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

Ke Kamenci 151, Pardubice

Analýza síťového provozu za využití Cacti

Syrůček, Matěj

4.B

Informační Technologie 18-20-M/01

2024/2025

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

V Pardubicích 30. 3. 2023

(vlastnoruční podpis)

Zadání maturitního projektu z informatických předmětů

Jméno a příjmení: *Matěj Syrůček*

Pro školní rok: *2024/2025*

Třída: *4.*

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

Téma práce: Analýza síťového provozu za využití Cacti

Vedoucí práce: doc. Mgr. Josef Horálek, Ph.D.

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

Cílem práce je popsat principy fungování síťového provozu. Dále autor podrobně popíše možnosti nástroje Cacti. V praktické části pak autor navrhne implementaci nástroje Cacti pro dohled síťového provozu v prostředí vzdělávací instituce.

Stručný časový harmonogram (s daty a konkretizovanými úkoly):

Principy síťového dohledu

Možnosti nástroje Cacti

Návrh testovací topologie a její konfigurace

Implementace Cacti

Návrh a implementace Cacti v prostředí vzdělávací instituce

Testování a ověření výsledků

Poděkování

Rád bych poděkoval vedoucímu maturitní práci panu doc. Mgr. Josef Horálek, Ph.D. za vedení, trpělivost, návrhy a celkovou pomoc. Také svému otci Karlu Syrůčkovi za pomoc a motivaci při práci.

Resumé

Tento text se zabývá monitorováním sítě a systémem Cacti. Nabízí ucelený pohled na fungování tohoto nástroje, jeho možnosti a využití v praxi. Autor se věnuje způsobu sběru a vizualizace dat, konfiguraci systému a jeho přínosu pro správu sítí. Cílem textu je poskytnout přehled o monitorování síťového provozu s využitím Cacti a jeho efektivním nasazením.

Klíčová slova

Monitorování sítí, monitorovací systém, SNMP, NetFlow, Syslog, Cacti, MariaDB, RRDTool, Plugin

Resumé

This text focuses on network monitoring and the Cacti system. It provides a comprehensive overview of the functionality of this tool, its capabilities, and practical applications. The author examines data collection and visualization methods, system configuration, and its benefits for network management. The aim of the text is to offer an insight into network traffic monitoring using Cacti and its effective deployment.

Keywords

Network monitoring, monitoring systems, SNMP, Netflow, Syslog, Cacti, MariaDB, RRDTool, Plug

Obsah

Úvod

Moderní infrastruktura vyžaduje neustálé monitorování. V dnešní době je pro správce sítě nemožné sledovat celou síť bez speciálních monitorovacích programů, které zajišťují její nepřetržitou kontrolu a monitorování.

Například může nastat situace, kdy dojde k poruše systému, což povede ke ztrátě informací a poškození zařízení nebo systému. V takovém případě musí správce systému chybu nebo útok rychle najít a opravit a to dříve, než napáchá velkou škodu. Je sice možné odhalit takovou chybu bez speciálních sledovacích programů, ale tímto způsobem se chyba nalézá velice obtížně a také to trvá mnohem déle.

Jedním z důvodů, proč je nutné síťové monitorování, je okamžitá detekce a zajištění rychlé reakce a odpovědi. V případě nalezení nějakého problému správce IT chybu co nejdříve najde a opraví. V tom mu pomáhají speciálně vyvinuté monitorovací systémy, které okamžitě reagují na jakékoliv změny v síti. V mém projektu budu popisovat systém jménem Cacti.

1 Základy monitorování sítí

Monitorování nad síťovým provozem je klíčový pro správu, optimalizaci a zabezpečení počítačových sítí. Pomáhá identifikovat problémy v síťové infrastruktuře, předcházet výpadkům a optimalizovat výkon sítě.

Monitorování se provádí u všech komponentů v síti, například u směrovačů, přepínačů, mostů a mezi různými aplikacemi. Proto, aby bylo zaručené, že síť bude fungovat bez problémů, je třeba sledovat všechny její komponenty.

V malých sítích, kde se síťová architektura sestavuje z několika komponentů, funguje osobní kontrola nad monitorováním, kdy v poměrně rychlém čase dokážeme problém identifikovat a opravit ho. Ve velkých sítích, které se vyskytují ve velkých firmách, konvenční osobní monitorování nefunguje dostatečně efektivně, protože při sebemenší chybě, by správce sítě musel trávit spoustu času jen identifikací problému.

Monitorování síťového provozu umožňuje detekovat podezřelé aktivity, například pokusy o útoky typu DDoS, skenování portů nebo neautorizovaný přístup k citlivým

datům. Pokud správce sítě včas identifikuje anomálie v síťovém provozu, může rychle reagovat a minimalizovat škody.

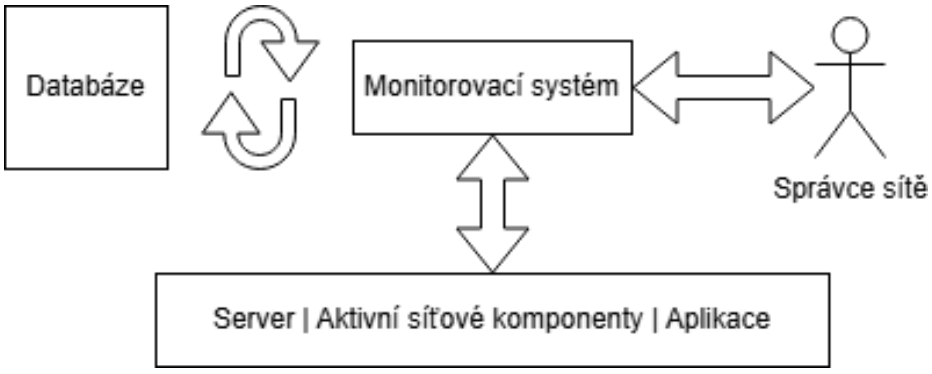
Monitorovací systém Cacti má jeden z hlavních úkolů u těchto systémů, a to je okamžitá detekce změny v síti. Jakákoliv chyba nebo porucha v síti je okamžitě detekována a program informuje správce o poruše. Tímto způsobem pomáhá zkrátit správci sítě čas při řešení problémů. Díky monitorovacímu systému má správce všechny informace o stavu infrastruktury sítě.

