Usporedna analiza programske podrške za nadzor mrežnih uređaja

Bužanić, Zvonimir

Undergraduate thesis / Završni rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:428357

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**

Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Zvonimir Bužanić

USPOREDNA ANALIZA PROGRAMSKE PODRŠKE ZA NADZOR MREŽNIH UREĐAJA

ZAVRŠNI RAD

Zagreb, 2022.

Sveučilište u Zagrebu
Fakultet prometnih znanosti

ZAVRŠNI RAD

USPOREDNA ANALIZA PROGRAMSKE PODRŠKE ZA NADZOR MREŽNIH UREĐAJA

COMPARATIVE ANALYSIS OF NETWORK MONITORING TOOLS

Mentor: izv. prof. dr. sc. Ivan Grgurević

Student: Zvonimir Bužanić
JMBAG: 1192010413

ZAGREB, svibanj 2022.

USPOREDNA ANALIZA PROGRAMSKE PODRŠKE ZA NADZOR MREŽNIH UREĐAJA

SAŽETAK

Kroz prikaz načina rada, podjelu računalnih mreža i osnovnih mrežnih protokola prikazani su temelji mreže svih mreža, Interneta. Ipak, sve veći broj mrežnih uređaja unosi dodatnu nesigurnost kao i nestabilnost same mreže te ih je poželjno nadzirati kako bi se povećala dostupnost mreže, a i samih mrežnih uređaja. Nadzor mrežnih uređaja je moguće obavljati raznim standardiziranim protokolima za prikupljanje podataka mrežnih uređaja. Usporednom analizom programske podrške za nadzor mrežnih uređaja prikazan je detaljan proces instalacije i konfiguracije Nagios-a kao i Zabbix-a te koja razina „znanja“ je potrebna za korištenje i upravljanje programskom podrškom za nadzor, potrebne hardverske i softverske resurse kao i mogućnosti programske podrške za nadzor.

KLJUČNE RIJEČI: nadzor, računalna mreža, mrežni uređaji, programska podrška, usporedna analiza, snmp, wmi, zabbix, nagios, sustavi za nadzor mrežnih uređaja

SUMMARY

Through the presentation of the mode of operation, the division of computer networks and basic network protocols, the foundations of the network of all networks, the Internet, are presented. However, an increasing number of network devices introduce additional uncertainty as well as instability of the network itself, and it is desirable to monitor them in order to increase the availability of the network and the network devices themselves. Monitoring of network devices can be performed by various standardized protocols for data collection of network devices. A comparative analysis of software tools for monitoring network devices shows the detailed process of installation and configuration of Nagios and Zabbix, and what level of "knowledge" is required to use and manage software monitoring tools, required hardware and software resources and software capabilities monitoring tools.

KEYWORDS: monitoring, computer network, network devices, software, programs, comparative analysis, snmp, wmi, zabbix, nagios, software tools for monitoring network devices

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 4. travnja 2022.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Računalne mreže**

ZAVRŠNI ZADATAK br. 6813

Pristupnik: **Zvonimir Bužanić (1192010413)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Usporedna analiza programske podrške za nadzor mrežnih uređaja**

Opis zadatka:

U završnom radu je potrebno prikazati način rada i podjelu računalnih mreža. Opisati načine prikupljanja podataka o radu određene vrste računalne mreže. Prikupiti podatke o radu i funkcionalnosti programske podrške i mrežnih uređaja. Prikazati i opisati sustave za nadzor mrežnih uređaja. Napraviti usporednu analizu programske podrške za nadzor mrežnih uređaja (primjerice PRTG, Nagios XI, SpiceWorks, Zabbix i dr.).

Mentor:

izv. prof. dr. sc. Ivan Grgurević

Predsjednik povjerenstva za završni ispit:

Sadržaj

1. Uvod 6

2. Računalne mreže 8

2.1. Referentni model Open Systems Interconnection 11
2.2. Referentni model TCP/IP 13

3. Mrežni protokoli za prikupljanja podataka 15

3.1. Simple Network Managment Protocol (SNMP) 16
3.2. Internet Control Protocol Message (ICMP) 18
3.3. Windows Management Instrumentation (WMI) 19
3.4. Extendible Markup Language-Remote Procedure Call (XML-RPC) 22

4. Programska podrška za nadzor mrežnih uređaja 23

4.1. Zabbix 26
4.1.1. Mogućnosti Zabbix-a 26
4.1.2. Instalacija Zabbix-a 27
4.1.3. Administracija Zabbix korisnika i grupa 32
4.1.4. Dodavanje mrežnih uređaja u Zabbix 33
4.1.5. Detekcija i prikaz grešaka mrežnih uređaja - Zabbix 35
4.1.6. Slanje obavijesti o greškama – Zabbix 36
4.1.7. Pregled i izrada izvještaja - Zabbix 37
4.1.8. Nadogradnja Zabbix-a 38
4.2. Nagios XI 39
4.2.1. Mogućnosti Nagios XI-a 39
4.2.2. Instalacija Nagios-a 40
4.2.3. Administracija Nagios korisnika 43
4.2.4. Postupak dodavanje mrežnih uređaja u Nagios 44
4.2.5. Detekcija i prikaz grešaka mrežnih uređaja u Nagios-u 45
4.2.6. Slanje obavijesti o greškama u Nagios-u 47
4.2.7. Pregled i izrada izvještaja u Nagios-u 49
4.2.8. Nadogradnja Nagios-a 49

5. Usporedba programske podrške za nadzor mrežnih uređaja 51

6. Zaključak 56

Popis literature 57

Popis ilustracija 59

Popis tablica 61

Popis kratica 62

1. Uvod

Od početka stvaranja prvih mreža koje su prerasle u današnji Internet, mreže su doživjele značajne promjene. Počevši od načina njihovog povezivanja, načina i vrste komunikacije između njih, do vrste veza i konačno današnje potrebe da se Internetom prenese praktički svaki oblik komunikacije bez obzira bio on podatak, govor ili video. Kako je Internet globalan, korisnici moraju imati mogućnost neprekidno pristupati mrežnim servisima putem definiranih standardnih protokola kao što su HTTP, SMTP, FTP, IMAP i drugi. Takvi zahtjevi uzrokovali su od proizvođača da ugrade podršku za nadzor u svoje uređaje i ponude rješenja za nadzor koja vrlo često nisu kompatibilna sa uređajima drugih proizvođača. Ipak, zahvaljujući otvorenim standardima većinu uređaja je moguće nadzirati sa jednog centralnog mjesta.

Današnji Internet servisi sposobni su godinama raditi pouzdano i bez grešaka, i vrlo često koriste ravnomjerno opterećenje poslužitelja za raspodjelu zahtjeva (engl. *load balancing*), redundantnost poslužitelja na geografski odvojenim lokacijama, neizostavno dnevno, tjedno i mjesečno sigurnosno arhiviranje (eng. *backup*) i brojne druge tehnologije i načine da ti sustavi budu neprekidno raspoloživi.

Ipak, potrebno je obratiti posebnu pažnju kada dođe do neočekivane greške ili značajnog opterećenja mrežnih uređaja kako bi primjerice aktivni, aktivno-pasivni način rada, raspodjela zahtjeva i redundantnost besprekidno radili, a mrežni podaci uvijek bili dostupni korisniku/klijentu. Iz tog razloga stvorene su brojne programske podrške za nadzor koje olakšavaju nadzor mrežnih uređaja pomoću otvorenih standarda (protokola) kao SNMP, ICMP, WMI, JMX i drugi.

Sistem administratori mogu koristiti mnogobrojnu programsku podršku za nadzor mrežnih uređaja, a u ovom završnom radu usporedno će se analizirati dvije programske podrške za nadzor koje su dostupne besplatno (uz ograničenja) i vrlo popularne među administratorima: Zabbix i Nagios XI. Svaki sistem administrator današnjice susresti će se s nekom vrstom mrežnog nadzora, bila ona centralizirana ili usmjerena na određeni mrežni segment tj. područje nadzora poput printera, mrežnih usmjerivača, bežičnih pristupnih točaka ili poslužitelja te je svrha ovog rada prikazati koliko je komplicirano koristiti programsku podršku za nadzor mrežnih uređaja, koji su hardverski/softverski zahtjevi za instalaciju i na kraju kako i zašto nadzirati mrežne uređaje tom programskom podrškom.

Programska podrška Zabbix i Nagios XI postoji preko petnaestak godina i sadrži značajnu količinu mogućnosti te će se ovim radom opisati otvoreni standardi koji će se koristiti u analizi programske podrške i testirati osnovne funkcionalnosti na primjeru nadzora jednog mrežnog printera i MikroTik RB2011 usmjerivača, Linux CentOS 7 i Windows 2012 poslužitelja te Windows 8.1 desktop računala kako bi mogli usporediti prednosti i nedostatke.

Cilj završnog rada je provesti usporednu analizu programske podrške za nadzor mrežnih uređaja kroz instalaciju, konfiguraciju, mogućnosti, jednostavnost korištenja i konačno sama korisnost upotrebe programske podrške za nadzor mrežnih uređaja kroz šest poglavlja:

1. Uvod
2. Računalne mreže
3. Mrežni protokoli za prikupljanje podatka
4. Programska podrška za nadzor mrežnih uređaja (Zabbix i Nagios XI)
5. Usporedba programske podrške za nadzor mrežnih uređaja
6. Zaključak

Uvod opisuje potrebe mrežnih sustava današnjice i njihovog nadzora pomoću identičnih programske podrške radi bolje dostupnosti te kvalitetne i pravovremene podrške sistem administratora mrežnom sustavu ili mrežnim elementima.

Drugo poglavlje prolazi kroz osnove računalnih mreža, podjelu prema vrsti mreže, načinu komunikacije, temeljne modele komuniciranja i prikazuje bazični primjer nadzora mrežnih uređaja.

U trećem poglavlju obrađena je problematika nadzora različitih mrežnih uređaja, te na koji način ih je sve moguće nadzirati obzirom na problem nemogućnosti centralnog nadzora zbog zatvorenih standarda od strane proizvođača te nekompatibilnosti s ostalim proizvođačima. Objašnjeni su najčešće korišteni mrežni protokoli za prikupljanje podataka s mrežnih uređaja kao što su SNMP, ICMP i WMI.

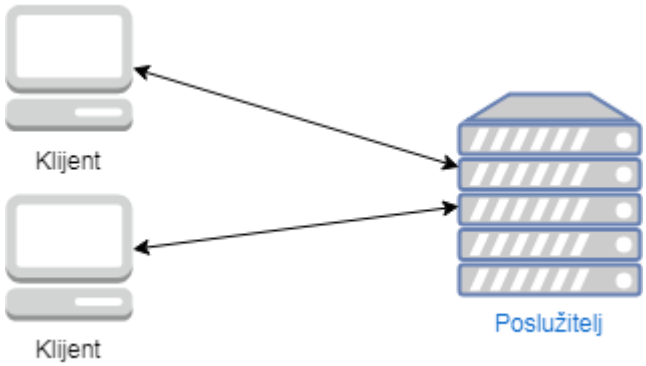
Četvrto poglavlje opisuje povijest programske podrške Zabbix i Nagios XI te princip rada oba. Zatim se opisuje postupak njihove instalacije, konfiguracije, mogućnosti i primjer podešavanja nadzora mrežnih uređaja za potrebe ovog završnog rada.

Usporedba programske podrške za nadzor mrežnih uređaja, tj. prednosti i mane opisani su u četvrtom poglavlju.

Završno poglavlje donosi zaključak o dvije uspoređene programske podrške za nadzor mrežnih uređaja kao i odgovor na pitanje je li takva programska podrška doista potrebna sistem administratorima i u kojim slučajevima.

