 3. Konfigurační soubor se nachází ve výchozím adresáři `/etc/snmp/` a jeho název je `snmpd.conf`

V tomto souboru je nutné specifikovat IP adresu rozhraní, na které bude agent naslouchat, a port, který se má používat. V rámci tohoto nastavení byla použita IP adresa konkrétního síťového rozhraní a výchozí port SNMP, tedy 161. Pokud by toto nastavení nebylo upraveno, SNMP démon by naslouchal pouze na adrese localhost.

Pro snadné přidání SNMPv3 uživatele byla rovněž nainstalována knihovna libsnmp-dev, která umožňuje vytvořit uživatele přímo pomocí jednoduchého příkazu. Bez této knihovny by bylo nutné ručně generovat hash hodnoty autentizačního a šifrovacího hesla a ty následně manuálně vložit do konfiguračního souboru.

Uživatel byl vytvořen příkazem:

```
1 sudo net-snmp-create-v3-user -ro -a SHA -A Zabbix_0wczarzy -x  
   AES -X Zabbix_0wczarzy linux_0wczarzy
```

Výpis 13.1 Příkaz pro vytvoření SNMP uživatele (zdroj: vlastní)

V tomto příkazu `linux_0wczarzy` představuje uživatelské jméno SNMPv3 (SNMP username), a `Zabbix_0wczarzy` je použito jako heslo pro autentizaci (authorization password) i jako heslo pro šifrování (privacy password).

Přepínače:

- `-ro` znamená, že uživatel bude mít pouze práva pro čtení (read-only),
- `-a SHA` určuje použití algoritmu SHA pro autentizaci,
- `-x AES` stanoví použití šifrování dat algoritmem AES.

Po úspěšném přidání uživatele je potřeba restartovat SNMP démona, aby se změny projevíly: `sudo systemctl restart snmpd`

13.3 Monitorování hosta na Zabbix serveru pomocí SNMP

Dále je potřeba přidat hosta na straně Zabbix serveru. Tato operace se provádí v záložce Hosté, obdobně jako při přidávání hostů s agentem Zabbix Agent.

Je nutné upřesnit název hosta – v tomto případě může být název libovolný. Dále je třeba vybrat šablonu, zde byla zvolena výchozí šablona Linux by SNMP, která obsahuje sadu předdefinovaných SNMP dotazů a metrik zaměřených na běžné parametry linuxových systémů (například vytížení CPU, využití paměti, stav disků apod.). Poté je nutné zařadit hosta do skupiny, v tomto případě do skupiny Linux servers, která byla vytvořena v předchozích krocích.

Nejdůležitějším krokem je přidání rozhraní. Zde je nutné vybrat typ SNMP, zadat IP adresu zařízení nakonfigurovaného v konfiguračním souboru a ponechat výchozí port 161.

Použitá verze SNMP je SNMPv3 s bezpečnostní úrovní authPriv, tedy kombinací autentizačního a šifrovacího hesla. Jako autentizační protokol je použit SHA (SHA1) a autentizační heslo Zabbix_Owczarzy, stejně jako bylo zadáno při konfiguraci agenta. Šifrovací protokol, Zabbix ho překládá jako protokol utajení, je nastaven na AES128, a šifrovací heslo (privacy password) je rovněž Zabbix_Owczarzy.

Po přidání hosta bude v přehledu hostů ihned viditelné, zda host správně odpovídá na SNMPv3 dotazy. Je však třeba být velmi pečlivý při zadávání údajů, protože i drobná chyba v uživatelském jménu nebo heslech znemožní navázání komunikace a monitoring pomocí SNMP protokolu nebude funkční.

The screenshot displays the 'Nové zařízení' (New device) configuration page in the Zabbix web interface. The 'Hostitel' (Host) tab is selected. The configuration includes:

- Název hosta** (Host name): SNMP_Owczarzy
- Zobrazované jméno** (Displayed name): SNMP_Owczarzy
- Šablony** (Templates): Linux by SNMP (selected)
- Skupina hostů** (Host group): Linux servers (selected)
- Rozhraní** (Interface): SNMP
- Typ** (Type): SNMP
- IP adresa** (IP address): 192.168.10.4
- Jméno DNS** (DNS name):
- Připojit k** (Connect to): IP
- Port** (Port): 161
- Výchozí** (Default): Odstranit (Remove)
- Verze SNMP** (SNMP version): SNMPv3
- Maximální počet opakování** (Maximum number of retries): 10
- Jméno kontextu** (Context name):
- Bezpečnostní jméno** (Security name): linux_Owczarzy
- Bezpečnostní úroveň** (Security level): authPriv
- Autentizační protokol** (Authentication protocol): SHA1
- Autentizační přístupové heslo** (Authentication password): Zabbix_Owczarzy
- Protokol utajení** (Privacy protocol): AES128
- Fráze utajení** (Privacy phrase): Zabbix_Owczarzy
- ☒ Použít kombinované žádosti (Use combined requests)
- Popis** (Description):
- Monitorováno** (Monitored): Server

Obrázek 13.1 Nastavení SNMP na straně Zabbix serveru, zdroj: vlastní

14 NÁVRH ZABEZPEČENÍ DOPORUČENÉHO ŘEŠENÍ

Zabbix server jako centrální prvek monitorovací infrastruktury představuje kritický bod v rámci celé IT architektury společnosti. Z tohoto důvodu je nezbytné věnovat jeho zabezpečení maximální pozornost.

