Návrh vizualizace dat z Graylogu

Ondřej Novotný

Bakalářská práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Ondřej Novotný**
Osobní číslo:	**A20505**
Studijní program:	**B0613A140020 Softwarové inženýrství**
Forma studia:	**Prezenční**
Téma práce:	**Návrh vizualizace dat z Graylogu**
Téma práce anglicky:	**Graylog Data Visualization Design**

Zásady pro vypracování

1. Prozkoumejte možnosti monitoringu a sběru logů platformou Graylog.
2. Definujte kritické informace, keré o sledovaných systémech budete uchovávat.
3. Navrhněte princip sběru logů ze serverů, NASů a síťových prvků do Graylogu.
4. Proveďte nasazení Vašeho řešení v testovací infrastruktuře.
5. Vytvořte dashboardy s využitím Graylogu pro monitoring stavu chráněné infrastruktury.
6. Dashboardy doplňte o systém zasílání alertů.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. VAZAO, Ana, Leonel SANTOS, Maria Beatriz PIEDADE a Carlos RABADAO. SIEM Open Source Solutions: A Comparative Study. _2019 14th Iberian Conference on Information Systems and Technologies (CISTI), Information Systems and Technologies (CISTI), 2019 14th Iberian Conference on_ [online]. 2019, , 1-5 [cit. 2021-11-30]. ISBN 9789899843493. ISSN edseee.IEEEConferenc. Dostupné z: doi:10.23919/CISTI.2019.8760980
2. BIRUNDHA, S, R Kingsy GRACE a T JEYARAM. Network Monitoring and Analysis. _2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Advanced Computing and Communication Systems (ICACCS), 2021 7th International Conference on_ [online]. 2021, **1**, 1400-1403 [cit. 2021-11-30]. ISBN 9781665405201. ISSN 25757288. Dostupné z: doi:10.1109/ICACCS51430.2021.9441767
3. BEKRI, W., R. JMAL a L.C. FOURATI. Softwarized Internet of Things Network Monitoring. _IEEE Systems Journal, Systems Journal, IEEE_ [online]. 2021, **15**(1), 826-834 [cit. 2021-11-30]. ISSN 19328184. Dostupné z: doi:10.1109/JSYST.2020.3015435
4. TRAORÉ, Issa, Ahmed AWAD a Isaac WOUNGANG. _Information security practices: emerging threats and perspectives_. Cham, Switzerland: Springer, [2017], 1 online resource. Dostupné z: doi:9783319489476
5. STALLINGS, William a Lawrie BROWN. _Computer security: principles and practice_. Fourth edition. Chennai: Pearson, [2020], 800 atrn. ISBN 978-93-534-3886-9

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

Datum zadání bakalářské práce: **5. listopadu 2023**
Termín odevzdání bakalářské práce: **13. května 2024**

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

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 5. ledna 2024

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou 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;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 13.5.2024

Ondřej Novotný v.r.
podpis studenta

ABSTRAKT

Tato práce se zabývá analýzou logů a možnostmi monitoringu pomocí platformy Graylog. Popisuje, jaké možnosti tato platforma nabízí pro sběr logů ze serverů, NASů, routerů a počítačů a jaké poskytuje možnosti pro jejich analýzu. Dále se zaměřuje na definici klíčových událostí, které jsou v testovací infrastruktuře sledovány a vizualizovány pomocí přehledných dashboardů. Ty jsou doplněny o systém zasílání notifikací při zachycení klíčových událostí.

Klíčová slova: správa logů, analýza logů, vizualizace dat, dashboard, notifikace, Graylog

ABSTRACT

This thesis deals with the analysis of logs and the possibilities of monitoring using the Graylog platform. It describes what possibilities this platform offers for collecting logs from servers, NAS, routers and computers and what it provides for their analysis. It also focuses on defining key events that are monitored and visualized in the test infrastructure using clear dashboards. These are complemented by a system for sending notifications when key events are detected.

Keywords: log management, log analysis, data visualization, dashboard, notification, Graylog

Rád bych touto cestou poděkoval vedoucímu mé bakalářské práce, panu Ing. Davidu Malaníkovi, Ph.D., za poskytnutí příležitosti toto téma zpracovat a za jeho vstřícný přístup při konzultacích. Nesmím také zapomenout na svou rodinu, přátele a na dary mojí rodné jižní Moravy. Vám všem vděčím nejen za podporu v průběhu celého studia, ale také za podporu a zejména motivaci tuto práci dokončit.

Motto:

„Pro člověka, který chce a má vědomosti, není nic nemožné.“

Tomáš Baťa

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Prohlašuji, že při tvorbě této práce jsem použil/a nástroj generativního modelu AI ChatGPT; https://chatgpt.com/ za účelem korekce napsaného textu. Po použití tohoto nástroje jsem provedl/a kontrolu obsahu a přebírám za něj plnou zodpovědnost.

OBSAH

ÚVOD

V dnešní digitální době, kdy jsou počítače klíčové pro provoz spousty organizací, nabývá sběr a analýza logů zásadního významu. Pro některé organizace může být sběr a uchovávání logů nařízeno legislativou, ať už interní směrnicí nebo např. směrnicí NIS 2, která by v brzké době měla vstoupit v platnost. Pokud je ovšem sběr logů doplněn také jejich analýzou, je možné získat poměrně efektivní nástroj, díky kterému budeme mít přehled nejen, o dění v síti, což nám umožní rychleji reagovat na vzniklé problémy, případně jim zcela předcházet a zajistit tak větší stabilitu a spolehlivost celé sítě, ale i předcházet bezpečnostním hrozbám, čímž můžeme zajistit větší bezpečnost IT infrastruktury a chránit citlivá data.

Cílem této práce je prozkoumat možnosti sběru logů pomocí platformy Graylog. Navrhnout možnosti odesílání logů ze serverů, NASů a síťových prvků do této platformy. Dále definovat kritické informace, které je vhodné sledovat a navrhnout řešení, pro sledování těchto informací v chráněné infrastruktuře. S tím souvisí tvorba dashboardů, které budou informovat o stavu testovací infrastruktury a vytvoření systému zasílání notifikací.

V první části práce jsou shrnuty informace o lozích, logování, správě logů a formátech logů. Dále představuje možnosti platformy Graylog, které budou využity v této práci a popisuje kritické informace a možnosti sběru logů z různých platforem.

Ve druhé části práce je popsána analýza testovací infrastruktury a její příprava před nasazením řešení. Dále následuje popis tvorby jednotlivých dashboardů pro služby a zařízení v testovací infrastruktuře. V závěru je uveden systém nadefinovaných událostí, při jejichž zachycení budou odeslány notifikace, které upozorní na problémy v testovací infrastruktuře.

I. TEORETICKÁ ČÁST

1 LOGOVÁNÍ A LOGOVACÍ PLATFORMY

Log je záznam, který obsahuje informace o události nebo akci, která se v uskutečnila v systému nebo síti. Každý takový záznam by se měl skládat z informaci: kdy k události došlo, na jakém zařízení se událost stala, co se stalo a kdo nebo co to způsobilo. [1] Vytváření, sběru a ukládání těchto záznamů do logovacích souborů se říká logování.

1.1 Využití logů

Dříve se logy využívali pouze k upozornění uživatele, pokud se v systému vyskytla závažnější chyba. S rozvojem výpočetní techniky a jejího využívání se zvýšila potřeba, aby byli správci informování o tom, co se v systémech, ale i celých sítích odehrává. V dnešních dnech umožňují logy získat správcům poměrně komplexní přehled o událostech probíhajících v systémech i sítích.

Jedním z hlavních důvodů logování je bezpečnost. Z logů z antimalwarového softwaru může být správce upozorněn např. na pokus o infikaci operačního systému malwarem nebo podezřelé chování softwaru. Logy ze softwaru pro správu zranitelnosti mohou upozornit na problémy při instalaci bezpečnostních záplat. Software pro vzdálený přístup zase vytváří logy, které upozorňují na úspěšné a neúspěšné vzdálené přístupy do sítě např. pomocí VPN. Routery a firewally mohou správce upozornit pomocí logů na podezřelý síťový provoz a logy z autentizačních a souborových serverů zase na úspěšné nebo neúspěšné pokusy o přihlášení, případně na provedené operace na souborovém serveru. Všechny tyto informace mohou být užitečné k předcházení bezpečnostních incidentů nebo k analyzování již proběhlých incidentů. Také je lze využít k dokazování např. pokud zaměstnanec neoprávněně manipuluje s daty.

Dalšími významnými producenty logů jsou operační systémy. Ty mohou např. s předstihem informovat o softwarových, ale hlavně hardwarových problémech, kdy lze včasným zásahem předejít vážným problémům, které by výrazně ovlivnili nebo zcela znemožnili použitelnost zařízení. Také informují o spouštění, restartování a vypínání služeb nebo úspěšných a neúspěšných auditech neboli situacích, kdy se musí uživatel přihlásit, kontroluje se oprávnění při práci se soubory nebo pokud musí uživatel zvýšit své oprávnění kvůli zásahu do systému.

Kromě spousty dalších možností využití logů stojí za zmínku také jejich použití k optimalizaci výkonu systému nebo sítě. Můžeme např. zjistit vytíženost webové služby z přístupových logů webového serveru a na základě toho upravit škálování výkonu. [2] [3]

1.2 Formáty logů

Jednou z potřeb vzniku strukturovaných formátů logů bylo jejich snadnější strojové zpracování. Logy zapsané v nestrukturovaném textovém formátu jsou pro počítače hůře zpracovatelné, aby se tato činnost zjednodušila a zefektivnila, začaly vznikat formáty logů, které umožňují snadnější strojové zpracování, což je velmi užitečné zejména u softwarů pro centralizovanou správu logů, kam proudí velké množství logů z různých zařízení a aplikací. [4]

Zde je popis pár vybraných formátů logů, se kterými bych se mohl v rámci své práce setkat.

1.2.1 Syslog

Protokol Syslog vznikl v 80. letech minulého století. Jeho původní využití bylo pro poštovní server Sendmail. I přes velikou popularitu, kterou si získal díky své jednoduché funkcionalitě se jej podařilo standardizovat až o více jak dvě desetiletí později. K zásadní změně došlo v roce 2009, kdy byl vytvořen RFC dokument 5424, kde je popsán strukturovaný formát zpráv nebo se zde řeší některé bezpečnostní aspekty.

Tento protokol se využívá k přenosu zpráv o proběhlých událostech na server, který se stará o sběr těchto zpráv ze zařízení v síti. Pro přenos se využívá protokol UDP a port číslo 514, který ovšem nemůže zaručit, že všechny odeslané zprávy dorazí příjemci, proto se v některých případech, pokud to zařízení umožňuje, může využít přenosu pomocí protokolu TCP a portu číslo 1468.

Všechny zprávy vytvořené aplikacemi nebo systémovými komponentami dodržují jednotný tvar daný právě protokolem Syslog. Každá zpráva se skládá ze tří součástí. První je hlavička, která obsahuje prioritu zprávy, verzi použitého protokolu Syslog, časové razítko, název hostitele a aplikace, ID procesu a ID zprávy.

Priorita zprávy je číselná hodnota uvedena v lomených závorkách a jedná se o hodnotu matematicky vypočítanou. K jejímu výpočtu je nutné nejprve znát v jaké součásti systému nebo zařízení k události došlo, dle toho lze zjistit číselný kód tzv. Facility (kategorii zaří-

zení), ten se následně vynásobí číslem 8 a přičte se k němu číselný kód tzv. Severity (Závažnosti). [5]

Tabulka 1. Facility zpráv Syslogu [7]

Hodnota	Popis
0	Zprávy jádra
1	Zprávy na úrovni uživatele
2	Poštovní systém
3	Systémoví démoni
4	Zabezpečení/autorizační zprávy
5	Zprávy generované interně syslogem
6	Subsystém tiskáren
7	Subsystém síťových zpráv
8	Subsystém UUCP
9	Hodinový démon
10	Zprávy o zabezpečení/autorizaci
11	FTP démon
12	Subsystém NTP
13	Audit logů
14	Upozornění logů
15	Hodinový démon
16–23	Místní použití 0–7

Hodnoty 16–23 jsou určené pro vlastní potřeby uživatele nebo specifické aplikace, jejich použití není přesně specifikované.

Tabulka 2. Závažnosti zpráv Syslogu [7]

Hodnota	Popis
0	Nouzový stav: Systém je nepoužitelný
1	Výstraha: Vyžaduje okamžitou pozornost
2	Kritický stav
3	Chybový stav
4	Varování
5	Upozornění: Vyžaduje pozornost
6	Informační zprávy
7	Ladění: Zprávy ladění

Časové razítko obsahuje čas vzniku události s přesností na mikrosekundy. Čas je uváděn v časovém pásmu UTC, je ale možné přenášet i časovou odchylku od pásma UTC a docílit tak přenosu časového razítka s konkrétním časovým pásmem.

Jako název hostitele může být použito jeho FQDN, statická IP adresa, hostname, dynamická IP adresa. Pokud se protokolu Syslog nepodaří získat ani jednu tuto hodnotu využije NILVALUE, tento stav by měl být vysoce nepravděpodobný.

Další součástí zprávy jsou strukturovaná data. Formát těchto dat je určen RFC dokumentem. Tato data mohou obsahovat např. metainformace ke zprávě nebo specifické informace pro určitou aplikaci.

Poslední součástí je samotná zpráva. Ta obsahuje informace o proběhlé události ve volném formátu, pro kódování by mělo být použito UTF-8. [7]

Protokol Syslog byl vyvinut pro použití v UNIXovém operačním systému. V dnešní době má širokou podporu ve spoustě UNIX a UNIX-like distribucích. Díky tomu ho můžeme využít jak na desktopových OS, serverových OS, ale i různých síťových prvcích, NASech a spoustě dalších zařízení včetně zařízení s macOS. [6]

1.2.2 Windows Event Log

Windows Event Log je součástí funkcionality systému Windows. Poprvé se objevila v operačním systému Windows NT a od té doby prošla řadou změn a vylepšení. Tato funkcionalita se stará o zaznamenávání proběhlých událostí v operačním systému a aplikacích.

O každé události se zaznamenávají tyto údaje: Názvu události, Datum a čas kdy došlo k události, Kategorie, Jednoznačné ID události, Úroveň závažnosti, Zdroj nebo název softwaru, který událost způsobil, Uživatel, pod kterým událost vznikla a Počítač, na kterém událost vznikla. [8][9]

Proběhlé události jsou řazeny do následujících kategorií:

- Systémové události – zaznamenávají události proběhlé v systému a jeho komponentách např. selhání součásti systému při spouštění nebo při načítání ovladače
- Bezpečnostní události – zaznamenávají události vznikající činností procesu auditování v systému Windows např. úspěšná a neúspěšná přihlášení, operace se soubory nebo změny v konfiguraci systému
- Události nastavení – zaznamenávají události vznikající při instalaci operačního systému a služby Active directory, pokud je tato služba nainstalována
- Aplikační události – zaznamenávají události vznikající činností aplikací nainstalovaných v operačním systému např. pád aplikace. O tom, jaké události se budou zaznamenávat rozhodují vývojáři aplikací. [8][10]

Dále se můžeme také setkat s přeposlanými událostmi, což jsou události přijaté z jiných počítačů v síti nebo s vlastními událostmi, které využívají aplikace, jež potřebují přizpůsobený formát události.

Tyto události se ještě rozdělují do 5 typů:

- Chyba – označuje závažný problém např.: ztráta dat, neúspěšné načtení služby
- Varování – označuje události, které aktuálně nejsou závažné, nicméně při jejich ignorování by v budoucnu mohli způsobit vážnou událost např.: málo místa na disku
- Informace – označuje úspěšné události např.: načtení ovladače
- Úspěšný audit – zaznamenává úspěšné události v procesu auditování např.: úspěšné přihlášení uživatele
- Neúspěšný audit – zaznamenává neúspěšné události v procesu auditování např.: pokus uživatele o provádění změn v systému s nedostatečným oprávněním [11]

U každé události se také zaznamenává její závažnost, ta se rozděluje na:

- Informace – takto označená událost nám sděluje, že se něco úspěšně podařilo, není třeba jí klást zvláštní pozornost
- Podrobný – takto označená událost nás velmi podrobně informuje o průběhu nebo úspěšném dokončení události
- Varování – takto označená událost nám sděluje, že se vyskytl nějaký méně závažný problém, který je třeba sledovat a řešit, aby se předešlo závažnějším problémům
- Chyba – takto označená událost nám sděluje, že se vyskytl vážný problém, jež mohl ovlivnit chod aplikace nebo systému, ale aplikace nebo systém se z tohoto problému dokázali zotavit
- Kritické – takto označená událost nám sděluje, že se vyskytl velmi závažný problém, kvůli kterému je aplikace nebo systém nefunkční a vyžaduje okamžité řešení [8]

K prohlížení všech zaznamenaných událostí systému Windows je možné využít nástroje Event Viewer (Prohlížeč událostí). [8] Zde můžeme vidět protokoly roztříděné podle závažnosti, typu, kategorie nebo dokonce dle jednotlivých aplikací. Také je možné vytvořit vlastní zobrazení, které bude zobrazovat pouze logy odpovídající nastaveným filtrovacím kritériím. Zde je možné nastavit i filtrování logů pocházejících od konkrétního uživatele nebo stroje v síti, jak staré události nás zajímají, případně i vybrat klíčová slova.

1.2.3 Textové logy

Textové logy jsou ukládány ve formě prostého textu. Struktura takových logů není pevně stanovena. Každý si ji může libovolně přizpůsobit svým potřebám, podle toho, jaké události potřebuje protokolovat. Takto mohou vznikat jak strojově snadno zpracovatelné logy, které jsou pro lidi hůře čitelné, ale i logy, které jsou lidmi snadno čitelné, ale hůře strojově zpracovatelné. [12] Mimo jiné se zde také mohou objevit problémy související s požitým kódováním, které se mohou vyskytnou zejména při zpracování logů na odlišné platformě, než na které vznikly.