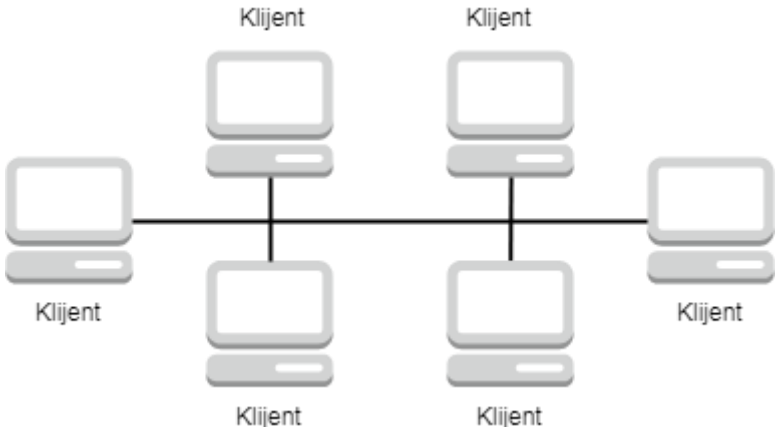
2. Računalne mreže

Računalnu mrežu čine minimalno dva povezana mrežna uređaja, pri tome je jedan mrežni uređaj klijent koji preuzima ili šalje podatke prema drugom mrežnom uređaju, najčešće mrežnom poslužitelju koji je dediciran za takav način pristupa i uvijek dostupan klijentu (Slika 1.). Takav način mrežne strukture poznat je kao klijent-poslužitelj gdje se svi podaci nalaze na jednom mrežnom poslužitelju ili više njih, ali se način pristupa do podataka ne mijenja za klijente bez obzira o broju poslužitelja [1]. Ovaj način mrežne strukture bit će podloga za ovaj rad obzirom da se Internet bazira upravo na ovakvoj centraliziranoj strukturi. Iako više klijenata pristupa poslužitelju, njegove performanse su značajno veće od klijenta te je u stanju posluživati na tisuće klijenata istovremeno zbog redundantnosti komponenti (napajanje, diskovi, mrežne kartice, i dr.) i stabilnosti te ga je upravo iz tog razloga potrebno konstantno pratiti i nadzirati.



Slika 1. Struktura mreže: klijent-poslužitelj, Izvor: [1]

Postoji i necentralizirana struktura mreže u kojoj se podaci šalju i preuzimaju između više jednakih mrežnih klijentskih uređaja (engl. *peer-to-peer*) [1]. U takvoj mrežnoj strukturi nema poslužitelja tj. svi mrežni klijenti su ujedno i poslužitelji (Slika 2.), a podaci mogu biti na jednom ili na svim uređajima. Kod ovakve strukture potrebno je posebno konfigurirati svaki mrežni uređaj i sigurnost pristupa tom uređaju. Kako dijeljeni podaci nisu centralizirani već se mogu nalaziti na više računala potrebno je znati na kojem klijentu se nalaze koji podaci i kako im pristupiti što otežava administraciju. U ovakvoj mrežnoj strukturi bilo bi potrebno nadzirati sve klijente što značajno komplicira konfiguraciju nadzora i iz tog razloga se ovakvi sustavi najčešće koriste u manjim poduzećima.



Slika 2. Struktura mreže: klijent-klijent, Izvor: [1]

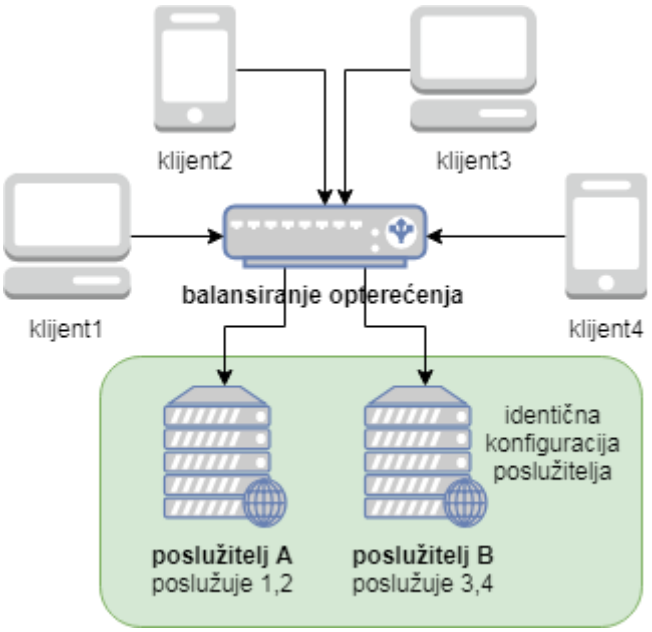
Mreže se mogu podijeliti na osobne mreže (personal area network – PAN), lokalne mreže (engl. *local area network* – LAN) i na mreže koje pokrivaju veća područja (engl. *wide area network* – WAN), na primjer, spajaju dva odvojena ureda, dva grada ili primjerice više država u jednu mrežu [2].

Internet je globalna centralna mreža koja služi za povezivanje više WAN mreža ili na primjer dvije intranet mreže putem virtualne privatne konekcije (engl. *virtual private network* - VPN). Intranet je zapravo lokalna mreža koja oponaša svojstva Interneta, ali do nje nije moguće pristupiti putem Interneta. Na primjer, poslužitelji u intranet mreži su dostupni samo uređajima koji su spojeni na lokalnu intranet mrežu.

U primjerima nadzora mrežnih uređaja koristiti će se lokalna tj. Internet mreža obzirom da se većina poslužitelja nalazi na lokalnoj mreži koja se nadzire, no nekada se određeni mrežni servisi nalaze na udaljenim lokacijama (engl. *cloud*) ili u demilitariziranoj zoni kada je uređaj otežano nadzirati zbog nemogućnosti direktnog pristupa.

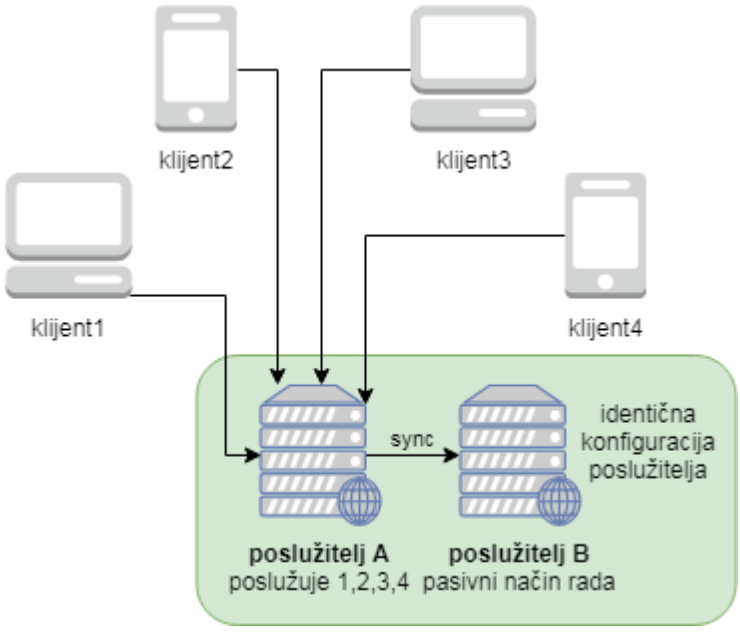
Današnji mrežni sustavi trebaju biti neprekidno dostupni kako bi mogli zadovoljiti brojne zahtjeve koji dolaze sa Interneta, što znači da mrežni sustav mora raditi pouzdano tj. ispravno raditi. Pouzdanost znači da će mrežni sustav raditi zadovoljavajuće unutar promatranog vremenskog razdoblja [4], a pouzdanost možemo povećati na način da u sustavu postoje dva ili više identičnih mrežnih elementa. Sve do sada navedeno označava potrebu za visokom raspoloživošću mrežnog sustava (engl. *high availability*). Postoje aktivni (Slika 3.) i aktivno-pasivni (Slika 4.) načini rada visoko raspoloživog sustava kao i kombinacija oba kod zahtjevnijih mrežnih sustava.

Kod aktivnog načina rada, uređaj za balansiranje opterećenja (engl. *load balancer*) neprekidno provjerava dostupnost oba web poslužitelja i šalje upite prema web poslužitelju ukoliko je on dostupan. Na taj način kada su oba poslužitelja dostupna promet bude ravnomjerno raspoređen između njih. Kada poslužitelj A ne radi, klijenti će i dalje biti posluženi od strane poslužitelja B. U ovom slučaju uređaj za balansiranje opterećenja je kritična točka koja može uzrokovati prekid rada cijelog sustava te je potrebno razmatrati dodavanje redundantnog uređaja ili kombinirati aktivni i aktivno-pasivni način rada.



Slika 3. Aktivni način rada

Kod aktivno-pasivnog načina rada mrežnog sustava, u slučaju greške tj. prestanka rada poslužitelja A, zahtjevi se automatski preusmjeravaju na poslužitelj B. Kada oba poslužitelja rade, podaci se sa poslužitelja A sinkroniziraju na poslužitelj B kako bi u trenutku prekida rada poslužitelja A identični podaci bili dostupni na poslužitelju B.



Slika 4. Aktivno-pasivni način rada

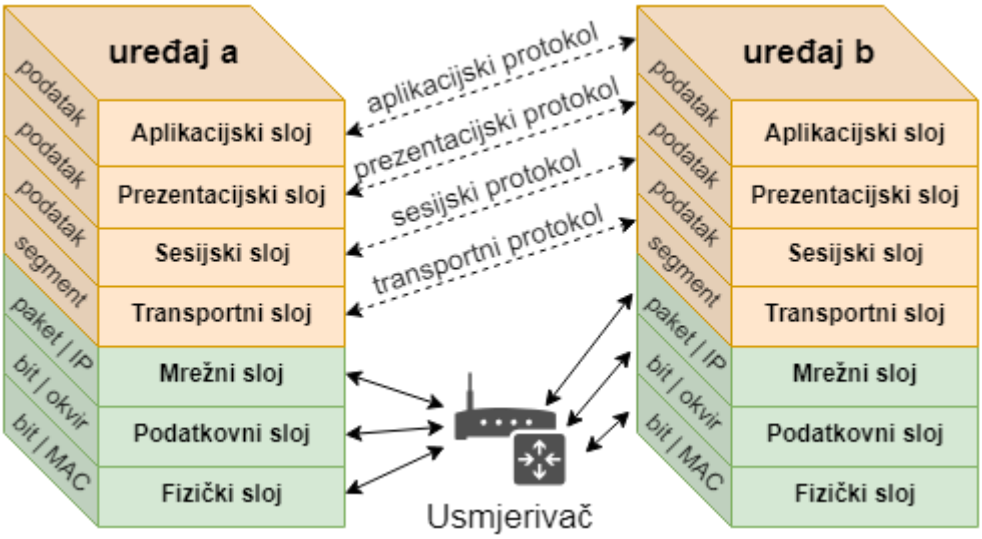
U oba načina rada potrebno je neprekidno nadzirati sustav, detektirati grešku na poslužitelju i obavijestiti administratora o grešci kako bi mogao napraviti provjeru, po potrebi otkloniti kvar ili preusmjeriti promet na redundantni sustav kada grešku/kvar nije moguće otkloniti u kratkom vremenu.

2.1. Referentni model Open Systems Interconnection

U referentnom modelu OSI (engl. *Open Systems Interconnection*) definirano je sedam slojeva i metoda za otvoreno povezivanje mrežnih sustava. Koristi se pri apstraktnom opisu arhitekture mreže koji opisuje komunikaciju hardvera, softvera, programa i aplikacija u mreži te je osnovan od strane ISO (engl. *International Standards Organization*) organizacije [2].

Kako bi mrežna komunikacija sa jednog mrežnog uređaja do drugog bila kompletna, podaci iz jednog mrežnog uređaja putuju iz gornjeg sloja postepeno prema donjim slojevima, zatim kroz medij (žicu ili zrak) i konačno u drugom mrežnom uređaju ponovno putuju kroz donje slojeve postepeno do zadnjeg aplikacijskog.