V moderní síťové infrastruktuře se žádný podnik neobejde bez podobných systémů. Tyhle programy nejen rychle detekují problémy v síti, ale také je mohou správce varovat předem o možném selhání určitého zařízení. To umožňuje síti pracovat nepřetržitě.

Další z hlavních důvodů monitorování je optimalizace výkonu sítě. Pokud síť trpí vysokou latencí, přetížením nebo jinými problémy, dohled umožňuje tyto potíže odhalit a efektivně řešit. Správci sítí mohou například sledovat vytížení síťových rozhraní, identifikovat nejvytíženější spoje a následně přijmout opatření, jako je rozšíření kapacity nebo lepší distribuce zátěže.

Správa kapacity je dalším důležitým aspektem dohledu nad sítí. Organizace musí plánovat dostatečnou kapacitu síťové infrastruktury, aby pokryly rostoucí potřeby uživatelů. Pomocí monitorovacích nástrojů lze sledovat dlouhodobé trendy ve využití šířky pásma a včas přijmout opatření, například upgrady síťových zařízení.

V některých případech je monitorování nad sítí vyžadován i z důvodu souladu s regulačními předpisy. Některé organizace, zejména v bankovnictví, zdravotnictví nebo státní správě, musí splňovat přísné požadavky na zabezpečení a uchovávání záznamů o síťovém provozu.



Obrázek 1 Monitorování sítě (Zdroj: autor)

2 Jak se provádí dohled síťového provozu

Dohled nad síťovým provozem se provádí různými metodami a technologiemi, které umožňují sledovat různé aspekty sítě.

2.1 SNMP

SNMP je standardní internetový protokol pro správu zařízení v IP sítích na základě architektur TCP / UDP. Existuje několik verzí SNMP. První verze SNMPv1 (RFC 1067, RFC 1057, RFC 1213) se objevila v roce 1988 a v současné době, i když je považována za zastaralou, je stále velmi populární. Během vývoje první verze se o bezpečnost skoro nikdo nestaral, takže v SNMPv1 nebyla žádná ochrana. Verze číslo 2 se objevila v dubnu 1993 jako SNMPv2 (RFC 1441-RFC 1452) a byla nekompatibilní s první verzí. Hlavními novinkami druhé verze protokolu byla výměna informací mezi řídicími počítači. Navíc se objevil nový příkaz, který přijímal několik proměn najednou (GetBulk). Bezpečnost však zůstávala velkým problémem. V roce 2004 se objevila třetí verze SNMPv3 (RFC 3411-3418), která přináší mnoho změn. Zabezpečení je však výrazně vylepšeno. Nyní každá zpráva obsahuje nastavení zabezpečení, která jsou kódována jako řetězec oktetu. V praxi je v implementacích SNMP často podporováno několik verzí: v1, v2c a v3.

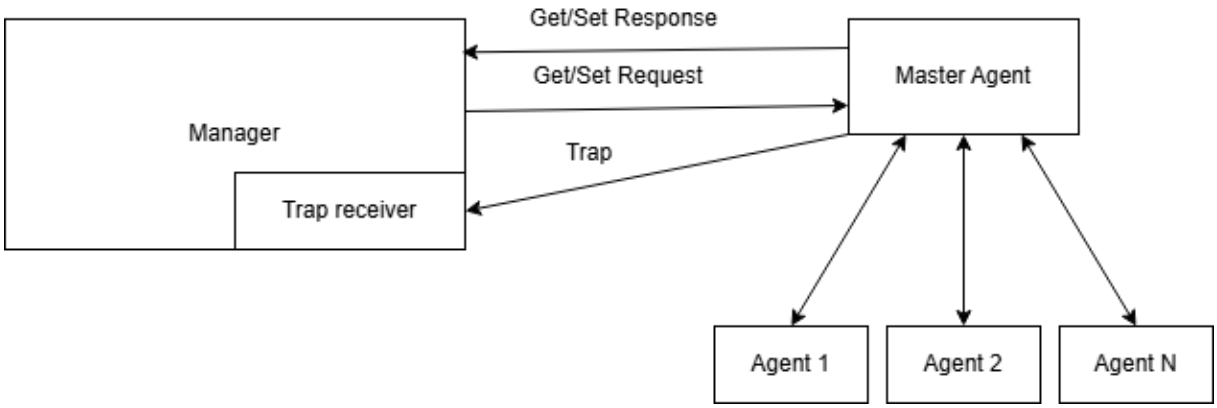
2.1.1 Architektura SNMP

Síť, která používá pro správu SNMP, obsahuje tři hlavní součásti:

- Manager SNMP – je to software nainstalovaný v počítači správce. Toto je klient, který žádá agenta, aby získal informace, které potřebuje. Funguje na portu UDP/162.
- Agent SNMP – Software běžící na síťovém uzlu, který je monitorován. Můžeme říci, že agent je určitá služba běžící na některém zařízení, které zpracovává požadavky na portu UDP/161. Agent shromažďuje informace o zařízení a předává je manažerovi.
- SNMP MIB - je manažerská informační základna. Tato součást systému poskytuje strukturovaná data vyměňovaná mezi agenty a manažery. Ve skutečnosti se jedná o druh databáze ve formě textových souborů. Agenti shromažďují informace o zařízení a zapisují shromážděná data do proměnných hodnot v databázi MIB. Tím je zpřístupněn manažerům.

