LIBRENMS-SUSTAV ZA NADZIRANJE RAČUNALNE MREŽE

Balajić, Dujo

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Preddiplomski stručni studij Informacijska tehnologija

DUJO BALAJIĆ

Z A V R Š N I R A D

LibreNMS – sustav za nadziranje računalne mreže

Split, rujan 2022.

SVEUČILIŠTE U SPLITU
SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Preddiplomski stručni studij Informacijska tehnologija

Predmet: Sigurnost računala i podataka

Z A V R Š N I R A D

Kandidat: Dujo Balajić

Naslov rada: LibreNMS – sustav za nadziranje računalne mreže

Mentor: Lada Sartori, v. pred.

Split, rujan 2022.

SADRŽAJ

SAŽETAK

Računalne mreže danas postaju sve složenije što rezultira potrebom implementacije sustava za nadzor, a time i razvojem velikog broja takvih sustava. Za ovaj rad izabran je LibreNMS sustav. U prvom dijelu rada odrađena je analiza te proučavanje sustava. Zatim je slijedila instalacija u virtualnom okruženju koja je uključivala instalaciju te konfiguraciju virtualne mašine, PHP podrške, baze podataka te poslužitelja. Testirane su mnoge prednosti sustava uključujući nadzornu ploču na kojoj se nalaze blokovi poput „Najboljih uređaja“ te „Upozorenja“ koji pružaju puno informacija. Sustav za obavještavanje je postavljen i testiran tako da šalje obavijesti na e-mail. Zatim je sustav migriran u produkcijsko okruženje gdje su dodani stvarni uređaji iz stvarne mreže. Ponovno se konfigurirao te testirao rad sustava čime je završio praktički dio rada.

KLJUČNE RIJEČI: sustav za nadzor mreže, LibreNMS, SNMP

SUMMARY

LibreNMS – computer network monitoring system

Computer networks are becoming more and more complex today, which results in the need to implement a monitoring system, and thus of a large number of such systems has been developed. The LibreNMS system was chosen for this work. The analysis and study of the system was done in the first part of the work. Then followed the installation in the virtual environment, which included the installation and configuration of the virtual machine, PHP support, the database and the servers. Many benefits of the system have been tested, including a dashboard with blocks like "Top Devices" and "Alerts" that provide a lot of information. The notification system has been set up and tested to send notifications to e-mail. Then the system was migrated to a production environment where real devices from a real network were added. It was reconfigured and the system was tested, thus completing the practical part of the work.

KEYWORDS: Network Monitoring System, LibreNMS, SNMP

1. UVOD

U posljednjih nekoliko godina, mrežna sigurnost i dizajn postali su složeniji s evolucijom virtualizacije, distribuiranog računalstva i virtualnog oblaka. Jednostavne mreže više ne zadovoljavaju zahtjeve moderne infrastrukture. Kako bi se osiguralo da mreža pruža očekivane performanse, uključujući dobru brzinu propusnosti, neprekinutu komunikaciju i visoku dostupnost, potrebna je snažna strategija nadzora mreže. Usmjernici, poslužitelji i prospojnici obavljaju poslove kritične za poslovanje, pa te komponente zahtijevaju češće praćenje. Drugim riječima, intervali praćenja internetskog prometa oslanjaju se na određene parametre i korištenje i trebaju se birati na temelju činjenica određene situacije. Najbolji sustavi omogućuju korisnicima stvaranje prilagođenih upozorenja. Dizajn mrežnog nadzora trebao bi pokrivati svaki aspekt IT infrastrukture, kao što su povezanost, mreža i sigurnosni sustavi. Konačno, siguran sustav za praćenje mreže trebao bi biti jednostavan za korištenje i nuditi osnovne funkcije detaljnog pregleda i izvješćivanja.

U drugom poglavlju opisane se tehnologije i protokoli korišteni u radu. Treće poglavlje opisuje procese instalacije i konfiguracije za vrste različitih mrežnih uređaja i poslužitelja s različitim operativnim sustavima. Predstavlja se i raspravlja o konačnom izgledu nadzorne ploče aplikacije i dobivenim prednostima. Sustav koji se koristi u radu je LibreNMS. LibreNMS je open source, moćan i bogat značajkama, automatski otkrivajući PHP sustav za nadzor mreže koji zasniva svoj rad na SNMP protokolu. Uz operativne sustave kao što su Linux, FreeBSD i drugi, LibreNMS također podržava mnoštvo mrežnih uređaja od kojih su nabrojeni samo sljedeći: Juniper, Brocade, Cisco, HP, Foundry.

Postoji mnogo dostupnih aplikacija koje se mogu koristiti i konfigurirati, ali neki od glavnih razloga zašto je odabran LibreNMS su da je besplatan za korištenje, da podržava skaliranje za proširenje zajedno s mrežom, podržava API (Application Programming Interface**)** tj. programsko sučelje aplikacije za upravljanje i dohvaćanje podataka iz sustava, zatim njegova fleksibilnost i prilagodljivost u obavještavanju korisnika, odnosno mogućnost odabira više načina obavještavanja (irc, slack, e-pošta).

2. SUSTAVI ZA NADZOR

Tehnologije u nastajanju poput bežične veze, oblaka i VPN-a proširile su spektar umrežavanja za prijenos podataka, mobilnu ili daljinsku komunikaciju i isporuku usluga. Mrežni elementi i uređaji također su se razvili od jednostavnih prospojnika do višeslojnih prospojnika, proxy poslužitelja, usmjernika, vatrozida, itd. U mrežama broj poslužitelja i usluga koje nude svakodnevno raste. Upravo stoga, praćenje toga koliko dobro ili učinkovito radi mreža i uređaji spojeni na nju postaje ključni čimbenik. Nadzor mreže kontinuirana je analiza računalne mreže ili cijele mrežne infrastrukture pomoću sustava za otkrivanje sporih ili neispravnih elemenata na mreži.

2.1. Potreba sustava za nadzor

Rastuće potrebe za IT uslugama u svakodnevnim procesima nastave i istraživanja na sveučilištima u posljednjih nekoliko desetljeća doveli su do velikog opterećenja IT inženjerima u ovom sektoru. Veliki broj uređaja i poslužitelja u mreži ne može se lako nadzirati od strane jedne osobe ako reprezentacija njihovih stanja i resursa nije skupljena na jednom mjestu, npr. na jednoj web stranici. Praćenje i procjena mreže način je brzog lociranja problema u mreži. Praćenje performansi mreže može pokazati uzrok i izvor mrežnog problema, gdje i kada se pojavio. Kada se aktivno nadzire mreža, mogu se otkriti sve promjene performansi koje bi mogle biti problematične korisnicima prije nego što se dogode. Uz dostupnost osnovnih podataka, alati za nadzor mreže mogu kontinuirano i automatski uspoređivati podatke. [6]

2.2. O sustavima za nadzor

Mrežni nadzor, podskup upravljanja mrežom, sustavni je pokušaj računalne mreže da identificira spore ili neispravne komponente prije nego što prouzrokuju probleme. Na primjer, srušeni, zamrznuti ili preopterećeni poslužitelji, neispravni prospojnici, neispravni usmjernici i druge problematične komponente mogu potencijalno uzrokovati prekide ili kvarove na mreži. Ako se pojavi neki problem i izazove prekid rada, uloga sustava za nadzor mreže je da na vrijeme upozori mrežnog administratora. U slučaju pada performansi, sustav šalje upozorenje i možete odmah riješiti problem. Prethodno spremljeni podaci daju točku usporedbe kako bi se odredila optimalna izvedba mreže ili

identificirala loša izvedba. To omogućuje rješavanje mrežnih problema prošlih događaja. Obično administratori nadziru i upravljaju mrežom pomoću alata za praćenje mreže i softverskih aplikacija. Ove usluge mrežnog nadzora pomažu korisnicima da prate performanse i otkriju je li web poslužitelj ispravno povezan sa svjetskim mrežama i funkcionira li prema očekivanjima. Mnogi alati za praćenje performansi mreže također nude vizualizaciju mreža i aplikacija. [4]

Prvi korak učinkovitog nadzora mreže je identificiranje uređaja koji se nadziru i njihove povezane metrike izvedbe. Sljedeći korak je odabir odgovarajućeg intervala praćenja.