14.1 Rizika

Pokud by Zabbix server nebyl řádně zabezpečen, útočník by mohl:

- Získat kompletní mapu infrastruktury – IP adresy, hostname zařízení, typy systémů, verze OS, síťové segmentace.
- Přistoupit k přihlašovacím údajům uloženým v Zabbixu - hesla do SNMP zařízení, agentů, databází.
- Manipulovat s monitoringem – například zakázat alarmy na kritické systémy a tím maskovat svůj útok v síti.
- Provádět laterální pohyb – využít monitorovací server jako pivot k dalšímu šíření po síti.
- Získat přístup k citlivým datům– protože některé informace v monitorovacích nástrojích mohou být považovány za neveřejné (například názvy projektů, služby).
- Provádět DoS útoky – například zahlcením serveru velkým množstvím SNMP požadavků, nebo vytvořením falešných hostů. Útočník by přesně věděl, které zařízení je více vytíženo, tudíž by si ho mohl jednoduše vybrat jako cíl pro tento typ útoku.

14.2 Síťová architektura a přístupová politika

Zabbix server musí být umístěn ve vnitřní síti (intranetu) společnosti za firewallovou ochranou. Přístup k management rozhraní (webové UI a API) by měl být řízen pomocí principu RBAC. Zabbix server by měl být integrován s AAA serverem, který bude uživatele rozdělovat podle jejich rolí. Administrátoři by tak byli zařazeni do skupiny admins s plnými oprávněními, zatímco běžní uživatelé nebo manažeři by měli přidělena pouze práva pro čtení.

Dále je třeba také zakázat veškerý přístup z veřejného internetu na server. Vzdálený přístup k management rozhraní by měl být umožněn pouze z VLAN nasazené v kancelářích dané společnosti, případně prostřednictvím bezpečného připojení přes VPN.

Bezpečná komunikace:

Standardní port TCP/10051 by měl být změněn na nestandardní hodnotu a správně nastaven ve všech agentech/proxy.

Šifrovaná komunikace: všechna spojení mezi Zabbix serverem, agenty a proxy servery by měla být nějakou formou zabezpečená zabezpečená.

Například pomocí PSK, což zjednoduší implementaci, vhodná pro kontrolované prostředí.

Také pomocí TLS/SSL certifikátů pro vyšší bezpečnost díky autentizaci zařízení a možnosti certifikáty spravovat a revokovat.

Také je vhodné mít v intranetu certifikační autoritu. Pokud je použit protokol TLS, je vhodné vystavit si vlastní interní certifikáty.

14.3 Zabezpečení databáze

Databázový server by měl běžet na separátním serveru v chráněné síťové zóně (tzv. Crown Jewels segment). Crown jewels jsou nejcennější IT aktiva firmy, jako třeba data nebo systémy, které musí být nejvíc chráněné.

Typicky sem patří: databáze zákazníků, interní aplikace, Active Directory, kritická konfigurace, atd. V tomto segmentu určitě databáze Zabbixu má své místo.

Mezi další zabezpečení databáze nepochybně patří šifrování dat na disku i komunikace mezi Zabbix serverem a databází (např. TLS pro MySQL). Také omezení komunikace mezi Zabbix serverem a databázovým serverem. Ideálně tudíž omezení přístupu na databázový server pouze z IP adresy Zabbix serveru.

Samozřejmě mezi zabezpečení databáze patří také pravidelné zálohování databáze do bezpečného úložiště a ověřování obnovitelnosti záloh.

14.4 Vysoká dostupnost

Jakýkoliv výpadek Zabbix serveru by mohl vést ke ztrátě monitorovacích dat, nemožnosti detekce incidentů v reálném čase, a celkovému ohrožení bezpečnosti provozované infrastruktury. Tudíž od verze 5.0 LTS nabízí Zabbix nativní podporu pro high-available cluster serverů.

14.4.1 Předpoklady pro vysokou dostupnost

Pro dosažení vysoké dostupnosti je zapotřebí docílit určitých technických předpokladů. Těmi předpoklady jsou :

- 2 fyzické nebo virtuální servery s OS Linux
- Sdílená databáze
- Sdílené přístupové údaje k databázi.
- Shodná verze Zabbix serveru na obou uzlech
- Servery mohou komunikovat mezi sebou. V tomto případě přes privátní síť.