Agenti a manažeři používají několik hlavních příkazů:

- Trap - jednosměrné oznámení od agenta SNMP k manažerovi o jakékoli události.
- GetReponse – odezva agenta na manažera, který vrací požadované hodnoty proměnné.
- GetRequest – požadavek agenta od manažera, který se používá k získání hodnoty jedné nebo více proměnných.
- GetNextRequest – požadavek agenta od manažera, který se používá k získání další hodnoty proměnné v hierarchii.
- SetRequest – požadavek agenta na nastavení hodnoty jedné nebo více proměnných.
- GetBulkRequest – žádost agentovi o přijetí pole dat (vyladěn GetNextRequest) (Tento příkaz byl představen v SNMPv2.).
- InformRequest - jednosměrné oznámení mezi manažery. Může být použit například pro výměnu informací o MIB. Jako odpověď generuje správce podobný balíček, jako potvrzení, že zdrojová data byla přijata.



Obrázek 2 SNMP (Zdroj: autor)

2.2 NetFlow

Netflow je protokol původně vyvinutý společností Cisco pro sledování síťového provozu. K dnešnímu dni tento protokol používá mnoho výrobců ve svých zařízeních. Existuje několik verzí protokolu Netflow a funkční rozdíly jsou mezi všemi verzemi velmi malé. Architektura Netflow se skládá ze tří částí: senzoru, kolektoru a analyzátoru. Senzor shromažďuje provozní data a přenáší všechny přijaté statistiky do kolektoru. Senzorem může být router nebo přepínač. Kolektor stejně jako senzor shromažďuje různé statistiky ze zařízení, přijímá data ze senzoru a ukládá je. Kolektor běží na serveru.

Analyzátor, jak je již patrné z názvu, analyzuje a zpracovává data, která jsou v kolektoru. Poskytuje také různé zprávy, grafy atd. Kolektor shromažďuje veškeré informace z tzv. paketových toků.

Tok je skupina paketů, které obsahují:

• adresu odesílatele,

• adresu příjemce,

• zdrojový port (pro TCP (Transmission Control Protocol) nebo UDP (User Datagram Protocol)),

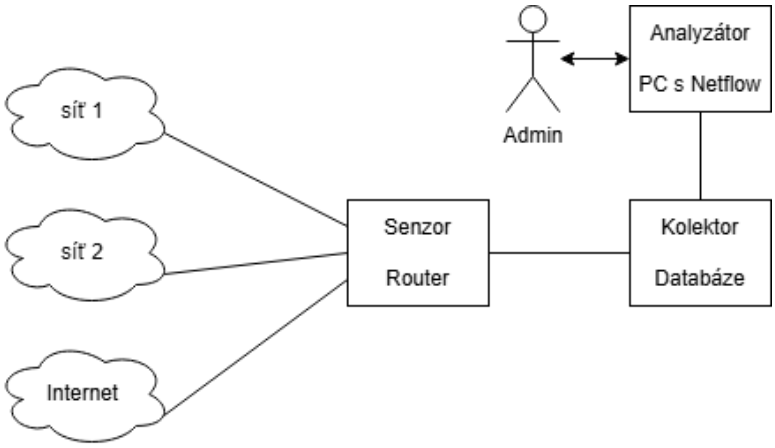
• port příjemce (pro TCP nebo UDP),

• typ a kód zprávy (pro ICMP),

• hodnotu pole ToS,

• rozhraní, na kterém se paket objevil.

Můžeme tedy říci, že proud je sada paketů, které se pohybují v jednom směru z bodu A do bodu B. Všechny shromážděné informace jsou zasílány ve formě záznamů, které mohou obsahovat takové parametry jako: číslo verze protokolu, číslo záznamu, příchozí a odchozí síťové rozhraní, čas začátku a konce proudu, počet bajtů a paketů v proudu, zdrojová a cílová adresa, zdrojový a cílový port, číslo protokolu IP. Aby se snížilo zatížení procesoru, lze použít „sampled NetFlow“. V tomto případě senzor neanalyzuje vše, ale každý n-tý paket, kde n může být nastaven správcem sítí, nebo náhodně. Při použití vzorkovaného NetFlow nebudou výsledné hodnoty přesné.



Obrázek 3 Netflow (Zdroj: autor)

2.3 Syslog

Syslog (System Logging Protocol) je standardizovaný protokol pro odesílání logovacích zpráv z různých zařízení a aplikací do centrálního logovacího serveru (Syslog serveru). Používá se k monitorování událostí, identifikaci problémů a analýze bezpečnostních incidentů. Analýza systémových logů je klíčovým prvkem monitorování sítě, protože umožňuje sbírat, uchovávat a vyhodnocovat události z různých síťových a systémových zařízení.

Cacti nemá vestavěnou podporu Syslogu, ale lze jej propojit se Syslog servery (např. Rsyslog, Graylog, Syslog-NG). Syslog může sloužit jako doplňkový zdroj dat pro síťový monitoring. Lze např. kombinovat grafické vizualizace v Cacti s logy událostí ze Syslogu.