2.3. Simple Network Management Protocol (SNMP)

Ukoliko se želi pratiti stanje uređaja na mreži i njihovih usluga, na njima mora biti instaliran, konfiguriran i omogućen Simple Network Management Protocol (SNMP) protokol.

Osiguravanje optimalne i sigurne mreže danas može predstavljati veliki izazov, no zahvaljujući SNMP-u taj zadatak je puno lakši. Osnova SNMP-a je skup operacija koje administratorima daju mogućnost promjene stanja nekog uređaja. Npr. može se koristiti za isključivanje sučelja na usmjerniku ili za promjenu brzine Ethernet sučelja. Uređaji koji obično podržavaju SNMP uključuju kabelske modeme, usmjernike, prospojnike, poslužitelje, radne stanice, pisače i još mnogo toga. SNMP-ov prethodnik, Simple Gateway Management Protocol (SGMP) razvijen je sa svrhom upravljanja internetskim usmjernicima dok se SNMP koristi za upravljanje pisačima, Windows sustavima, izvorima napajanja, Unix sustavima, i više. Još jedna od velikih prednosti je da se može upravljati ne samo fizičkim uređajima nego i softverskim, kao što su web poslužitelj ili baza podataka. Sve što treba je imati softver koji omogućuje dohvaćanje SNMP informacija. SNMP izlaže upravljačke podatke u obliku varijabli o upravljanim sustavima organiziranim u bazi upravljačkih informacija koje opisuju status i konfiguraciju sustava. Te se varijable zatim mogu daljinski ispitivati (i, u nekim okolnostima, manipulirati) upravljanjem aplikacijama. U principu SNMP svojim korisnicima pruža jednostavan (simple) skup operacija kojima omogućuju da svojim uređajima upravljaju na daljinu. To također daje mogućnost promjene stanja nekog uređaja.

2.3.1. Uvod u SNMP

Dvije vrste sistema osnovna su ideja svakog sustava za upravljanje mrežom, a to su upravitelji i agenti (Slika 2.1.). Upravitelji su poslužitelji, također poznati kao NMS (Network monitoring station) tj. stanicama za upravljanje mrežom. Oni su zaduženi za primanje informacija od agenata putem zahtjeva. Zahtjev je, u kontekstu upravljana mrežom, postavljanje upita od poslužitelja prema agentu. Agent putem zamke (trap) šalje informacije upravitelju, tj. NMS-u da se nešto dogodilo. One se šalju asinkrono, odnosno nevezano za upite od upravitelja. Agenti mogu biti uređaji kao što su usmjernik, prospojnik, Unix poslužitelj i slično. Agentski modul nalazi se u svakom čvoru mreže s kojim se mora upravljati (npr. poslužitelj, usmjernik,...). Agent je odgovoran za:

- nadziranje lokalnog okruženja o kojem sakuplja informacije
- slanje odgovora na zahtjev NMS-a
- mijenjanje lokalne konfiguracije na upraviteljev zahtjev

Svaki agent ima svoju bazu upravljačkih informacija (MIB - management information base). Baza podataka o upravljanju (MIB) može se smatrati bazom podataka upravljanih objekata koje agent prati. Bilo koje status ili statističke informacije kojima može pristupiti NMS definirane su u MIB-u. Poput rječnika, koji pokazuje kako se piše riječ i zatim daje njezino značenje ili definiciju, MIB definira tekstualni naziv za upravljani objekt i objašnjava njegovo značenje.

Slika 2.1. – Odnos upravitelja (NMS) i agenta [1]

Protokol sadrži četiri osnovne funkcije: Get, Set, Trap, Inform.

GET – ovu funkciju koristi NMS za dobivanje jedne informacije od upravljanog uređaja (npr. NMS može zahtijevati konfigurirani naziv uređaja)

SET – NMS koristi ovu funkciju za konfiguriranje upravljanog uređaja

TRAP – ovu funkciju koristi agent da bi poslao zamku koja sadrži upozorenje da je da je dosegnut prag definiran od strane NMS-a

INFORM – ovu funkciju koriste NMS-ovi da bi poruku zamke proslijedili drugim NMS-ovima

Važnost SNMP-a potvrđuje vrijeme prije nego je korišten, u vrijeme kada se mreži nije moglo pristupiti iz daljine. To znači, da ukoliko bi došlo do kvara, netko bi morao biti fizički prisutan da bi se popravio kvar. Štoviše, uz konstantan nadzor mreže, čak i kada niste tu, SNMP omogućuje upozorenja na probleme koji vode do kvara na nekome uređaju. Na primjer, ako više krivih paketa prolazi kroz usmjernik, te taj broj raste, to vjerojatno znači da će se usmjernik, zbog preopterećenja, urušiti.

SNMP koristi UDP (User Data Protocol) kao protokol za transport tj. prosljeđivanje podataka, koji je izabran umjesto TCP-a (Transmission Control Protocol) jer se za njega ne mora uspostaviti „end to end“ komunikacija, dok za TCP treba. To čini UDP nepouzdanim jer nema načina da se potvrdi ima li izgubljenih podataka u transferu. Taj problem SNMP rješava odgodom, tj. vremenskim ograničenjem. NMS pošalje UDP zahtjev agentu i čeka na odgovor. Ukoliko je isteklo vrijeme, a odgovor nije stigao, pretpostavka je da je paket izgubljen te se ponovno šalje zahtjev. U konfiguraciji je moguće promijeniti broj puta koliko će upravitelj slati ponovno paket. U najgorem slučaju, upravitelj izdaje zahtjev i nikada neće dobiti odgovor. Postoji veći problem od toga, a to je slučaj kada agent šalje zamku, a ona nikada ne stigne do upravitelja. Razlog zbog kojeg je to veći problem je taj što niti upravitelj (NMS) nema nikakvog načina da sazna da je agent poslao zamku niti agent ne zna da treba ponovno poslati zamku. S druge strane, jedna od prednosti UDP-a je što korištenjem minimalnih funkcija protokola smanjiva opterećenje mreže. UDP priključak 161 je priključak koji SNMP koristi za primanje i slanje zahtjeva, dok se za primanje zamki od agenata koristi priključak 162, ali neki proizvođači dozvoljavaju

promjenu ovih postavki u konfiguraciji agenta. Svaki uređaj koji implementira SNMP mora koristiti ove brojeve priključaka kao zadane pa tako čini i LibreNMS.

Prve dvije verzije SNMP-a, SNMPv1 i SNMPv2 koriste pojam „zajednica“ (community) za uspostavljanje povjerenja između NMS-a i agenta. Ne postoji razlika između niza zajednice (community string) i lozinke koja se koristi za pristup na račun tako da su imena zajednice zapravo lozinke.