1.2.4 CSV logy

Formát CSV byl navržen pro přenos dat mezi různými tabulkovými procesory. Tento formát na rozdíl od prostého textu již musí dodržovat danou strukturu, jednotlivá data jsou zde oddělena oddělovačem např. čárkou, tabulátorem nebo mezerou, což usnadňuje ná-

sledné zpracování pomocí softwarových nástrojů, ale může být hůře čitelné pro lidi. [13] Formát CSV se využívá zejména pro přenos logů mezi logovacími platformami, případně mezi loggerem a logovací platformou. [14]

1.2.5 JSON logy

Protokolování do formátu JSON má výhody jak ve snadné čitelnosti pro lidi, tak také ve snadném zpracování pomocí softwarových nástrojů. Jednotlivé zprávy jsou tvořeny vždy pomocí párů klíč-hodnota např.: *"timestamp": "2024-03-13T22:15:36"*. Zde je přenášen klíč „timestamp“ – časová značka, kdy k události došlo a následně hodnota s datem a přesným časem. [12]

1.2.6 CLF, ELF, GELF

Formát NCSA Common někdy označovaný také jako Common Log Format (CLF) je jedním z nejstarší logovacích formátů, který byl určen pro webové servery. Tento formát je pevně daný a není tedy možné jej jakkoliv přizpůsobit, což může být v některých případech omezující. V každém záznamu je v následujícím pořadí uvedeno: IP adresa klienta, identifikace uživatele, který provedl požadavek na server, identifikace uživatele, který byl ověřen pomocí autentizačního mechanizmu, datum a čas včetně časové zóny, požadavek a verzi protokolu, HTTP status kód a počet odeslaných bajtů. Pokud není některý údaj známý, vloží se na jeho místo pomlčka. [15]

Formát Extended Log Format (ELF) se podobá výše popsanému formátu CLF, ale na rozdíl od něj nabízí daleko větší škálu informací, které může zaznamenávat. Také nám umožňuje si zvolit pomocí tzv. direktivy pouze ta pole s informacemi, které budeme skutečně využívat a nemusíme tak sbírat ty, které jsou pro nás nepotřebné. Tento formát je vhodný např. pokud potřebujeme detailnější informace o přístupech a chování uživatelů. Nejprve se zaznamená: verze, použitý software, datum a čas spuštění protokolování, direktivou definovaná pole (jaké informace se budou ukládat), poté následuje záznam samotných událostí. Na závěr se doplní ještě datum a čas ukončení protokolování, také je možné vložit i komentář. Všechny tyto informace, až na záznam události začínají znakem #. [15]

Formát Graylog Extended Log Format (GELF) je formát vyvinutý přímo pro platformu Graylog. Vychází z výše popsaného formátu ELF, ale přidává do něj další rozšíření. Tento formát již není přímo určen na zaznamenávání událostí z webového serveru, ale byl vyvinut, aby odstranil nedostatky protokolu Syslog. Hlavní výhodou tohoto formátu je umož-

nění přenosu velkých zpráv. Syslog má omezení délky zprávy na 1024 bajtů, což může být v některých případech nedostatečné. Proto formát GELF umožňuje odesílání i delších zpráv, toho docílil nejen využití maximální velikosti datagramu UDP, která činí 8192 bajtů, ale zprávy posílá jako bloky dat, což umožňuje zprávu rozdělit do více bloků a každý blok poté odeslat v samotném UDP paketu. Další výhodou je podpora komprimování zpráv pomocí GZIP nebo ZLIB, což sníží objem přenášených dat po síti. Zprávy v tomto formátu obsahují: Identifikaci zařízení, na kterém došlo k události, časové razítko, verzi, krátkou a dlouho verzi zprávy a dále pak vlastní pole, která si můžeme nakonfigurovat dle našich potřeb. [4][16]

1.2.7 Apache access/error logy

Webový server apache ukládá logy vzniklé při provozu do několika souborů, ty se rozdělují dle toho, s čím obsah logu souvisí. Mezi nejpodstatnější patří soubory s přístupovými (access) logy a soubory s chybovými (error) logy. [17]

Do souborů s přístupovými (access) logy se zaznamenávají požadavky uživatelů přistupujících na webový server. Takovéto informace lze využít např. pro ladění chyb webové aplikace nebo k její optimalizaci a zlepšení výkonu. Použitý formát logů lze nastavit v konfiguračních souborech webového serveru. Je možné zvolit výše popsaný Common Log Format (CLF), kombinovaný log formát, který rozšiřuje CLF o odkaz, ze kterého uživatel na webovou stránku přišel a také o informaci, jaký prohlížeč použil. Poslední možností je zvolit přizpůsobený formát logu, kdy si lze pomocí direktivy nastavit, jaké informace se budou ukládat, podobně jako ve výše popsaném formátu ELF. [18]

Soubor s chybovými (error) logy zaznamenává chyby, které vzniknou při zpracování požadavků na serveru. Tyto zprávy mohou upozornit např. na různé chyby a výjimky spojené s problémy ve webové aplikaci nebo konfigurací webového serveru, případně také na nedostupnost některých zdrojů. Informace, které budou zaznamenávány lze upravit v konfiguračním souboru webového serveru. Ve výchozím nastavení se zaznamenává: čas, úroveň závažnosti zprávy, IP adresa klienta a chybová zpráva. Toto nastavení lze změnit a ukládat i jiné informace, které jsou zapotřebí. [19]

1.3 Správa logů

Jak již bylo zmíněno výše, v dnešní době generuje logy spousta zařízení, systémů a aplikací, také přibývá hrozeb a útoků na tyto zařízení a systémy. Z těchto důvodů vznikla tzv. správa logů (log management), která zajišťuje celý proces od vygenerování logu, přes jeho přenos a uložení až po analýzu a následnou likvidaci. [2]

1.3.1 Generátory logů

Generátorem logů je jakékoliv zařízení, systém nebo aplikace, které vytváří logy. Tyto logy se ukládají do souborů, někdy jsou určité logy uchovávány pouze v operační paměti. To vytváří několik problémů. Každý generátor logů může využívat vlastní formát zpráv, což komplikuje následné čtení logů nebo strojové zpracování. Dalším problémem je velké množství souborů, které je nutné kontrolovat. Posledním problémem je, možnost přepsání logů např. útočníkem při průniku do systému, aby po sobě zahladil stopy. Tyto problémy řeší stanovení formátu logů a centralizované ukládání logů, kdy je možné logy ukládat lokálně a zároveň je odesílat na logovací server.

Neopomenutelnou funkcí generátorů logů je rotace logů. Jedná se o funkci, která dle nastavených kritérií uzavře aktuálně používaný log soubor a založí nový. Jako kritérium lze zvolit např. velikost souboru nebo časové období. Dále lze nastavit, co se s uzavřeným log souborem stane. Je možné nastavit archivaci protokolu na jiné úložiště, zvolit komprimaci log souboru pro zmenšení jeho velikosti, spustit skripty na analýzu obsahu log souboru nebo smazání starších log souborů z paměti zařízení. Díky této funkci je možné se lépe v lozích orientovat a také je zajištěno, že zařízení bude mít dostatek volného místa na ukládání nových logů. [2]

Důležitým údajem u logů je čas. Abychom mohli logy správně vyhodnocovat potřebujeme vědět přesný čas, kdy k určité události došlo. Proto je nutné mít na zařízení nebo v systému nastaven přesný čas i se správným časovým pásmem. S udržením správného času na zařízení nám může pomoci protokol NTP, který zajistí přenos přesné časové informace, ze serveru, kde je přesný čas zajištěn např. pomocí GPS nebo radiovým signálem, na klientské zařízení.

1.3.2 Logovací servery a analyzátory logů

Logovací servery jsou služby běžící na serveru, které přijímají logy z generátorů a ukládají je. Buď opět v podobě log souborů nebo je zapisují do databáze, to se využívá zejména u

serverů spojených s funkcí analyzátoru. Jednoduché analyzátory mohou fungovat jako skripty procházející log soubory. Ty pokročilé, jako např. Graylog, využívají ke svému běhu databázi, do které jsou logy ukládány. To umožňuje následné snadné filtrování logů a přehledné zobrazení výsledků pro správce, doplněné o vhodnou formu upozornění nebo automatizovaný zásah pomocí předem připravených skriptů. Pro takové řešení je vhodný příjem logů ze zařízení v reálném čase a ne např. až v momentě rotace logů. Některé analyzátory logů již ke své činnosti využívají umělou inteligenci. [2] [20]

2 MOŽNOSTI PLATFORMY GRAYLOG

Graylog je platforma sloužící primárně k centrálnímu sběru logů, jejich analýze a snadnému vyhledávání potřebných informací obsažených v lozích. Díky rozsáhlé podpoře logovacích formátů a protokolů dokáže efektivně sbírat a zpracovávat logy ze spousty různých zařízení a aplikací. Další užitečnou funkcionalitou této logovací platformy je možnost nastavení zasílání oznámení pomocí různých komunikačních prostředků, při výskytu předem nadefinovaných událostí, ale také přehledná vizualizace informací z logů. Tato platforma je k dispozici pro použití zdarma, ale využití některých profesionálních funkcí je zpoplatněno.

2.1 Sběr logů

První, nejpodstatnější částí, je sběr logů. Platforma Graylog disponuje rozsáhlými možnostmi pro příjem logů z různorodých generátorů např. operačních systémů, aplikací, služeb, síťových prvků, serverů, cloudových služeb, virtualizačních a kontejnerizačních platforem nebo zařízení internetu věcí. Díky rozsáhlé podpoře logovacích formátů a protokolů, mezi které lze zařadit např. Syslog, NetFlow, JSON, GELF, CEF nebo Beats je možné sbírat logy i z vlastních aplikací nebo specifických systémů. Pokud by byly tyto formáty nedostatečné je zde také podpora zpracování logů ve formě prostého textu, případně lze vybrat nějaký z mnoha doplňků, který tuto řadu podporovaných vstupů rozšíří.

Velmi užitečnou věcí, v dnešní době, je i možnost přijímat logy přímo z cloudových platforem např. Amazon Web Services, služby Google (Cloud, Workspace, Gmail), služby Microsoft (Azure, Defender for Endpoint, Office 365), Okta a další. [21]

Protože přenos logů probíhá po síti, nabízí tato platforma možnosti na zabezpečení přenosu. Je možné např. využití protokolu TCP namísto UDP, který zaručuje spolehlivé doručení všech logů, využití protokolu TLS, pro zajištění šifrování přenášených informací, a tedy i ochranu proti odposlechům a zajištění integrity zpráv nebo využití certifikátu pro ověření identity Graylog serveru. [22]

2.2 Ukládání logů

Platforma Graylog ke svému běhu využívá databázový server MongoDB. Do databáze na tomto serveru ukládá všechny přijaté logy. Graylog je tedy možné využít nejen k analýze logů, ale také k jejich archivaci. Vybrané logy lze také exportovat do CSV souboru. Pro

následnou analýzu se využívají nástroje Elasticsearch nebo od nejnovějších verzí pouze OpenSearch. [23]

2.3 Analýza logů

O první roztřídění příchozích logů se starají streamy. Při jejich vytváření je třeba zvolit zdroj logů (buď přímo nějaký ze vstupů nebo již existující stream) a následně zapsat podmínku, kterou musí logy procházející streamem splňovat. Takto lze efektivně roztřídit přicházející logy, pokud přes jeden vstup přichází logy z více zařízení a na každém zařízení běží více služeb. [24]

Další analyzační funkcionalitou jsou pipelines. Jedná se sadu pravidel pro další zpracování přicházejících logů ze streamů. [28] Příkladem jejich použití může být extrakce informací z logů. Některé protokoly jako např. GELF nebo Beats umožňují předávání informací z logů v dobře strukturovaném a snadno filtrovatelném formátu. Pokud ale budeme mít pouze textovou zprávu, nebude možné informace z ní automatizovaně zpracovávat. V takových případech je možné pomocí sady pravidel, extrahovat jednotlivé důležité informace z logů a umožnit jejich následné strojové zpracování. Pravidla se většinou skládají z podmínky, která vyhodnocuje, zda přišla zpráva, ze které chceme informace extrahovat a následně se pomocí tzv. grok patternu nastaví vzor, které části zprávy obsahují, pro nás podstatné, informace. Takto nastavená pravidla se poté musí připojit k pipeline do tzv. stage (fází), ty se následně postupně vykonávají a v případě, že nejsou splněny podmínky v jedné fázi, tak se další fáze již nevykonají. [28]

Dalším filtrováním, které by mělo následovat po vytvoření streamů je definice událostí. Každá událost je tvořena jednou nebo několika podmínkami a zvolením vhodného streamu nebo vstupu logů, poté jsou všechny přicházející logy kontrolované nadefinovanými podmínkami a pokud jsou splněny, je zobrazena výstraha upozorňující na neobvyklí stav ve sledované infrastruktuře např. chyba hardwaru nebo pokusy o neúspěšné přihlášení. [25]

2.4 Zasílání oznámení

K vytvořeným událostem je možné nastavit zaslání oznámení, což by mělo pomoci rychleji upozornit na případné nestandardní situace, které ve sledované infrastruktuře nastanou. Graylog umožňuje zasílání oznámení pomocí více komunikačních kanálů. Je možné zvolit zasílání pomocí komunikačních platforem Microsoft Teams nebo Slack, elektronickou poštou nebo zasláním POST požadavku s využitím protokolu HTTP. Po získání provozní

licence pro funkci Graylog Operations je možné odesílání upozornění do cloudové platformy PagerDuty nebo spuštění skriptu, který bude reagovat na vzniklou událost. Pro Graylog existuje také spousta doplňků, díky kterým je možné zasílat oznámení i dalšími způsoby.

U komunikačních platforem je možné nastavit, zda se budou oznámení odesílat konkrétní osobě nebo do určitého kanálu, také lze upravit obsah zprávy, která bude zaslána. V případě oznámení pomocí e-mailu určíme příjemce pomocí e-mailové adresy a opět můžeme nastavit, jak bude tělo e-mailu vypadat, k tomu je možné využít i šablonu vytvořenou pomocí HTML. U zasílání oznámení na HTTP API nastavujeme údaje potřebné pro komunikaci s API, autentizační údaje a URL adresu. Oznámení zasílaná touto formou jsou ve formátu JSON. [26]

2.5 Vizualizace logů

Informace z logů je také možné přehledně vizualizovat pomocí dashboardů. Na ně je možné umístit tzv. widgety, které mohou zobrazovat různé typy grafů a počítadel, ty umožňují zobrazovat různá minima, maxima a průměry hodnot nebo počty, trendy a jiné. Dále lze vložit tabulku zpráv, která umožňuje filtrování logů a zobrazuje pouze vybrané informace z logů např. časové razítko, zdroj, krátkou zprávu nebo přímo nějakou vybranou hodnotu. Zajímavou možností může být zobrazení mapy, kde můžeme zobrazovat např. lokalizované IP adresy. U widgetů je také možné nastavit časové období neboli jak staré logy se mají zobrazovat, případně z jak starých logů se mají čerpat data pro počítadla a grafy. Další výhodou je možnost vytváření stránek, kdy jeden dashboard např. pro určitou službu, může pro větší přehlednost obsahovat více stránek a na každé stránce může být jen určitá část, spolu souvisejících widgetů. To zajišťuje větší přehlednost dashboardů a snadnější orientaci pro uživatele. [27]

3 DEFINICE KRITICKÝCH INFORMACI

Definování kritických informací pro následnou analýzu a uchovávání je poměrně náročný a důkladný proces. Povinné uchovávání některých informaci bylo doposud specifikováno legislativou nebo některými ISO standardy. Nyní přijde zásadní změna v podobě směrnice NIS2, která je krokem Evropské unie, proti stále přibývajícím kybernetickým útokům a nově vznikajícím hrozbám. Ta by měla specifikovat, jaké informace je třeba uchovávat pro případnou analýzu bezpečnostních incidentů. Organizace, které nemají legislativní povinnost uchovávat informace, případně chtějí svou kritickou infrastrukturu sledovat komplexněji, musí nejprve analyzovat, co je, pro ně samotné, cílem log managementu. Je zapotřebí specifikovat prioritní oblasti sledování (např. místa s nejcitlivějšími daty nebo nejzranitelnější body), naplánovat postup v případě výskytu bezpečnostního incidentu, či identifikovat potenciální výkonnostní problémy, které by mohly výrazně ovlivnit kvalitu služeb pro uživatele. [29]

V rámci log managementu je obecně vhodné sledovat následující skupiny logů.

3.1 Bezpečnostní logy

Bezpečnostní logy může generovat antimalwarový software, který může informovat o detekci malwaru, pokusech o infikaci souborů nebo systému. Dalším zdrojem jsou síťové prvky. Routery, switche, firewally a IDS/IPS systémy mohou informovat zejména o blokování komunikace dle nastavených pravidel nebo o podezřelé síťové aktivitě. Software pro vzdálený přístup zaznamenává informace o každém pokusu připojení a statistikách navázaných připojení. Pokud je tento systém kombinován s karanténním serverem, lze získávat informace o úspěšné, případně neúspěšné kontrole klienta. Velmi užitečným zdrojem logů jsou auditní logy z autentizačních serverů např. ActiveDirectory, kdy se při každém pokusu o autentizaci podrobně zaznamenávají informace např. o zdrojovém zařízení, uživatelském jménu nebo úspěšnost. [2]

3.2 Logy z operačních systémů

Většina operačních systémů ať už serverových, desktopových nebo různých síťových prvků, zařízení internetu věcí apod. umožňuje logování. Z těchto logů je vhodné sledovat události systému, které informují o tom, co se v systému odehrává např. selhání služby nebo změna konfigurace. Dále je vhodné sledovat výkonnostní logy, ty mohou upozornit na problémy s výkonem např. velké využití systémových prostředků nebo docházející místo

na disku. Užitečné jsou také auditní logy, které zaznamenávají informace o úspěšných a neúspěšných přihlášeních, přístupech k souborům, změn bezpečnostních politik, nastavení účtů nebo využívání oprávnění. [2]

3.3 Aplikační logy

U aplikačních logů je vhodné sledovat žádosti klientů a následné odpovědi serveru. Díky tomu můžeme mít přehled o využívání zdrojů, případných bezpečnostních incidentech, mohou pomoci při optimalizaci webové aplikace nebo upozornit na nesprávnou funkcionalitu a nedostupnost zdrojů. Pokud aplikace umožňuje autentizaci uživatelů, můžeme zaznamenávat pokusy o neúspěšné přihlášení nebo činnosti prováděné uživateli v aplikaci. Vhodné je také sledování chybových logů aplikace. Díky tomu můžeme být informováni o selhání aplikace, jejím vypnutí nebo restartu. [2]

4 SBĚR LOGŮ ZE ZAŘÍZENÍ

Pro sběr logů ze zařízení je nutné v Graylogu vytvořit vstup. Při vytváření vstupu je důležité zvolit v jakém formátu budou logy přicházet, dále lze nastavit zabezpečení komunikace pomocí TLS nebo upravit parametry síťové komunikace. Graylog umožňuje jedním vstupem přijímat logy z více generátorů, ale je také možné nakonfigurovat více stejných vstupů, které budou naslouchat na rozdílných portech a tím snížit množství logů přicházející jedním vstupem, ovšem k většímu roztřízení logů je vhodné využít streamy.[21]

Dále je nutné vhodně nakonfigurovat zařízení, které má logy do Graylogu odesílat.