2.3.1 Jak funguje Syslog

- Generování logů – síťová zařízení (routery, switche, firewally, servery) vytvářejí zprávy o svém stavu, chybách nebo bezpečnostních událostech.
- Odesílání zpráv – tyto zprávy jsou přeposílány přes síť do Syslog serveru pomocí UDP (často port 514), méně často TCP.
- Ukládání a analýza – Syslog server zprávy zpracovává, třídí a ukládá. Administrátoři pak mohou logy analyzovat pomocí specializovaných nástrojů.

2.3.2 Význam Syslogu v síťovém monitorování

- Odhalování bezpečnostních incidentů – například neautorizované pokusy o přihlášení nebo podezřelé síťové aktivity.
- Diagnostika chyb – zaznamenání chyb hardwaru, selhání služeb, výpadků spojení atd.
- Analýza provozu – sledování změn konfigurací, restartů zařízení, přetížení sítě.
- Historie událostí – uchování logů umožňuje zpětnou analýzu problémů a audit.

2.4 ICMP a DPI

Pro sledování dostupnosti zařízení a kvality připojení se často používají ICMP (ping) testy. Tyto testy umožňují zjistit, zda jsou síťová zařízení dostupná a s jakou latencí reagují na požadavky. Pokud například správce sítě zjistí, že latence mezi dvěma body v síti je neobvykle vysoká, může to znamenat problém s připojením nebo přetížení linky.

Pokročilejší metody, jako je DPI (Deep Packet Inspection), umožňují detailní analýzu obsahu síťových paketů. Tato metoda je často využívána pro detekci malware, identifikaci neautorizovaných aplikací v síti nebo řízení priorit síťového provozu.

3 Funkce monitorovacího systému sítě

3.1 Monitorování sítí a aplikací

Moderní nástroje jako například Cacti pro monitorování a diagnostiku výkonu sítě umožňují sledovat objekty síťové architektury. Je důležité vědět o všech síťových komponentách, aby byl rychle nalezen a opraven problém, který může nastat. Protokol, který shromažďuje data ze síťových zařízení a serverů, se nazývá SNMP (Simple Network Management Protocol). S ním můžeme shromažďovat data ohledně sítě, ale také sledovat stav různých hardwarů, napájecích zdrojů, využití paměti atd.

Je také možné nastavení monitorovacího nástroje, který pomáhá přijímat a odesílat zprávy protokolu Syslog. Tento protokol je standardem pro zprávu protokolu všech zařízení v síťové infrastruktuře. Tyto zprávy jsou posílány na server monitorovacího systému, který ukládá, analyzuje a upozorňuje správce IT o možném narušení běžného provozu systému.

3.2 Detekce problémů

Hlavní funkce monitorovacích systémů je detekce problémů nebo chyb. Neexistují žádné dokonalé systémy, které by dokázaly detekovat všechny problémy nebo chyby.
V systému nebo síti se mohou pokaždé objevit poruchy nebo chyby. Pokud se v systému objeví nějaký problém, je pro správce obtížné tuto chybu najít jen procházením logů. Monitorovací systémy jsou dobré proto, že problém v síti naleznou a upozorní na to správce sítě.

3.3 Analýza problémů v síti

Další důležitou funkcí je analýza problémů v sítí. V mnoha případech nestačí problém jen detekovat a opravit ho. Je nutné zabezpečit, aby se tento problém v budoucnu neobjevil. Proto v monitorovacímu systému existuje takzvaný SNMP agent, který shromažďuje informace z daných síťových uzlů a odesílá je na server. Tam se data zobrazují ve formě grafu, tabulky. Díky tomu můžeme analyzovat stav sítě, jak dané zařízení funguje, a také napomáhá předcházet možným problémům v budoucnosti.

3.4 Hledání hlavní příčiny poruchy nebo problému

Je jednou z časově nejnáročnějších funkcí, protože vyžaduje dokonalou konfiguraci všech zařízení a monitorovacího systému. Pokud například není čas zařízení synchronizován pomocí protokolu NTP (Network Time Protocol), bude skutečný a

zaznamenaný čas událostí odlišný. Takováto odchylka dokáže podstatně ovlivnit probíhající analýzu, což vede k nesprávnému závěru a stanovení chybné hlavní příčiny incidentu nebo problému.

3.5 Upozornění

Jakmile program zjistí problém nebo chybu v síti, okamžitě o tom informuje správce systému. Toto upozornění napomáhá správci dostatečně rychle a efektivně reagovat na jakékoli problémy v síti a jejich odstraňování.

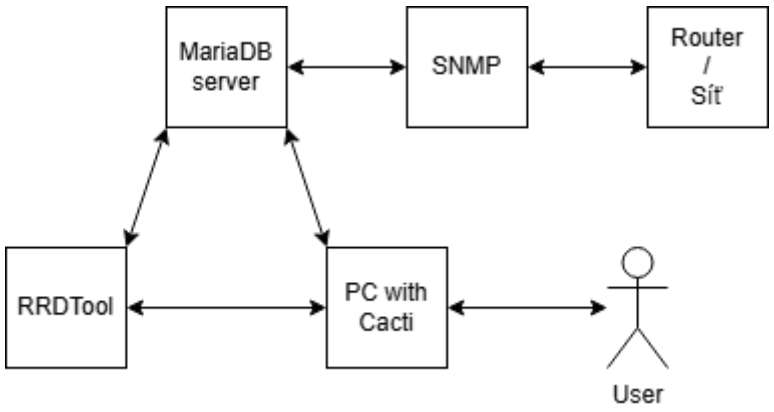
4 Topologie a základní princip Cacti

Cacti je navrženo jako flexibilní a škálovatelné řešení, které může být nasazeno v různých síťových topologiích, od jednoduchých LAN sítí až po komplexní podnikové sítě s tisíci zařízeními. Základní principy topologie Cacti zahrnují centrální monitoringový server, který sbírá data z různých síťových zařízení prostřednictvím pollerů. Tyto pollery jsou zodpovědné za pravidelné dotazování síťových zařízení a shromažďování relevantních dat.