Na agentu se mogu konfigurirati tri imena zajednice:

- samo za čitanje (read only) - dozvoljava samo čitanje, no ne i izmjenu podataka
- čitanje i pisanje (read and write) – dozvoljava i čitanje i pisanje (npr. uz čitanje brojača mogu se resetirati njihove vrijednosti)
- trap (zamka) - omogućuje primanje zamki od agenata

S obzirom da su nizovi zajednice u stvari lozinke, treba se tako i odnositi prema njima, tj. za njihov odabir ne koristiti osobne podatke kao imena, datume rođenja i slično. No i uz jaku lozinku, problem autentifikacije SNMP-a je što se nizovi šalju u obliku teksta što znači da ih se lako presretne. Taj je problem riješen u trećoj verziji SNMP-a, SNMPv3. Rješava se tako da se dopušta sigurna autentifikacija i komunikacija između SNMP uređaja. Uz vatrozid (firewall) i filtre smanjena je mogućnost nanošenja štete na bilo koji upravljani uređaj putem SNMP-a. Iako vatrozidi nisu 100% učinkoviti, male mjere opreza kao ta uvelike smanjuju rizik. Sigurnosne postavke se mogu konfigurirati na proizvoljan način (npr. UDP promet u mreži je dopušten samo ako dolazi iz te mreže).

Način na koji su podaci predstavljeni u kontekstu SNMP-a objašnjava Structure of Management information (SMI). Prva verzija SMI-a definira kako se objekti nazivaju i specificira njihove tipove podataka, dok druga verzija pruža poboljšanja za SNMPv2. Ime ili identifikator objekta (OID) definira objekt te se obično pojavljuje u dva oblika a to su numerički i „human readable“ (čitljiv čovjeku). Oba imena su dugačka te u SNMP aplikacijama puno je posla potrebno za pomoć pri navigaciji kroz imena. Abstract Syntax Notation One (ASN.1) je način određivanja kako se podaci predstavljaju i prenose između NMS-a i agenta. Prednost je ta da ne ovisi o stroju, što znači da različiti sustavi mogu komunicirati bez problema kao što su poredak bajtova u prijenosu i slično. Koriste se osnovna pravila kodiranja za kodiranje upravljanog objekta. To osigurava prijenos preko sigurnosnog medija.

Imenovanje identifikatora objekata se radi pomoću hijerarhije grananja stabla. Struktura stabla je osnova za shemu imenovanja kod SNMP-a. ID objekta sastoji se od niza cijelih brojeva temeljenih na čvorovima u stablu, odvojenih točkama. Postoji i oblik koji je lakše čitljiv čovjeku ali u principu to je samo niz imena koji su razdvojeni točkama, gdje svako ime predstavlja jedan čvor u stablu. Mogu se koristiti ili brojevi ili niz imena koja predstavljaju brojeve. Slika 2.2 predstavlja nekoliko razina strukture stabla. [1]

Slika 2.2. – Stablo objekta [1]

Najviši čvor, čvor na vrhu stabla, naziva se korijen. Svaki čvor koji ima djecu naziva se podstablo, a svaki čvor koji nema djecu naziva se list.

2.3.1. Arhitektura NMS-a

NMS arhitektura pomaže da se učinkovito koristi NMS za upravljanje mrežom. Ključni korak upravljanjem mrežom je odabir hardvera koji će pokretati NMS. Također, treba osigurati da su upravljačke stanice smještene na način da mogu učinkovito promatrati uređaje na mreži.

Upravljanje velikom mrežom zahtijeva NMS sa značajnom računalnom snagom. U današnjim mrežnim okruženjima, mreže mogu biti toliko velike da sadrže do nekoliko tisuća čvorova. Tolike mreže mogu opteretiti i najbolju hardversku opremu. Većina dobavljača ima formule koje određuju koliko radne memorije će trebati da se postigne željena razina performansi, s obzirom na zahtijevanu mrežu. Proizvođači preporučuju računalo sa sljedećim karakteristikama:

- 2 ili 3 GHz procesor
- 512 MB do 1 GB radne memorije
- 1-2 GB prostora na disku

Najjednostavnija arhitektura je ona koja je odgovorna za jednu upravljačku stanicu, tj. jedan NMS. Prikazana je na slici 2.3.

Slika 2.3. – Arhitektura s jednim NMS-om [1]

Kao što je prikazano na slici, NMS u New Yorku odgovoran je za upravljanje cijele mreže. Sve zamke iz San Josea i Atlante moraju putovati internetom kako bi došle do NMS-a. U drugom smjeru zahtjevi od upravljačke stanice također moraju putovati putem interneta. Ova arhitektura može funkcionirati dobro za manju mrežu no ukoliko dođe do točke kada NMS više ne može upravljati svime, ova arhitektura postaje problematična.

Drugi tip arhitekture je arhitektura distribuiranih NMS-ova. Kod ovog tipa, upotrebljava se više upravljačkih stanica. Prikazana je na slici 2.4.

Slika 2.4. – Arhitektura distribuiranih NMS-ova [1]

Uz ostale prednosti, ova arhitektura je puno fleksibilnija od prvog tipa. Vidljivo je na slici da NMS-ovi u Atlanti i San Joseu mogu djelovati kao samostalne upravljačke jedinice, a mogu i proslijediti događaje NMS-u u New Yorku. Druga prednost je da, ukoliko jedna od stanica izgubi vezu s internetom, ostale stanice će nastaviti raditi. Međusobno će razmjenjivati podatke kao da se ništa nije dogodilo, samo neće imati vezu sa stanicom koja je odspojena od interneta.

Problem kod obje arhitekture je to što koriste Internet za slanje i primanje informacija. To predstavlja sigurnosne probleme i smanjuje pouzdanost mreže. Najbolje rješenje je koristiti privatne veze za obavljanje funkcija upravljanja mrežom. Na slici 2.5. prikazano je proširenje distribuirane NMS arhitekture koje omogućuje korištenje takvih veza.

Slika 2.5. – Korištenje privatnih veza za upravljanje mrežom [1]

U ovom primjeru mreže, San Jose preko privatne veze može doći do New Yorka, ali preko New Yorka također može doći do Atlante. U obrnutom smjeru Atlanta će isto koristiti vezu preko New Yorka da stigne do San Josea. Dodatna prednost korištenja privatnih veza je da se nizovi zajednice nikada ne šalju putem Interneta. [1]

Ovaj način komuniciranja privatnim vezama funkcionirao bi jednako dobro i s jedinstvenom NMS arhitekturom.

3. IMPLEMENTACIJA LIBRENMS SUSTAVA

Izveden iz drugog projekta (Observium), LibreNMS je napisan u PHP-u kao web aplikacija. Glavna razlika LibreNMS-a i Observiuma je da je LibreNMS besplatan za korištenje svima dok se Observium plaća. Još neke od razlika su: odluke o razvoju donosi zajednica, cilj je napraviti softver koji ispunjava potrebe korisnika, nema planova za verziju koja se plaća te što se koristi GitHub kako bi se stvaranje privatnih verzija bilo što jednostavnije.

3.1. LibreNMS

LibreNMS (Slika 3.1.) nudi sveobuhvatne mogućnosti nadzora za umrežene uređaje. Može nadzirati širok raspon uređaja, uključujući usmjernik, prospojnik, vatrozide i još mnogo toga. Može se koristiti za nadzor malih i velikih mreža. Nudi širok raspon značajki i jednostavan je za instalaciju i konfiguraciju. LibreNMS također podržava širok raspon protokola za nadzor, kao što su ICMP i TCP te već navedeni SNMP. LibreNMS pruža web sučelje za upravljanje i nadzor mreže. Sučelje je vrlo prilagodljivo i omogućuje pregled informacija o dodanim uređajima na razne načine. Također se mogu izraditi prilagođene nadzorne ploče za prikaz informacija koje korisnik odredi da su najvažnije. LibreNMS pruža i sveobuhvatan i moćan sustav upozorenja koji administratora može obavijestiti o svim problemima u mreži. Slanje upozorenja može se konfigurirati na način da se odvija putem e-pošte, SMS-a ili čak push obavijesti na administratorov mobilni uređaj. Upozorenja se mogu pokrenuti zbog brojnih uvjeta, kao što je velika upotreba CPU-a, malo prostora na disku ili čak prekid rada određenog priključka.