4.1 Operační systémy

Pro sběr logů z linuxových a unixových operačních systémů je nejvhodnější možností využít nativně podporovaný protokol Syslog. V takovém případě stačí pouze vhodně nakonfigurovat použitou logovací utilitu např. syslog-ng nebo rsyslog. Při sběru logů z operačních systémů Windows již nastává problém, protože Windows Event Log neumožňuje přeposílání logů na Graylog server. V tomto případě je nutné zvolit nějaký z externích logovacích nástrojů např. NXLog, který dokáže posílat logy do Graylog serveru pomocí protokolu GELF. Ještě vhodnější variantou je využití Winlogbeat, jež svou komplexní strukturou usnadňuje následnou analýzu logů. [30]

4.2 Síťové prvky

Sběr logů ze síťových prvků může být složitý, protože se možnosti logování mohou lišit u jednotlivých modelů nebo firmwarových verzí, případně možnost logování může zcela chybět. Nicméně síťové prvky z profesionálních řad od výrobců jako např. MikroTik, Cisco, Ubiquiti a další, ve většině případů již podporují logovací protokol Syslog a umožňují zasílání logů po síti. V takovém případě stačí jen zařízení vhodně nakonfigurovat.

4.3 IoT zařízení

Velmi podobná situace, jako u síťových prvků, panuje i u zařízení internetu věcí. Kdy u IoT zařízení mohou být implementovány různé logovací protokoly a mohou nabízet různé možnosti odesílání svých log souborů na logovací servery, případně nemusí být tato možnost dostupná vůbec.

4.4 Aplikace a služby

U aplikací a služeb je nutné se nejprve seznámit s možnostmi logování, které nabízí. V nejlepších případech odesílá aplikace své logy pomocí API do Windows Event Logu nebo lze vhodným nastavením zajistit předávání logů z aplikace do Syslogu. V případě, že toto aplikace neumožňuje, je nutné použít jiný způsob např. pomocí externího nástroje odesílat její log soubory na Graylog server.

4.5 Virtualizační a kontejnerizační platformy

U virtualizačních platforem je opět nutné zjistit, jaký způsob logování a předávání logů umožňují. Některé virtualizační platformy založené na linuxových operačních systémech podporují protokol Syslog např. ESXi od VMware. Platforma Hyper-V od Microsoftu zase ke svému běhu využívá Event Log, stejně jako ostatní operační systémy Windows.

U kontejnerizačních platforem je situace podobná. Např. platforma Docker má sice vlastní logovací nástroj, ale podporuje různé logovací formáty např. Syslog nebo GELF a také umožňuje nastavení zasílání svých logů na logovací server. [31]

4.6 Cloudové služby

Graylog také umožňuje příjem logů z cloudových platforem. Tento typ vstupu, na rozdíl od předchozích, nečeká, až jsou logy odeslané zařízením, ale sám posílá požadavky na API rozhraní cloudové platformy, která mu následně zašle logy. Zde se již vyžaduje nastavení ověřování a není vhodné podceňovat ani zabezpečení této síťové komunikace. Mezi nejznámější podporované cloudové platformy patří např. Microsoft Office 365, Microsoft Azure, Amazon Web Services, služby Google (Cloud, Workspace, Gmail) nebo Okta. [21]

II. PRAKTICKÁ ČÁST

5 NASAZENÍ ŘEŠENÍ DO TESTOVACÍ INFRASTRUKTURY

Před samotným vytvořením řešení bylo nutné nejprve důkladně analyzovat testovací infrastrukturu. Důkladná analýza se skládala z určení, jaká zařízení se v testovací infrastruktuře nachází, dále jakými způsoby zasílají logy na logovací server a jaké druhy logů generují. Následně bylo možné začít pomocí správně nakonfigurovaných streamů a pipeline třídit přicházející logy a extrahovat z nich potřebná data. Po dokončení této konfigurace teprve následovala tvorba dashboardů. Posledním krokem byla tvorba oznámení, kdy bylo nejprve nutné nakonfigurovat komunikační kanály, které může Graylog využívat. Následovalo definování událostí, při kterých je zasíláno oznámení a na závěr bylo zapotřebí ještě upravit obsah zpráv, které se zasílají při výskytu nadefinované události.

5.1 Analýza testovací infrastruktury

Důkladnou analýzou příchozích logů bylo zjištěno, že se v testovací infrastruktuře nachází tato zařízení:

- 2 počítače s OS Windows
- NAS
- Router Ubiquiti Dream Machine Pro
- Server s OS Linux a Apache webovým serverem

Pro zasílání logů z počítačů s OS Windows je nakonfigurován vstup typu Beats a je využito softwaru Wazuh agent, který odesílá logy z PC na Graylog server. Druhým nakonfigurovaným vstupem je Syslog UDP, který přijímá logy ze zbylých zařízení, tedy NASu, routeru a serveru.

Při důkladné analýze obsahu logů, byly vybrány ty logy, které je vhodné sledovat pro získání přehledu o dění v testovací infrastruktuře, zajištění její bezpečnosti a stability.

Na počítači s operačním systémem Windows se budou pomocí logů monitorovat následující události:

1. Neúspěšné přihlášení

   Je nutné sledovat zejména opakované neúspěšné pokusy o přihlášení, protože ty mohou naznačovat pokus o neoprávněný přístup nebo útok na systém. Včasným upozorněním a rychlím zásahem lze předejít případnému bezpečnostnímu incidentu.

2. Instalace softwaru

   Je důležité sledovat změny v prostředí operačního systému, zejména instalaci nového softwaru. Takto můžeme být včasně upozorněni na nainstalování nové aplikace nebo na chyby při instalaci aplikací např. pomocí softwaru pro hromadnou správu zařízení.

3. Potřeba restartovat zařízení

   Sledování logů upozorňující na potřebu restartu zařízení je důležité zejména pro udržení operačního systému a některých aplikací aktuálních. Toto řešení je vhodné zejména pro servery nebo jiná zařízení, která pracují nepřetržitě a bez obsluhy, která by si mohla všimnout zprávy od operačního systému informující o potřebě zařízení restartovat.

4. Změna časového pásma

   Informace o změně časového pásma může být opět užitečné sledovat na serverech, kdy při špatně nastaveném času na serveru, mohou být některé jeho služby zcela nedostupné. Správné zpracování těchto logů může informovat např. o tom, zda se při přechodu mezi letním a zimním časem tato změna aplikovala na všech zařízeních.

5. Nedostupnost DNS serveru

   Logy obsahující informaci o nemožnosti překladu doménových názvů mohou informovat o problémech s DNS serverem případně o problémech s připojením k síti nebo síťovou konektivitou.

6. Problémy při registraci IP adresy

   Tyto zprávy mohou správce upozornit na možné problémy se službou DHCP nebo na chyby v konfiguraci sítě např. na kolizi IP adres v síti.

Z logů z NASu je možné sledovat:

1. Přihlašování k NASu

   Zprávy o přihlášení uživatele do administračního rozhraní NASu je vhodné sledovat a uchovávat, lze je využít ke sledování aktivit uživatelů, případně mohou upozornit na neoprávněný přístup.

2. Stav VPN spojení

   Sledování stavu VPN spojení je velmi důležité. V případě jeho výpadku může být NAS z některých částí sítě nedostupný, a to může způsobit nemalé problémy. Proto je vhodné sledovat zejména výpadky spojení a včasně na ně reagovat.

Sledováním logů z routeru můžeme být informováni o následujících událostech:

1. Stav linek

   Z příchozích logů je možné sledovat stav WAN rozhraní a upozorňovat na výpadky připojení k síti Internet nebo např. změnu IP adresy WAN rozhraní. Dále může být užitečné sledovat i některé parametry linky jako např. její rychlost a odezva z pravidelných měření.
2. Nedostupnost služeb

   Druhou skupinou logů jsou ty, které mohou informovat o problémech při navazování komunikace s některými službami např. NTP nebo UTM Cloud Service, což může usnadnit diagnostiku problémů se síťovým připojením.
3. Konfigurace a chyby služeb

   Velmi užitečné je sledování změn konfigurace routeru nebo nastavení firewallu, což může upozornit na neoprávněný zásah do zařízení. Užitečné je také sledování zpráv např. o neúspěšné lokalizaci IP adres pomocí služby GeoIP nebo vypršení platnosti certifikátu pro službu wifiman-proxy.
4. Hardwarové prostředky

   Další důležitou skupinou logů jsou ty, které informují o využití hardwarových prostředků routeru např. v případě vysokého využití operační paměti. Pokud k takovému stavu bude docházet často, může to naznačovat problémy s konfigurací nebo nedostatečnost hardwarových zdrojů.
5. Firewallem zablokovaná komunikace

   Tyto logy jsou klíčové pro zajištění monitorování síťového provozu a bezpečnosti síťové infrastruktury. Díky nim lze snadno odhalit pokusy o útoky nebo neoprávněný přístup a předcházet tak bezpečnostním hrozbám. Např. sledování náhlého navýšení počtu zpráv o zablokované komunikaci může naznačovat pokus o útok na infrastrukturu. Dále jsou dobrým pomocníkem pro diagnostiku problémů s neúspěšnou komunikací mezi síťovými zařízeními.

Logy ze serveru je možné rozdělit do několika skupin: systémové logy, logy firewallu a logy webového serveru Apache.

Z první skupiny systémových logů je vhodné sledovat následující:

1. Neúspěšná přihlášení

   Pro tento bod platí totéž jako pro sledování neúspěšných přihlášení na počítači s OS Windows, které bylo popsáno výše.
2. Vypnutí systému

   Sledování logů informujících o vypnutí systému poskytuje správcům přehled o činnostech systému. Také může upozornit na případný bezpečnostní incident nebo lidský omyl.
3. Změny uživatelských účtů

   Kontrolou logů týkajících se uživatelských účtů můžeme mít přehled o vytváření nových účtů nebo např. změně hesel k účtům, a tedy i dohlížet na dodržování nastavených bezpečnostních politik.
4. Restart služeb

   Monitorováním logů o restartu služeb lze odhalit anomálie v provozu serveru a včasně na ně reagovat. Tím lze předcházet rozsáhlejším problémům a zabezpečit spolehlivější poskytování služeb.
5. Nedostupnost síťových služeb

   Sledováním logů informujících o nedostupnosti služeb jako např. DNS nebo NTP je možné zjistit problémy se síťovou komunikací, případně výpadek těchto služeb. Také mohou být nápomocny při řešení problémů se sítí.
6. Spouštění skriptů

   Díky těmto logům lze mít přehled o dění na serveru, je možné např. sledovat spouštění naplánovaných úloh apod.

Z druhé skupiny logů z firewallu je vhodné sledovat:

1. Firewallem zablokovaná komunikace

   Pro tento bod platí totéž jako pro sledování logů firewallu na routeru, které bylo popsáno výše.
2. Přidání IP adresy na blacklist

   Logy informující o přidání IP adresy na blacklist je vhodné sledovat z bezpečnostních důvodů, mohou odhalit např. pokus o DoS útok na infrastrukturu. Také je užitečné tyto adresy pro přehled kontrolovat a sledovat případný náhlý nárůst.

Z poslední skupiny logů ze služby Apache je vhodné sledovat:

1. Access logy

   Tyto logy je důležité sledovat, protože mohou upozornit na problémy s webem nebo webovou aplikací, díky analýze HTTP stavových kódů je možné rychle objevit chyby při zpracování požadavků od uživatelů nebo nedostupnost některých zdrojů. Také je možné sledovat počet přístupů na webový server nebo objem přenesených dat.
2. Error logy

   Sledování error logů je důležité pro zachování plynulého provozu webového serveru. Poskytují důležité informace pro diagnostiku chyb vzniklých při provozu webového serveru, případně jsou nápomocny při ladění a optimalizaci webových aplikací. Tyto logy jsou také velmi důležité při identifikaci potenciálních bezpečnostních hrozeb, obsahují informace o útocích na server nebo o pokusech o neoprávněný přístup.

5.2 Konfigurace streamů a pipeline

Po dokončení důkladné analýzy následovalo nadefinování třízení příchozích logů. První roztřízení obstarávají streamy ServerLogs, RouterLogs, NASLogs a PCLogs.

- ServerLogs obsahuje všechny logy, jejichž zdrojem je server s hostname blockchain a přicházející vstupem Linux Syslog, dále je vybrána možnost, aby byly tyto logy odstraněny z „Default Stream“
- RouterLogs obsahuje všechny logy, jejichž zdrojem je router s hostname UDMpro-B108 a přicházející vstupem Linux Syslog, dále je vybrána možnost, aby byly tyto logy odstraněny z „Default Stream“
- NASLogs obsahuje všechny logy, jejichž zdrojem je NAS s hostname NAS-BatovaVila2 a přicházející vstupem Linux Syslog, dále je vybrána možnost, aby byly tyto logy odstraněny z „Default Stream“
- PCLogs obsahuje všechny logy, jejichž zdrojem jsou zařízení s hostname začínajícím na „WIN-“ a přicházející vstupem winlogbeats (Beats), dále je vybrána možnost, aby byly tyto logy odstraněny z „Default Stream“

Logy ze serveru a routeru jsou pomocí pipeline třízeny do dalších streamů, podle služeb, které tato zařízení poskytují a budou sledovány. Také z logů extrahují potřebné informace pro tvorbu dashboardů.

5.2.1 Pipeline Server - Apache

Pomocí pipeline *Server - Apache* jsou směrovány Apache access a error logy do streamu *ApacheAE*. Vstupem pro tuto pipeline je stream *ServerLogs*.

Ve stage 0 je obsaženo pravidlo *Apache – HTTPAccessError message*.

Ve stage 1 jsou obsažena pravidla *Apache – HTTPAccess extraction* a *Apache – HTTPError extraction*.

5.2.1.1 Apache – HTTPAccessError message

Toto pravidlo kontroluje, zda zpráva obsahuje řetězec „http_access“ nebo řetězec „http_error“. Pokud je alespoň jedna podmínka splněna je log přesměrován do streamu *ApacheAE*.

5.2.1.2 Apache – HTTPAccess extraction

Toto pravidlo zachytává zprávy obsahující řetězec „http_access“ a pomocí grok patternu `http_access %{IP:client_ip} \\- %{DATA} \"%{DATA}\" %{NUMBER:status_code:int} %{NUMBER:send_bytes:float}` extrahuje informace o IP adrese klienta, který přistupoval k webovému serveru, HTTP status kód odpovědi a počet odeslaných bajtů.

5.2.1.3 Apache – HTTPError extraction

Toto pravidlo zachytává zprávy obsahující řetězec „http_error“ a pomocí grok patternu `client %{IP:client_ip}` se pokouší extrahovat IP adresu klienta, pokud se v logu nachází, jehož požadavek tuto chybu způsobil.

5.2.2 Pipeline Firewall

Pomocí pipeline *Firewall* jsou směrovány logy z routeru a webového serveru, obsahující informace o činnosti firewallu na těchto zařízeních, do streamu *FirewallsLogs*. Vstupem pro tuto pipeline jsou streamy *RouterLogs* a *ServerLogs*.

Ve stage 0 je obsaženo pravidlo *FW messages*.

Ve stage 1 jsou obsažena pravidla *UFW extract message* a *Firewall Blacklisting Ex*.

5.2.2.1 FW messages

Toto pravidlo kontroluje, zda zpráva obsahuje řetězec „UFW BLOCK“, „Blacklisting address“ nebo „SRC=“. Pokud je alespoň jedna podmínka splněna, je log přesměrován do streamu *FirewallsLogs*.

5.2.2.2 UFW extract message

Toto pravidlo zachytává zprávy, o firewallem zablokované komunikaci, které obsahují řetězec „SRC“ a pomocí grok patternu `SRC=%{IP:source_ip} DST=%{IP:destination_ip} %{DATA} PROTO=%{WORD:protocol} SPT=%{NUMBER:source_port} DPT=%{NUMBER:destination_port} %{GREEDYDATA}` extrahuje informace o zdrojové a cílové IP adrese, zdrojovém a cílovém portu a použitém protokolu.

5.2.2.3 Firewall Blacklisting Ex

Toto pravidlo zachytává zprávy informující o přidání IP adresy na blacklist, které obsahují řetězec „Blacklisting address“ a pomocí grok patternu `Blacklisting address %{IP:client_ip}: %{GREEDYDATA:reason}` extrahuje informace o zablokované IP adrese a důvodu zablokování.

5.2.3 Pipeline Router – Speed

Pomocí pipeline *Router – Speed* jsou směrovány logy z routeru, obsahující informace z nástroje měření rychlosti připojení k internetu, do streamu *RouterSpeed*. Vstupem pro tuto pipeline je stream *RouterLogs*.

Ve stage 0 je obsaženo pravidlo *Router - LinkCheck messages*.

Ve stage 1 je obsaženo pravidlo *RouterSpeed*.