Cacti umožňuje nasazení v různých typech topologií, včetně centralizovaných a distribuovaných systémů. V centralizované topologii je jeden hlavní Cacti server, který sbírá a analyzuje data ze všech zařízení v síti. Tato architektura je vhodná pro menší sítě nebo sítě s nízkou komplexitou.

Pro rozsáhlé nebo geograficky rozptýlené sítě je vhodnější distribuovaná topologie. V této topologii existuje více pollerů, které jsou rozmístěny po celé síti a komunikují s centrálním serverem. Tento přístup umožňuje efektivnější sběr dat a snížení zátěže na centrální server, což je klíčové pro udržení vysokého výkonu a spolehlivosti v rozsáhlých sítích.

Jednou z hlavních výhod topologie Cacti je její flexibilita a schopnost přizpůsobit se specifickým potřebám různých typů sítí. Díky modulárnímu designu a podpoře pluginů mohou uživatelé snadno rozšířit funkcionalitu Cacti a přizpůsobit jej svým konkrétním požadavkům



Obrázek 4 Topologie Cacti (zdroj: Autor)

4.1 Architektura systému

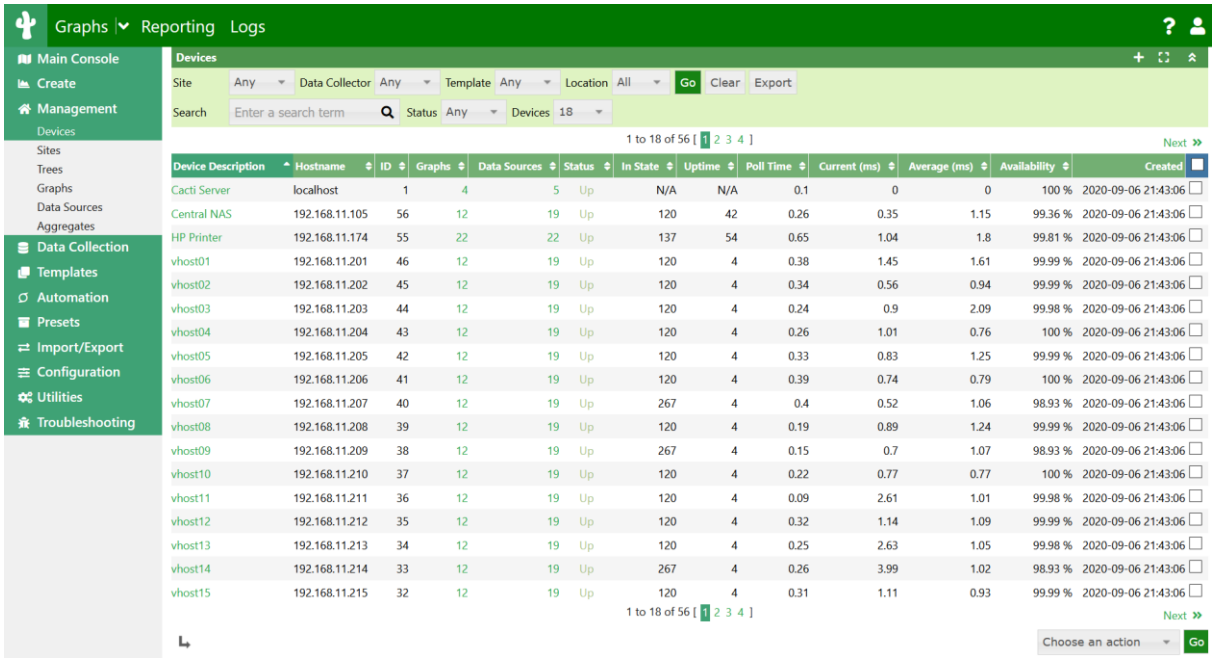
Cacti je postaveno na LAMP (Linux, Apache, MySQL, PHP) nebo LEAP (Linux, Nginx, MariaDB, PHP) stacku, což zahrnuje čtyři klíčové komponenty. Linux slouží jako operační systém, Apache nebo Nginx jako webový server, MySQL nebo MariaDB jako databázový systém a PHP jako programovací jazyk pro webovou aplikaci.

4.1.1 Hlavní komponenty

- Webový server: Apache nebo Nginx hostují webové rozhraní Cacti, které umožňuje uživatelům přístup k systému prostřednictvím webového prohlížeče. Tento server přijímá požadavky uživatelů, zpracovává je a poskytuje jim odpovědi ve formě webových stránek.
- Databázový server: MySQL nebo MariaDB ukládají strukturovaná data, jako jsou informace o zařízení, nastavení grafů a konfigurace uživatelů. Tento databázový systém je klíčový pro správu a organizaci všech uložených informací v systému Cacti.
- RRDTool: Tento nástroj je zodpovědný za ukládání časových řad dat, které jsou shromažďovány z různých síťových zařízení. RRDTool komprimuje data a uchovává je v optimálním formátu, který umožňuje rychlé zpracování a vizualizaci.
- Data Collectory: Tyto komponenty jsou zodpovědné za sběr dat z monitorovaných zařízení. Pollery pravidelně dotazují zařízení, shromažďují data a ukládají je do RRDTool. Data Collectory mohou být rozšířeny o pluginy, které umožňují sběr dat z různých typů zařízení a protokolů.