Slika 3.1. – LibreNMS logo

3.2. Radno okruženje

Osnovna konfiguracija LibreNMS-a omogućuje korisnicima pregled cijele mreže, odnosno svih dodanih uređaja, njihovih stanja, zapisnika najnovijih događaja, uređaja s najvećim prometom, kao i drugih podesivih pogleda.

Prema dokumentaciji LibreNMS-a, minimalni zahtjevi sustava za početnu instalaciju bili bi:

- fizički ili virtualni stroj s verzijom operacijskog sustava Linux
- 2 jezgreni CPU
- 2 GB RAM-a
- 20 GB prostora na disku

Ovi minimalni zahtjevi zadovoljavaju osnovnu potrebu za nadzorom više uređaja. To bi bilo dovoljno za prvotnu instalaciju LibreNMS-a na virtualnoj mašini, no ona je izrađena na računalu s boljom konfiguracijom čime su omogućene bolje postavke same virtualne mašine. Konfiguracija virtualne mašine je:

- virtualni Linux stroj instaliran na Oracle VM VirtualBox platformi s Ubuntu 20.04.2.0 operativnim sustavom
- 4 virtualna procesora
- 4 GB RAM-a
- 50 GB prostora na disku

Instalacija i par testiranja ispunili su 17 GB prostora na disku, zajedno s operativnim sustavom i svim instaliranim paketima. Sustav je prvotno instaliran na navedenoj virtualnoj mašini gdje su se obavljale konfiguracije te testiranja prije migriranja na stvarni sustav.

3.3. Proces instalacije LibreNMS-a

Prvi dio instalacije sastoji se od instalacije operativnog sustava. Na službenoj web stranici LibreNMS-a predložene su distribucije Ubuntu, CentOS i Debian, ali se softver može instalirati i na sve ostale distribucije. U ovom slučaju odabrana je verzija Ubuntu Server 20.04.2.0.

Glavni potrebni paketi potrebni za instalaciju LibreNMS-a su web poslužitelj, SQL poslužitelj, PHP, Python i SNMP poslužitelj.

Iako LibreNMS može raditi na Apache web poslužitelju, Nginx preporučuju i LibreNMS i programeri, pa je i odabran. Minimalna verzija PHP-a koju LibreNMS podržava je 7.4, tako da je instalirana verzija 7.4.3. Izbor SQL poslužitelja može biti između MySQL i MariaDB. Glavne prednosti MariaDB-a su: softver otvorenog koda, nudi pohranu u stupcima za bržu izvedbu analitike, podržava popularni i standardni jezik upita i podržava PHP. To su samo neke od prednosti zbog kojih je MariaDB odabrani SQL poslužitelj. [5] [6]

Nakon instalacije operacijskog sustava, svi paketi su ažurirani. Naredbu za ažuriranje mora pokrenuti ili root korisnik ili se pokreće pomoću sudo naredbe.

```
apt update

apt upgrade
```

Dokumentacija predlaže instalaciju paketa koji omogućuje upravljanje izvorima softvera neovisnog dobavljača softvera. Bez tog paketa dodavanje dodatnih spremišta trebalo bi odraditi ručno.

```
apt install software-properties-common

add-apt-repository universe

apt update
```

Zatim su jednom naredbom instalirani svi potrebni paketi za LibreNMS.

```
apt install acl curl composer fping git graphviz
imagemagick mariadb-client mariadb-server mtr-tiny
nginx-full nmap php7.4-cli php7.4-curl php7.4-fpm
```

```
php7.4-gd php7.4-gmp php7.4-json php7.4-mbstring php7.4-
mysql php7.4-snmp php7.4-xml php7.4-zip rrdtool snmp
snmpd whois unzip python3-pymysql python3-dotenv
python3-redis python3-setuptools python3-systemd
python3-pip
```

Nakon što je instalacija paketa uspješna, korisnika librenms treba dodati u sustav, a direktorij u koji će biti instaliran LibreNMS definira se kao početni direktorij za korisnika librenms.

```
useradd librenms -d /opt/librenms -M -r -s "$(which
bash)"
```

Sljedećim naredbama klonira se git hub repozitorij LibreNMS-a čime se instalira sam software programa. Nakon toga postavljena su dopuštenja. Ovo je postavljanje kućnog (home) direktorija korisnika i postavljanje svih dozvola za LibreNMS datoteke.

```
cd /opt

git clone https://github.com/librenms/librenms.git

chown -R librenms:librenms /opt/librenms

chmod 771 /opt/librenms

setfacl -d -m g::rwx /opt/librenms/rrd
/opt/librenms/logs /opt/librenms/bootstrap/cache/
/opt/librenms/storage/

setfacl -R -m g::rwx /opt/librenms/rrd
/opt/librenms/logs /opt/librenms/bootstrap/cache/
/opt/librenms/storage/
```

Glavni programski jezik je PHP. Zatim slijedi instalacija PHP ovisnosti, koja mora biti izvedena od librenms korisnika.

```
su - librenms

./scripts/composer_wrapper.php install --no-dev

exit
```

Ponekad, kada se koristi proxy za dobivanje pristupa internetu, gornja skripta možda neće uspjeti. Zaobilazno rješenje je ručno instalirati skladateljski paket. Za globalnu instalaciju koriste se naredbe:

```
wget https://getcomposer.org/composer-stable.phar

mv composer-stable.phar /usr/bin/composer

chmod +x /usr/bin/composer
```

Kako bi se baza podataka instalirala i koristila, vremenske zone moraju biti ispravno konfigurirane u konfiguracijskim datotekama php.ini.

```
vi /etc/php/7.4/fpm/php.ini

vi /etc/php/7.4/cli/php.ini
```

Postavlja se i vremenska zona. Format vremenske zone za Hrvatsku je Europe/Zagreb. Ako nije postavljena tijekom procesa instalacije, vremenska zona sustava također treba biti postavljena:

```
timedatectl set-timezone Europe/Zagreb
```

3.3.1. Konfiguracija MariaDB

U konfiguraciji MariaDB SQL poslužitelja potrebno je dodati sljedeće dvije linije u konfiguracijsku datoteku /etc/mysql/mariadb.conf.d/50-server.cnf pod odjeljkom [mysqld]:

```
innodb_file_per_table=1

lower_case_table_names=0
```

Nakon toga potrebno je omogućiti uslugu baze podataka, te ponovo pokrenuti poslužitelj kako bi se promjene primjene.

```
systemctl enable mariadb

systemctl restart mariadb
```

Kreiranje baze podataka za LibreNMS izvodi se iz naredbenog retka poslužitelja baze podataka. Sa sljedećom naredbom dobije se root pristup poslužitelju baze podataka i prikazuje se mysql prompt:

```
mysql -u root
```

Sljedećim naredbama kreira se baza podataka, korisnik, šifra te se daju sve potrebne privilegije korisniku.

```
CREATE DATABASE librenms CHARACTER SET utf8mb4 COLLATE
utf8mb4_unicode_ci;

CREATE USER 'librenms'@'localhost' IDENTIFIED BY
'password';

GRANT ALL PRIVILEGES ON librenms.* TO
'librenms'@'localhost';

FLUSH PRIVILEGES;

exit
```

Na mjesto 'password' ide nova, što snažnija zaporka po izboru korisnika, jer su baze podataka česte mete sigurnosnih napada.

3.3.2. Konfiguracija PHP-FPM

PHP-FPM (FastCGI Process Manager) je učinkovita metoda za smanjenje potrošnje memorije i povećanje performansi za web stranice s velikim prometom. Značajno je brži od tradicionalnih metoda temeljenih na Common Gateway Interface (CGI) skriptama u višekorisničkim PHP okruženjima.