5.2.3.1 Router - LinkCheck messages

Toto pravidlo kontroluje, zda zpráva obsahuje řetězec „linkcheck“. Pokud je tato podmínka splněna, je log přesměrován do streamu *RouterSpeed*.

5.2.3.2 RouterSpeed

Toto pravidlo zachytává zprávy, které obsahují řetězec „linkcheck“ a pomocí grok patternu `Downlink %{NUMBER:download:float} %{DATA} Uplink %{NUMBER:upload:float}` extrahuje informace o rychlosti stahování a odesílání. Pomocí dalšího grok patternu `ping\\[%{NUMBER:ping:float}\\]` se extrahuje informace o velikosti odezvy ping.

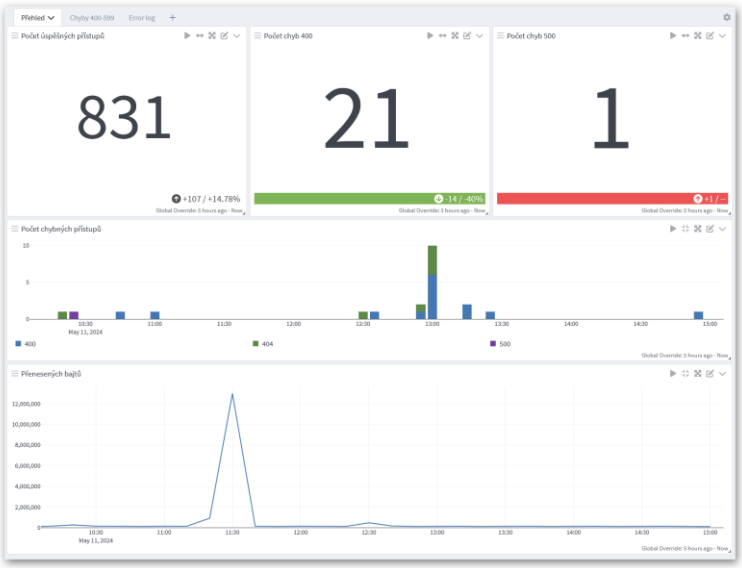
6 TVORBA DASHBOARD

Poté, co byla dokončena konfigurace třídění logů pomocí streamů a extrahování dat bylo možné začít vytvářet dashboardy. Nejprve bylo nutné navrhnout skupiny logů, které spolu souvisí a zvolit pro ně vhodnou formu vizualizace. Všechny logy byli seskupeny podle zařízení nebo služeb, kterým patří. Pro zvýšení přehlednosti jsou logy rozděleny do spolu souvisejících podskupin a jsou vizualizovány na jednotlivých stránkách dashboardů. Pro rychlejší orientaci mezi již existujícími dashboardy, obsahují všechny názvy prefix *BP_*.

6.1 Apache

Dashboard BP_Apache obsahuje 3 stránky. Na první stránce Přehled, se zobrazují statistické údaje o provozu serveru, jako jsou počty úspěšných přístupů na webový server, počítadla s odpověďmi webového serveru s HTTP status kódy 400 až 499 a 500 až 599. Ty jsou také znázorněny podrobněji graficky na časové ose s názvem „Počet chybných přístupů“. Dále se zde nachází graf s názvem „Přenesených bajtů“, který na časové ose zobrazuje množství přenesených bajtů v úspěšných odpovědích serveru. Na druhé stránce Chyby 400-599 se nachází 2 tabulky zobrazující informace, kterým klientům vrátil webový server odpověď se status kódem v rozsahu 500 až 599 nebo 400 až 499. Na poslední stránce je zobrazena tabulka, obsahující nedávné Apache Error logy. Všechny prvky na tomto dashboardu čerpají logy ze streamu ApacheAE.

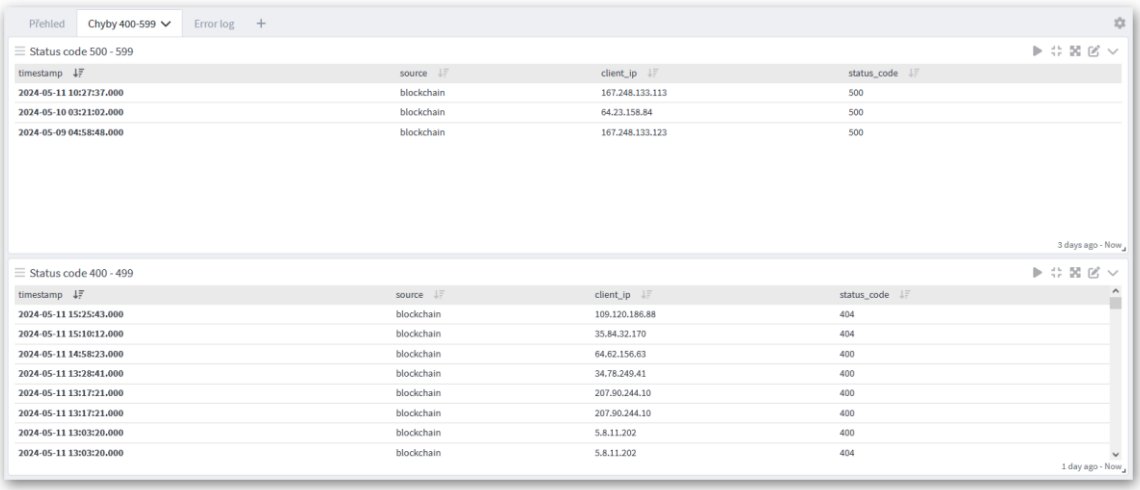
6.1.1 Přehled



Obrázek 1. Apache - Přehled

Na stránce Přehled jsou umístěna tři počítadla. První počítalo s názvem „Počet úspěšných přístupů“ zobrazuje počet zpráv odpovídajících podmínce `status_code:200` a je vybrána možnost zobrazení trendu s neutrální preferencí. Druhé počítalo s názvem „Počet chyb 400“ zobrazuje počet zpráv odpovídajících podmínce `status_code:[400 TO 499]` a je vybrána možnost zobrazení trendu s klesající preferencí. Třetí počítadlo s názvem „Počet chyb 500“ zobrazuje počet zpráv odpovídajících podmínce `status_code:[500 TO 599]` a je také vybrána možnost zobrazení trendu s klesající preferencí. Graf s názvem „Počet chybných přístupů“ je nastaven, aby zobrazoval na řádku hodnotu *timestamp* a ve sloupci počet hodnot *status_code*, jako typ zobrazení je zvolen sloupcový graf. Data pro tento graf odpovídají podmínce `status_code:[400 TO 599]`. Druhý graf s názvem „Přenesených bajtů“ je nastaven, aby zobrazoval na řádku hodnotu *timestamp* a dále součet všech hodnot *send_bytes*, jako typ zobrazení je zvolen spojnicový graf. Data pro tento graf odpovídají podmínce `status_code:200`.

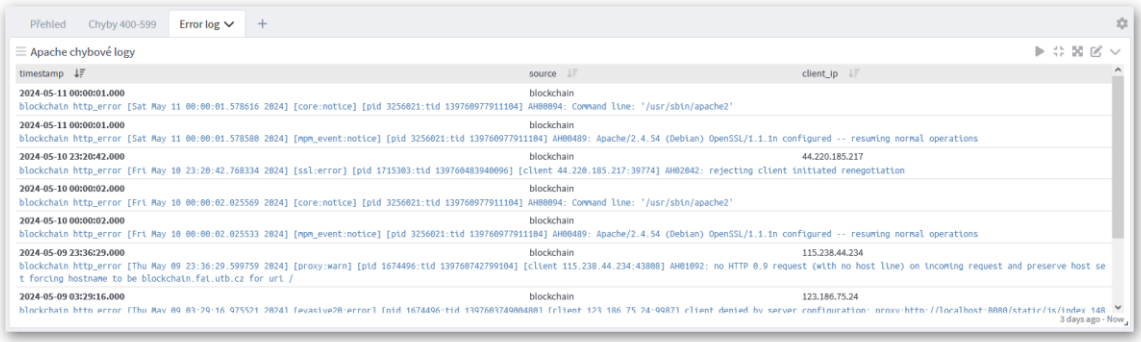
6.1.2 Chyby 400-599



Obrázek 2. Apache – Chyby 400-599

Stránka Chyby 400-599 obsahuje dvě tabulky. První tabulka s názvem „Status code 500 – 599“ zobrazuje pole *timestamp, source, client_ip a status_code* všech logů, které odpovídají nastavené podmínce `status_code:[500 TO 599]`. Tato tabulka tak zobrazuje čas a datum, kdy událost nastala, na kterém zařízení událost nastala, IP adresu klienta, který ji způsobil a HTTP status kód, který byl klientovi serverem vrácen. Druhá tabulka s názvem „Status code 400 – 499“ je vytvořena stejným způsobem a zobrazuje data odpovídající podmínce `status_code:[400 TO 499]`.

6.1.3 Error log



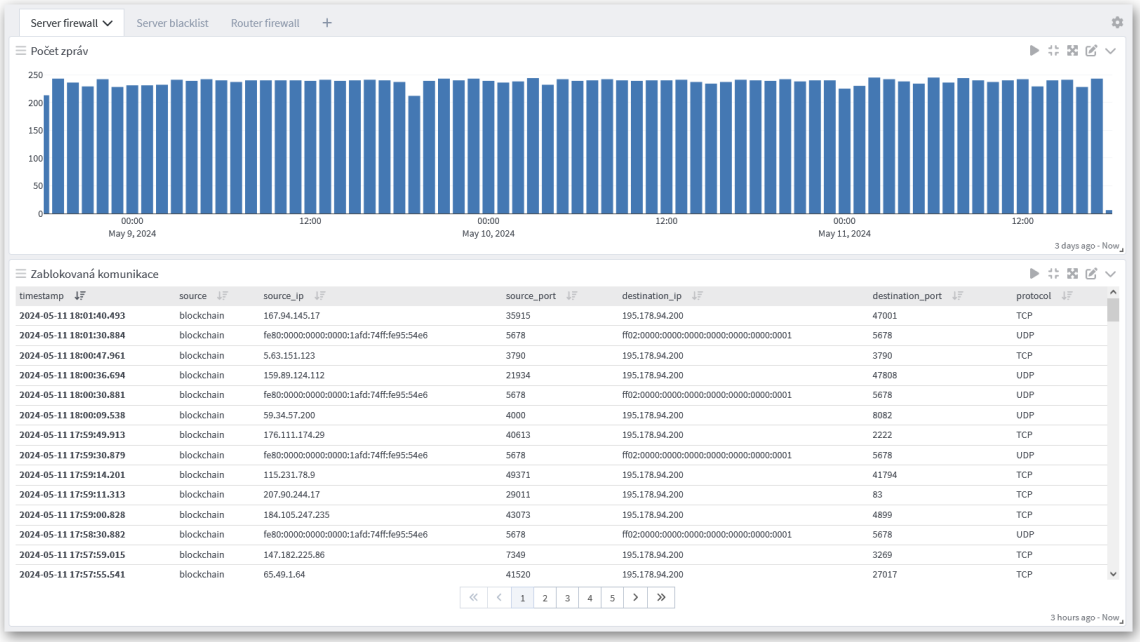
Obrázek 3. Apache – Error log

Stránka Error log obsahuje tabulku s názvem „Apache chybové logy“, která zobrazuje pole *timestamp, source, client_ip a message preview* všech logů, které odpovídají nastavené podmínce `message:"http_error"`. Tato tabulka tak zobrazuje čas a datum, kdy událost nastala, na kterém zařízení událost nastala, IP adresu klienta, který ji způsobil, pokud je k dispozici a náhled obsahu zprávy z logu.

6.2 Firewall

Dashboard BP_Firewall obsahuje tři stránky. Na první straně Server firewall se zobrazuje graf s přehledem počtu přijatých zpráv o zablokované komunikaci firewallem webového serveru. Za tímto grafem následuje tabulka s podrobnostmi o zablokované komunikaci, jako je zdrojová a cílová IP adresa a číslo portu nebo použitý protokol. Na druhé straně Server blacklist, se nachází tabulka s přehledem IP adres přidaných na blacklist, která obsahuje IP adresu přidanou na blacklist a důvod jejího přidání. Na poslední straně Router firewall, se nachází podobný přehled, jako na první straně, ale zdrojem dat pro tento přehled je v tomto případě firewall routeru. Všechny prvky na tomto dashboardu čerpají logy ze streamu FirewallsLogs.

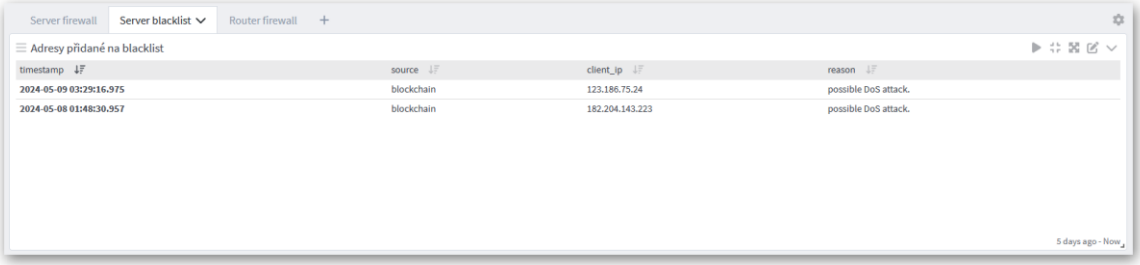
6.2.1 Server firewall



Obrázek 4. Firewall – Server firewall

Stránka Server firewall obsahuje graf s názvem „Počet zpráv“, který je nastaven tak, aby zobrazoval na řádku hodnotu *timestamp* a dále počet přijatých zpráv, jako typ zobrazení je zvolen sloupcový graf. Data pro tento graf odpovídají podmínce `source:blockchain`. Dalším prvkem je tabulka s názvem „Zablokovaná komunikace“, která zobrazuje pole *timestamp, source, source_ip, source_port, destination_ip, destination_port a protocol* všech logů, které odpovídají nastavené podmínce `source:blockchain`. Tato tabulka tak zobrazuje čas a datum, kdy událost nastala, na kterém zařízení událost nastala, zdrojovou IP adresu a číslo portu, cílovou IP adresu a číslo portu a také protokol, který byl použit.

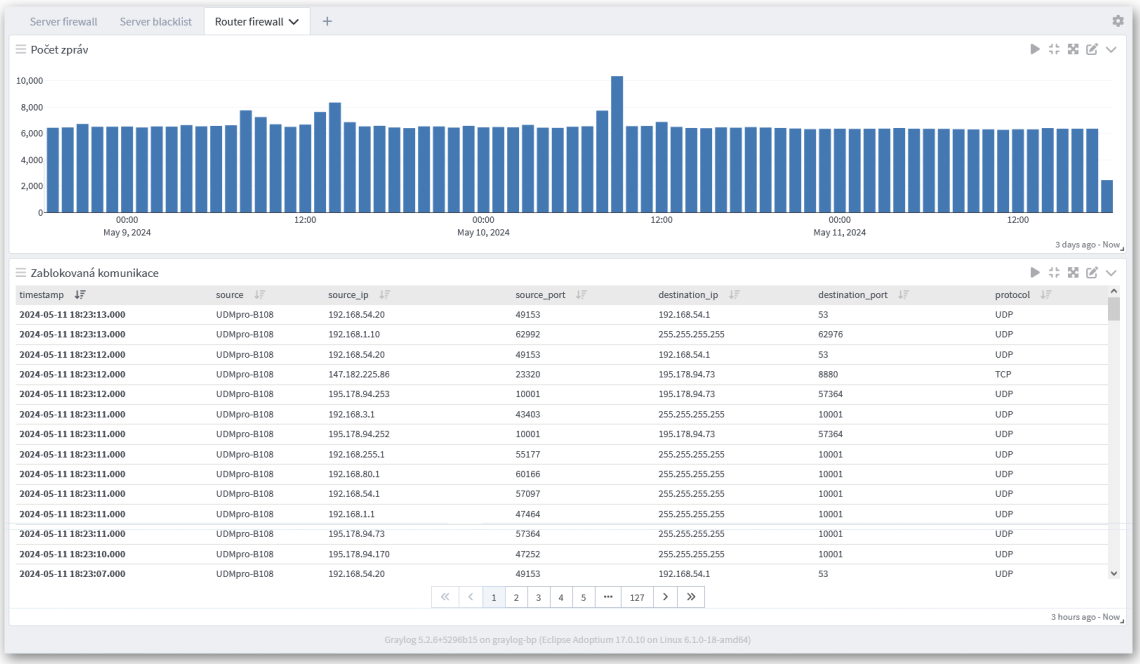
6.2.2 Server blacklist



Obrázek 5. Firewall – Server blacklist

Na stránce Server blacklist se nachází tabulka s názvem „Adresy přidané na blacklist“, která zobrazuje pole *timestamp, source, client_ip a reason* všech logů, které odpovídají nastavené podmínce `source:blockchain AND message:"Blacklisting address"`. Tato tabulka tak zobrazuje čas a datum, kdy došlo k přidání IP adresy na blacklist, které zařízení IP adresu na blacklist přidalo, samotnou IP adresu a důvod jejího přidání na blacklist.

6.2.3 Router firewall



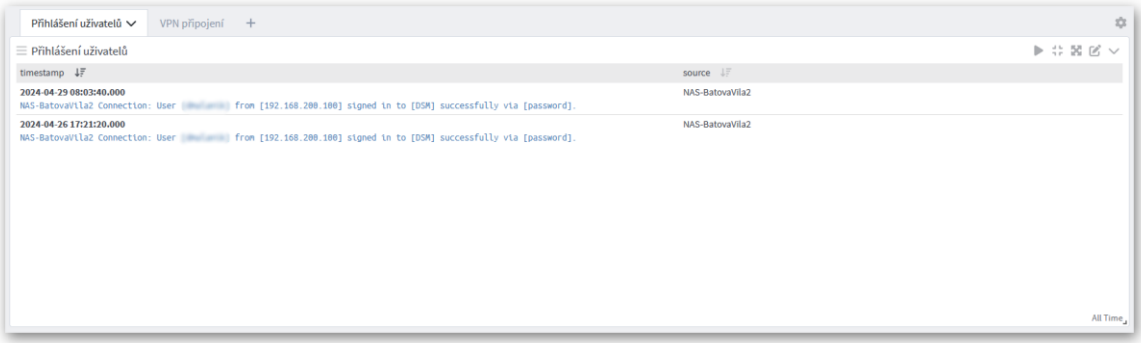
Obrázek 6. Firewall – Router firewall

Stránka Router firewall byla vytvořena obdobně jako stránka Server firewall, ale bylo použito jiné podmínky `source:udmpro\-b108`, pro výběr logů z routeru.