4.2 Uživatelské rozhraní

Cacti poskytuje intuitivní webové rozhraní, které umožňuje uživatelům snadno konfigurovat zařízení, vytvářet grafy a sledovat výkonnostní metriky. Uživatelské rozhraní je navrženo tak, aby bylo přehledné a uživatelsky přívětivé, což usnadňuje správu a monitorování sítí i méně zkušeným administrátorům.



Obrázek 5 Rozhraní Cacti (zdroj: cacti.net)

4.3 Rozšiřitelnost a pluginy

Jedním z klíčových prvků architektury Cacti je podpora pluginů, které umožňují rozšíření funkcionality systému. Pluginy mohou přidávat nové funkce, zlepšovat existující moduly nebo integrovat další nástroje pro monitorování a správu sítí. Tato modularita zajišťuje, že Cacti může růst a přizpůsobovat se potřebám uživatelů.

5 Nástroje v programu Cacti pro dohled sítě

Cacti je open-source monitorovací nástroj, který je široce využíván pro sledování výkonu síťových zařízení a serverů. Jeho hlavní výhodou je schopnost vytvářet přehledné grafy na základě dat získaných pomocí SNMP.

Jednou z klíčových funkcí Cacti je SNMP monitoring, který umožňuje sběr dat o výkonnosti síťových zařízení. Správce sítě může například sledovat vytížení CPU na routeru, využití paměti na serveru nebo rychlost přenosu dat na jednotlivých portech síťového přepínače.

Velkou předností Cacti je schopnost vytvářet vizuální přehledy pomocí nástroje RRDTool. Historická data se ukládají do RRD databáze a jsou následně zobrazována ve formě grafů. Tyto grafy umožňují snadno identifikovat vzorce a trendy v síťovém provozu, což pomáhá při dlouhodobém plánování a optimalizaci sítě.

Cacti také podporuje šablony pro různá síťová zařízení, což usnadňuje nasazení a konfiguraci monitoringu. Uživatelé si mohou stáhnout předpřipravené šablony pro populární zařízení, jako jsou Cisco routery, HP switche nebo Linux servery.

Další užitečnou funkcí je možnost nastavení upozornění a integrace s jinými monitorovacími nástroji. Cacti sice nemá vestavěný systém alertů jako například Zabbix nebo Nagios, ale lze jej s těmito nástroji propojit a zajistit tak notifikace v případě problémů.

Jednou z výhod Cacti je také rozšiřitelnost pomocí pluginů. Například plugin THold umožňuje nastavit prahové hodnoty pro sledované metriky a generovat upozornění, když jsou překročeny. Dalším užitečným rozšířením je Weathermap, který umožňuje vizualizaci síťové topologie a zatížení jednotlivých spojů.

I když je Cacti skvělým nástrojem pro dlouhodobý monitoring a analýzu trendů, není určen pro detailní analýzu síťového provozu v reálném čase. Pokud je potřeba hloubková inspekce síťových paketů, je vhodné jej kombinovat s nástroji jako Wireshark, ntopng nebo Zabbix, které umožňují podrobnější sledování a analýzu síťového provozu.

6 Principy architektury Cacti

Cacti je open-source monitorovací nástroj, který se využívá pro sledování výkonu síťových zařízení, serverů a dalších IT komponent. Jeho architektura je navržena tak, aby byla efektivní, škálovatelná a rozšiřitelná. Systém se skládá z několika klíčových komponent, které spolupracují na sběru, ukládání, zpracování a vizualizaci dat.

Jedním ze základních principů architektury Cacti je modularita. Tento princip umožňuje přidávat nové funkce prostřednictvím pluginů a přizpůsobit si tak systém podle specifických potřeb organizace. Dalším důležitým aspektem je efektivní ukládání dat, které je řešeno prostřednictvím RRDTool. Tato technologie minimalizuje nároky na úložiště tím, že ukládá data v kruhových databázích s pevnou velikostí, což znamená, že se databáze nerozrůstají nekontrolovaně.

Sběr dat v Cacti je automatizovaný a probíhá v pravidelných intervalech. Systém pravidelně dotazuje síťová zařízení a servery, čímž poskytuje aktuální informace o výkonu infrastruktury. Díky tomu mohou administrátoři snadno sledovat historické trendy a odhalovat možné problémy dříve, než dojde k výpadkům.

Dalším klíčovým principem je škálovatelnost. Cacti je navrženo tak, aby bylo schopné monitorovat i velmi rozsáhlé sítě s velkým množstvím zařízení. V případě potřeby lze systém rozšířit o distribuované sběrače dat (pollery), které rozloží zátěž mezi více serverů a umožní tak efektivnější zpracování velkého množství informací.

7 Klíčové komponenty architektury Cacti

7.1 Webové rozhraní (Frontend)

Cacti využívá webové rozhraní postavené na PHP, které umožňuje uživatelům jednoduše konfigurovat monitorovací systém a prohlížet vizualizace dat. Toto rozhraní je přístupné z jakéhokoli zařízení s připojením k síti, což umožňuje snadnou správu a monitoring infrastruktury odkudkoli.

V rámci webového rozhraní mají administrátoři možnost přidávat nová zařízení do systému a definovat, jaké metriky budou monitorovány. Mohou zde také konfigurovat způsoby sběru dat, nastavovat parametry grafů a vizualizací a spravovat uživatelské účty včetně jejich oprávnění. Webové prostředí je navrženo tak, aby bylo intuitivní, což usnadňuje práci i méně zkušeným uživatelům.