OSI model sastoji se od sedam slojeva podijeljenih u dvije grupe, gdje prve tri (fizički, podatkovni i mrežni sloj) opisuju metodu po kojoj se obavlja komunikacija između klijenata, a ostali slojevi (transportni, sesijski, prezentacijski i aplikacijski) opisuju proces komunikacije između računala i korisnika, rad korisnika sa aplikacijom i međusobnu komunikaciju između aplikacija (Slika 5.) [1].



Slika 5. Slojevi OSI modela i komunikacija između njih, Izvor: [3]

Fizički sloj definira električne i fizičke specifikacije podatkovne veze tj. vezu između uređaja i fizičkog medija za prijenos podataka uključujući primjerice naponske razine, broj pinova na konektorima, unutarnji otpor, specifikaciju kablova, mrežnih uređaja i dr.. Također definira protokol za uspostavljanje ili prekid komunikacije između dva direktno povezana uređaja, protokol za kontrolu prijenosa podataka (engl. *flow control*), vrstu prijenosa kao što je jednosmjeran (engl. *simplex*), obo smjerni naizmjenični (engl. *half duplex*), obo-smjerni (engl. *full duplex*) i topologiju mreže.

U podatkovnom sloju ostvaruje se pouzdan prijenos podataka između uređaja detekcijom i ispravkom grešaka koje se mogu pojaviti u fizičkom sloju. Dijeli se na dva pod-sloja: fizička adresa (engl. *Media Access Control* - MAC) i logička kontrola

prijenosa (engl. *Logical Link Control* – LLC). MAC je odgovoran za kontrolu na koji način računala u mreži ostvaruju pristup podacima i dozvolu za prijenos istih. LLC provjerava i korigira greške pri prijenosu podataka te kombinira ili dekodira protokole slane MAC pod-slojem.

Mrežni sloj obavlja većinu mrežnih funkcija i definira na koji način će se prenijeti paket od jednog mrežnog uređaja do drugog u istoj mreži prevodeći logičku mrežnu IP adresu (engl. *Internet Protocol* - IP) u fizičku adresu uređaja (MAC adresa). Na mrežnom sloju svaki uređaj ima svoju adresu te dozvoljava slanje poruka drugim uređajima koristeći samo sadržaj poruke i adresu odredišnog uređaja. Mrežni sloj određuje kojim putem tj. usmjerava poruku do odredišnog uređaja. Po potrebi može poruku podijeliti u više dijelova i svaki dio dostaviti drugom rutom te ih zatim spajati na odredištu. Slanje paketa mrežnim slojem nije pouzdano. U mrežnom sloju nalaze se protokoli za usmjeravanje, upravljanje višesmjernim slanjem, informacije o mrežnom sloju i greškama i adresiranje.

Transportni sloj omogućuje funkcioniranje i proceduru prijenosa podataka varijabilnih duljina od izvora do krajnjeg odredišta putem jedne ili više mreža istovremeno održavajući kvalitetu stanja servisnih funkcija. Kontrola pouzdanosti određenog linka odvija se pomoću kontrole upravljanja protokom, segmentacijom/de-segmentacijom i kontrolom grešaka. Na taj način se prati pakete i ponovno šalje one koji su neispravni ili nisu stigli. Nakon što je paket u cijelosti poslan i primljen transportni sloj šalje potvrdu o primitku paketa i šalje slijedeći paket ako nije bilo grešaka u prijenosu. Poruku primljenu od aplikacijskog sloja pretvara u pakete. Postupak dijeljenja velikih poruka u male zove se pakiranje. Protokoli za tuneliranje koriste transportni sloj za prijenos protokola poput IPX-a (engl. *Internetwork Packet Exchange*) i IPsec-a (engl. *Internet Protocol Security*). U transportnom sloju nalaze se Transmission Control Protocol (TCP) i User Datagram Protocol (UDP) protokoli.

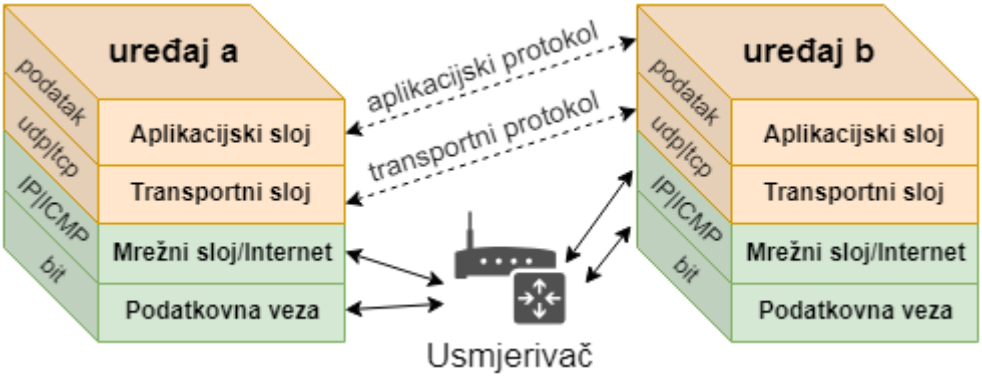
Sesijski sloj kontrolira vezu između dva uređaja tj. uspostavlja, održava, sinkronizira i prekida vezu između lokalne i udaljene aplikacije. Također omogućuje obo smjerni (engl. *full-duplex*), obo smjerni naizmjenični (engl. *half-duplex*) i jednosmjerni (engl. *simplex*) prijenos podataka.

Prezentacijski sloj povezuje podatke između aplikacijskih slojeva obzirom da različiti uređaji u aplikacijskom sloju mogu imati drugačiju sintaksu ili kodiranje podataka. Ovaj sloj je neovisan o vrsti podataka obzirom da prevodi podatke između aplikacije i mrežnih formata u format koji će aplikacija prihvatiti. U ovom sloju obavlja se enkripcija i formatiranje podataka za slanje mrežom.

Aplikacijski sloj je najbliži krajnjem korisniku gdje aplikacijski sloj i korisnik zajedno obavljaju interakciju sa softverskom aplikacijom tj. pruža mrežne usluge korisničkim aplikacijama poput uspostavljanja i sinkroniziranja procedure prijenosa datoteka. Funkcije aplikacijskog sloja su utvrđivanje komunikacije, dostupnosti i sinkronizacija komunikacije.

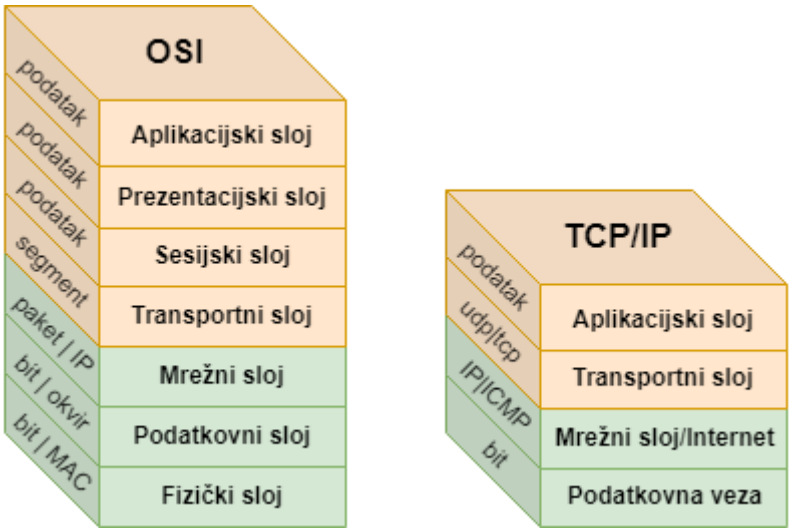
2.2. Referentni model TCP/IP

Paralelno sa OSI modelom kreiran je TCP/IP model od strane Sveučilišta u Berkleyu kojim se omogućuje komunikacija međusobno povezanih mreža, što ga danas čini najrasprostranjenijim protokolom obzirom da se na njemu zasniva globalna mreža Internet. Razlika OSI referentnog modela i TCP/IP-a je u tome što TCP/IP ima samo četiri sloja (Slika 6.) za razliku od OSI modela koji ima sedam slojeva, što se može vidjeti iz Slike 7.



Slika 6. Slojevi TCP/IP modela i komunikacija između njih, Izvor: [3].

U aplikacijskom sloju aplikacije kreiraju podatke i komuniciraju podacima s drugim aplikacijama na nekom drugom računalu ili na istom računalu. Aplikacije koriste niže slojeve poput transportnog sloja koji pruža sigurnu putanju do drugih procesa. Komunikacija između klijenata ovisi o samoj aplikaciji i može biti na primjer klijent-poslužitelj ili klijent-više klijenata. U ovom sloju se za primjer nalaze SMTP (engl. *Simple Mail Trasport Protocol*), FTP (engl. *File Transfer Protocol*), SSH (engl. *Secure Shell*), HTTP (engl. *Hyper Text Transport Protocol*) i za ovaj rad najinteresantniji SNMP (engl. *Simple Network Management Protocol*) protokol.



Slika 7. Usporedba OSI i TCP/IP referentnih modela, Izvor: [2], [3].

Transportni sloj održava komunikaciju između klijenata na nekom drugom računalu ili na istom računalu kao i kod aplikacijskog sloja. On kreira kanal za komunikaciju za potrebe aplikacija. UDP je osnovni transportni protokol kod kojeg ne postoji kontrola slanja podataka te je iz tog razloga nepouzdan za određene servise, dok TCP koristi kontrolu tijeka prometa, provjeru uspostave konekcije i pouzdan transfer podataka.

Internet (mrežni) sloj ima zadaću razmjene segmenta unutar mreže i pruža uniformno sučelje koje prikriva topologiju mrežnih konekcija. Definira adrese i usmjeravanje koje koristi TCP/IP protokol gdje je Internet protokol primarni jer definira IP adresu. Putem ovog sloja prenose se segmenti do idućeg IP usmjerivača koji je bliže odredištu.

Podatkovna veza definira način umrežavanja unutar lokalne mreže na kojoj klijenti komuniciraju bez pomoći usmjerivača. U ovom sloju nalaze se protokoli kojima se opisuje topologija lokalne mreže i sučelja potrebna za prijenos segmenta do slijedećeg mrežnog klijenta.

3. Mrežni protokoli za prikupljanja podataka

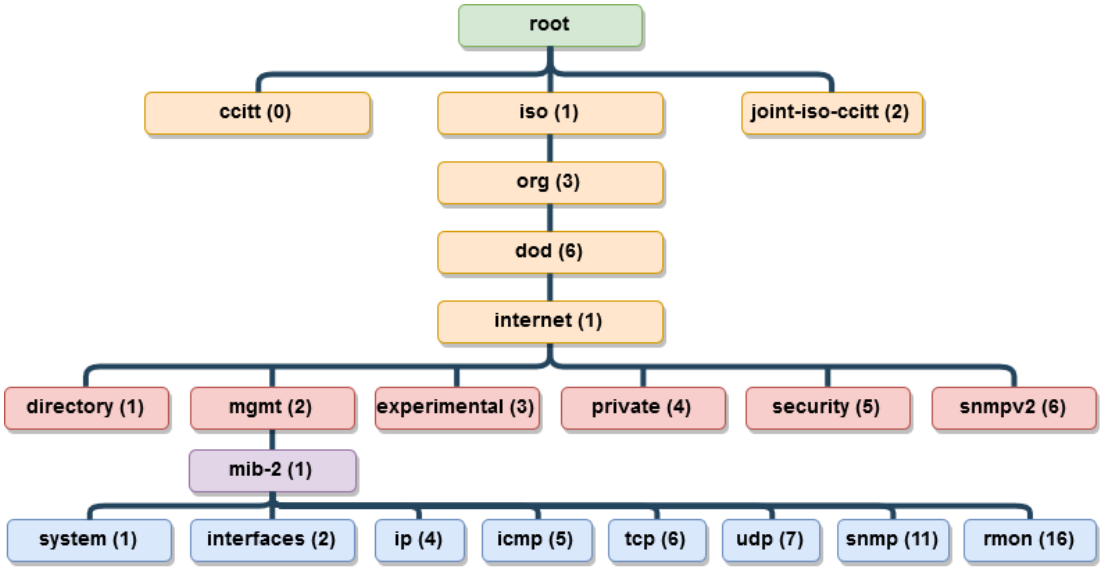
Nadzor mrežnih uređaja najčešće se obavlja s odvojene tj. udaljene mrežne lokacije, iako većina mrežnih uređaja pruža mogućnost nadzora i kontrole putem komandnog sučelja (engl. *Command Line Interface* - CLI) ili grafičkog sučelja (engl. *Graphic User Interface* - GUI) u web pregledniku, neefikasno je spajati se na stotine mrežnih uređaja kako bi se napravila osnovna provjera je li ispravno rade ili je li postoje kakva upozorenja ili eventualne greške koje su se pojavile tokom rada.