6.3 NAS

Dashboard BP_NAS obsahuje dvě stránky. Na první straně Přihlášení uživatelů se zobrazuje tabulka informující o přihlášení uživatele k NASu. Na druhé straně VPN připojení se nachází graf, který na časové ose zobrazuje červenou barvou počet odpojení od VPN sítě a zelenou barvou počet připojení k VPN síti. Pod tímto grafem se nachází tabulka s podrobnějšími informacemi o připojení a odpojení od sítě VPN. Všechny prvky na tomto dashboardu čerpají logy ze streamu NASLog.

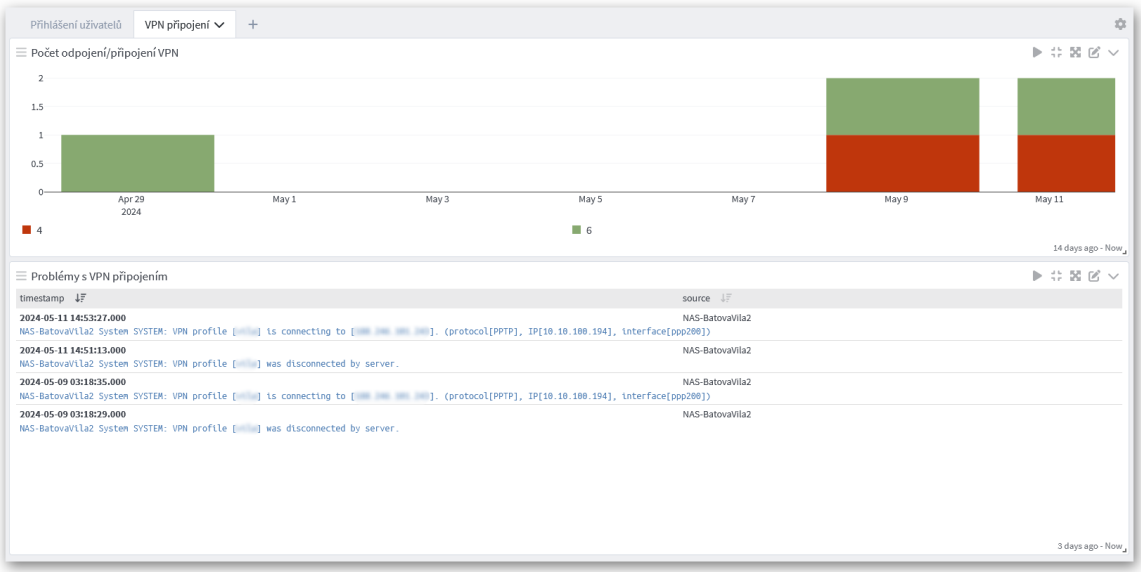
6.3.1 Přihlášení uživatelů



Obrázek 7. NAS – Přihlášení uživatelů

Na stránce Přihlášení uživatelů se nachází tabulka s názvem „Přihlášení uživatelů“, která zobrazuje pole *timestamp, source a message preview* všech logů, které odpovídají nastavené podmínce `message:"signed in to"`. Tato tabulka tak zobrazuje čas a datum, kdy došlo k přihlášení, které zařízení zprávu odeslalo a náhled zprávy s podrobnostmi přihlášení.

6.3.2 VPN připojení



Obrázek 8. NAS – VPN připojení

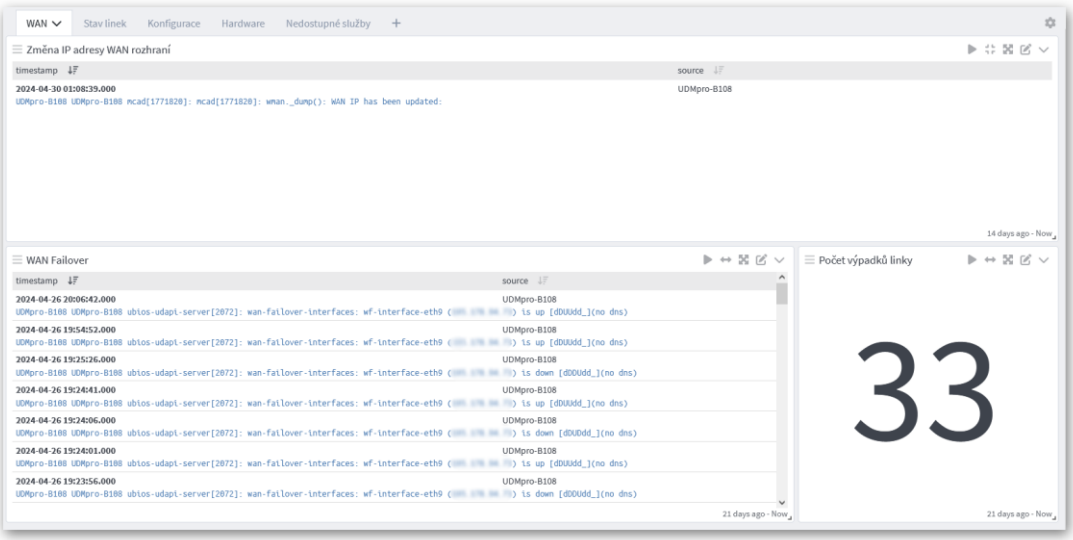
Na stránce VPN připojení se nachází graf s názvem „Počet odpojení/připojení VPN“, který je nastaven tak, aby zobrazoval na řádku hodnotu *timestamp* a ve sloupci hodnotu *level*, dále je nastaveno zobrazování počtu přijatých zpráv a jako typ zobrazení je zvolen sloupcový graf. Data pro tento graf odpovídají podmínce `message:"was disconnected"`

`OR message:"is connecting to"`. Zde je využito rozdílné závažnosti zpráv, zatímco logy informující o odpojení VPN mají úroveň závažnosti zpráv 4 (Varování), logy informující o připojení k VPN mají úroveň závažnosti 6 (Informační). To je také důvodem popisků tohoto grafu, jejichž změnu nástroj Graylog velmi komplikuje, proto jsou hodnoty odlišeny alespoň barevně. Dalším prvkem na stránce je tabulka s názvem „Problémy s VPN připojením“, která zobrazuje pole *timestamp, source a message preview* všech logů, které odpovídají nastavené podmínce `message:"VPN profile"`. Tato tabulka zobrazuje čas a datum, kdy došlo ke změně stavu VPN připojení, které zařízení zprávu odeslalo a náhled zprávy s podrobnostmi o změně stavu.

6.4 Router

Dashboard BP_Router obsahuje pět stránek. Na první straně WAN se zobrazuje tabulka, informující o změnách IP adresy WAN rozhraní. Dále tabulka informující o výpadcích WAN připojení a počítalo výpadků linky WAN. Na druhé straně Stav linek se nachází tabulka, informující o změnách stavů linky wgsrv1. Třetí strana obsahuje dvě tabulky, informující o změnách pravidel firewallu a změnách v konfiguraci routeru. Na čtvrté straně je umístěn graf zobrazující na časové ose, počet příchozích zpráv o využití více jak 75 % paměti RAM. Pod ním je umístěna tabulka, ve které je náhled těchto zpráv. Poslední strana obsahuje dvě tabulky s informacemi o nedostupnosti některých služeb. Všechny prvky na tomto dashboardu čerpají logy ze streamu RouterLogs.

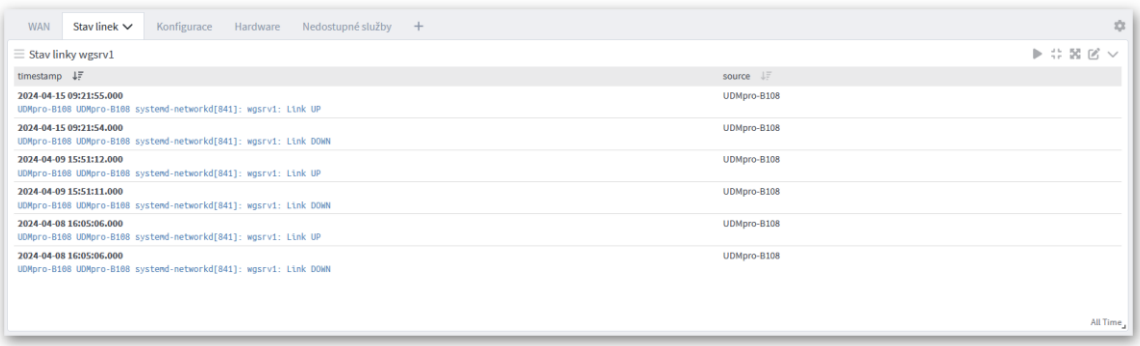
6.4.1 WAN



Obrázek 9. Router – WAN

Na stránce WAN se nachází tabulka s názvem „Změna IP adresy WAN rozhraní“, která zobrazuje pole *timestamp, source a message preview* všech logů, které odpovídají nastavené podmínce `message:"WAN IP has been updated"`. Tato tabulka tak zobrazuje čas a datum, kdy došlo ke změně IP adresy, které zařízení zprávu odeslalo a náhled zprávy s podrobnostmi. Další tabulka „WAN Failover“ má obdobnou konfiguraci, liší se v podmínce `message:"wan-failover-interfaces"`. Také zobrazuje časové razítko, kdy k události došlo, jaké zařízení ji vytvořilo a podrobnosti zprávy. Poslední součástí této stránky je počítadlo „Počet výpadků linky“, které zobrazuje počet zpráv odpovídajících podmínce `message:"wan-failover-interfaces" AND message:"is down"`.

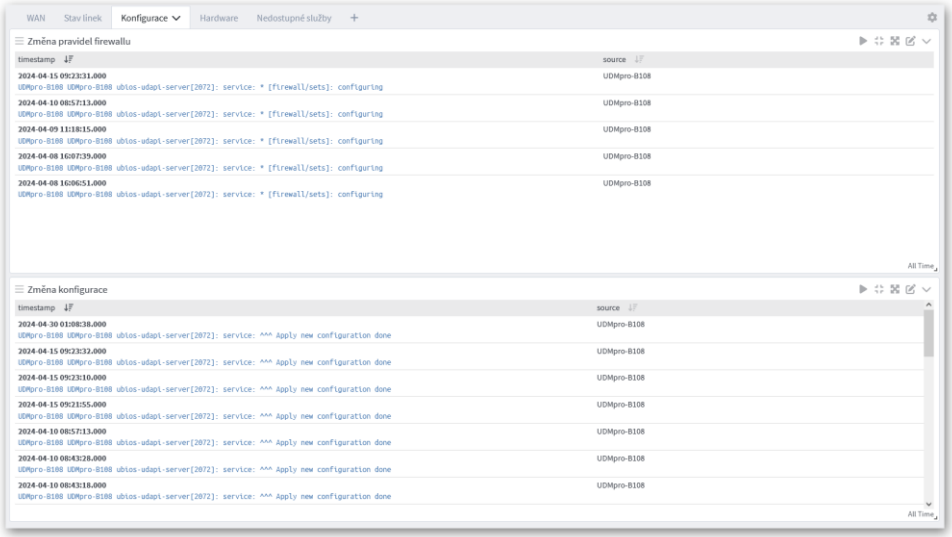
6.4.2 Stav linek



Obrázek 10. Router – Stav linek

Na stránce Stav linek se nachází tabulka s názvem „Stav linky wgsrv1“, která zobrazuje pole *timestamp, source a message preview* všech logů, které odpovídají nastavené podmínce `message:"wgsrv1: Link"`. Tato tabulka tak zobrazuje čas a datum, kdy došlo ke změně stavu linky, které zařízení zprávu odeslalo a náhled zprávy s podrobnostmi.

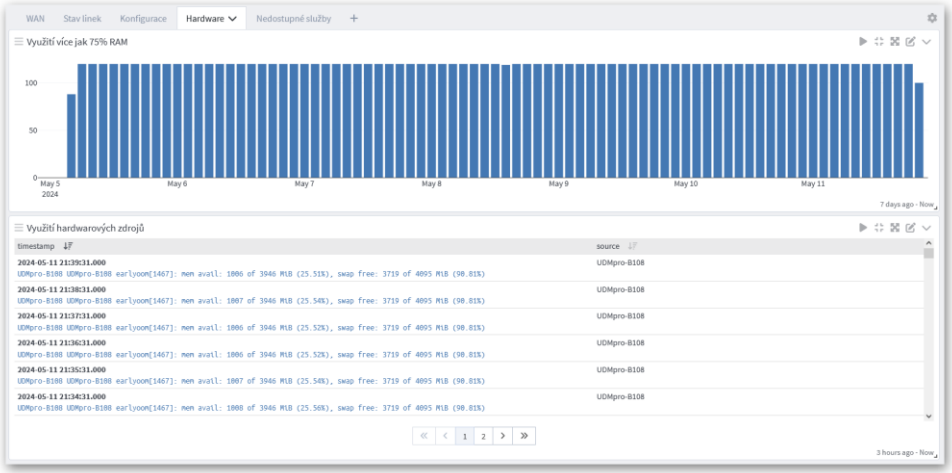
6.4.3 Konfigurace



Obrázek 11. Router – Konfigurace

Na stránce Konfigurace se nachází tabulka s názvem „Změna pravidel firewallu“, která zobrazuje pole *timestamp, source a message preview* všech logů, které odpovídají nastavené podmínce `message:"[firewall/sets]: configuring"`. Tato tabulka zobrazuje datum a čas, kdy došlo k úpravě pravidel firewallu, které zařízení zprávu odeslalo a podrobnější náhled zprávy. Druhá tabulka „Změna konfigurace“ je vytvořena obdobným způsobem s rozdílnou podmínkou `message:"Apply new configuration done"`. Zde se zobrazují, podobně jako v předchozí tabulce, informace o změně konfigurace routeru.

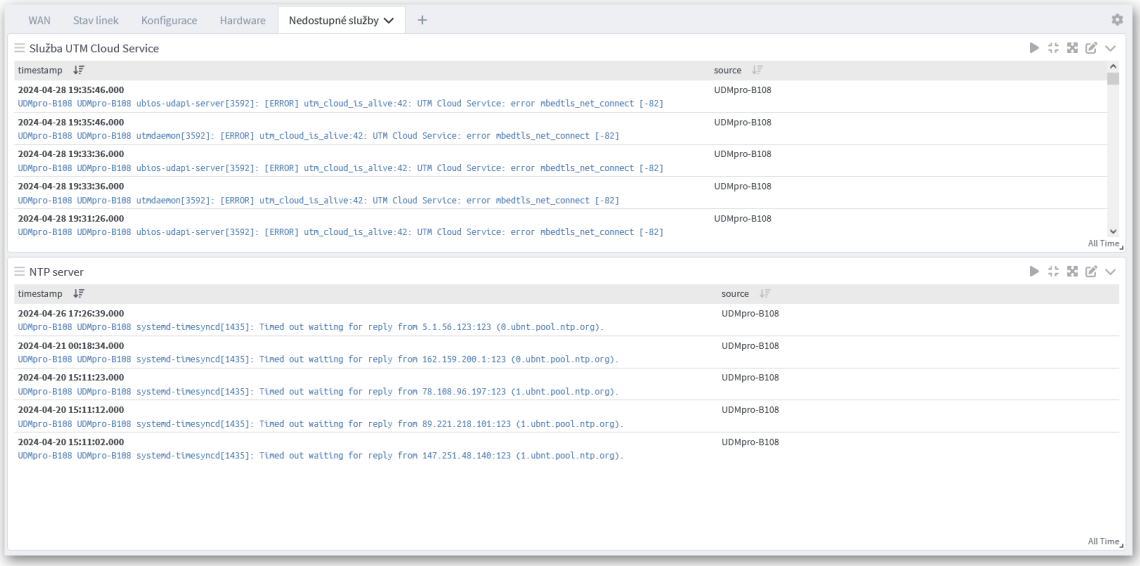
6.4.4 Hardware



Obrázek 12. Router – Hardware

Stránka Hardware obsahuje graf, s názvem „Využití více jak 75% RAM“, který je nastaven tak, aby zobrazoval na řádku hodnotu *timestamp*, dále je nastaveno zobrazování počtu přijatých zpráv a jako typ zobrazení je zvolen sloupcový graf. Data pro tento graf odpovídají podmínce `message:"mem avail"`. Následuje tabulka s názvem „Využití hardwarových zdrojů“, která zobrazuje pole *timestamp, source a message preview* všech logů, které odpovídají nastavené podmínce `message:"mem avail"`. Tato tabulka zobrazuje datum a čas, kdy došlo k této události, které zařízení zprávu odeslalo a podrobnější náhled zprávy.