7.2 Databázová vrstva (MySQL/MariaDB)

Cacti využívá databázový systém MySQL nebo jeho alternativu MariaDB pro ukládání konfiguračních informací. Tato databáze obsahuje například seznam monitorovaných zařízení, definice metrik a grafů nebo informace o uživatelských oprávněních.

Ačkoli databáze MySQL/MariaDB obsahuje mnoho důležitých informací, samotná monitorovací data nejsou uložena zde. Pro ukládání historických hodnot se využívá RRDTool, který je optimalizován pro efektivní správu časových řad.

7.3 Sběr dat (Poller)

Sběr dat v Cacti zajišťuje proces nazývaný poller, který běží na pozadí a v pravidelných intervalech dotazuje monitorovaná zařízení. Tento proces využívá různé metody sběru dat, mezi které patří SNMP (Simple Network Management Protocol), různé skripty nebo přímé příkazy prováděné na serverech.

Poller je navržen tak, aby minimalizoval zátěž na síť a sledovaná zařízení. Toho je dosaženo optimalizovanými dotazy a možností nastavit různou frekvenci sběru dat pro jednotlivé typy metrik. V případě rozsáhlejší infrastruktury lze poller distribuovat mezi více serverů, čímž se zajišťuje škálovatelnost systému.

7.4 Ukládání a zpracování dat (RRDTool)

Jedním z klíčových prvků architektury Cacti je RRDTool, který slouží k ukládání a analýze časových řad. Tento nástroj je optimalizován pro efektivní správu velkého množství historických dat.

RRDTool pracuje na principu kruhových databází s pevnou velikostí, což znamená, že starší data jsou automaticky agregována do delších časových úseků. Tímto způsobem se šetří úložný prostor a zároveň se zachovávají důležité trendy a vzory v monitorovaných datech. Díky této metodě je možné dlouhodobě sledovat výkon síťových zařízení a serverů bez rizika, že by databáze nekontrolovaně narostla.

7.5 Vykreslování grafů a vizualizace dat

Cacti generuje přehledné grafy, které vizualizují získaná data. Tyto grafy jsou velmi užitečné pro sledování trendů, identifikaci potenciálních problémů a analýzu výkonu infrastruktury.

V rámci webového rozhraní mohou uživatelé definovat různé typy grafů a přizpůsobit si je podle svých potřeb. Například lze sledovat využití síťového provozu, zatížení procesorů na serverech, množství aktivních připojení nebo jiné důležité metriky.

Vizualizace dat pomáhá administrátorům rychle rozpoznat anomálie a přijmout potřebná opatření dříve, než dojde k vážnějším problémům.

7.6 Pluginový systém

Cacti podporuje rozšíření pomocí pluginů, což umožňuje přidávat do systému nové funkce a přizpůsobit jej specifickým potřebám organizace. Mezi nejpoužívanější pluginy patří například THold, který umožňuje sledování prahových hodnot monitorovaných metrik a generování upozornění při jejich překročení. Další užitečný plugin je Weathermap, který vizualizuje síťovou topologii a zatížení jednotlivých spojů. Díky modulárnímu přístupu lze Cacti snadno rozšířit a přizpůsobit jej konkrétním požadavkům organizace.

8. Postup implementace

Aktualizace systému

```
dnf upgrade
```

- Aktualizuje všechny balíčky na nejnovější verzi v repozitářích.

Instalace Apache (HTTP server)

```
dnf install httpd httpd-devel
```

- **httpd** – Apache webový server.
- **httpd-devel** – Závislosti pro rozšíření a vývojové balíčky Apache.

Instalace MariaDB (náhrada za MySQL)

```
dnf install mariadb-server -y
```

- **MariaDB server** – Databázový server, který Cacti využívá.
- **-y** – Automaticky potvrzuje instalaci.

Instalace PHP

Pro starší verze Fedora (33, 32, 30)

```
dnf config-manager --set-enabled remi
dnf -y install epel-release
dnf module reset php
dnf module install php:remi-7.4
```

- **Povolení Remi repozitáře**, který obsahuje různé verze PHP.
- **Resetuje PHP modul** a nastaví konkrétní verzi PHP 7.4.

Pro Fedora 34 a novější

```
dnf install php php-cli php-fpm php-mysqlnd php-zip php-devel php-gd php-
mcrypt php-mbstring php-curl php-xml php-pear php-bcmath php-json
```

- **Balíčky PHP** potřebné pro provoz Cacti.
    - `php-cli` – PHP příkazová řádka.
    - `php-fpm` – PHP FastCGI Process Manager.
    - `php-mysqlnd` – Podpora pro MySQL.
    - `php-gd` – Grafická knihovna (nutná pro grafy v Cacti).
    - `php-mbstring` – Podpora vícebajtových znaků.
    - Další rozšíření jako JSON, XML, ZIP, CURL atd.

Instalace PHP-SNMP (Simple Network Management Protocol pro PHP)

```
dnf install php-snmp
```

- **Nutné pro SNMP monitoring** v Cacti.

Instalace NET-SNMP (SNMP nástroje a knihovny)

```
dnf install net-snmp-utils net-snmp-libs
```

- **SNMP nástroje** (net-snmp-utils) a **knihovny** (net-snmp-libs) umožňují sběr SNMP dat.

Instalace RRDTool (Round Robin Database Tool)

```
dnf install rrdtool
```

- **Nástroj pro ukládání a vizualizaci časových řad** – Cacti používá pro vykreslování grafů.