PHP-FPM je alternativna implementacija PHP FastCGI koja se koristi na jako opterećenim stranicama za ubrzavanje performansi PHP-a. Za konfiguraciju PHP-FPM-a preporučuje se kopiranje zadane datoteke www.conf i njezina promjena:

```
cp /etc/php/7.4/fpm/pool.d/www.conf
/etc/php/7.4/fpm/pool.d/librenms.conf
```

Uređivanje datoteke „librenms.conf“ sastoji se od preimenovanja odjeljka [www] u [librenms], promjene korisnika i grupe u librenms i promjene varijable *listen* u /run/php-fpm-librenms.sock.

```
[www] = [librenms]
```

```
user = librenms

group = librenms

listen = /run/php-fpm-librenms.sock
```

Ako na poslužitelju nema drugih PHP web aplikacija dokumentacija LibreNMS-a savjetuje da se ukloni www.conf kako bi se sačuvalo neke resurse. [2]

3.3.3. Konfiguracija web stranice

Konfiguracija je definirana u datoteci /etc/ngnix/conf.d/librenms.conf. Sadržaj datoteke je:

```
server {
 listen      80;
 server_name librenms.example.com;
 root        /opt/librenms/html;
 index       index.php;
 charset utf-8;
 gzip on;
 gzip_types text/css application/javascript
text/javascript application/x-javascript image/svg+xml
text/plain text/xsd text/xsl text/xml image/x-icon;
 location / {
  try_files $uri $uri/ /index.php?$query_string;
 }
 location ~ [^/]\.php(/|$) {
  fastcgi_pass unix:/run/php-fpm-librenms.sock;
  fastcgi_split_path_info ^(.+\.php)(/.+)$;
  include fastcgi.conf;
```

```
 }
 location ~ /\.(?!well-known).* {
  deny all;
 }
}
```

Zatim, sljedećom naredbom, uklanja se zadana stranica koja dolazi s ngnix poslužiteljem:

```
rm /etc/nginx/sites-enabled/default
```

U datoteci „librenms.conf“ server_name se mijenja imenom poslužitelja i web poslužitelj se ponovno pokreće, kao i php-fpm:

```
systemctl restart nginx
systemctl restart php7.4-fpm
```

3.3.4. Konfiguracija snmpd usluge

SNMP poslužitelj je već instaliran zajedno sa svim ostalim paketima potrebnim na sustavu. U konfiguracijskoj datoteci /etc/snmp/snmpd.conf definiran je community string. Community string je metoda provjere autentičnosti kojom poslužitelj može dobiti pristup klijentovim podacima. Ako se community string ne podudara, klijent će odbiti vezu i slanje podataka. Nakon postavljanja stringa, potrebno je omogućiti i ponovno pokrenuti snmpd:

```
systemctl enable snmpd
systemctl restart snmpd
```

3.3.5. Definiranje cron zadataka

LibreNMS redovito prikuplja podatke od klijenata. Cron izvršava zadatke u određenom vremenu ili intervalu. Datoteka s uputama za cron daemon je crontab. Unaprijed pripremljenu crontab datoteku treba kopirati u konfiguracijski direktorij cron.d.

```
cp /opt/librenms/librenms.nonroot.cron
/etc/cron.d/librenms
```

Ovaj cron posao prikuplja podatke od klijenata svakih 5 minuta, ali se može konfigurirati za bilo koji drugi interval. [2]

3.3.6. Web instalacijska procedura

Posljednji korak u instalacijskom postupku LibreNMS-a je pokretanje web instalacijskog programa na adresi http://server.domain.com/install.

Instalacijski program provjerava valjanost instaliranih komponenti (LibreNMS verzija, DB shema, PHP, MySQL, RRDTool i SNMP) što je prikazano na slici 3.2.

Slika 3.2. – Provjera valjanosti komponenti

Ako je sve u redu, program nastavlja na konfiguraciju baze podataka gdje traži prijavu korisnika (Slika 3.3.).

Slika 3.3. – Prozor prijave korisnika u bazu podataka

Nakon konfiguracije, ukoliko je sve točno određeno, stvara se baza podataka na sljedećoj stranici sučelja pritiskom na „Build database“ nakon čega se stvaraju sve tablice.

Na posljednjoj stranici sučelja (Slika 3.4.) prijavljuje se na administratorski račun LibreNMS-a i time je završen instalacijski proces.

Slika 3.4.. – Prijava administratora u LibreNMS

3.4. Dodavanje uređaja

Postoje dvije opcije za dodavanje novog uređaja u LibreNMS. Može se dodati uređaj putem komandne linije ili korištenjem web sučelja.

Pomoću web sučelja odlaskom na „Devices“ i klikom na „Add device“ otvara se prozor gdje se traže pojedinosti potrebne za dodati uređaj. Unose se podaci za uređaj koji se želi dodati te se potvrđuje klikom na "Add device".

Kao što je prikazano na slici 3.5., potrebno je unijeti ime ili adresu uređaja. Prema zadanim postavkama SNMP verzija je SNMPv2c, što znači da se predefinirano koristi port 161. Te još preostaje community string koji se postavio u instalacijskom procesu LibreNMS-a. Nakon toga, klikom na „Add device“ završeno je dodavanje uređaja putem web sučelja.

Slika 3.5. – Sučelje za dodavanje uređaja

Prema zadanim postavkama za podatke anketiranja koristit će se ime glavnog računala.

Korištenjem komandne linije može se dodati novi uređaj tako da se prijeđe u direktorij instalacije LibreNMS-a i upiše:

```
./lnms device:add yourhostname [--v1|--v2c] [-c
yourSNMPcommunity]
```

Na primjer, ako je uređaj s nazivom „mydevice.example.com“ konfiguriran za korištenje zajednice „my_company“ pomoću snmp v2c tada se unosi:

```
./lnms device:add --v2c -c my_company
mydevice.example.com
```

Da bi se dodalo uređaje u stvarnom okruženju bilo je potrebno promijeniti postavke SNMP-a kao što je prikazano na slikama 3.6. te 3.7.

Slika 3.6. – Web konfiguracija SNMP postavki

Slika 3.7. – Konfiguracija SNMP postavki određenog communitya

3.4.1. Dodavanje uređaja samo za provjeru dostupnosti (ping)

Za nadzor uređaja gdje je samo potrebna provjera dostupnosti (putem ping aplikacije) u LibreNMS sustavu ti se uređaju mogu dodati putem WebUI (User Interface) ili korištenjem CLI (Command Line Interface) tj. sučelja naredbenog retka.

Prilikom dodavanja uređaja preko WebUI SNMP gumb prebacuje se na "isključeno". Uređaj će biti dodan u LibreNMS kao uređaj samo za ping i pokazat će ICMP Response Graph.

Otvara se prozor prikazan na slici 3.8. koji zahtijeva unos određenih podataka za dodati uređaj, od kojih su najvažniji:

- IP adresa ili DNS ime.
- Hardver: Možete upisati što god želite (opcionalno).
- OS: Ovo će dodati ikonu OS uređaja (opcionalno).

3.8. – Sučelje za dodavanje uređaja za ping

Preko komandne linije se to se radi pomoću naredbe:

```
./lnms device:add [-P|--ping-only] yourhostname
```

3.4.2. Automatsko otkrivanje uređaja

Nakon što je dodan bar jedan uređaj, LibreNMS pruža mogućnost automatskog dodavanja uređaja na vašoj mreži, što se može učiniti putem nekoliko metoda. To je jedna od najvažnijih značajki LibreNMS-a.

Sve omogućene metode otkrivanja pokreću se kada se pokrene otkrivanje (svakih 6 sati prema zadanim postavkama i unutar 5 minuta za nove uređaje). Važno je napomenuti da se treba dodati najmanje jedan uređaj prije nego što automatsko otkrivanje počne raditi.