Kako bi bilo moguće obaviti nadzor stotina pa i tisuće mrežnih uređaja istovremeno, stvoreni su i implementirani mrežni protokoli kojima se omogućavaju razne provjere, informacije, stanja u kojima se uređaj nalazi, kao i udaljena konfiguracija kod protokola kao što su CMIS/CMIP (engl. *Content Management Interoperability Services*), SNMP, ICMP (engl. *Internet Control Message Protocol*), JMX (engl. *Java Management Extensions*), XML-RPC (engl. *EXtensible Markup Language – Remote Procedure Call*), SOAP (engl. *Simple Object Access Protocol*), WMI (engl. *Windows Managment Instrumentation*) i drugi. SNMP je inicijalno zamišljen kao kratkoročno rješenje od strane IAB-a (engl. *Internet Architect Board*), a CMOT kao dugoročno. Ipak, CMOT nije doživio popularnost koju je SNMP stekao te se danas smatra napuštenim iako ga neki proizvođači i dalje implementiraju u svoje uređaje [6]. Osim navedenih protokola moguće je provjere obavljati i ostalim protokolima ili testiranjem otvorenih sučelja (engl. *port*). Primjerice za testiranje FTP-a moguće je provjeriti da li postoji otvoreno sučelje 21, no bez pristupnih podataka nije moguće utvrditi da li FTP poslužitelj ispravno radi, u takvom slučaju je u postavkama programa za nadzora potrebno unijeti pristupne podatke kako bi se obavila cjelokupna provjera. Provjere je također moguće obavit i putem SSH, IMAP (engl. *Internet Message Access Protocol*), POP (engl. *Post Office Protocol*), SMTP, HTTP, Telnet i brojnih drugih protokola.

Lokalne mreže su vrlo često odvojene od Internet mreže radi sigurnosti (Slika 15.) i ukoliko imaju potrebu pružati servise prema Internetu tada se poslužitelj mora nalaziti u posebno zaštićenoj mreži (engl. *Demilitarized Zone - DMZ*) te mu je pristup iz lokalne mreže i u lokalnu mrežu najčešće ograničen na samo jedan poslužitelj sa kojeg preuzima podatke, a prema Internetu su mu zatvorena sva sučelja osim porta za komunikaciju, a to je najčešće port 80 ili 443. U takvom slučaju otežano je nadzirati poslužitelj u DMZ-u, no nije nemoguće. Podatke je moguće poslati preko dodatnog proxy poslužitelja u DMZ-u na koji će se slati prikupljeni podaci i zatim prosljeđivati u glavni nadzorni poslužitelj.

3.1. Simple Network Managment Protocol (SNMP)

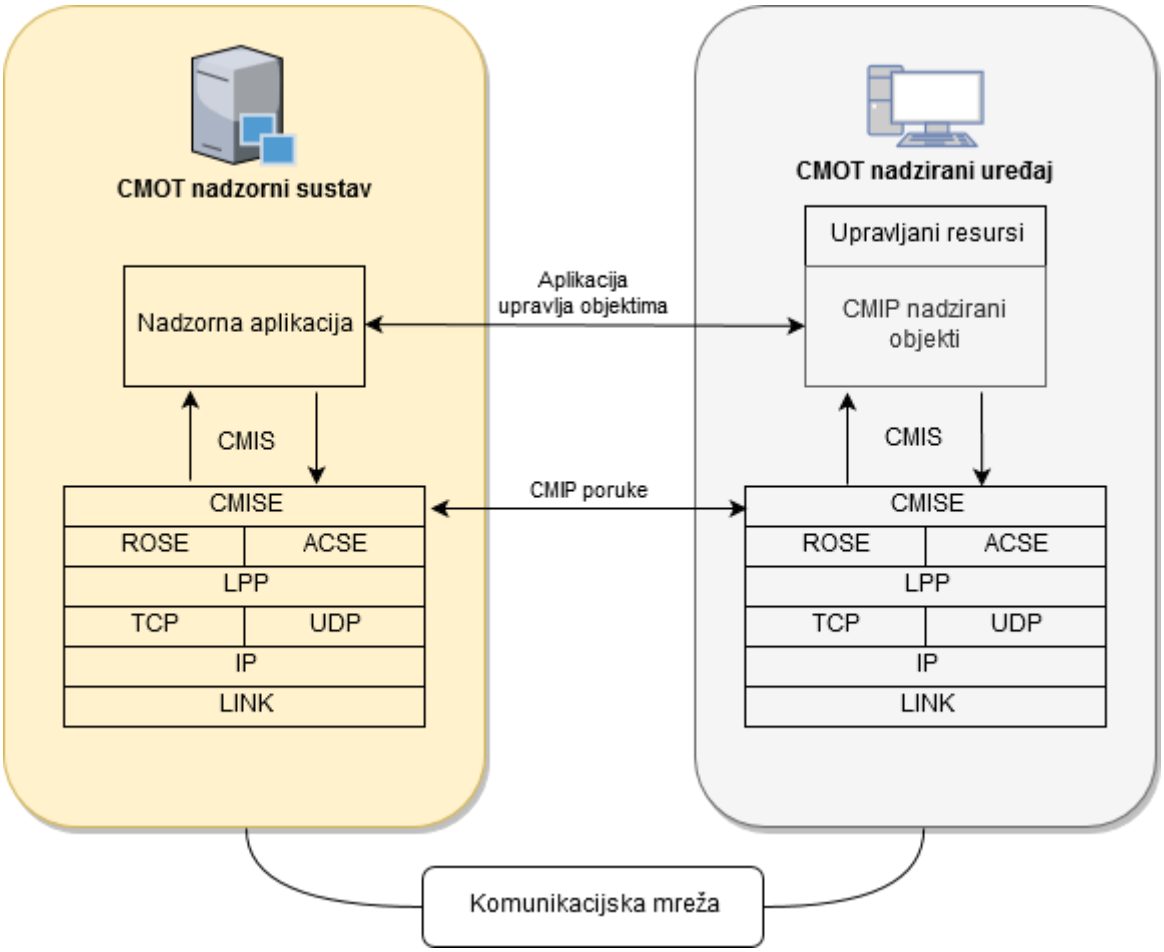
SNMP je jednostavan bez kontaktni mrežni protokol kojim je moguće prikupiti ili izmijeniti podatke i upravljačke informacije o udaljenom mrežnom uređaju putem UDP/IP protokola putem bilo koje vrste IP mreže, kao što je lokalna mreža ili Internet definiran po RFC-u 1157 [9]. Mrežni uređaji moraju imati implementiran *Management Information Base* (MIB) prema SMI (engl. *Structure of Management Information*) arhitekturi (Slika 8.) i agenta sa SNMP ili *Common Management Information Services* (CMOT) protokolom koji šalje tražene podatke prema programskoj podršci za nadzor [3]. Obzirom da je CMOT značajno kompliciraniji za implementaciju te je u RFC „draftu“ preporuča se korištenje SNMP protokola za upravljanje mrežnim uređajima [10].



Slika 8. SMI arhitektura [5]

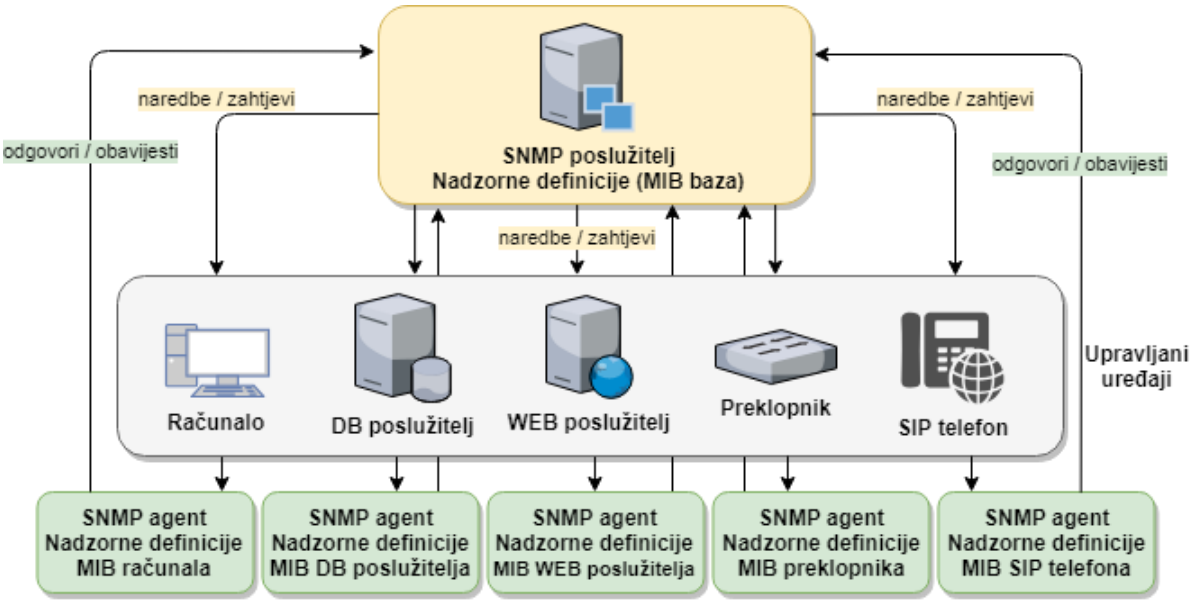
CMOT za razliku od SNMP-a je u potpunosti kontaktni i baziran na TCP/IP protokolu te prije slanja podataka ostvaruje vezu na aplikacijskoj razini kako bi se osigurao siguran prijenos podataka i oslanja se na tri OSI servisa: *Common Management Information Service Element* (CMISE), *Remote Operation Service Element* (ROSE) i *Association Control Service Element* (ACSE) (Slika 9.) [6].

Sve SNMP poruke prenose se aplikacijskim slojem IP-a te UDP protokolom. Kod klijenta je to UDP port 161, dok poslužitelj prima poruke na UDP portu 162, kada se koristi TLS, tada se koriste UDP portovi 10161 i 10162.



Slika 9. CMOT arhitektura [6]

Princip rada SNMP-a bazira se na modelu klijent-poslužitelj, pri čemu je poslužitelj uređaj za nadzor mrežnih uređaja i putem prethodno podešenog SNMP zajednice (engl. *community*) pokreće skripte ili aplikacije koje nadziru klijente, tj. mrežne uređaje kao što su računala, poslužitelji, printeri, mobiteli, usmjerivači, bežični usmjerivači, preklopnici, podatkovni sustavi, klima uređaji, uređaji za detekciju vatre, vode i slično, a koji moraju imati mrežne mogućnosti upravljanja i komunikacije (identičan SNMP *community*) koje od njih poslužitelj traži, tj. SNMP agenta (Slika 10.).