V konfiguračním souboru Zabbixu, je třeba nastavit high-availability. Důležité je zmínit, že HANodeName musí být odlišný na každém uzlu.

```
1 # Jméno aktuálního HA nodu - musí být unikátní pro každý
2 server
3 HANodeName=uzel1      # na prvním serveru
4 HANodeName=uzel2      # na druhém serveru
5 # Připojení k databázi (musí být stejné na obou)
6 DBHost=db-ha-cluster.internal
7 DBName=zabbix
8 DBUser=zabbix
9 DBPassword=securepassword
10
11 # Volitelně: Lze zvýšit frekvenci kontroly HA stavu
12 HAHeartbeatFrequency=5
```

Výpis 14.1 Konfigurace Zabbixu pro vysokou dostupnost (zdroj: vlastní)

Parametr HAHeartbeatFrequency v Zabbixu je udáván v sekundách.

To znamená, že každých 5 sekund si jednotlivé Zabbix servery (členové HA clusteru) mezi sebou vyměňují heartbeat zprávu, aby zjistily, zda jsou ostatní členové online a funkční.

Následně už zbývá na jednom serveru spustit registraci uzlů v HA clusteru pomocí příkazu:

```
sudo zabbix_server -R ha_node_add ha_node=uzel1
```

```
sudo zabbix_server -R ha_node_add ha_node=uzel2
```

Stav vysoké dostupnosti můžeme zkontrolovat pomocí příkazu :

```
sudo zabbix_server -R ha_status
```

Díky této výchozí funkci Zabbixu, není nutno nasazovat do sítě Load Balancer. Ačkoliv pro velké sítě řešení s Load Balancerem přináší více možností, pro tento případ středně velkých sítí bude výchozí funkcionalita Zabbixu plně dostačovat.

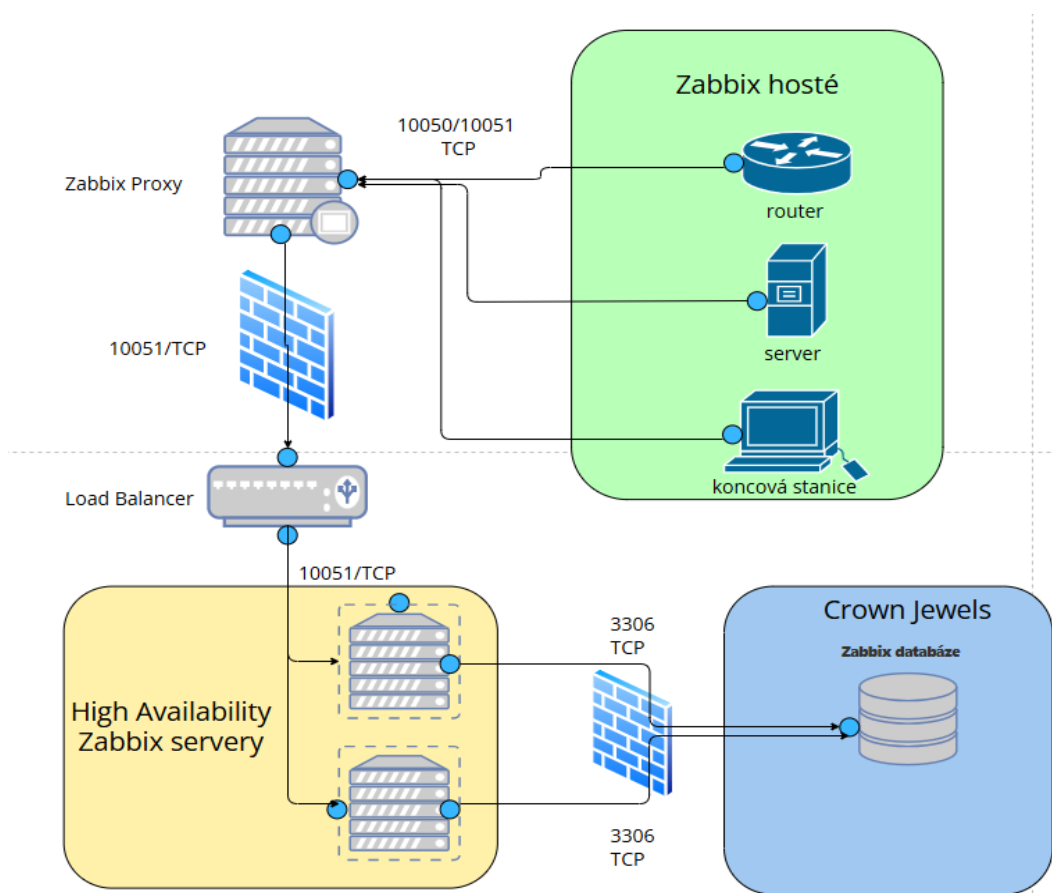
14.5 Využití proxy serverů

Ve středně velkých a velkých sítích je běžné, že síť je geograficky rozprostřená do více částí. Může být rozdělena například v rámci jednoho kontinentu. Například jednotlivé pobočky firmy po celé Evropě, nebo dokonce napříč kontinenty. V takovém případě je ideálním řešením využít funkcionalitu Zabbix Proxy. Pomocí Zabbix Proxy se může společnost Axians vyhnout nutnosti nasazovat samostatné Zabbix servery v každém regionu a zachovat tak unifikovanou a centralizovanou architekturu.