Za automatsko dodavanje uređaja moraju se znati snmp detalji. Primjeri informacija koje se moraju znati za SNMP v1, v2c i v3 su sljedeći:

```
// v1 or v2c

$config['snmp']['community'][] = "my_custom_community";

$config['snmp']['community'][] = "another_community";

// v3

$config['snmp']['v3'][0]['authlevel'] = 'authPriv';

$config['snmp']['v3'][0]['authname'] = 'my_username';

$config['snmp']['v3'][0]['authpass'] = 'my_password';

$config['snmp']['v3'][0]['authalgo'] = 'SHA';

$config['snmp']['v3'][0]['cryptopass'] = 'my_crypto';

$config['snmp']['v3'][0]['cryptoalgo'] = 'AES';
```

Ovi će se detalji pokušati dodati prilikom dodavanja uređaja, moguće je navesti bilo koju njihovu kombinaciju.

Da bi se dodalo uređaje, mora se znati koje su podmreže ovlaštene kako se ne bi slijepo pokušalo dodati uređaje koji su pod tuđom kontrolom.

```
$config['nets'][] = '192.168.0.0/24';

$config['nets'][] = '172.2.4.0/22';
```

Ukoliko unutar mreže, koja je dodana kao što je objašnjeno iznad, postoji jedan uređaj koji se ne može ili ne želi automatski dodati, tada se to isključuje na sljedeći način:

```
$config['autodiscovery']['nets-exclude'][] =
'192.168.0.1/32';
```

Prema zadanim postavkama LibreNMS ne dodaje uređaje prema IP adresi nego traži da se pronađe obrnuto ime DNS-a i dodaje s njim. U dodatnim postavkama je to promijenjeno i postavljeno da se uređaji dodaju prema IP adresi.

Također LibreNMS zahtijeva jedinstvena imena prilikom dodavanja uređaja (što vraćaju uređaji preko SNMP-a). Ukoliko se želi dopustiti dodavanje uređaja s dvostrukim imenima također se može dozvoliti naredbom:

```
$config['allow_duplicate_sysName'] = true;
```

Ima više metoda za automatsko otkrivanje uređaja. Svaka metoda se može omogućiti ili onemogućiti i može imati dodatne opcije konfiguracije.

Kratak opis metoda:

- ARP (onemogućen) – Dodaju se uređaju koji su navedeni u ARP tablici drugog uređaja. Ovaj modul ovisi o tome je li modul arp-table omogućen i vraća li podatke.
- XDP (omogućen) - XDP veze sa susjedima uvijek su otkrivene ako je omogućen modul otkrivanja. LibreNMS dodaje samo one uređaje otkrivene pomoću XDP kojima je modul omogućen.
- OSPF (Open Shortest Path First) - Omogućen po zadanim postavkama. Uređaji razmjenjuju informacije sa svojim najbližim susjedima, po kojima se tim redoslijedom i dodaju.
- BGP (Border Gateway Protocol) - Omogućen po zadanim postavkama. Razmjena informacija o usmjeravanju i dostupnosti odvija se među rubnim usmjernicima.
- SNMP Scan - LibreNMS proaktivno skenira mrežu za uređaje s omogućenim SNMP-om koristeći konfiguriranu verziju. SNMP Scan skenira mreže prema zadanim postavkama i poštuje koje mreže su isključene iz pretrage.

Novootkriveni uređaji bit će dodani u „default_poller_group“, ova vrijednost je zadana na 0 ako nije postavljena.

3.4.3. Grupiranje uređaja

LibreNMS podržava grupiranje uređaja na sličan način kao i konfiguriranje upozorenja. Kod dinamičkih grupa pravilo se temelji na MySQL strukturi u kojoj se nalaze

podaci. Ako se zna što se traži može se pregledati unutar MySQL-a koristeći „show tables“. Najčešća grupiranja su po nazivu glavnog računala ili prema vrsti uređaja.

Također se stvaraju statične grupe (koje se mogu pretvoriti u dinamičke) da bi se određene uređaje stavili u grupu. Samo treba za vrstu odabrati statički te dodati željeni uređaj u grupu. Tada možete odabrati tu grupu s veze „Uređaji“ -> „Svi uređaji“ u navigaciji na vrhu. Također možete koristiti grupu za mapiranje pravila upozorenja. Na slici 3.9. je prikazan prozor za dodavanje nove grupe uređaja te svi podaci potrebni za unos pri dodavanju.

Slika 3.9. – Sučelje za kreiranje nove grupe uređaja

3.5. Sučelje LibreNMS-a

LibreNMS nadzorna ploča je prvo što je prikazano nakon instalacije programa. Ploča je skoro u potpunosti prazna, jedino što se pojavljuje na njoj je blok na kojem su upute za uređivanje nove ploče. Stvorene su prilagođene nadzorne ploče u LibreNMS-u po odabiru korisnika. Nadzorne ploče mogu se dijeliti s drugim korisnicima. Također se može napraviti prilagođena nadzornu ploču koja će biti postavljena kao zadana ploča za sve korisnike u LibreNMS-u.

Postoji više dopuštenja nadzorne ploče:

1. Privatno: Nadzorna ploča koju može pregledavati i uređivati samo korisnik koji je stvorio.
2. Zajedničko čitanje: Nadzorna ploča koja je vidljiva i drugim korisnicima kojima je onemogućeno raditi promjene na njoj.
3. Dijeljeno: Nadzorna ploča koja omogućuje svim korisnicima pregled te uređivanje.

Nakon su odabrana dopuštenja nadzorne ploče postavljena je određena globalna nadzorna ploča za sve korisnike. To se izvršava u postavkama korisničkog sučelja odlaskom na postavke nadzorne ploče i postavljajući je kao globalnu.

LibreNMS bogat je raznovrsnim mogućnostima konfiguracije po potrebi i želji korisnika. U konfiguraciji nadzorne ploče korisnik može birati između mnogo različitih widgeta (blokova). Widget je dodatna značajka ili proširenje softverskog programa (grafičkog sučelja ili web stranice) koja omogućuje dodatne značajke. Osmišljen je kako bi poboljšao korisničko iskustvo. Pojavljuje se u više oblika kao što su dijaloške kutije, privremeni prozori, padajući izbornici, ikone, prozori, vrpce za pomicanje stranice itd.

Prelaskom u način uređivanja na ploču dodajemo bilo koji od mnogih ponuđenih blokova. Neki od značajnijih blokova su:

- Availability Map (Mapa dostupnosti)

Slika 3.10. - Availability Map - Mapa koja prikazuje sve dodane uređaje i dijeli ih prema njihovom stanju: gore (zeleno), dolje (crveno) i upozorenje (narančasto)

Ovom bloku, kao i svakom drugom, može se promijeniti ime. Uz to, u dodatnim postavkama može se: promijeniti izgled prikaza polja iz kvadrata u kompaktni

izgled bez imena, grupirati po grupi uređaja, promijeniti parametar koji se gleda za raspored uređaja te promijeniti interval osvježavanja bloka u slučaju dodavanja novog uređaja (što je po zadanim postavkama postavljeno na 60 sekundi).

- Top Devices (Najbolji uređaji)

Slika 3.11. - Najbolji uređaji po upitu administratorovog izbora

Određuje se broj najboljih uređaja koje se želi promatrati zatim se za kriterij uzima jedan od sljedećih izbora: količina prometa (traffic), vrijeme od zadnjeg pokretanja (uptime), količina iskorištene memorije (memory usage), količina iskorištenog diska (disk usage), vrijeme odziva (response time), duljina trajanja poziva (poller duration), opterećenje procesora (processor load).