Instalace všech balíčků jedním příkazem

```
dnf install httpd httpd-devel mariadb-server php-mysqlnd php-pear php-common php-gd php-devel php php-mbstring php-cli php-snmp net-snmp-utils net-snmp-libs rrdtool
```

- **Instaluje všechny potřebné komponenty** v jednom kroku.

Spuštění služeb (Apache, MariaDB, SNMP)

```
systemctl start httpd.service
systemctl start mariadb.service
systemctl start snmpd.service
```

- **Spustí Apache, MariaDB a SNMP služby**.

Úprava PHP konfigurace (/etc/php.ini)

```
memory_limit = 512M
max_execution_time = 60
date.timezone = Europe/Prague
```

- **Zvětšení limitu paměti na 512 MB** (Cacti může pracovat s velkým množstvím dat).
- **Nastavení maximální doby vykonání skriptu na 60 sekund**.
- **Nastavení časového pásma** (nutné sladit s časem systému)

Kontrola dostupných časových pásem

```
timedatectl list-timezones
```

- Zobrazí všechna podporovaná časová pásma.

Nastavení správného časového pásma na Fedoře

```
timedatectl set-timezone Europe/Prague
```

- **Změní časové pásmo systému**, aby odpovídalo PHP.

Povolení automatického spuštění služeb při startu systému

```
systemctl enable httpd.service
systemctl enable mariadb.service
```

```
systemctl enable snmpd.service
```

- **Zajistí, že Apache, MariaDB a SNMP se spustí automaticky po restartu**.

Tuning databáze (MariaDB)

```
nano /etc/my.cnf.d/mariadb-server.cnf
```

- **Otevře konfigurační soubor MariaDB**.

Přidání doporučených parametrů pro Cacti

```
collation-server = utf8mb4_unicode_ci
character-set-server=utf8mb4
max_heap_table_size = 64M
tmp_table_size = 64M
join_buffer_size = 128M
innodb_file_format = Barracuda
innodb_large_prefix = 1
innodb_flush_log_at_timeout = 3
innodb_buffer_pool_size = 1GB
innodb_buffer_pool_instances = 10
innodb_io_capacity = 5000
innodb_io_capacity_max = 10000
```

- **Zlepšuje výkon MariaDB** pro práci s větším množstvím dat v Cacti.

Vypnutí SELinux (doporučeno pro Cacti)

```
nano /etc/sysconfig/selinux
```

- **Otevře konfigurační soubor SELinux**.

Změna z "permissive" na "disabled"

```
SELINUX=permissive
```

Na

```
SELINUX=disabled
```

- **Zakáže SELinux**, aby neblokoval přístup ke Cacti.

Povolení Apache a SNMP služeb v chkconfig (alternativní metoda)

```
chkconfig httpd on
systemctl enable httpd.services
systemctl start httpd.services
chkconfig snmpd on
```

- **Zajišťuje automatické spouštění Apache a SNMP** při startu systému.

Oprávnění pro Cacti logy

```
sudo chown -R apache:apache /usr/share/cacti/log/
chown -R root:root /usr/share/cacti/log/
sudo chown -R normal_user_name:normal_User_NAME /usr/share/cacti/log/
```

- **Nastavení správných oprávnění pro logy** Cacti, aby je mohl zapisovat správný uživatel.

Příklad pro konkrétního uživatele:

```
sudo chown -R saad:saad /usr/share/cacti/log/
```

- **Změní vlastníka složky log/ na uživatele saad**.

9. Závěr

Monitorování síťového provozu je nezbytným nástrojem pro efektivní správu a zabezpečení moderních sítí. Umožňuje nejen detekci problémů a anomálií v reálném čase, ale také pomáhá optimalizovat výkon, plánovat kapacitu a zajistit soulad s regulačními požadavky.

Díky monitorovacím nástrojům, jako je Cacti, mohou správci sítí získat podrobné informace o stavu infrastruktury, rychle reagovat na výpadky a analyzovat dlouhodobé trendy. Implementace těchto systémů přispívá k vyšší spolehlivosti a bezpečnosti podnikových sítí, čímž minimalizuje riziko neplánovaných výpadků a kybernetických hrozeb.

Vzhledem k neustále rostoucím nárokům na síťové infrastruktury je efektivní monitorování stále důležitější. Organizace, které investují do moderních monitorovacích řešení, získávají nejen lepší kontrolu nad svou sítí, ale také strategickou výhodu v oblasti IT správy a bezpečnosti.

10. Literatura

1. CACTI. Home website. Online. Dostupné z: https://www.cacti.net. [cit. 2025-03-26].
2. CACTI. Cacti Documentation. Online. Dostupné z: https://docs.cacti.net/#cacti-tm-documentation. [cit. 2025-03-26].
3. WIKIPEDIE. Simple Network Management Protocol. Online. Dostupné z: https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol. [cit. 2025-03-26].
4. WIKIPEDIE. Netflow. Online. Dostupné z: https://en.wikipedia.org/wiki/NetFlow. [cit. 2025-03-26].
5. WIKIPEDIE. Syslog. Online. Dostupné z: https://en.wikipedia.org/wiki/Syslog. [cit. 2025-03-26].
6. CISCO. What Is Network Monitoring? Online. Dostupné z: https://www.cisco.com/c/en_uk/solutions/automation/what-is-network-monitoring.html. [cit. 2025-03-26].
7. CISCO. Cybersecurity Essentials course. Online. Dostupné z: https://www.netacad.com. [cit. 2025-03-26].

11. Seznam obrázků