Doporučuje se dále rozdělit jednotlivé kontinenty na menší geografické oblasti, například Východní Evropa, Střední Evropa a Západní Evropa. V každé této oblasti by měla být nasazena samostatná Zabbix Proxy, která bude shromažďovat a předávat monitorovací data do centrálního Zabbix serveru.

V případě větší sítě, geograficky rozložené na více kontinentů, je plně dostačující nasadit Zabbix proxy pro každý kontinent. Proxy servery budou lokálně shromažďovat monitorovací data a následně je bezpečně odesílat do centralizovaného Zabbix serveru.

Toto centralizované řešení usnadní práci jak administrátorům, tak také manažerům, kteří budou Zabbix používat. Nemusí se totiž přihlašovat na více různých Zabbix Serveru a pracovat tam, ale jenom na jeden a mít tam všechna potřebná data.



Obrázek 14.1 Navrhovaná architektura Zabbixu zdroj: vlastní

15 OVĚŘENÍ FUNKČNOSTI VYBRANÉHO ŘEŠENÍ A SPLNĚNÍ POŽADAVKŮ ZADAVATELE

V souladu s požadavky společnosti Axians byly jednotlivé funkcionality monitorovacího nástroje Zabbix důkladně otestovány. Zabbix nabízí široké možnosti v oblasti komplexního monitoringu, a to včetně podpory protokolů SNMP, Flow či IPFIX. Společnost Axians preferovala implementaci monitorování prostřednictvím protokolu SNMP, a to zejména z důvodu interní expertízy v této oblasti – firma disponuje specialisty, kteří se na tento protokol dlouhodobě zaměřují.

Požadavek týkající se upozorňování na incidenty byl prakticky ověřen v části práce věnované tzv. spouštěčům. V příslušné podkapitole je podrobně popsán postup konfigurace e-mailových notifikací. Zabbix v tomto ohledu plně vyhovuje požadavkům společnosti Axians, včetně podpory pěti úrovní závažnosti incidentů, které byly v rámci zadání specifikovány.

Další klíčovou oblastí testování byla vizualizace dat. Zabbix disponuje pokročilými nástroji pro vizualizaci monitorovaných údajů ve formě grafů a přehledových panelů. Testování této funkcionality zároveň sloužilo jako nástroj pro ověření funkčního propojení monitorovaných zařízení se systémem Zabbix – v okamžiku, kdy byl Zabbix schopen úspěšně zpracovat přijatá data, automaticky generoval odpovídající vizualizace.

Jak již bylo v této práci několikrát zmíněno, Zabbix je open-source řešení. To znamená, že jeho implementace a provoz nejsou spojeny s nutností úhrady licenčních poplatků.

Součástí této práce byl rovněž návrh vysoce dostupné architektury systému Zabbix. V podkapitole věnované vysoké dostupnosti je uveden praktický příklad konfigurace, která umožňuje dosažení vysoké provozní spolehlivosti. Po nasazení takové architektury bude dosažena úroveň dostupnosti odpovídající hodnotě SLA 99%, což odpovídá požadavkům společnosti Axians.

Z hlediska kybernetické bezpečnosti byla v rámci této práce implementována a otestována komunikace prostřednictvím předem sdíleného klíče (PSK). Dále byl zpracován návrh komplexní architektury nasazení systému Zabbix, která splňuje všechny definované požadavky společnosti Axians, jak z hlediska funkcionality, tak i bezpečnosti a provozní spolehlivosti.

ZÁVĚR

Tato diplomová práce se zaměřila na návrh a testování monitorovacího řešení pro potřeby společnosti Axians. Cílem bylo vytvořit návrh pro monitorování středně velkých a velkých infrastruktur pro zákazníky Axians. Tento cíl byl úspěšně splněn.

V této práci byla nejprve provedena analýza deseti nejpoužívanějších monitorovacích platform – Nagios Core, Prometheus, ManageEngine OpManager, SolarWinds Network Performance Monitor, PRTG Network Monitor, Datadog, Icinga 2, Site24x7 a nakonec Zabbix. Každý nástroj byl hodnocen podle šesti klíčových kritérií: šíře pokrytí monitorovacích scénářů, schopnost spolehlivého upozorňování na incidenty, kvalitu vizualizace dat, model open-source nebo komerční licencování, podporu vysoké dostupnosti (HA) a úroveň kybernetické bezpečnosti.