6.4.5 Nedostupné služby



Obrázek 13. Router – Nedostupné služby

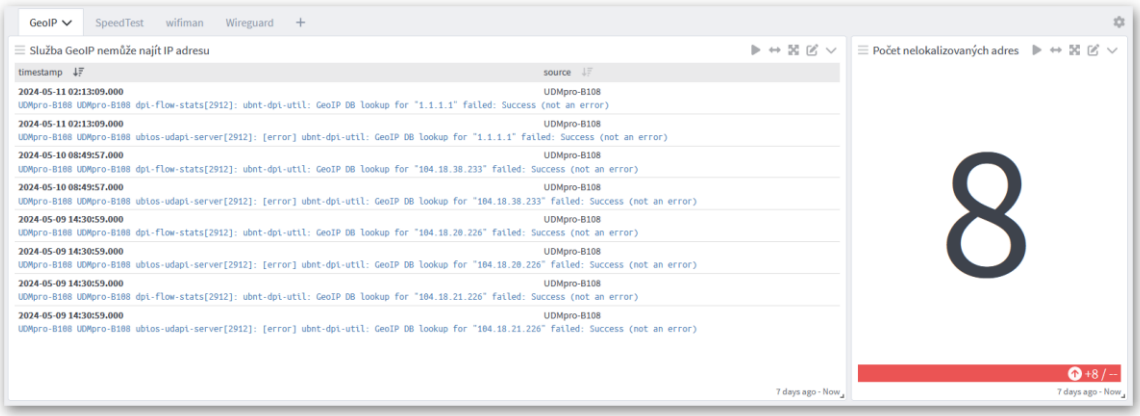
Stránka Nedostupné služby obsahuje tabulku s názvem „Služba UTM Cloud Service“, která zobrazuje pole *timestamp, source a message preview* všech logů, které odpovídají nastavené podmínce `message:"utm_cloud_is_alive:42"`. Tato tabulka zobrazuje datum a čas, kdy nebyla služba dostupná, jaké zařízení zprávu odeslalo a podrobnější náhled zprávy. Druhá tabulka „NTP server“ je vytvořena obdobným způsobem s jinou podmínkou `message:"Timed out waiting for reply from"`. Zde se jako v předchozí tabulce zobrazují informace, ale o nedostupnosti NTP serveru.

6.5 Router služby

Dashboard BP_Router služby obsahuje čtyři stránky. Na první stranu GeoIP, je vložena tabulka informující o neúspěšných pokusech lokalizovat IP adresu. Dále je vloženo počíta-

dlo těchto pokusů. Na druhé straně SpeedTest, se nachází graf, který na časové ose zobrazuje rychlost připojení k síti Internet a také odezvu ping. Třetí strana s názvem wifiman obsahuje tabulku, ve které jsou zobrazeny logy související s touto službou poskytovanou routerem, zejména logy informující o vypršení platnosti certifikátů. Na poslední straně Wireguard je umístěna tabulka s informacemi o připojení a odpojení zařízení pomocí této služby. Kromě prvků na stránce RouterSpeed čerpají všechny prvky na tomto dashboardu logy ze streamu RouterLogs.

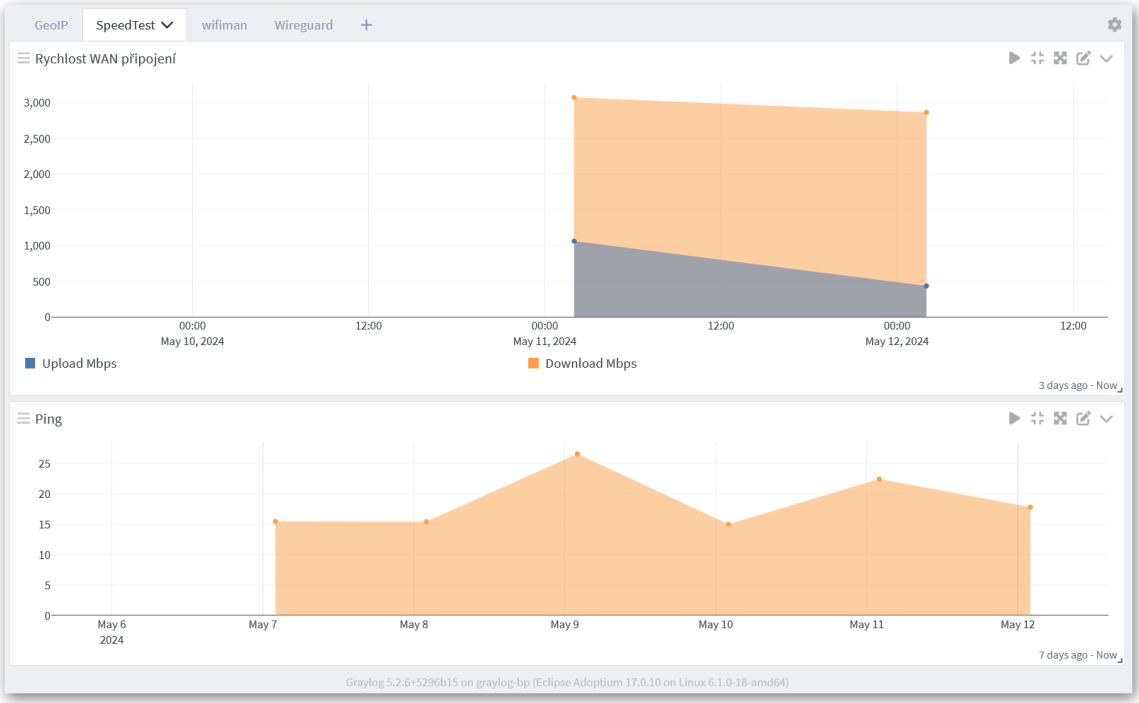
6.5.1 GeoIP



Obrázek 14. Router služby – GeoIP

Na stránce GeoIP se nachází tabulka s názvem „Služba GeoIP nemůže najít IP adresu“, která zobrazuje pole *timestamp, source a message preview* všech logů, které odpovídají nastavené podmínce `message:"GeoIP DB lookup for"`. Tato tabulka tak zobrazuje čas a datum, kdy došlo k události, které zařízení zprávu odeslalo a náhled zprávy s IP adresou, kterou nebylo možné lokalizovat. Další součástí této stránky je počítadlo „Počet nelokalizovaných adres“, které zobrazuje počet adres, které nebyly úspěšně lokalizovány. K tomu je využito téže podmínky jako u výše zmíněné tabulky. Dále je nastaveno zobrazování počtu těchto zpráv, jako číselná hodnota a je využito i zobrazení trendu s klesající preferencí.

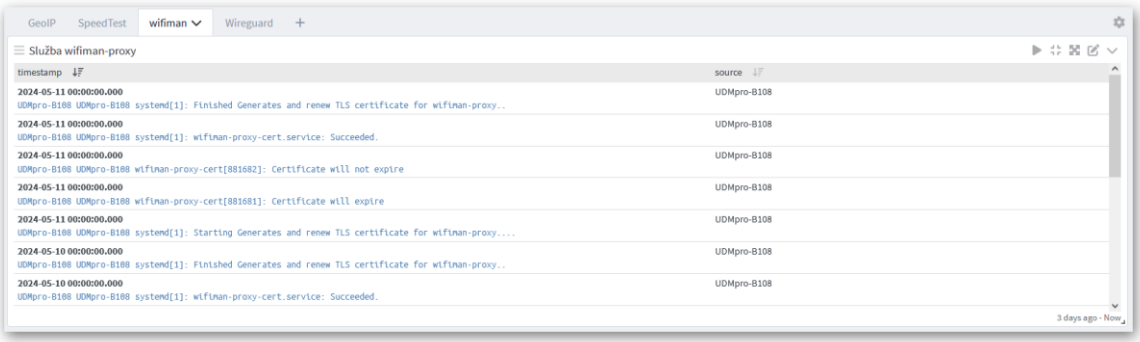
6.5.2 SpeedTest



Obrázek 15. Router služby – SpeedTest

Tato stránka s názvem SpeedTest obsahuje graf „Rychlost WAN připojení“, který je nastaven tak, aby zobrazoval na řádku hodnotu *timestamp* a dále průměr z pole *download* a průměr z pole *upload*, jako typ zobrazení je zvolen plošný graf. Druhý graf s názvem „Ping“ je nastaven, aby zobrazoval na řádku hodnotu *timestamp* a dále průměr z pole *ping*. Jako typ zobrazení je také zvolen plošný graf. Data poskytovaná těmto grafům jsou čerpána ze streamu RouterSpeed.

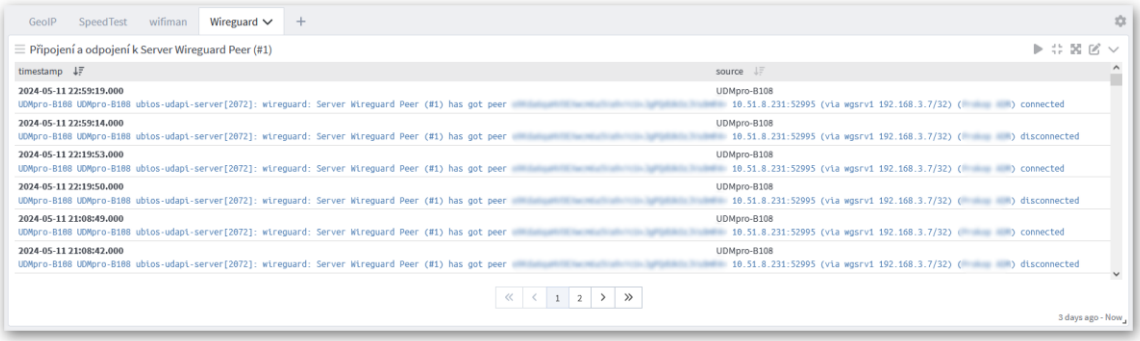
6.5.3 Wifiman



Obrázek 16. Router služby – wifiman

Na stránce wifiman je vložena tabulka s názvem „Služba wifiman-proxy“, která zobrazuje pole *timestamp, source a message preview* všech logů, které odpovídají nastavené podmínce `message:"wifiman"`. Tato tabulka tak zobrazuje čas a datum, kdy došlo k události, které zařízení zprávu odeslalo a náhled zprávy s podrobnostmi.

6.5.4 Wireguard



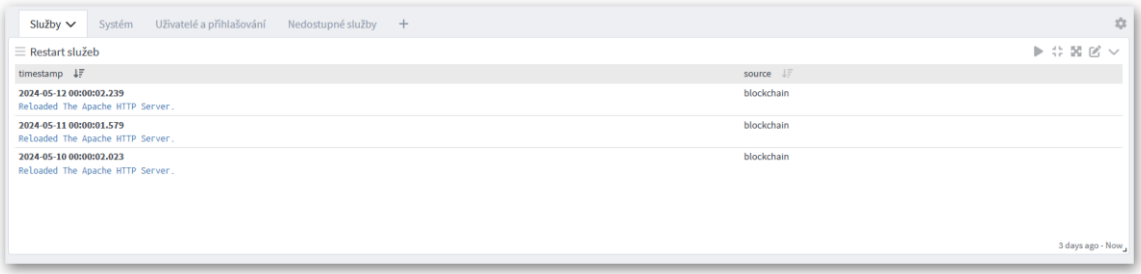
Obrázek 17. Router služby – Wireguard

Stránka Wireguard obsahuje podobnou tabulku, jako se nachází na předchozí stránce wifiman. Tato tabulka se odlišuje nastavenou podmínkou `message:"Server Wireguard Peer"`. Zde jsou v náhledu zpráv uvedeny podrobnosti o připojení a odpojení zařízení od služby Wireguard.

6.6 Server

Dashboard BP_Server má čtyři stránky. Na první straně s názvem Služby je vložena tabulka, která poskytuje informace o stavu služeb běžících na serveru. Druhá strana Systém obsahuje dvě tabulky. První „CMD“ poskytuje informace o spuštěných skriptech, druhá tabulka „Systém“ poskytuje informace o vypnutí systému. Třetí strana „Uživatelé a přihlašování“ obsahuje graf, který zobrazuje na časové ose počet neúspěšných pokusů o přihlášení k systému. Tyto údaje se také zobrazují v tabulce pod grafem, pro lepší přehlednost informací. Poslední tabulka na této stránce se nazývá „Změny uživatelských profilů“. Zde se zobrazují informace při změně údajů uživatelského profilu, např. při změně hesla. Na čtvrté straně se nachází graf s počítadlem, které informuje o počtu neúspěšných spojení s DNS serverem, podrobnosti těchto neúspěšných spojení jsou následně zobrazeny v tabulce pod grafem. Všechny prvky v tomto dashboardu čerpají data ze streamu Server-Logs.

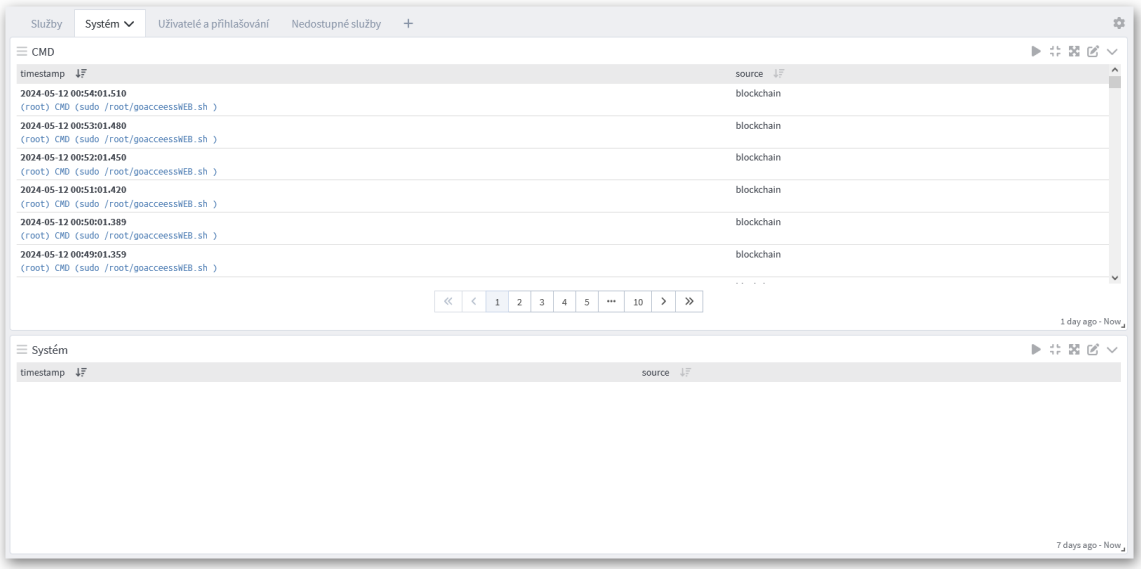
6.6.1 Služby



Obrázek 18. Server – Služby

Na stránce Služby je umístěna tabulka „Restart služeb“, která zobrazuje pole *timestamp, source a message preview* všech logů, které odpovídají nastavené podmínce `message:"Reloaded"`. Tato tabulka zobrazuje datum a čas, kdy došlo k této události, které zařízení zprávu odeslalo a podrobnější informace o tom, jaká služba se restartovala.

6.6.2 Systém

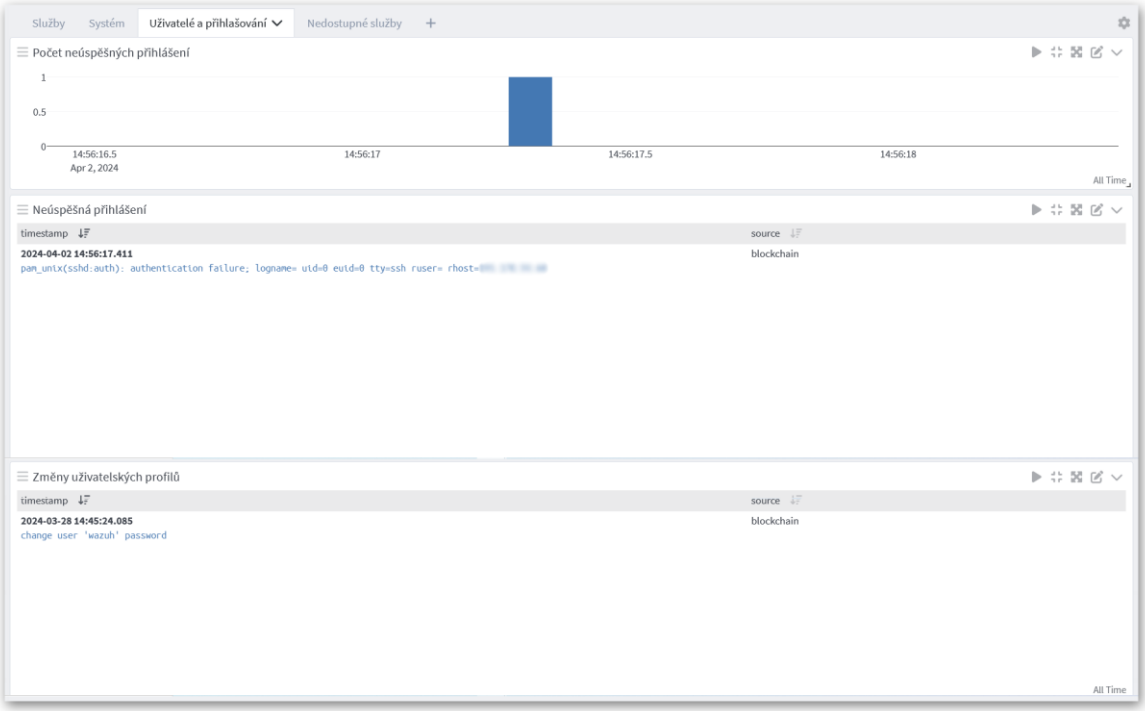


Obrázek 19. Server – Systém

Na stránce Systém je vložena tabulka CMD, která zobrazuje pole *timestamp, source a message preview* všech logů, které odpovídají nastavené podmínce `message:"CMD"`. Tato tabulka zobrazuje datum a čas, kdy došlo k této události, které zařízení zprávu odeslalo a podrobnější informace o tom, jaký příkaz nebo skript byl spuštěn. Druhá tabulka na této stránce Systém je vytvořena podobně, jako předchozí tabulka, jen je nastavena jiná

podmínka `message:"Reached target Shutdown"`. Výstupem této tabulky jsou informace, jaké zařízení bylo kdy vypnuto.