Slika 10. Arhitektura SNMP-a, Izvor [6]

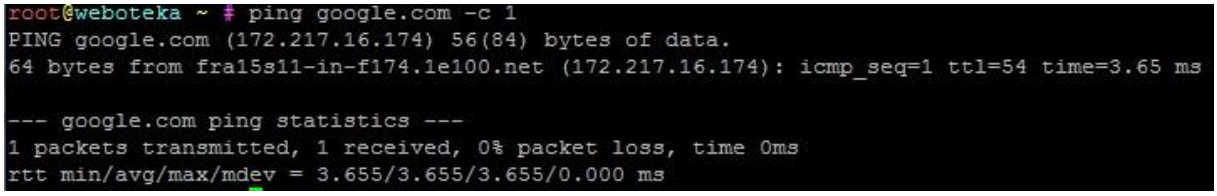
Obzirom da se radi o bez kontaktnom protokolu, ne garantira se isporuka poruka, no ipak većina poruka bude isporučena, a one koje ne budu isporučene se ne šalju ponovno [6].

Postoje tri verzije SNMP protokola, a najčešće se koriste verzija 1 i 2c zbog kompatibilnosti i podrške uređaja. Obzirom da poslani podaci nisu kriptirani moguće je otkriti SNMP *community* snimanjem i analizom mrežnog prometa (npr. programskom podrškom *Wireshark*) i uz pomoć otkrivenog naziva *community*-a izmijeniti konfiguraciju MIB baze. SNMP v1 podatke šalje isključivo na zahtjev i to prema samo jednoj programskoj podrški za nadzor mrežnih uređaja. SNMP v2 omogućava spajanje na više programskih podrški za nadzor kao i sigurnost, ali zbog kompliciranosti podešavanja istog izdana je v2c i ponovno uvedeno korištenje nesigurnog *community*-a. Tek sa SNMP v3 uvedena je potpuna sigurnost prijenosa poruka autentikacijom, enkripcijom i provjerom integriteta poruke [9].

3.2. Internet Control Protocol Message (ICMP)

Protokol ICMP (engl. *Internet Control Protocol Message*) koristi IP protokol mrežnih uređaja poput usmjerivača za slanje poruka o greškama, obavijestima kada datagram ne može doći do odredišta, kada usmjerivač (engl. *gateway*) ne može zaprimiti datagram ili kada usmjerivač želi obavijestiti pošiljatelja da može slati podatke kraćom mrežnom rutom ili može slati obavijesti o dostupnim servisima tog uređaja. ICMP je u pravilu dio IP protokola te je implementiran u svakom IP podržanom uređaju no uređaji ga ne tretiraju kao dio IP protokola zbog poruka koje prenosi, a radi u mrežnom sloju za razliku od TCP/UDP protokola [12].

Primjer korištenja ICMP protokola je sa naredbama *ping* ili *traceroute* preko kojih možemo dobiti korisne informacije. Primjerice sa *ping* naredbom moguće je provjeriti slijedeća stanja, koja pak ovise o samoj implementacije naredbe:
- da li je mrežni uređaj dostupan
- koliko je vrijeme potrebno da paket stigne od početne mrežne točke do odredišne točke uključujući vrijeme povratka informacije do početne točke
- koliko je mrežnih točaka prošao na svojem putu (engl. *hops*) i sl.



Slika 11. Primjer informacija koju pruža Linux *ping* naredba

Naredba *Traceroute* prikazuje sve mrežne točke kroz koje je paket putovao kao i informaciju o potrebnom vremenu da paket dođe do svake od tih mrežnih točaka.

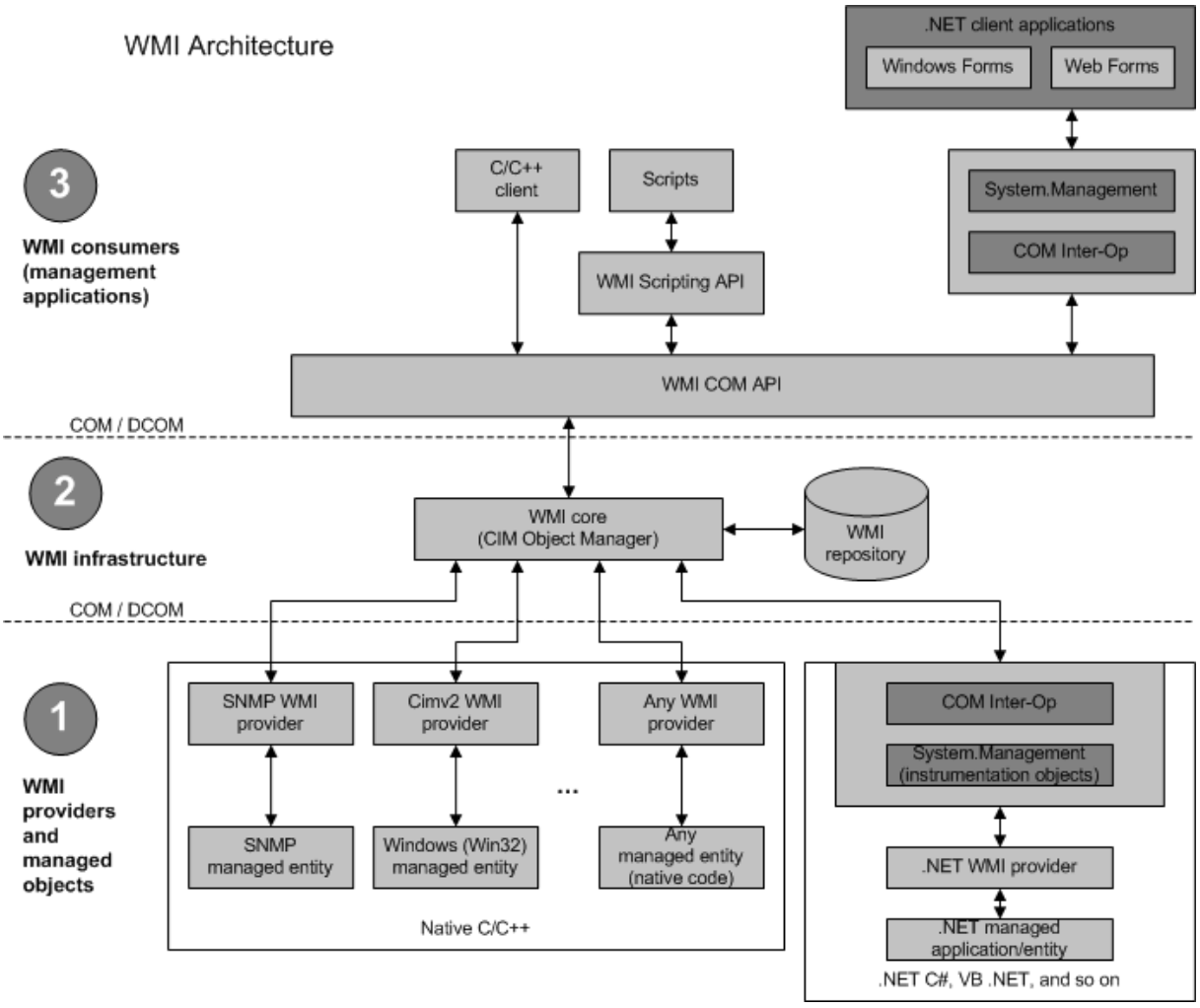
3.3. Windows Management Instrumentation (WMI)

WMI je tehnologija nastala 1998. godine zajedničkim udruženjem Microsofta, Intela, Compaq-a i BMC-a radi lakšeg nadzora i održavanja Windows baziranih računala u poduzećima i u to vrijeme se zvala *Web-Based Enterprise Management* (WBEM), a današnja nasljednica WMI-a se zove *Windows Management Infrastructure* (MI) i potpuno je kompatibilna sa WMI tehnologijom [3]. Mogućnosti WMI su značajne i vrlo korisne te je moguće pomoću bilo kojeg programskog jezika koji podržava WMI *Component Object Model* (COM) sučelje (engl. *Application Programming Interface* - API) napisati WMI skripte koje automatiziraju nadzor i održavanje Windows osobnih računala i poslužitelja uključujući nadzor log datoteka, podatkovnih sustava, printera, procesa, internu bazu (engl. *registry*), sigurnost, servise, dijeljene direktorije, mrežne servise (engl. *Domain Name Server* - DNS, IP, SNMP), sve Windows .NET aplikacije (Exchange, SQL, Operations Manager) i razne druge opcije operativnog sustava [7]. Mogućnost nadziranja stanja i slanja obavijesti sustava putem WMI skripti je u pravilu vrlo slična SNMP principu rada.

Princip funkcioniranja WMI skripti se bazira u tri koraka:
- spajanje na WMI servis
- prikupljanje podataka o određenoj WMI klasi
- obrada prikupljenih podataka (spremanje u bazu, prikaz na ekranu, i sl.)

Cjelokupna arhitektura WMI sustava se sastoji od:

- WMI skripte ili aplikacija (C/C++, .NET),
- WMI infrastrukture (WMI jezgra i repozitorij)
- WMI upravljanih resursa koji pružaju podatke o sustavu (SNMP, CIM, .NET, WMI provider) (Slika 12):



Slika 12: WMI arhitektura, [8]

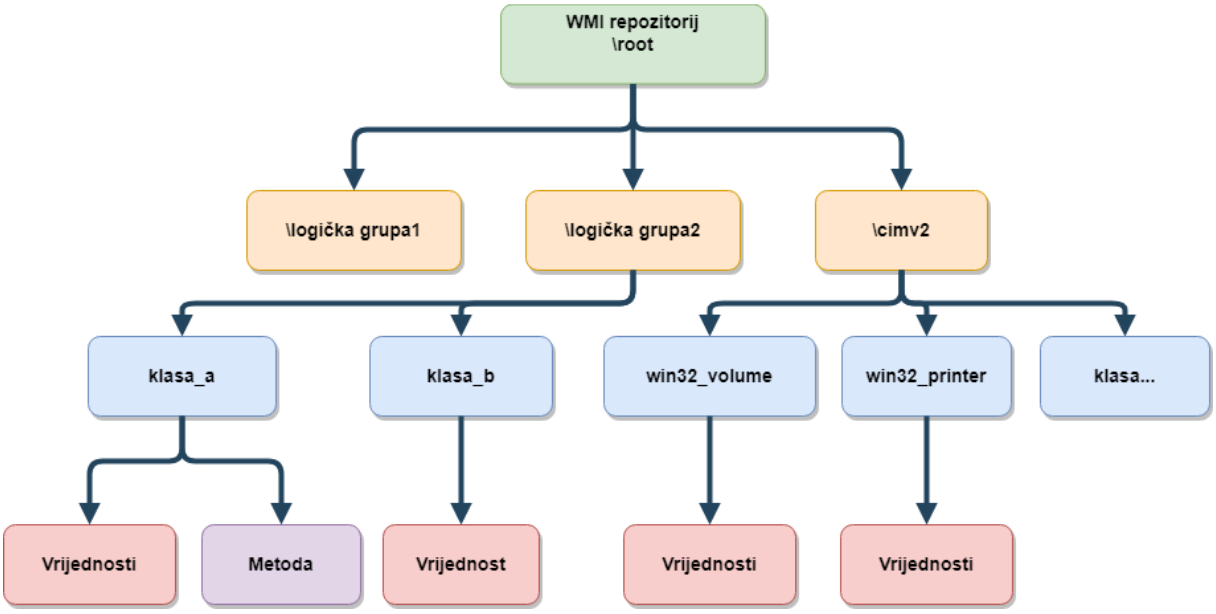
WMI upravljani resursi su svi Windows resursi kojima se može pristupati ili upravljati putem WMI-a poput mrežnog ili podatkovnog sustava, logova, datoteka, komponenti operativnog sustava, baze (engl. *registry*), printera, procesa, sigurnosti, korisnika, *Active Directory*-a, *Windows Installer*-a, WDM upravljačkih programa kao i SNMP podatkovne baze (MIB) i dr. [6].