Na základě této podrobné komparativní analýzy byl jako nejvhodnější nástroj pro společnost Axians vybrán Zabbix, neboť splňuje nejlépe všechna klíčová kritéria a v analýze získal nejvíce bodů.

Z hlediska praktického přínosu byla ověřena funkčnost celého řešení v testovacím prostředí a navrženy konkrétní kroky pro implementaci do produkční sítě. Výsledkem je moderní a bezpečná infrastruktura monitoringu, která plně pokrývá potřeby dané společnosti a zároveň reflektuje aktuální požadavky na kybernetickou bezpečnost.

SEZNAM POUŽITÉ LITERATURY

- [1] NOVÁK, Jan, 2021. Diploma thesis (in Czech), Masaryk University, Brno, Czech Republic.
- [2] DALLE VACCHE, Andrea a LEE, Stefano Kewan, 2015. *Mastering Zabbix*. Packt Publishing. 2 vyd. ISBN 978-1785289262.
- [3] SINGH, Rahul a GUPTA, Anil, 2020. Comparative Study of Open-Source Monitoring Tools. *International Journal of Network Management*. 2020. 30, č. 3, s. 1–8. Article details (authors/journal) not verified.
- [4] JULIAN, Mike, 2017. *Practical Monitoring: Effective Strategies for the Real World*. O'Reilly Media. ISBN 978-1491957356.
- [5] ADAMS, Roger, 2022. *Cloud Monitoring: A Practical Approach*. Independently Published. Publisher not verified.
- [6] CLARK, John, 2021. *Modern Monitoring: Real-Time Insights into IT Systems*. Unknown Publisher. Publisher not verified.
- [7] AUTHORS, Prometheus, 2023. *Prometheus Documentation*. Online. Dostupné z: <https://prometheus.io/docs/>. Accessed 2023-04.
- [8] SIA, Zabbix, 2023. *Zabbix Documentation*. Online. Dostupné z: <https://www.zabbix.com/documentation/current/en/>. Accessed 2023-04.
- [9] BEYER, Betsy; JONES, Chris; MURPHY, Niall Richard a PETOFF, Jennifer, 2016. *Site Reliability Engineering: How Google Runs Production Systems*. O'Reilly Media. ISBN 978-1491929124.
- [10] TURNBULL, James, 2015. *The Art of Monitoring*. Foresee Press. ISBN 978-0988820241.
- [11] AXIANS ICT CZ, S.R.O., 2023. *Axians ICT CZ – O nás*. Online. Dostupné z: <https://www.axians.cz/o-nas/>. Accessed 2023-04-28.

- [12] VINCI ENERGIES, 2023. *VINCI Energies – Global Energy and Information Technology Services*. Online. Dostupné z: <https://www.vinci-energies.com/>. Accessed 2023-04-28.
- [13] NAGIOS ENTERPRISES, LLC, 2023. *Nagios Documentation*. Online. Dostupné z: <https://www.nagios.org/documentation/>. Accessed 2023-04.
- [14] NAGIOS ENTERPRISES, LLC, 2023. *Nagios Documentation*. Online. Dostupné z: <https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/toc.html>. Accessed 2023-04.
- [15] NAGIOS ENTERPRISES, LLC, 2023. *Nagios Support Home*. Online. Dostupné z: <https://support.nagios.com/>. Accessed 2023-04.
- [16] AUTHORS, Prometheus, 2023. *Prometheus: Monitoring System & Time Series Database*. Online. Dostupné z: <https://prometheus.io/>. Accessed 2023-04.
- [17] AUTHORS, Prometheus, 2023. *Prometheus: Monitoring System & Time Series Database*. Online. Dostupné z: <https://prometheus.io/docs/visualization/grafana/>. Accessed 2023-04.
- [18] AUTHORS, Prometheus, 2023. *Prometheus: Monitoring System & Time Series Database*. Online. Dostupné z: <https://prometheus.io/docs/tutorials/getting-started/#what-is-prometheus>, note={Accessed 2023-04},.
- [19] AUTHORS, Prometheus, 2023. *Prometheus: Monitoring System & Time Series Database*. Online. Dostupné z: <https://prometheus.io/docs/alerting/latest/alertmanager/#high-availability>. Accessed 2023-04.
- [20] AUTHORS, Prometheus, 2023. *Prometheus: Monitoring System & Time Series Database*. Online. Dostupné z: <https://prometheus.io/docs/operating/security/#security-model>. Accessed 2023-04.
- [21] MANAGEENGINE, 2023. *Network Monitoring Software & Solutions - ManageEngine*. Online. Dostupné z: <https://www.manageengine.com/network-monitoring/>. Accessed 2023-04.