- Server Stats (Statistika poslužitelja)

Slika 3.12. – Izgled bloka statistike poslužitelja za uređaj localhost

Prikazuju se indikatori upotrebe CPU-a, memorije i pohrane. Uređaj mora biti naveden kao poslužitelj da bi se mogao dodati u ovaj blok. Svaki blok prikazuje samo za jedan, odabrani uređaj. Može se birati u koliko stupaca će se podaci prikazivati, što je ovdje izabrano u 3. Također, ime bloka je opcionalno, a po zadanim postavkama je „ime uređaja“ + „Stats“.

- Eventlog (Dnevnik događaja)

Slika 3.13. - Prikaz svih događaja uređaja i LibreNMS-a koji se mogu konfigurirati po vrsti uređaja i po vrsti događaja.

- Alerts (Upozorenja)

Slika 3.14. - Prikazuje sve obavijesti upozorenja

U postavkama se može promijeniti da prikazuje ovisno o ozbiljnosti upozorenja (ok, warning, critical). Također se može pretražiti određena obavijest.

Preostali blokovi koje administrator ili korisnik mogu dodati su:

- Component Status - Navodi status "normalan", status "upozorenje" i "kritičan" status svih komponenti.

- Device Summary Horizontal - Popis ukupnog broja uređaja, gore, dolje, zanemareni i onemogućeni.

- Device Summary Vertical – Popis ukupnog broj uređaja, gore, dolje, zanemareni i onemogućeni.

- External Images - Može se koristiti za prikaz vanjskih slika na nadzornoj ploči. Ili slike iz LibreNMS-a.

- Globe map - Prikazuje kartu globusa.

- Grafika - Može se koristiti za prikaz grafike u uređaju.

- Graylog - Prikazuje sve unose dnevnika sustava Graylog. Koristi se za html oznake, ugrađene veze i vanjske web stranice.

- Syslog - Prikaz svih unosa u zapisnik sustava.

- World map - Prikazuje lokacije svih vaših uređaja.

- Device Types - Sortira uređaje po vrstama.

- Top interfaces - Navodi najbolja sučelja prema korištenju prometa.

Nakon konfiguriranja i dodavanja svih željenih uređaja, LibreNMS nadzorna ploča prikazuje sve dodane uređaje. Uređaji se automatski dijele na odjeljke:

- Mrežni (sadrži prospojnike, usmjernike, vatrozide)
- Poslužitelj (sadrži Linux i Windows poslužitelje)
- Bežični (sadrži bežični LAN kontroler, budući da se pristupne točke u mreži konfiguriraju od strane kontrolera i ne mogu se konfigurirati pojedinačno).

U pregledu su prikazana platforma uređaja, operativni sustav i vrijeme rada. Kada je uređaj odabran, prikazuju se informacije o njemu. Ako je uređaj prospojnik, glavne informacije koje se prikazuju su pregled prometa, stanja portova, VLAN podaci, susjedi i STP informacije. Ako je uređaj poslužitelj, grafovi resursa sustava su fokus podataka.

Svaki dio se može dodatno proširiti, npr. blok Processors na naslovnoj stranici pregleda uređaja prikazuje opterećenje procesora tijekom posljednja 24 sata, ali kada se klikne na njega, mogu se odabrati razdoblja od 6, 24, 48 sati, jedan ili dva tjedna, jedan ili dva mjeseca i jedne ili dvije godine. Isto vrijedi i za memorijski blok. Drugi važan podatak je status prostora za pohranu, podijeljen po particijama. Ove informacije mogu biti vrlo korisne u planiranju resursa, jer mogu pokazati trend potrošnje resursa omogućavajući procjenu kada bi nadogradnja hardvera mogla biti potrebna ili kada bi se trebao nabaviti novi uređaj. [6]

Slika 3.15. – Izgled nadzorne ploče LibreNMS-a instaliranog u virtualnoj okolini

3.6. Sustav obavještavanja

Postoji više načina da alati za praćenje mrežnog prometa kao dio sustava za nadzor mreže mogu upozoriti administratore na probleme u izvedbi i sigurnosti koji mogu naštetiti mreži. Okidači su događaji koji će generirati alarme u sustavu. Događaj se može odnositi na odstupanje od srednje vrijednosti parametra ili vrijednost parametra prijeđenog praga.

Kršenja praga generiraju većinu upozorenja, ali korisnici također mogu postaviti monitor mrežne aktivnosti da generira upozorenja na temelju vremenskih kašnjenja ili broja ponavljanja kršenja praga. Na primjer, sustav za praćenje i održavanje mreže može se konfigurirati tako da ne generira upozorenje ako je prag probijen, sve dok se ne probije dvaput u 15 minuta. Slično, upozorenje se može generirati nakon što se početno kršenje praga vrati na svoju osnovnu vrijednost ili se poništi.

Prvo određujemo neka pravila upozorenja koja će reagirati na promjene na uređajima prije podizanja upozorenja. Nakon toga govorimo LibreNMS-u kako da izda obavijest kada se pojavi upozorenje, što se radi pomoću „Alert Transports“. Sljedeći korak je stvaranje prilagođenih predložaka upozorenja koja pomažu da se maksimalno iskoristi prednosti sustava upozorenja. Iako se uključuje zadani predložak upozorenja, ograničen je u podacima koji se primaju u upozorenjima. [3]

Pravila su definirana pomoću logičkog jezika. GUI (Graphical User Interface) odnosno grafičko sučelje pruža jednostavan način stvaranja pravila. Stvaranje složenijih pravila koja mogu uključivati matematičke izračune i MySQL upite omogućeno je pomoću makronaredbi.

Pravila se moraju sastojati od najmanje 3 elementa: entiteta, uvjeta i vrijednosti. Vrijednosti mogu biti entitet ili bilo koji podatak. Entiteti se temelje na nazivima tablica i stupaca unutar baze podataka.

Ovo su druge dostupne opcije prilikom dodavanja pravila upozorenja:

- Rule name (Naziv pravila): Naziv povezan s pravilom.
- Severity (Ozbiljnost): Koliko je pravilo "važno".
- Max alerts (Maksimalni broj upozorenja): Najveći broj upozorenja poslanih za događaj. -1 znači neograničeno.
- Delay (Odgoda): Količina vremena u sekundama za čekanje nakon podudaranja s pravilom prije slanja upozorenja putem prijenosa.
- Interval: Vremenski interval u sekundama između upozorenja za događaj do postizanja maksimalnog upozorenja.
- Mute alerts (Isključi upozorenja): Onemogućuje slanje pravila upozorenja putem prijenosa upozorenja, ali i dalje će prikazivati upozorenje u web sučelju.
- Recovery alerts (Upozorenja o oporavku): Onemogućuje slanje obavijesti o oporavku ako je isključeno.

Kada se upozorenje aktivira, prikaže se na stranici Upozorenja u obliku obavijesti unutar web sučelja. Taj popis ima nekoliko dostupnih opcija. Ovaj stupac pruža pregled statusa upozorenja. Ikone statusa upozorenja su:

Slika 3.16. - Ovo upozorenje je trenutno aktivno i šalje upozorenja [3]

Slika 3.17. - Ovo upozorenje trenutno je potvrđeno dok se upozorenje ne očisti [3]

Slika 3.18. - Ovo upozorenje trenutno se potvrđuje sve dok se upozorenje ne pogorša ili ne poboljša, u kojoj će fazi biti automatski poništeno i upozorenja će se nastaviti [3]

Slika 3.19. - Ova ikona omogućuje pristup potvrđenim odnosno nepotvrđenim bilješkama za ovo upozorenje [3]

Klikom na bilo koju od ovih ikona upozorenja potvrđuje se upozorenje.