WMI infrastruktura je srednji sloj arhitekturnog modela , te definira način na koji se može pristupiti ili prikupiti konfiguracija i upravljati njome, a sastoji se od tri sljedeće komponente [6]:

- **Common Information Model Object Manager (CIMOM)** poznat kao i WMI servis preko kojeg prolaze svi zahtjevi WMI skripte ili aplikacije. CIMOM ne pruža direktno podatke već locira odgovarajući WMI upravljivi resurs i zatraži podatke od njega. Kada dobije tražene podatke od WMI upravljivog resursa šalje odgovor nazad skripti ili aplikaciji.

- **Common Information Model (CIM)** repozitorij poznat i kao WMI repozitorij koji ima funkciju da podaci za konfiguraciju i upravljanje dobiveni iz različitih izvora budu predstavljeni na identičan način, točnije, shematski prema *Distributed Management Task Force Common Information Model* (DMTF CIM) standardu i sastoji se od dinamičkih klasa koje su grupirane po imenima, tj. u logičke grupe (engl. *namespace*) koje predstavljaju određeno područje. Na primjer root\cimv2 sadrži podatke o računalu i operativnom sustavu (Slika 13.).

- **WMI upravljivi resursi** su primjerice Active Directory, Event Log, Performance Counter, Registry, SNMP, WDM, Win32, Windows Installer i dr..



Slika 13. WMI repozitorij, [8]

Sigurnost WMI je vrlo bitna obzirom da je moguće pristupiti ili upravljati praktički svim podacima Windows računala, čak i s udaljenog računala. Zbog toga je WMI skripte moguće pokretati samo sa pravima koja korisnik ima. Ukoliko korisnik nehotice pokrene malicioznu skriptu koja primjerice treba administratorske ovlasti, ona se neće obaviti obzirom da su korisnici u većini slučajeva bez administratorskih prava. Također nije moguće pokretati WMI skripte na udaljenom računalu bez administratorskih prava.

3.4. Extendible Markup Language-Remote Procedure Call (XML-RPC)

Protokol XML-RPC (engl. *Extendible Markup Language-Remote Procedure Call*) je jednostavan XML protokol za razmjenu podataka između dva mrežna uređaja [13]. Koristi HTML protokol za slanje informacija od klijenta do poslužitelja i omogućava izvršavanje naredbi na udaljenom mrežnom uređaju (klijentu) nakon čega se rezultat izvršavanja šalje nazad poslužitelju.

Primjer XML-RPC zahtjeva:

```
POST /xmlrpc HTTP 1.0
User-Agent: myXMLRPCClient/1.0
Host: 192.168.1.2
Content-Type: text/xml
Content-Length: 180
<?xml version="1.0"?>
<methodCall>
  <methodName>Get.HDD.Health.Status</methodName>
  <params>
    <param>
        <value><hdd>1</hdd></value>
    </param>
  </params>
</methodCall>
```

Primjer XML-RPC odgovora:

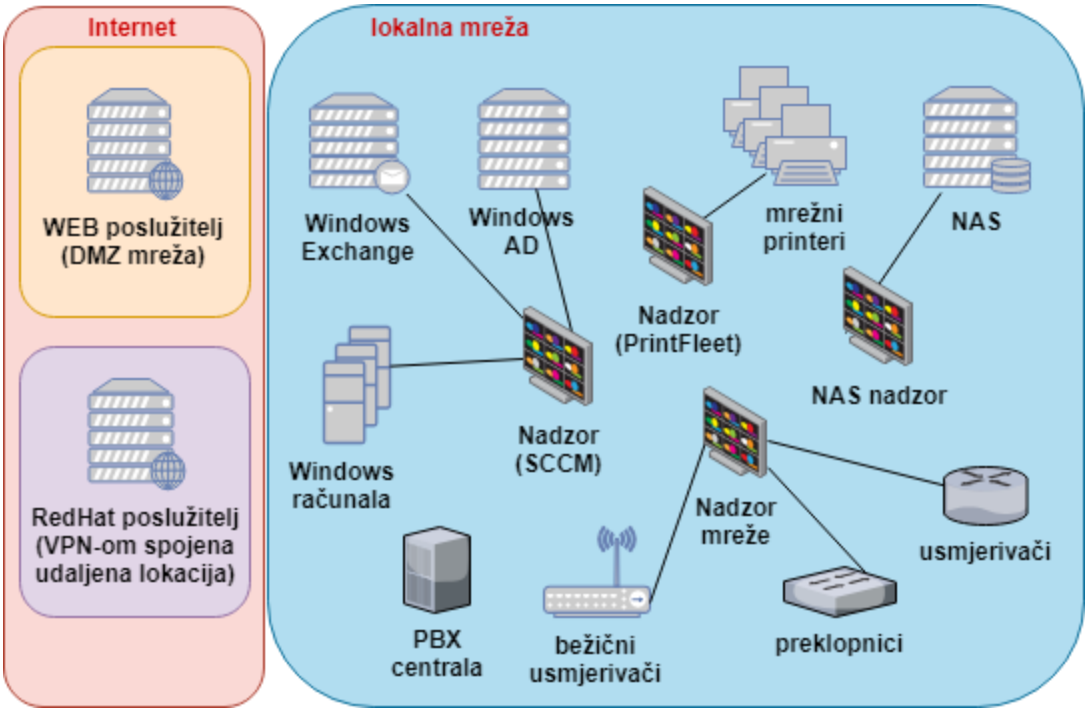
```
HTTP/1.1 200 OK
Date: Tue, 06 Oct 2019 22:44:04 GMT+2
Server: Apache.2.4.39 (Unix)
Connection: close
Content-Type: text/xml
Content-Length: 134
<?xml version="1.0"?>
<methodResponse>
  <params>
    <param>
        <value><string>OK</string></value>
    </param>
  </params>
</methodResponse>
```

Iz XML-RPC primjera se od mrežnog uređaja na IP adresi 192.168.1.2 pomoću metode „Get.HDD.Health.Status“ traži stanje tvrdog diska na poziciji „1“, a povratni odgovor vraća da je stanje za navedeni disk na poziciji „1“ ispravno, tj. odgovor „OK“. Ovakva vrsta dohvata podataka se koristi sve češće zbog jednostavne komunikacije i obrade povratnih informacija.

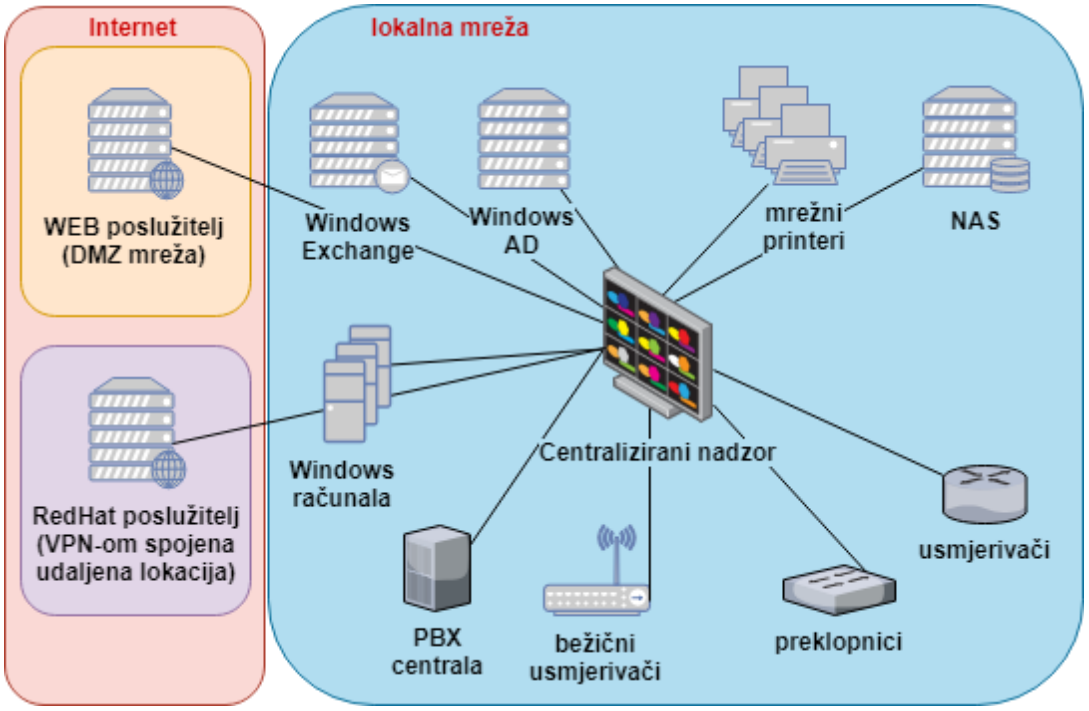
4. Programska podrška za nadzor mrežnih uređaja

Poslovni sustavi vrlo često imaju više vrsta različitih programske podrške za nadzor mrežnih uređaja iz razloga što su ti programi zatvorenog koda i samo proizvođač zna na koji način je moguće dohvatiti informacije s takvog uređaja [14]. Stariji mrežni uređaji često nemaju nikakvo udaljeno sučelje preko kojeg ih je moguće konfigurirat ili nadzirat što u konačnici onemogućava centralizaciju nadzora te iziskuje dodatne troškove kod održavanja (Slika 14). Preporučljivo je zastarjele uređaje zamijeniti onima koji podržavaju neku vrstu udaljenog upravljanja i nadzora kao što je SNMPv3.

Prednosti centraliziranog mrežnog nadzora su višestruke (Slika 15) [15]:
- dostupnost svih mrežnih uređaja te priključaka, veza i servisa na tom uređaju
- detekcija mrežnih uređaja i komponenti
- nadzor i praćenje stanja mrežnih uređaja, priključaka, veza, servisa i slično
- mjerenje opterećenja i detekcija zagušenja mreže
- udaljena konfiguracija mrežnih uređaja ukoliko je podržano
- izrada izvještaji
- kontrola sigurnosti, obavijesti o svakom neovlaštenom pokušaju napada
- prilagodljivost sustava u slučaju povećanog ili smanjenog opterećenja mreže, korisnika i slično.
- detekcija pada sustava i brzi oporavak
- evidencija problema i grešaka
- manji troškovi zbog pravovremene reakcije
- manje radne snage



Slika 14. Primjer nadzora mrežnih uređaja bez unificiranog rješenja, [14]



Slika 15: Primjer centralnog nadzora lokalnih i udaljenih mrežnih uređaja, [14]

Većina programske podrške za nadzor nudi detekciju otvorenih portova, pokrenutih servisa i stanja sustava putem SNMP-a ili putem vlastitog agenta koji je potrebno instalirati na nadzirani sustav. Automatskom detekcijom moguće je utvrditi mogućnosti nadzornih sustava i razlike između njih, a u tablici 1. su navedeni nadzirani mrežni uređaji, portovi i servisi koji su bitni za rad te prema njima je moguće napraviti usporedbu.

Sustav	IP	Portovi	Servisi
CentOS 7	159.69.195.216	22, 53, 443	FTP, DNS, HTTPS
Windows 2012	10.111.100.80		Samba share
Mikrotik RB2011	10.111.100.1	161	Status routera
Canon TS5050	10.111.100.251	161	Status printera
Microsoft IIS	161.53.97.54	443	Web server

Tablica 1. Popis nadziranih mrežnih uređaja

Usporedba programske podrške za nadzor fokusirana je na više razina, prvotno kroz instalaciju čime bi se utvrdili svi potrebni preduvjeti i zahtjevi za korištenje programske podrške, zatim jednostavnost konfiguracije pri čemu će se obratiti pažnja na intuitivnost dodavanja korisnika, grupa i mrežnih uređaja, podrške mrežnih uređaja i podrške agenata za praćenje mrežnih uređaja kao i personalizaciju ili izradu istih u slučaju da postoji potreba za time ako nije nativno podržano od strane programske podrške za nadzor.