- [22] MANAGEENGINE, 2023. *Network Monitoring Software & Solutions - ManageEngine*. Online. Dostupné z: <https://www.manageengine.com/network-monitoring/fault-monitoring.html?opm-index>. Accessed 2023-04.
- [23] MANAGEENGINE, 2023. *Network Monitoring Software & Solutions - ManageEngine*. Online. Dostupné z: <https://www.manageengine.com/network-monitoring/server-virtualization.html>. Accessed 2023-04.
- [24] MANAGEENGINE, 2023. *Network Monitoring Software & Solutions - ManageEngine*. Online. Dostupné z: <https://www.manageengine.com/network-monitoring/opmanager-editions.html?opm-index>. Accessed 2023-04.
- [25] MANAGEENGINE, 2023. *Network Monitoring Software & Solutions - ManageEngine*. Online. Dostupné z: <https://www.manageengine.com/products/ad-manager/help/admin-settings/high-availability.html>. Accessed 2023-04.
- [26] MANAGEENGINE, 2023. *Network Monitoring Software & Solutions - ManageEngine*. Online. Dostupné z: https://www.manageengine.com/products/ad-manager/help/managing_security_roles/managing_security_roles.html. Accessed 2023-04.
- [27] CORPORATION, Zoho, 2023. *Site24x7: All-in-One Monitoring Solution*. Online. Dostupné z: <https://www.site24x7.com/>. Accessed 2023-04.
- [28] CORPORATION, Zoho, 2023. *Site24x7: All-in-One Monitoring Solution*. Online. Dostupné z: <https://www.site24x7.com/network-monitoring.html?src=Productbox&pg=home>. Accessed 2023-04.
- [29] CORPORATION, Zoho, 2023. *Site24x7 Help Center*. Online. Dostupné z: <https://www.site24x7.com/help/>. Accessed 2023-04.
- [30] CORPORATION, Zoho, 2023. *Site24x7 Help Center*. Online. Dostupné z: <https://www.site24x7.com/help/network-metrics/visualization.html>. Accessed 2023-04.
- [31] CORPORATION, Zoho, 2023. *Site24x7 Help Center*. Online. Dostupné z: <https://www.site24x7.com/site24x7-pricing.html>. Accessed 2023-04.

- [32] CORPORATION, Zoho, 2023. *Site24x7 Help Center*. Online. Dostupné z: <https://www.site24x7.com/help/getting-started/high-availability-on-premise-poller.html>. Accessed 2023-04.
- [33] CORPORATION, Zoho, 2023. *Site24x7 Help Center*. Online. Dostupné z: <https://www.site24x7.com/help/admin/server-monitor/server-agent-documentation.html>. Accessed 2023-04.
- [34] GMBH, Icinga, 2023. *Icinga: Open Source Monitoring for Complex IT Environments*. Online. Dostupné z: <https://icinga.com/>. Accessed 2023-04.
- [35] GMBH, Icinga, 2023. *Icinga: Open Source Monitoring for Complex IT Environments*. Online. Dostupné z: <https://icinga.com/docs/icinga-2/latest/doc/03-monitoring-basics/>. Accessed 2023-04.
- [36] GMBH, Icinga, 2023. *Icinga: Open Source Monitoring for Complex IT Environments*. Online. Dostupné z: <https://icinga.com/products/notifications/>. Accessed 2023-04.
- [37] GMBH, Icinga, 2023. *Icinga: Open Source Monitoring for Complex IT Environments*. Online. Dostupné z: <https://icinga.com/blog/creating-dashboards-based-on-custom-filters/>. Accessed 2023-04.
- [38] GMBH, Icinga, 2023. *Icinga: Open Source Monitoring for Complex IT Environments*. Online. Dostupné z: <https://icinga.com/community/open-source/>. Accessed 2023-04.
- [39] GMBH, Icinga, 2023. *Icinga: Open Source Monitoring for Complex IT Environments*. Online. Dostupné z: <https://icinga.com/blog/how-to-set-up-high-availability-masters/>. Accessed 2023-04.
- [40] GMBH, Icinga, 2023. *Icinga: Open Source Monitoring for Complex IT Environments*. Online. Dostupné z: <https://icinga.com/docs/icinga-web/latest/doc/06-Security/>. Accessed 2023-04.
- [41] SOLARWINDS WORLDWIDE, LLC, 2023. *SolarWinds Documentation*. Online. Dostupné z: <https://documentation.solarwinds.com/>. Accessed 2023-04.