Najjednostavniji način testiranja hoće li pravilo upozorenja odgovarati uređaju je odlazak na uređaj, klik na „Uredi“, odabir „Snimanje“. Na tom novom zaslonu odabirom „Upozorenja“ i klikom „Pokreni“. Izlaz kruži kroz sva upozorenja primjenjiva na uređaj i pokazuje naziv pravila, samo pravilo, MySQL upit i podudara li se pravilo.

Za uređaj je moguće postaviti jednog ili više roditeljskih uređaja. Cilj je da ako svi roditeljski uređaji ne rade, kontakti s upozorenjem neće primati suvišna upozorenja za ovisne uređaje. Ovo je vrlo korisno kada se dogodi prekid rada gdje se inače zaprime stotine upozorenja, ali kad je ovo ispravno konfigurirano, stižu upozorenja samo za nadređene tj. roditeljske uređaje.

Postoje tri načina za konfiguriranje ove značajke. Prvi je iz općih postavki uređaja. Druge dvije izvršavaju se u stavci „Ovisnosti uređaja“ u izborniku „Uređaji“. Na ovoj stranici se vide svi uređaji i njihovi roditelji. Klikom na ikonu „bin“ briše se postavka ovisnosti. Klikom na ikonu „pen“ uređuje se ili mijenja trenutna postavka za odabrani uređaj.

Slika 3.20. – Sučelje za uređivanje ovisnosti uređaja

Na vrhu se nalazi i gumb "Upravljanje ovisnostima uređaja". To omogućuje postavljanje roditelja za više uređaja odjednom (prikazano na slici 3.6.6.).

Slika 3.21. – Sučelje za postavljanje ovisnosti za više uređaja

3.6.1. Postavljanje sustava obavještavanja

U općim postavkama LibreNMS-a odlaskom na „Alerting“ postavljen je sustav za obavještavanje na e-mail, tj. elektroničku poštu. U zadanim postavkama upozorenja omogućeno je obavještavanje na e-mail, nakon čega se unose e-mail na koji se šalju notifikacije, te se postavlja enkripcija (izabrana je TLS – Transport Layer Security enkripcija). SMPT autentikacija je također omogućena.

Slika 3.22. – Sučelje za konfiguraciju upozorenja

Pri konfiguraciji odgoda tj. delay je promijenjena na 0 tako da notifikacije stižu čim se dogode. Ako uključimo opciju „Mute alerts“ upozorenja će biti vidljiva samo na korisničkom sučelju nadzorne ploče u bloku „Upozorenja“, što znači da se notifikacije na e-mail neće slati. Značajka „Recovery alerts“ je također omogućena. Ona šalje notifikaciju ukoliko je došlo do oporavka kvara koji je uzrokovao upozorenje.

3.7. Privatnost

Cijeli kod koji obrađuje podatke i šalje ih uključen je u standardnu LibreNMS instalaciju. Kod koji prihvaća podatke i zauzvrat generira grafikone je otvorenog koda i dostupan je svima na GitHubu. Slobodan je svima za pregled, komentar i prijedlog izmjene ili poboljšanja.

Postavke podataka:

- Svi podaci su anonimni.
- Statistike su preuzete iz baze podataka, a uključuju stvari kao što su broj uređaja, tip uređaja, operacijski sustav uređaja, tipovi, brzine i broj portova.
- sysDescr i sysObjetID s uređaja s malim količinama, da bi se spriječilo slanje stvari poput imena hosta.
- Bilježe se brojevi verzija php-a, MySQL-a, net-snmp-a i rrdtool-a
- Prilikom instalacije se generira nasumični UUID (Univerzalni jedinstveni identifikator).
- IP nije zabilježen, čak ni putem web usluge LibreNMS-a koja prihvaća podatke.

LibreNMS sprema podatke, no ne predugo. Trenutno na 3 mjeseca, iako bi se to u budućnosti moglo promijeniti. Koristi ih za pomoć u određivanju prioriteta problema i značajki na kojima treba raditi. Podaci se šalju jednom dnevno putem crona. Ako se cron onemogući, uključivanje značajke neće imati nikakvog utjecaja. Ne mogu se vidjeti neobrađeni podaci, ali LibreNMS uspoređuje sve podatke zajedno i pruža dinamičnu web-lokaciju tako da se mogu vidjeti rezultati svih pridonesenih statistika. Ako korisnik nije zadovoljan ovim postavkama uvijek može isključiti sustav za povratne informacije.

4. ZAKLJUČAK

Zahvaljujući internetu povezanost svijeta je sve veća i veća iz dana u dan. Uz sve veće napretke tehnologije dolazi do širenja količine podataka do onih razina koje čovjek ne može sam nadzirati. Napredak sigurnosnih sustava uz ostale komponente digitalnog svijeta je neizbježan. Sustavi za nadzor već su dokazali i nastavljaju dokazivati da su jedan od glavnih linija obrane od napada, od samih grešaka sustava koji nadziru te od ljudske pogreške. Većina poslovanja danas ovisi o upravljanju mrežom te njihovim web stranicama. Današnje mreže mogu biti zapanjujuće u svojoj složenosti. Usmjernici, prospojnici i čvorišta povezuju mnoštvo radnih stanica s kritičnim aplikacijama na bezbroj poslužitelja i s Internetom. Instalirani su brojni sigurnosni i komunikacijski uslužni programi i aplikacije, uključujući vatrozid, virtualne privatne mreže (VPN) te filtere neželjene pošte i virusa. Upravljanje mrežom nije ograničeno samo na određene industrije ili samo na velika javna poduzeća. Razumijevanje sastava i složenosti mreže i sposobnost da se ostane informiran o tome kako svi pojedinačni elementi rade u bilo kojem trenutku, ključni je čimbenik uspjeha u održavanju performansi i integriteta mreže. Administratori moraju znati što se događa na njihovim mrežama u svakom trenutku, uključujući podatke u stvarnom vremenu i povijesne informacije o upotrebi, izvedbi i statusu svakog uređaja, aplikacije i svih podataka na mreži. To čini sustave za nadzor poput LibreNMS-a neophodnim.

LibreNMS pruža sve te potrebe korisnicima. Činjenica da je besplatan svima na korištenje te da je otvorenog koda je samo dodatan bonus jer to znači da više ljudi može pridonijeti poboljšanju aplikacije. Jednostavno korisničko sučelje koje pruža raznovrsne alate koji prikazuju mnogo informacija još je jedna od prednosti LibreNMS-a. Uz sve to navedeno, odličan sustav obavještavanja čini ga jednim od najboljih sustava za nadzor mreže danas.

U samom radu je obrađen osnovni protokol koji se koristi za nadzor mreža i uređaja (SNMP). Detaljno je prikazan postupak instalacije i konfiguracije LibreNMS sustava za nadzor, kao i dodavanje uređaja u sustav nadzora. Prikazane su najbitnije funkcionalnosti sustava, te prednosti koje sustav pruža administratorima.

5. LITERATURA

[1] Douglas R. Mauro, Kevin J. Schmidt, Essential SNMP, Second Edition, O'Reilly Media (2005)

[2] https://docs.librenms.org/Installation/Install-LibreNMS/ (zadnje posjećeno 30.07.2022.)

[3] https://docs.librenms.org/Alerting/ (zadnje posjećeno 30.07.2022.)

[4] https://www.tek-tools.com/network/an-introduction-to-network-monitoring (zadnje posjećeno 22.06.2022.)

[5] https://www.datavail.com/blog/the-advantages-of-mariadb-platform-for-analytics/ (zadnje posjećeno 27.06.2022.)

[6] L. Sartori, N. Grgić, B. Džaja „Installing and configuring an opensource network monitoring system on a university campus network", CIET, Valencia, Spain, 2022, pp. 767-779.