Prikaz trenutnog stanja tj. problema, točnije radna ploča (engl. *dashboard*) u kojoj se prate problemi svih mrežnih uređaja i mogućnost filtriranja te pregleda po grupama, klijentima ili vremenu od iznimne je važnosti ukoliko nas interesira određeni period za određeni mrežni uređaj ili grupu uređaja. Kako bi proces bio potpun, trenutne probleme je potrebno javiti osobi odgovornoj za administraciju tog uređaja što se prati kroz slanje obavijesti i podržanom načinu obavještavanja poput email-a, SMS-a (engl. *Short Message Service*), jabber-a i slično. Jabber je otvoreni protokol XMPP (engl. *Extensible Messaging and Presence Protocol*) za razmjenu poruka između klijenata uz pomoć servera.

Za utvrđivanje periodičnih greški bitno je imati i uvid u povijest grešaka radi preventivnog djelovanja nad mrežnim uređajima što je također jedna od bitnih točaka na koje će se obratiti pažnja u ovom radu. U konačnici, ukoliko se nadziru uređaji trećih osoba generiranje periodičnih izvještaja od iznimne je važnosti kako bi klijent imao uvid u dostupnost svojih sustava i na temelju izvještaja donosio odluke o daljnjim postupanjima kako bi povećao dostupnost sustava. Kako se radi o trećim osobama, kvaliteta prezentacije izvještaja može imati veliku razliku, primjerice, klijent će na vizualne grafičke izvještaje drugačije reagirati obzirom da će biti opterećenja sustava ili padovi biti bolje istaknuti nego u tekstualnim izvještajima.

Na kraju će se usporediti mogućnosti nadogradnje i održavanja programske podrške kako bi programska podrška za nadzor kontinuirano i bez greški obavljala svoj zadatak. Podržani operativni sustavi mogu biti odlučujući faktor, primjerice, programska podrška bazirana na Windows operativnom sustavu podrazumijeva i kupnju odgovarajuće Windows licence, za razliku od besplatnih operativnih sustava poput Linux-a, Unix-a i FreeBSD-a, no kod njih se očekuje složenija administracija što također povećava troškove samog sustava za nadzor. Konačno, trajanje životnog ciklusa programske podrške (engl. *End of Life* - EOL) i mogućnost produživanja istog daje dodatan uteg pri odluci o korištenju istog. Plaćeni sustavi za nadzor nude određenu garanciju kako će biti podržani kroz cijelo vrijeme korištenja, dok se kod besplatnih sustava za nadzor

korisnik sam mora brinuti o istom kroz dostupne nadogradnje koje mogu biti dostupne, ali kako se radi o besplatnom softveru to nije pravilo niti ne postoji jamstvo da će programska podrška za nadzor biti podržana nakon izvjesnog vremena.

4.1. Zabbix

Godine 1998. Alexei Vladishev je pokrenuo interni projekt iz kojeg je nastala Zabbix programska podrška za nadzor mrežnih uređaja. 2001. godine je objavljen kao projekt otvorenog koda. Tri godine kasnije, 2004-te službeno je izdana prva verzija 1.0, a danas se Zabbix smatra jednim od vodećih besplatnih poslovnih programske podrške za nadzor u inačici v4.2.

4.1.1. Mogućnosti Zabbix-a

Zabbix-om je moguće prikupljati podatke o dostupnosti mrežnih uređaja i performansama mrežnih sustava. Podržava SNMP trapping i polling, IPMI, JMX, VMware nadzor kao i personalizirani nadzor pomoću skripti ili modifikacija agenta obzirom da je otvorenog koda. Podatke je moguće prikupljati u točno određenim vremenskim intervalima, primjerice samo preko dana, noći ili u određeni sat putem servera, proxy-a, agenata ili vlastitih naredbi tj. skripti. Obzirom da se podaci spremaju u bazu minimalno godinu dana, moguće je definirati notifikacije koje se oslanjaju na prijašnje stanje nekog mrežnog uređaja u bazi podataka i to u određeno vrijeme. Sadržaj i izgled notifikacije se može prilagoditi pomoću macro varijabli, a notifikacije se korisnicima šalju SMS-om, XMPP-om ili email-om.

U slučaju da korisnik ne može odmah reagirati i napraviti provjeru mrežnog uređaja na pristiglu notifikaciju koja je primjerice javila da je prestao raditi servis. Slanjem emaila Zabbix-u s naredbom može inicirati ponovno pokretanje mrežnog uređaja ili određenog servisa mrežnog uređaja.

Stanje nadziranih uređaja i servisa moguće je u stvarnom vremenu vizualizirati pomoću grafova i to za više uređaja ili servisa na jednom prikazu kako bi se primjerice mogla napraviti usporedba opterećenja dva identična uređaja. Osim praćenja pojedinačnih uređaja, moguće je prikazati mrežnu topologiju, radne ploče, izvještaje, povijesne podatke o nekom uređaju i automatski otkriti mrežne uređaje koji su dostupni za nadzor, kao i detekciju vrste datotečnog sustava, mrežnih sučelja i SNMP OID-a.

Dodavanje i konfiguracija uređaja je vrlo jednostavna putem web sučelja kojem se može pristupati sa bilo kojeg uređaja. Čim se uređaj doda, započinje prikupljanje podataka o njemu, spremanje u bazu, izrada grafova, izvještaja i sl. Udaljene lokacije je moguće nadzirati instaliranjem Zabbix *proxy* poslužitelja koji sa udaljene lokacije šalje podatke o udaljenim mrežnim uređajima putem sigurne veze do Zabbix poslužitelja.

Dodatnu funkcionalnost pruža Zabbix API čime je primjerice moguće izraditi vlastite izvještaje, web stranicu sa prikazom problema ili integraciju sa nekom drugom programskom podrškom poput JIRE za otvaranje radnih naloga, CRM-a i slično.

Zabbix se može instalirati na većinu UNIX kompatibilnih sustava kao što su Linux, FreeBSD, MacOS, a za ovaj rad korišten je CentOS v7.6 operativni sustav i MySQL bazu, sa minimalnom instalacijom paketa, a minimalni sistemski zahtjevi za instalaciju traže samo dva procesora i dva gigabyte-a memorije. Podržane baze podataka za spremanje konfiguracije i povijesnih podataka su MySQL/MariaDB v5.0+, Oracle 10g+, PostgreSQL 8.1+, IBM DB2 9.7+ i SQLite v3.3.5+ [18].

4.1.2. Instalacija Zabbix-a

Instalacija i konfiguracija CentOS operativnog sustava [15], kao i ostalih potrebnih paketa neće biti obrađivana jer je fokus stavljen na usporedbu s drugom programskom podrškom za nadzor.

Nakon prijave u CentOS operativni sustav kao *root* potrebno je pokrenuti slijedeće naredbe:

Dodavanje Zabbix repozitorija putem Interneta:

```
root@zabbix ~ $ yum -y install https://repo.zabbix.com/zabbix/4.2/rhel/7/x86_64/zabbix-release-4.2-1.el7.noarch.rpm
```

Dodavanje i omogućavanje PHP v7.2 Remi repozitorija:

```
root@zabbix ~ $ yum -y install http://rpms.remirepo.net/enterprise/remi-release-7.rpm

root@zabbix ~ $ yum-config-manager --enable remi-php72
```

Osvježavanje lokalnog repozitorija i instalacija svih potrebnih paketa (Zabbix server, Zabbix agent, MariaDB server (MySQL), PHP, EPEL i dr.) :

```
root@zabbix ~ $ rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY*

root@zabbix ~ $ yum clean all

root@zabbix ~ $ yum -y install zabbix-server-mysql zabbix-web-mysql zabbix-agent mariadb-server yum-utils php php-mysql php-mbstring epel-release net-snmp libssh2 fping libcurl libxml2

root@zabbix ~ $ yum update
```

Konfiguracija MariaDB servera i kreiranje inicijalne Zabbix baze te Zabbix tablica. Pristupni podaci korišteni za bazu, tj. korisničko ime je „zabbix“, a pristupna šifra „password“:

```
root@zabbix ~ $ systemctl enable mariadb.service
root@zabbix ~ $ systemctl start mariadb.service
root@zabbix ~ $ mysql_secure_installation
root@zabbix ~ $ mysql -uroot -p
root@zabbix ~ $ mysql> create database zabbix character set utf8 collate utf8_bin;
root@zabbix ~ $ mysql> grant all privileges on zabbix.* to zabbix@localhost
identified by 'password';
root@zabbix ~ $ flush privileges;
root@zabbix ~ $ mysql> quit;
root@zabbix ~ $ zcat /usr/share/doc/zabbix-server-mysql*/create.sql.gz | mysql -
uzabbix -p password
```

Nakon toga je potrebno podesiti konfiguraciju Zabbix servera tj. šifru za MariaDB bazu:

```
root@zabbix ~ $ sed -i 's:# DBPassword=:DBPassword=password:g'
/etc/zabbix/zabbix_server.conf
```

Kao i vremensku zonu te PHP konfiguraciju za HTTPD server:

```
root@zabbix ~ $ sed -i 's:IfModule mod_php5.c:IfModule mod_php7.c:g'
/etc/httpd/conf.d/zabbix.conf
root@zabbix ~ $ sed -i 's:# php_value date.timezone:php_value date.timezone:g'
/etc/httpd/conf.d/zabbix.conf
root@zabbix ~ $ systemctl restart httpd.service
```

Na kraju je potrebno pokrenuti Zabbix server, Zabbix agent i HTTPD server:

```
root@zabbix ~ $ systemctl start zabbix-server zabbix-agent httpd
root@zabbix ~ $ systemctl enable zabbix-server zabbix-agent httpd
```

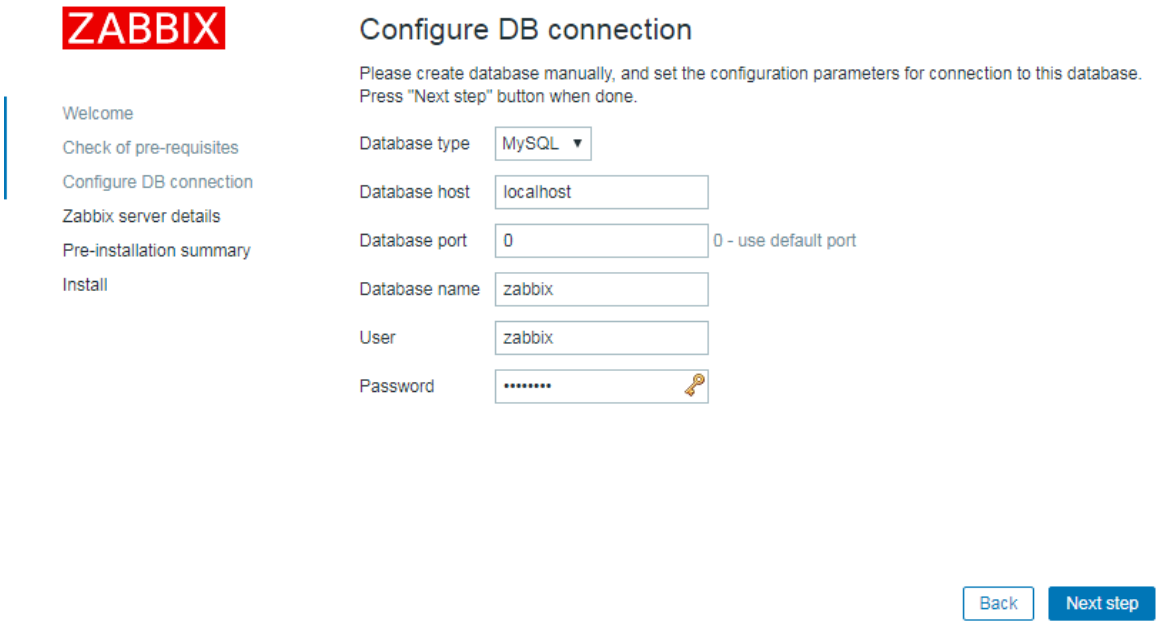
Finalna konfiguracija Zabbix servera kao i dodavanje mrežnih uređaja obavlja se putem Internet preglednika te je u njemu potrebno otvoriti lokacijsku adresu na kojoj smo instalirali Zabbix server, što je u ovom slučaju: http://10.111.100.82/zabbix/ i zatim proći kroz završni dio instalacije.
Nakon učitavanja pojaviti će se Zabbix ekran dobrodošlice što znači da je instalacija prošla bez poteškoća (Slika 16.).