- [42] SOLARWINDS WORLDWIDE, LLC, 2023. *SolarWinds Documentation*. Online. Dostupné z: <https://www.solarwinds.com/network-performance-monitor>. Accessed 2023-04.
- [43] SOLARWINDS WORLDWIDE, LLC, 2023. *SolarWinds Documentation*. Online. Dostupné z: https://documentation.solarwinds.com/en/success_center/orionplatform/content/core-creating-and-managing-alerts-sw1277.htm. Accessed 2023-04.
- [44] SOLARWINDS WORLDWIDE, LLC, 2023. *SolarWinds Documentation*. Online. Dostupné z: <https://www.solarwinds.com/log-analyzer/use-cases/log-visualization>. Accessed 2023-04.
- [45] SOLARWINDS WORLDWIDE, LLC, 2023. *SolarWinds Documentation*. Online. Dostupné z: <https://www.solarwinds.com/pricing>. Accessed 2023-04.
- [46] SOLARWINDS WORLDWIDE, LLC, 2023. *SolarWinds Documentation*. Online. Dostupné z: https://documentation.solarwinds.com/en/success_center/orionplatform/content/ha_what_is_high_availability.htm. Accessed 2023-04.
- [47] SOLARWINDS WORLDWIDE, LLC, 2023. *SolarWinds Documentation*. Online. Dostupné z: <https://www.solarwinds.com/information-security>. Accessed 2023-04.
- [48] PAESSLER AG, 2023. *PRTG Network Monitor*. Online. Dostupné z: <https://www.paessler.com/prtg>.
- [49] PAESSLER AG, 2023. *PRTG Network Monitor*. Online. Dostupné z: <https://www.paessler.com/monitoring/network/network-monitoring-tool>.
- [50] PAESSLER AG, 2023. *PRTG Network Monitor*. Online. Dostupné z: https://www.paessler.com/manuals/prtg/device_and_sensor_setup.
- [51] PAESSLER AG, 2023. *PRTG Network Monitor*. Online. Dostupné z: https://www.paessler.com/manuals/prtg/notification_triggers_settings.
- [52] PAESSLER AG, 2023. *PRTG Network Monitor*. Online. Dostupné z: https://www.paessler.com/manuals/prtg/prtg_app_for_desktop.

- [53] PAESSLER AG, 2023. *PRTG Network Monitor*. Online. Dostupné z: https://www.paessler.com/manuals/prtg/failover_cluster.
- [54] PAESSLER AG, 2023. *PRTG Network Monitor*. Online. Dostupné z: <https://kb.paessler.com/en/topic/61108-what-security-features-does-prtg-include>.
- [55] DATADOG, INC., 2023. *Cloud Monitoring Platform*. Online. Dostupné z: <https://www.datadoghq.com/monitoring/cloud-monitoring/>.
- [56] DATADOG, INC., 2023. *Cloud Monitoring Platform*. Online. Dostupné z: https://docs.datadoghq.com/getting_started/monitors/.
- [57] DATADOG, INC., 2023. *Cloud Monitoring Platform*. Online. Dostupné z: https://docs.datadoghq.com/getting_started/incident_management/.
- [58] DATADOG, INC., 2023. *Cloud Monitoring Platform*. Online. Dostupné z: https://docs.datadoghq.com/getting_started/dashboards/.
- [59] DATADOG, INC., 2023. *Cloud Monitoring Platform*. Online. Dostupné z: <https://www.datadoghq.com/pricing/>.
- [60] DATADOG, INC., 2023. *Cloud Monitoring Platform*. Online. Dostupné z: https://docs.datadoghq.com/network_monitoring/devices/setup/#high-availability.
- [61] DATADOG, INC., 2023. *Cloud Monitoring Platform*. Online. Dostupné z: https://docs.datadoghq.com/security/cloud_security_management.
- [62] SIA, Zabbix, 2023. *Zabbix Documentation*. Online. Dostupné z: https://www.zabbix.com/documentation/current/en/manual/vm_monitoring. Accessed 2023-04.
- [63] SIA, Zabbix, 2023. *Zabbix Documentation*. Online. Dostupné z: <https://www.zabbix.com/documentation/current/en/manual/acknowledgment>. Accessed 2023-04.
- [64] SIA, Zabbix, 2023. *Zabbix Documentation*. Online. Dostupné z: <https://www.zabbix.com/documentation/7.2/en/manual/api/reference/dashboard/object#dashboard>. Accessed 2023-04.

- [65] SIA, Zabbix, 2023. *Zabbix Documentation*. Online. Dostupné z: https://www.zabbix.com/documentation/7.2/en/manual/installation/getting_zabbix?hl=source%2Ccode. Accessed 2023-04.
- [66] SIA, Zabbix, 2023. *Zabbix Documentation*. Online. Dostupné z: <https://www.zabbix.com/documentation/7.2/en/manual/concepts/server/ha?hl=High%2Cavailability%2Chigh%2CHA%2Ccluster>. Accessed 2023-04.
- [67] SIA, Zabbix, 2023. *Zabbix Documentation*. Online. Dostupné z: https://www.zabbix.com/documentation/7.2/en/manual/best_practices/security?hl=Security. Accessed 2023-04.
- [68] SOLARWINDS WORLDWIDE, LLC, 2023. *Network Monitoring Software - SolarWinds*. Online. Dostupné z: <https://www.solarwinds.com/network-performance-monitor/use-cases/network-monitoring-software>. Accessed 2023-04.
- [69] SIA, Zabbix, 2023. *Zabbix Documentation*. Online. Dostupné z: https://www.zabbix.com/cz/solutions#solutions_by_industry. Accessed 2023-04.
- [70] SIA, Zabbix, 2023. *Zabbix Documentation*. Online. Dostupné z: <https://www.zabbix.com/documentation/7.2/en/manual/quickstart>. Accessed 2023-04.
- [71] SIA, Zabbix, 2023. *Zabbix Documentation*. Online. Dostupné z: <https://www.zabbix.com/documentation/7.2/en/manual/api/reference/dhost/object#discovered-host>. Accessed 2023-04.
- [72] JACKSON, Kevin, 2022. *What is SNMP, and How Does It Work?* Online. Dostupné z: <https://www.fortra.com/resources/articles/snmp-basics-what-it-and-how-it-works>. Accessed 2023-04.