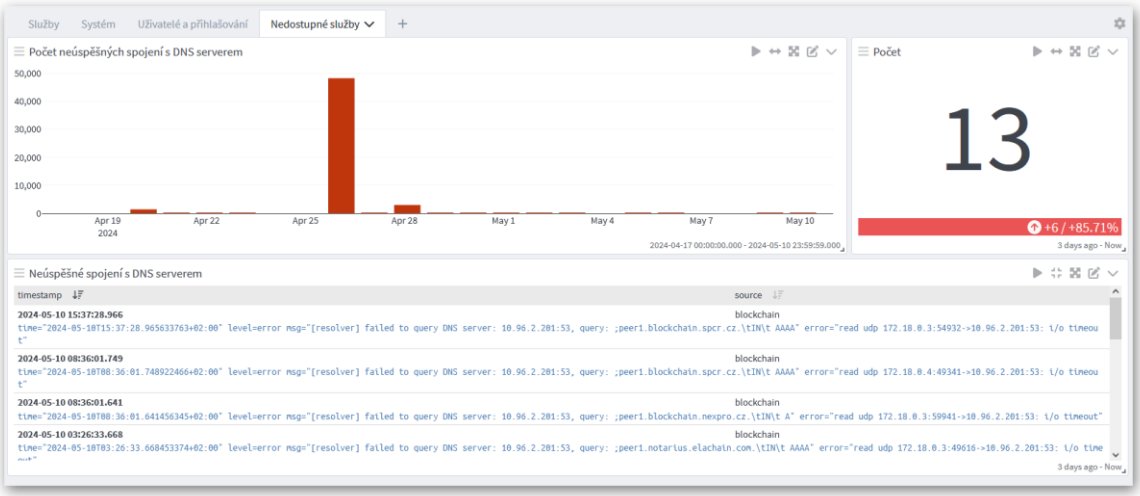
6.6.3 Uživatelé a přihlašování



Obrázek 20. Server – Uživatelé a přihlašování

Stránka „Uživatelé a přihlašování“ obsahuje graf, s názvem „Počet neúspěšných přihlášení“, který je nastaven tak, aby zobrazoval na řádku hodnotu *timestamp*, dále je nastaveno zobrazení počtu přijatých zpráv a jako typ zobrazení je zvolen sloupcový graf. Data pro tento graf odpovídají podmínce `message:"authentication failure"`. Následuje tabulka s názvem „Neúspěšná přihlášení“, která zobrazuje pole *timestamp, source a message preview* všech logů, které odpovídají nastavené podmínce `message:"authentication failure"`. Tato tabulka zobrazuje datum a čas, kdy došlo k této události, které zařízení zprávu odeslalo a podrobnější informace ze zprávy. Druhá tabulka „Změny uživatelských profilů“ byla vytvořena obdobným způsobem, ale s odlišnou podmínkou `message:" change user"` a zobrazuje informace podobným stylem.

6.6.4 Nedostupné služby



Obrázek 21. Server – Nedostupné služby

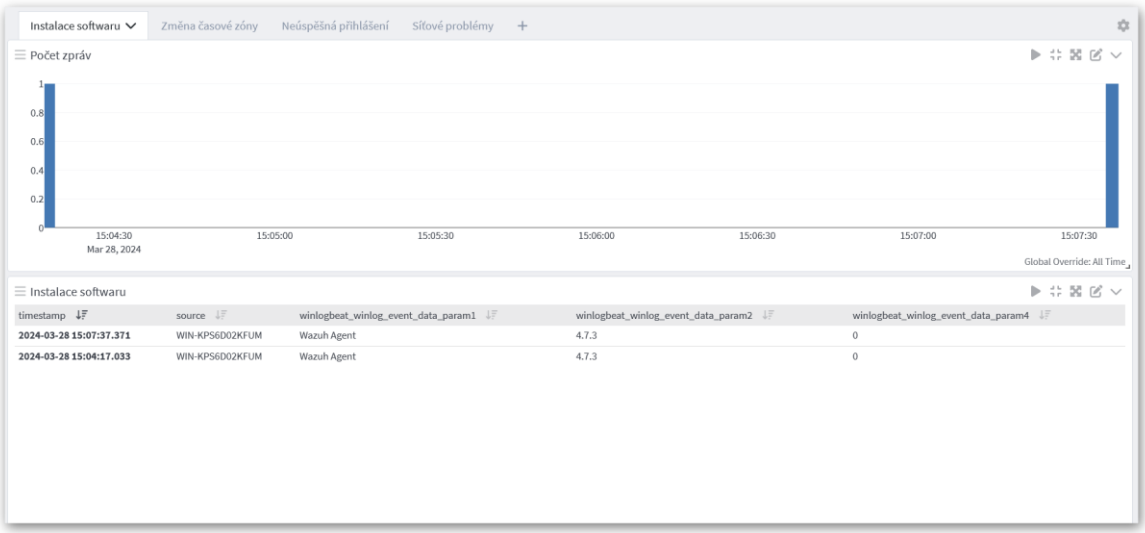
První částí stránky „Nedostupné služby“ je graf, zobrazující počet neúspěšných spojení s DNS serverem. Tento graf je nakonfigurován, aby zobrazoval na řádku hodnotu *timestamp* a dále počet zpráv odpovídající podmínce `message:"failed to query DNS server"`, jako typ zobrazení je zvolen sloupcový graf. Další součástí této stránky je počítadlo „Počet“, které zobrazuje počet zpráv odpovídajících podmínce `message:"failed to query DNS server`. U počítadla je také vybrána možnost zobrazení trendu s klesající preferencí. Ve spodní části stránky je umístněná tabulka s názvem „Neúspěšné spojení s DNS serverem“, která je nastavena tak, aby zobrazovala pole *timestamp, source a message preview* všech logů, které odpovídají nastavené podmínce `message:"failed to query DNS server"`. V této tabulce se nacházejí podrobnější informace o problému v komunikaci s DNS serverem.

6.7 Windows dashboard

Dashboard BP_Windows dashboard má čtyři stránky. Na první straně s názvem Instalace softwaru je vložen graf, znázorňující počet příchozích zpráv o instalaci softwaru a tabulka, která poskytuje podrobnější informace o nainstalovaném softwaru na zařízení. Druhá strana Změna časové zóny obsahuje tabulku zpráv s informacemi o změně časové zóny a počítadlo těchto zpráv. Třetí strana Neúspěšná přihlášení obsahuje časovou osu a počítadlo zobrazující počet zpráv informujících o neúspěšném přihlášení. Podrobnější informace jsou následně zobrazeny v tabulce Neúspěšná přihlášení. Na poslední čtvrté straně je časová osa zobrazující počet zpráv, informující o chybě při překladu DNS názvů. Dále je zde umístěna

tabulka s informacemi o problémech, vzniklých při registraci IP adresy zařízení. Všechny prvky v tomto dashboardu čerpají data ze streamu PCLogs.

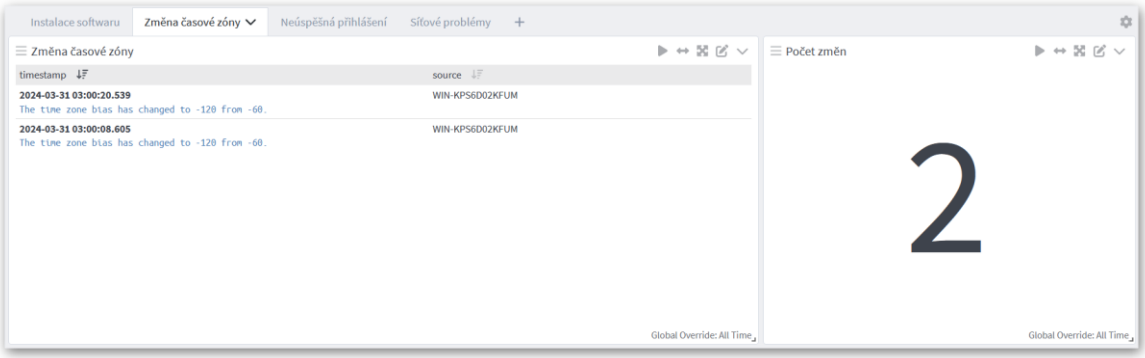
6.7.1 Instalace softwaru



Obrázek 22. Windows dashboard – Instalace softwaru

Stránka „Instalace softwaru“ obsahuje graf s názvem „Počet zpráv“, který je nastaven tak, aby zobrazoval na řádku hodnotu *timestamp*, dále je nastaveno zobrazení počtu přijatých zpráv a jako typ zobrazení je zvolen sloupcový graf. Data pro tento graf odpovídají podmínce `message:"Windows Installer installed the product"`. Následuje tabulka s názvem „Instalace softwaru“, která zobrazuje pole *timestamp, source, winlogbeat_winlog_event_data_param1* (název softwaru), *winlogbeat_winlog_event_data_param2* (verze sotwaru) a *winlogbeat_winlog_event_data_param4* (exit kód instalace), které odpovídají nastavené podmínce `message:"Windows Installer installed the product"`. Tato tabulka zobrazuje datum a čas, kdy došlo k instalaci softwaru, na jaké zařízení byl software nainstalován, název softwaru, verzi instalovaného softwaru a exit kód instalace.

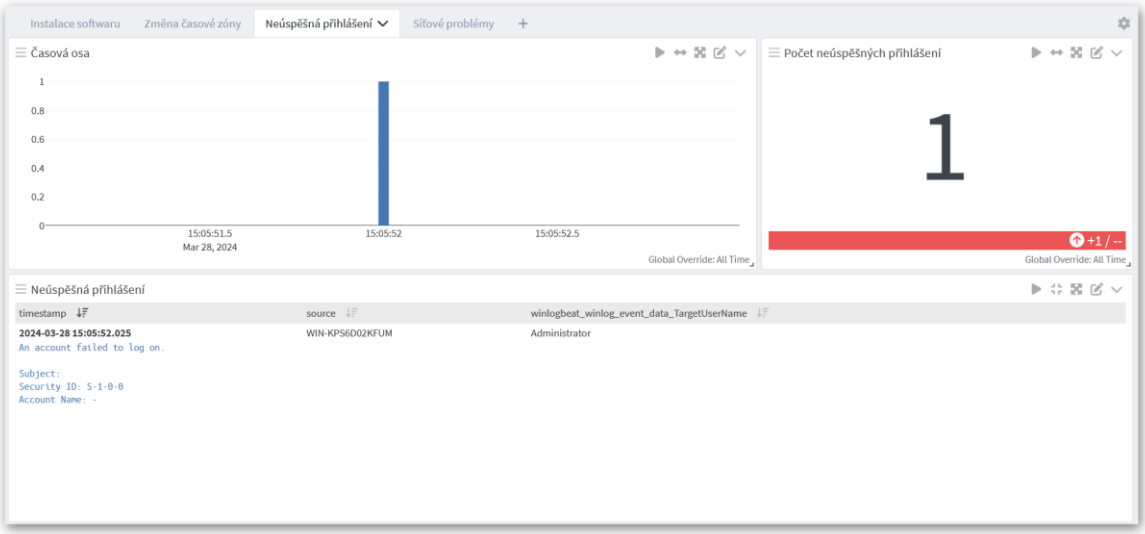
6.7.2 Změna časové zóny



Obrázek 23. Windows dashboard – Změna časové zóny

Stránka Změna časové zóny obsahuje tabulku s názvem „Změna časové zóny“, která je nastavena tak, aby zobrazovala pole *timestamp, source a message preview* všech logů, které odpovídají nastavené podmínce `message:"The time zone bias has changed"`. V této tabulce se zobrazují informace o zařízeních, na kterých proběhla změna časové zóny. Dalším prvkem na této stránce je počítadlo „Počet změn“, které zobrazuje počet zpráv odpovídajících podmínce `message:"The time zone bias has changed"`.

6.7.3 Neúspěšná přihlášení

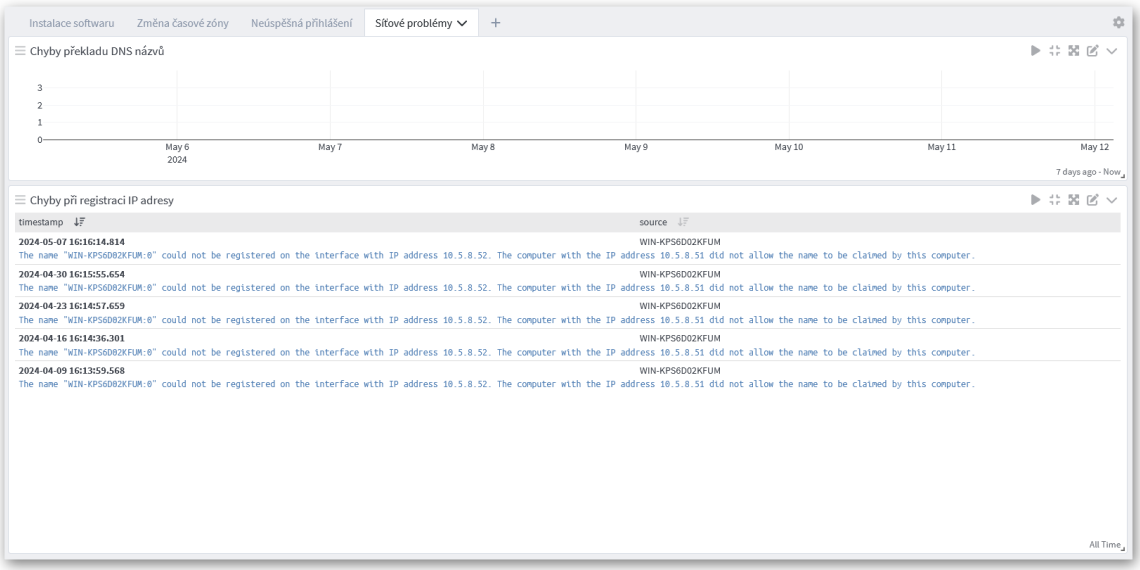


Obrázek 24. Windows dashboard – Neúspěšná přihlášení

Na stránce Neúspěšná přihlášení je umístěn graf s názvem „Časová osa“, který je nastaven tak, aby zobrazoval na řádku hodnotu *timestamp*, dále je nastaveno zobrazení počtu přijatých zpráv a jako typ zobrazení je zvolen sloupcový graf. Data pro tento graf odpovídají

podmínce `message:"An account failed to log on."`. Dalším prvkem na této stránce je počítadlo „Počet neúspěšných přihlášení“, které zobrazuje počet zpráv odpovídajících podmínce `message:"An account failed to log on."` a je u něj vybrána možnost zobrazení trendu s klesající preferencí. Posledním prvkem je tabulka s názvem „Neúspěšná přihlášení“, která je nastavena tak, aby zobrazovala pole *timestamp, source, winlogbeat_winlog_event_data_TargetUserName a message preview* všech logů, které odpovídají nastavené podmínce `message:"An account failed to log on."`. V této tabulce se zobrazuje datum a čas, kdy byl zaznamenán pokus o neúspěšné přihlášení, na jakém zařízení tento pokus proběhl a který uživatel se k zařízení přihlašoval.

6.7.4 Síťové problémy



Obrázek 25. Windows dashboard – Síťové problémy

Stránka Síťové problémy obsahuje graf s názvem „Chyby překladu DNS názvů“, který je nastaven tak, aby zobrazoval na řádku hodnotu *timestamp*, dále je nastaveno zobrazení počtu přijatých zpráv a jako typ zobrazení je zvolen sloupcový graf. Data pro tento graf odpovídají podmínce `message:"timed out after none of the configured DNS servers responded"`. Dále stránka obsahuje tabulku, s názvem „Chyby při registraci IP adresy“, která je nastavena tak, aby zobrazovala pole *timestamp, source a message preview* všech logů, které odpovídají nastavené podmínce `message:"could not be registered on the interface with IP address"`. V této tabulce se zobrazují informace o datumu a času, kdy selhala registrace IP adresy, názvu zařízení, které se o registraci IP adresy pokoušelo a podrobnější informace ze zprávy logu.

7 TVORBA SYSTÉMU UPOZORNĚNÍ

Vytvořené dashboardy slouží k vizualizaci dat a rychlému přehledu pro správce infrastruktury. Pokud je zapotřebí zajistit i rychlou reakci, je vhodné vytvořit i systém zasílání upozornění, který správce, při vzniku důležité události, upozorní.

7.1 Definice událostí

V testovací infrastruktuře je vhodné upozorňovat na následující události.

7.1.1 NAS_VPNodpojeni

Tato událost upozorní správce na odpojení NASu od sítě VPN. U této události je nadefinována vysoká priorita. Je vyvolána zachycením logu se zprávou "VPN profile [vila] was disconnected by server" ve streamu NASLog, který bude každých 5 minut prohledávat všechny příchozí logy za posledních 6 minut. Aby náhodou došlo k nezachycení nějaké zprávy.

7.1.2 Router_RAM75

Tato událost upozorní správce na využití více jak 75% paměti RAM na routeru. U této události je nadefinována normální priorita. Je vyvolána zachycením logu se zprávou "mem avail" ve streamu RouterLogs, který bude každých 5 minut prohledávat všechny příchozí logy za posledních 5 minut.

7.1.3 Router_link down

Tato událost upozorní správce na stav linky wgsrv1 down. U této události je nadefinována vysoká priorita. Je vyvolána zachycením logu se zprávou "wgsrv1: Link DOWN" ve streamu RouterLogs, který bude každých 5 minut prohledávat všechny příchozí logy za posledních 6 minut.

7.1.4 Router změna WAN IP

Tato událost upozorní správce na změnu IP adresy WAN rozhraní. U této události je nadefinována normální priorita. Je vyvolána zachycením logu se zprávou "WAN IP has been updated" ve streamu RouterLogs, který bude každých 5 minut prohledávat všechny příchozí logy za posledních 6 minut.

7.1.5 Router změna firewall

Tato událost upozorní správce na změnu pravidel firewallu routeru. U této události je nadefinována normální priorita. Je vyvolána zachycením logu se zprávou "[firewall/sets]: configuring" ve streamu RouterLogs, který bude každých 5 minut prohledávat všechny příchozí logy za posledních 6 minut.

7.1.6 Router_změna konfigurace

Tato událost upozorní správce na změnu konfigurace routeru. U této události je nadefinována normální priorita. Je vyvolána zachycením logu se zprávou "Apply new configuration done" ve streamu RouterLogs, který bude každých 5 minut prohledávat všechny příchozí logy za posledních 6 minut.

7.1.7 Server_Apache Error log

Tato událost upozorní správce na vzniklou chybu, která je zaznamenána v Apache error logu. U této události je nadefinována vysoká priorita. Je vyvolána zachycením logu se zprávou "http_error" ve streamu ApacheAE, který bude každých 5 minut prohledávat všechny příchozí logy za posledních 6 minut.