SEZNAM OBRÁZKŮ

Obrázek 4.1	Logo monitorovacího nástroje Prometheus [7].....	26
Obrázek 4.2	Logo monitorovacího nástroje Icinga [34]	37
Obrázek 4.3	Logo monitorovacího nástroje PRTG Network Monitor [48].....	41
Obrázek 4.4	Logo monitorovacího nástroje Datadog [55]	44
Obrázek 4.5	Logo monitorovacího nástroje Zabbix [8].....	48
Obrázek 8.1	Vystavení Zabbix frontendu, zdroj: vlastní	65
Obrázek 8.2	Grafy po přidání Zabbix agenta, zdroj: vlastní.....	68
Obrázek 8.3	Přidávání Windows agenta s aktivními kontrolami, zdroj: vlastní	70
Obrázek 9.1	Pravidlo pro automatickou detekci linuxového agenta, zdroj: vlastní.....	72
Obrázek 10.1	Konfigurace PSK na straně Windows agenta, zdroj: vlastní	75
Obrázek 11.1	Zabbix agent ping, zdroj: vlastní	78
Obrázek 12.1	Spouštěč pro nedostupnost hosta, zdroj: vlastní	80
Obrázek 13.1	Nastavení SNMP na straně Zabbix serveru, zdroj: vlastní.....	87
Obrázek 14.1	Navrhovaná architektura Zabbixu zdroj: vlastní	92

SEZNAM TABULEK

Tabulka 4.1	Porovnání monitorovacích nástrojů	53
-------------	---	----

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IT	Information Technology
CPU	Central Processing Unit
s.r.o.	společnost s ručením omezeným
SNMP	Simple Network Management Protocol
SMS	Short Message Service
SLA	Service Level Agreement
PSK	Pre-Shared Key
JMX	Java Management Extensions
WMI	Windows Management Instrumentation
IPMI	Intelligent Platform Management Interface
MTA	Mail Transfer Agent
SMTP	Simple Mail Transfer Protocol
RRD	Round-Robin Database
DRBD	Distributed Replicated Block Device
HA	High Availability
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
SSL	Secure Sockets Layer
TLS	Transport Layer Security
OID	Object Identifier
JVM	Java Virtual Machine
CNCF	Cloud Native Computing Foundation
HTML	HyperText Markup Language
PDF	Portable Document Format
API	Application Programming Interface
UI	User Interface
GSM	Global System for Mobile Communications
LLDP	Link Layer Discovery Protocol
CDP	Cisco Discovery Protocol
CSV	Comma-Separated Values
REST	Representational State Transfer
IIS	Internet Information Services
SAML	Security Assertion Markup Language

RBAC	Role-Based Access Control
ISO 27001	International Organization for Standardization 27001
SOC 2	Service Organization Control 2
SSH	Secure Shell
TSDB	Time Series Database
DSL	Domain-Specific Language
NOC	Network Operations Center
GNU	GNU's Not Unix
GPL	General Public License
SSO	Single Sign-On
ICMP	Internet Control Message Protocol
RAID	Redundant Array of Independent Disks
MS SQL	Microsoft SQL Server
NTLM	NT LAN Manager
KPI	Key Performance Indicator
URL	Uniform Resource Locator
iOS	iPhone Operating System
RMI	Remote Method Invocation
TCO	Total Cost of Ownership
APM	Application Performance Monitoring
LDAP	Lightweight Directory Access Protocol
HP	Hewlett-Packard
BI	Business Intelligence
NAT	Network Address Translation
AMD	Advanced Micro Devices
NVMe	Non-Volatile Memory Express
SSD	Solid-State Drive
OS	Operating System
MSI	Microsoft Installer
IP	Internet Protocol
SHA	Secure Hash Algorithm
AES	Advanced Encryption Standard

SEZNAM PŘÍLOH

PŘÍLOHA P I: Evidence úkonů praktické části

PŘÍLOHA P I: EVIDENCE ÚKONŮ PRAKTICKÉ ČÁSTI

Příloha obsahuje zkomprimovaný soubor obsahující všechny snímky z praktické části této diplomové práce. V práci je použito 9 snímků, celkové bylo vytvořeno 54 snímků.