7.1.8 Server_Přidání adresy na blacklist

Tato událost upozorní správce na přidání IP adresy na blacklist. U této události je nadefinována nízká priorita. Je vyvolána zachycením logu se zprávou "DoS attack" ve streamu FirewallsLogs, který bude každých 5 minut prohledávat všechny příchozí logy za posledních 6 minut.

7.1.9 Server_Přihlášení

Tato událost upozorní správce na 5 po sobě jdoucích neúspěšných pokusů o přihlášení během jedné minuty. U této události je nadefinována vysoká priorita. Je vyvolána zachycením logu se zprávou "authentication failure" ve streamu ServerLogs, který bude každou 1 minutu prohledávat všechny příchozí logy za poslední 1 minutu. Také je nastavena podmínka, že počet zpráv musí být větší nebo roven 5.

7.1.10 Server_Vypnutí

Tato událost upozorní správce na vypnutí serveru. U této události je nadefinována vysoká priorita. Je vyvolána zachycením logu se zprávou "Reached target Shutdown" ve streamu

ServerLogs, který bude každých 5 minut prohledávat všechny příchozí logy za posledních 6 minut.

7.1.11 Server_restart Apache

Tato událost upozorní správce na restart služby Apache. U této události je nadefinována vysoká priorita. Je vyvolána zachycením logu se zprávou "Reloaded The Apache HTTP Server" ve streamu ServerLogs, který bude každých 5 minut prohledávat všechny příchozí logy za posledních 6 minut.

7.1.12 WIN_Chyba registrace IP adresy

Tato událost upozorní správce na problém při registraci IP adresy. U této události je nadefinována normální priorita. Je vyvolána zachycením logu se zprávou "could not be registered on the interface with IP address" ve streamu PCLogs, který bude každých 5 minut prohledávat všechny příchozí logy za posledních 6 minut.

7.1.13 WIN_Instalace SW

Tato událost upozorní správce na instalaci nového softwaru na PC. U této události je nadefinována nízká priorita. Je vyvolána zachycením logu se zprávou " Windows Installer installed the product" ve streamu PCLogs, který bude každých 5 minut prohledávat všechny příchozí logy za posledních 6 minut.

7.1.14 WIN_Přihlášení

Tato událost upozorní správce na 5 po sobě jdoucích neúspěšných pokusů o přihlášení během jedné minuty. U této události je nadefinována vysoká priorita. Je vyvolána zachycením logu se zprávou "An account failed to log on" ve streamu PCLogs, který bude každou 1 minutu prohledávat všechny příchozí logy za poslední 1 minutu. Také je nastavena podmínka, že počet zpráv musí být větší nebo roven 5.

7.1.15 WIN_Restart PC

Tato událost upozorní správce na potřebu restartu PC. U této události je nadefinována nízká priorita. Je vyvolána zachycením logu se zprávou "Machine restart is required" ve streamu PCLogs, který bude každých 5 minut prohledávat všechny příchozí logy za posledních 6 minut.

7.2 Nastavení notifikací

K nadefinovaným událostem je možné nastavit zasílání oznámení pomocí komunikačních platforem. Poté bude při výskytu nadefinované události zasláno, přes zvolený komunikační kanál, oznámení, o zachycení události. Nejprve je nutné vytvořit notifikace.

7.2.1 E-mail notifikace

Při konfiguraci notifikací zasílaných pomocí e-mailu je nutné nastavit: název notifikace a zvolit typ notifikace: Email Notification. Dále je vhodné nastavit příjemce notifikací pomocí e-mailové adresy a je možné upravit předmět zprávy a její obsah. Při upravení předmětu e-mailu na `Graylog: ${event_definition_description}` se bude do předmětu vkládat popis události a zasílané notifikace budou srozumitelnější.

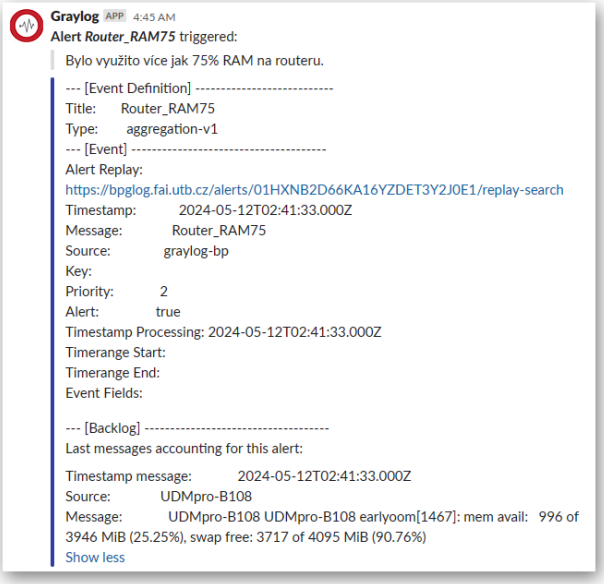
7.2.2 Slack notifikace

Při konfiguraci notifikací zasílaných platformy Slack je nutné nastavit: název notifikace a zvolit typ notifikace: Slack Notification. Dále je nutné nastavit incoming webhook URL, pomocí kterého budou notifikace odesílány a název kanálu nebo jméno uživatele, kterému budou doručeny. Dále je možné upravit, jakou barvou budou zprávy označeny, upravit obsah zprávy nebo jméno odesílatele nebo vybrat způsob upozornění uživatelů v kanálu.

7.2.3 Úprava obsahu zpráv

Pro zobrazení podrobnějších informací o události ve zprávě, je možné u definice události povolit možnost Message Backlog. Poté lze jednoduše upravit obsah zprávy např. přidáním těchto řádků do cyklu `foreach backlog message`, lze ve zprávě zobrazit zdroje logů, čas a datum jejich vzniku a obsah jejich zpráv:

```
Timestamp message:              ${message.timestamp}
Source:               ${message.source}
Message:              ${message.message}
```



Obrázek 26. Zpráva na platformě Slack

Zpráva poté může vypadat podobně jako tato, o využití více než 75 % paměti RAM na routeru. Kde jsou všechny důležité informace, jako je zejména popis události, zařízení, na kterém událost vznikla a čas, kdy tato událost nastala. Pomocí odkazu je možné přejít na stránku, kde bude provedeno vyhledání těch logů, na jejichž základě byla tato událost spuštěna. Podobný styl zpráv přichází také na e-mail.

Obrázek 27. Zpráva odeslaná e-mailem

7.2.4 Použité notifikace

V Graylogu jsou nakonfigurované čtyři způsoby zasílání notifikací.

První notifikace „E-mail def“ je využita k zasílání oznámení při výskytu těchto událostí:

- Neúspěšné přihlášení k počítači s OS Windows nebo serveru
- Problém s registrací IP adresy počítače
- Odpojení NASu od VPN
- Vypnutí serveru
- Změna IP adresy WAN rozhraní routeru

Druhá notifikace „Slack hálózat“ slouží k odesílání oznámení, souvisejících s problémy se sítí, pomocí platformy Slack. Odesílají se následující oznámení:

- Přidání IP adresy na blacklist
- Výpadek linky routeru
- Změny v konfiguraci routeru nebo jeho firewallu

Třetí notifikace „Slack informatikus“ slouží k odesílání oznámení, souvisejících s problémy s uživatelskými zařízeními. Jsou odesílána tato oznámení:

- Instalace softwaru
- Potřeba restartu PC

Čtvrtá notifikace „Slack infrastruktúra“ je využita k zasílání oznámení souvisejících s problémy v IT infrastruktuře. Odesílají se následující oznámení:

- Zaznamenán Apache error log
- Restart služby Apache
- Přidána IP adresa na blacklist
- Využití více jak 75 % RAM na routeru

ZÁVĚR

V rámci této bakalářské práce jsem se seznámil se správou logů. A to jak v teoretické části, při získávání informací o logovacích formátech, možnostech sběru logů nebo definováním kritických informací, které se z logů sledují, tak i v praktické části, při práci s platformou Graylog, při konfiguraci streamů, pipeline, dashboardů, definování událostí nebo nastavování zasílání oznámení.

Při vytváření své práce jsem zjistil, že platforma Graylog je poměrně komplexní nástroj na správu logů a při správném využití přináší řadu výhod. Vytvořené dashboardy umožňují rychlý přehled o stavu infrastruktury a notifikace u nadefinovaných událostech zase napomáhají k rychlejší reakci na vzniklé problémy, co mě naopak překvapilo byla velmi obtížná, v některých případech až nemožná, změna popisků u některých grafů nebo záhlaví tabulek.

S výsledkem mé práce jsem spokojen a myslím, že jsem splnil všechny stanovené cíle. Troufám si tvrdit, že některé části této práce by se dali využít i v produkčním prostředí, jiné zase spíše ukazují možnosti a funkcionality této platformy. Za jediný nesplněný cíl považuji implementaci události, která by zasílala oznámení, pokud by nějakému zařízení s OS Windows ve sledované infrastruktuře docházelo místo na disku. Tento log se v testovací infrastruktuře neobjevil a z časových důvodů nebylo možné jej nechat vygenerovat. Když jsem se o to pokoušel v domácím prostředí, tak se mi, i přes veškeré úsilí, nepodařilo tento log zachytit.

SEZNAM POUŽITÉ LITERATURY

[1] *Co je to Logování*. Online. LÁCHA, Miloš. ČISTÉ PC. C2024. Dostupné z: https://www.cistepc.cz/it-slovnik/logovani/. [cit. 2024-03-25].

[2] KENT, Karen a SOUPPAYA, Murugiah. *Guide to Computer Security Log Management*. Online. 800-92. National Institute of Standards and Technology, 2006. Dostupné z: https://doi.org/10.6028/nist.sp.800-92. [cit. 2024-04-05].

[3] *What Is Log Management?* Online. SOLARWINDS. IT Glossary | SolarWinds. C2024. Dostupné z: https://www.solarwinds.com/resources/it-glossary/log-management. [cit. 2024-04-05].

[4] THE GRAYLOG TEAM. *Log Formats – a (Mostly) Complete Guide*. Online. THE GRAYLOG BLOG. 2020. Dostupné z: https://graylog.org/post/log-formats-a-complete-guide/. [cit. 2024-03-28].

[5] *What is Syslog?* Online. SOLARWINDS. IT Glossary | SolarWinds. C2024. Dostupné z: https://www.solarwinds.com/resources/it-glossary/syslog. [cit. 2024-04-06].

[6] *What is syslog?* Online. SUMO LOGIC. Sumo Logic. C2024. Dostupné z: https://www.sumologic.com/syslog/. [cit. 2024-04-06].

[7] GERHARDS, R. *RFC 5424 - The Syslog Protocol*. Online. IETF. 2009, Last updated 2018-12-20. Dostupné z: https://datatracker.ietf.org/doc/rfc5424/. [cit. 2024-04-06].

[8] *What Is a Windows Event Log?* Online. SOLARWINDS. IT Glossary | SolarWinds. C2024. Dostupné z: https://www.solarwinds.com/resources/it-glossary/windows-event-log. [cit. 2024-04-10].

[9] KARL-BRIDGE-MICROSOFT ET AL. *About Event Logging - Win32 apps*. Online. Microsoft Learn. 2021. Dostupné z: https://learn.microsoft.com/en-us/windows/win32/eventlog/about-event-logging. [cit. 2024-04-10].

[10] KARL-BRIDGE-MICROSOFT A KOL. *Eventlog Key*. Online. Microsoft Learn. 2021. Dostupné z: https://learn.microsoft.com/en-us/windows/win32/eventlog/eventlog-key. [cit. 2024-04-10].

[11] KARL-BRIDGE-MICROSOFT; V-KENTS a MSATRANJR. *Event Types*. Online. Microsoft Learn. 2021. Dostupné z: https://learn.microsoft.com/en-us/windows/win32/eventlog/event-types. [cit. 2024-04-10].

[12] ANAND, Ankit. *JSON Logs | Best Practices, benefits, and examples*. Online. SigNoz. 2022. Dostupné z: https://signoz.io/blog/json-logs/. [cit. 2024-03-28].

[13] SHAFRANOVICH, Y. *Common Format and MIME Type for Comma-Separated Values (CSV) Files*. Online. IETF. 2005. Dostupné z: https://www.ietf.org/rfc/rfc4180.txt. [cit. 2024-03-28].

[14] *CSV (Comma-separated Values)*. Online. NXLog Docs. C2024. Dostupné z: https://docs.nxlog.co/glossary/csv.html. [cit. 2024-03-28].

[15] SHARIF, Arfan. *6 Common Log File Formats*. Online. CrowdStrike. 2022. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/observability/log-file-formats/. [cit. 2024-04-15].

[16] *GELF*. Online. Graylog. C2024. Dostupné z: https://graylog.org/features/gelf/. [cit. 2024-04-15].

[17] *Log Files*. Online. THE APACHE SOFTWARE FOUNDATION. Apache HTTP Server Version 2.4. C2024. Dostupné z: https://httpd.apache.org/docs/2.4/logs.html. [cit. 2024-04-17].

[18] FITZPATRICK, Scott. *Understanding the Apache Access Log: View, Locate and Analyze*. Online. Sumo Logic. 2020. Dostupné

z: https://www.sumologic.com/blog/apache-access-log/. [cit. 2024-04-17].

[19] MONTEIRO, Brena. *Apache Error Log Files*. Online. Sumo Logic. 2017. Dostupné z: https://www.sumologic.com/blog/apache-error-logs/. [cit. 2024-04-17].

[20] SHARIF, Arfan. *WHAT IS LOG MANAGEMENT? THE IMPORTANCE OF LOGGING AND BEST PRACTICES*. Online. CrowdStrike. 2022. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/observability/log-management/. [cit. 2024-04-21].

[21] *Graylog Inputs*. Online. GRAYLOG. Graylog Docs. C2024. Dostupné z: https://go2docs.graylog.org/5-2/getting_in_log_data/inputs.htm?tocpath=Getting%20in%20Logs%7CGraylog%20Inputs%7C____0. [cit. 2024-04-29].

[22] *Secure Inputs with TLS*. Online. GRAYLOG. Graylog Docs. C2024. Dostupné z: https://go2docs.graylog.org/5-2/getting_in_log_data/secure_inputs_with_tls.htm?tocpath=Getting%20in%20Logs%7C____2. [cit. 2024-04-29].

[23] *Installing Graylog*. Online. GRAYLOG. Graylog Docs. C2024. Dostupné z: https://go2docs.graylog.org/5-2/downloading_and_installing_graylog/installing_graylog.html?tocpath=Downloading%20and%20Installing%20Graylog%7CInstalling%20Graylog%7C____0. [cit. 2024-04-29].

[24] *Streams*. Online. GRAYLOG. Graylog Docs. C2024. Dostupné z: https://go2docs.graylog.org/5-2/making_sense_of_your_log_data/streams.html?tocpath=Sorting%20and%20Enriching%20Logs%7CStreams%7C____0. [cit. 2024-04-29].

[25] *Alerts and Events*. Online. Graylog Docs. C2024. Dostupné z: https://go2docs.graylog.org/5-2/interacting_with_your_log_data/alerts_and_events.html?tocpath=Visualizations%252C%20Alerts%252C%20and%20Reports%7CAlerts%20and%20Notifications%7CAlerts%20and%20Events%7C____0. [cit. 2024-02-29].

[26] *Notifications*. Online. Graylog Docs. C2024. Dostupné z: https://go2docs.graylog.org/5-2/interacting_with_your_log_data/notifications.html?tocpath=Visualizations%252C%20Alerts%252C%20and%20Reports%7CAlerts%20and%20Notifications%7CNotifications%7C____0. [cit. 2024-02-29].

[27] *Dashboards*. Online. GRAYLOG. Graylog Docs. C2024. Dostupné z: https://go2docs.graylog.org/5-2/interacting_with_your_log_data/dashboards.html?tocpath=Aggregating%20Data%7C____2. [cit. 2024-04-29].

[28] *Processing Pipelines*. Online. GRAYLOG. Graylog Docs. C2024. Dostupné z: https://go2docs.graylog.org/5-2/making_sense_of_your_log_data/pipelines.html?tocpath=Sorting%20and%20Enriching%20Logs%7CProcessing%20Pipelines%7C____0. [cit. 2024-05-01].

[29] MASTERDC a INGIMAGE. *Jak splnit NIS2 – krok za krokem*. Online. SystemOnLine. 2023. Dostupné z: https://www.systemonline.cz/it-security/jak-splnit-nis2-krok-za-krokem-z.htm?mobilelayout=false. [cit. 2024-05-01].

[30] *Ingest Windows Eventlog*. Online. GRAYLOG. Graylog Docs. C2024. Dostupné z: https://go2docs.graylog.org/5-2/getting_in_log_data/ingest_windows_eventlog.html?tocpath=Getting%

20in%20Logs%7CGraylog%20Sidecar%7CSet%20Up%20Sidecar%20Collectors%7C_____2. [cit. 2024-05-01].

[31] *Configure logging drivers*. Online. Docker Docs. C2024. Dostupné z: https://docs.docker.com/config/containers/logging/configure/. [cit. 2024-05-01].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

API	Application Programming Interface
CEF	Common Event Format
CLF	Common Log Format
CSV	Comma Separated Values
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Systém
DoS	Denial of Service
ELF	Extended Log Format
FQDN	Fully qualified domain name
FTP	File Transfer Protocol
GELF	Graylog Extended Log Format
GPS	Global Positioning Systém
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Informační technologie
JSON	JavaScript Object Notation
NAS	Network Attached Storage
NCSA	National Center for Supercomputing Applications
NIS	Network Information Security
NTP	Network Time Protocol
OS	Operating systém
RAM	Random Access Memory

RFC	Request for Comments
TCP	Transmmission Control Protocol
TLS	Transport Layer Security
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Universal Time Coordinated
UTF	Unicode Transformation Format
UTM	Unified Threat Management
UUCP	Unix-to-Unix Copy
VPN	Virtual private network
WAN	Wide Area Network

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: STRUKTURA CD

fulltext.pdf	Elektronická verze bakalářské práce
Dashboards	Adresář se snímky dashboardů
Config	Adresář s exportovanými kódy z Graylogu