Slika 16. Početna stranica inicijalne konfiguracije Zabbix servera

Na drugoj stranici inicijalne konfiguracije izvršava se provjera PHP/HTTPD konfiguracija te bi sve stavke trebale javljati stanje „OK“ (Slika 17.).

Slika 17. Provjera PHP i HTTPD konfiguracije

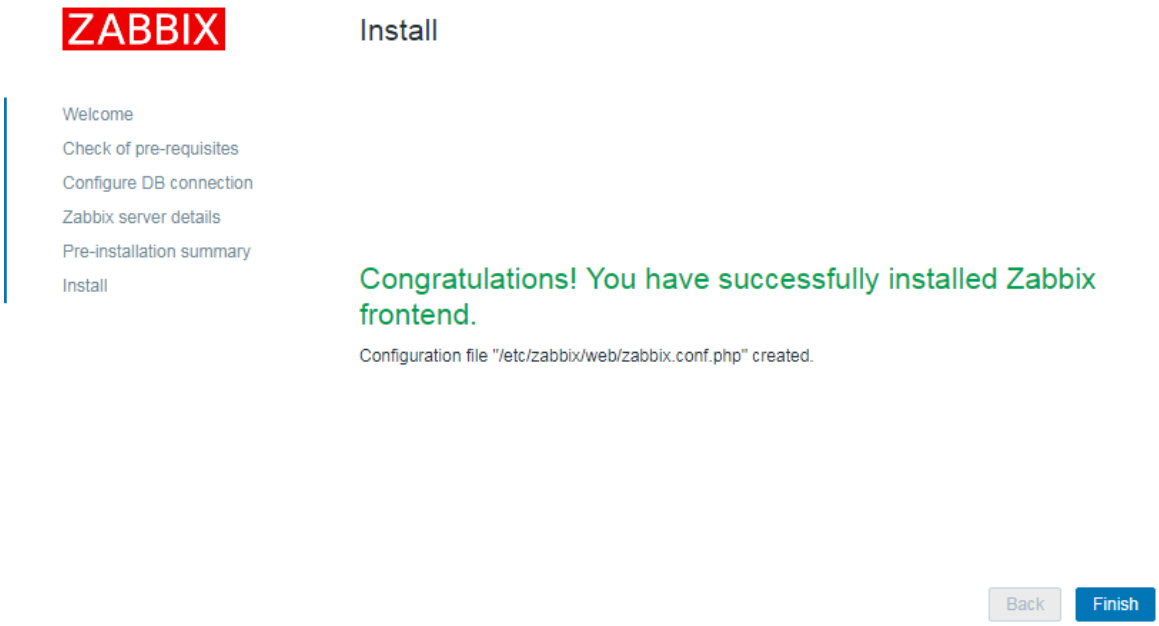
Na trećoj stranici potrebno je unijeti pristupnu šifru za bazu koja se pri inicijalizaciji Zabbix baze definirala s „password“ te je isto potrebno unijeti na ovoj stranici pod „Password“ (Slika 18.).



Slika 18. Podešavanje pristupnih podataka MySQL tj. MariaDB baze

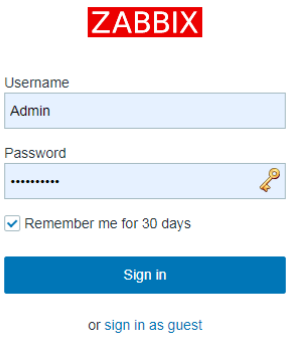
Na četvrtoj stranici je potrebno unijeti željeno ime Zabbix servera kako bi se mogao razlikovati u slučaju kada je instalirano više instanci Zabbix servera, no u ovom slučaju nije nužno i uneseno je „Zabbix server“ (Slika 19.). Nakon toga je dovoljno dva puta kliknuti „Next step“ kako bi došli do završne stranice konfiguracije (Slika 20.).

Slika 19. Unos naziva servera i porta, te imena Zabbix servera

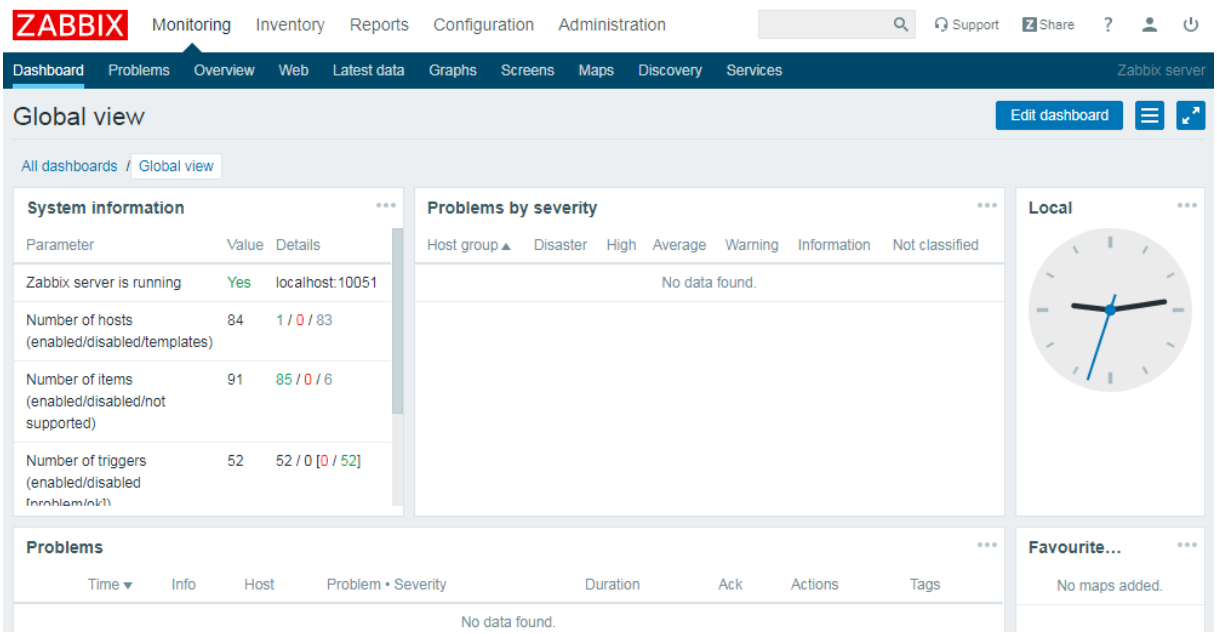


Slika 20. Završna stranica inicijalne konfiguracije Zabbix servera

Za inicijalnu prijavu postoji predefiniran korisnički račun „*Admin*“ s pristupnom šifrom „zabbix“ (Slika 21.), a nakon prijave prikazuje se radna ploča (engl. *Dashboard*) (Slika 22.).



Slika 21. Inicijalna prijava na Zabbix.



Slika 22. Zabbix radna ploča

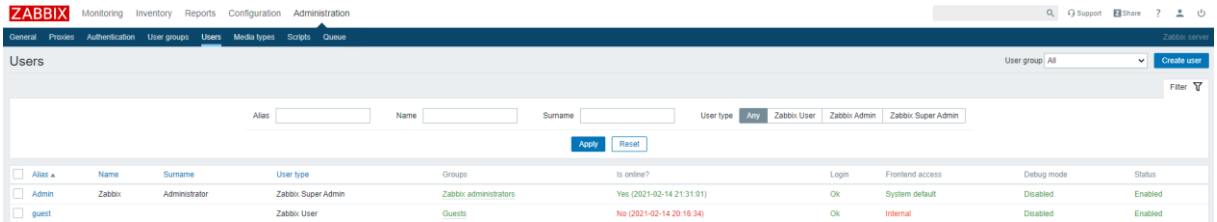
Radna ploča prikazuje generalno stanje Zabbix nadzornog sustava i listu problema na mrežnim uređajima, no moguće je kreirati vlastite radne ploče ili u potpunosti prilagoditi postojeću radnu ploču prema vlastitim željama.

4.1.3. Administracija Zabbix korisnika i grupa

Prije dodavanja mrežnih uređaja korisno je definirati korisnike i grupe te dodijeliti korisnike u grupe s odgovarajućim pristupnim pravima.

Moguće je korisnicima ili grupi korisnika dozvoliti samo pregled određenih podataka, ili u potpunosti zabraniti pregled podataka, ali omogućiti slanje obavijesti o greškama mrežnih uređaja. Podržana je integracija sa AD-om (engl. *Active Directory*) i LDAP-om (engl. *Lightweight Directory Access Protocol*) te se na taj način mogu korisnici dodati i administrirati putem jedinstvene centralne lokacije što olakšava administraciju korisnika. Osim lokalne i AD baze moguća je prijava i putem HTTP-a preko Internet poslužitelja kao što je httpd ili nginx.

Dodavanje korisnika obavlja se biranjem izbornika Administration, zatim Users i na desnoj strani klikom na „Create user“ dodajemo novog korisnika kao što je prikazano na slici 23..

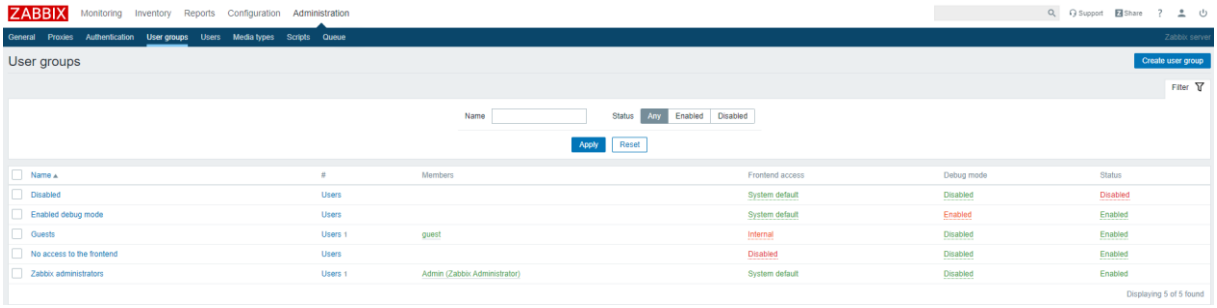


Slika 23. Kreiranje korisnika

Kod kreiranja korisnika dostupne su standardne opcije poput aliasa tj. korisničkog imena, imena, prezimena, šifre, jezika, izgleda i grupe. Klikom na izbornik Media

moguće je definirati vrstu komunikacije prema korisniku, email, Jabber i SMS poruka kao i vrijeme u koje će notifikacije biti aktivne, kao i koja razina notifikacija će se slati (neklasificirane, informacijske, upozorenja, srednje važnosti, visoke važnosti i katastrofe). Ukoliko se ne modificira postavljene vrijednosti, slati će se sve vrste notifikacija svaki dan od 0 do 24h. Vrste dostupnih medija moguće je izmijeniti, brisati i dodavati nove, a standardno su dostupne tri navedene.

Treći izbornik Permissions služi za izbor korisničke grupe, a nude se već predefinirane vrijednosti, „User“ – običan korisnik, „Admin“ – administrator i „Super Admin“ – administrator sa svim dozvolama. Ove tri predefinirane vrijednosti nije moguće uređivati ili dodavati nove.



Slika 24. Korisničke grupe

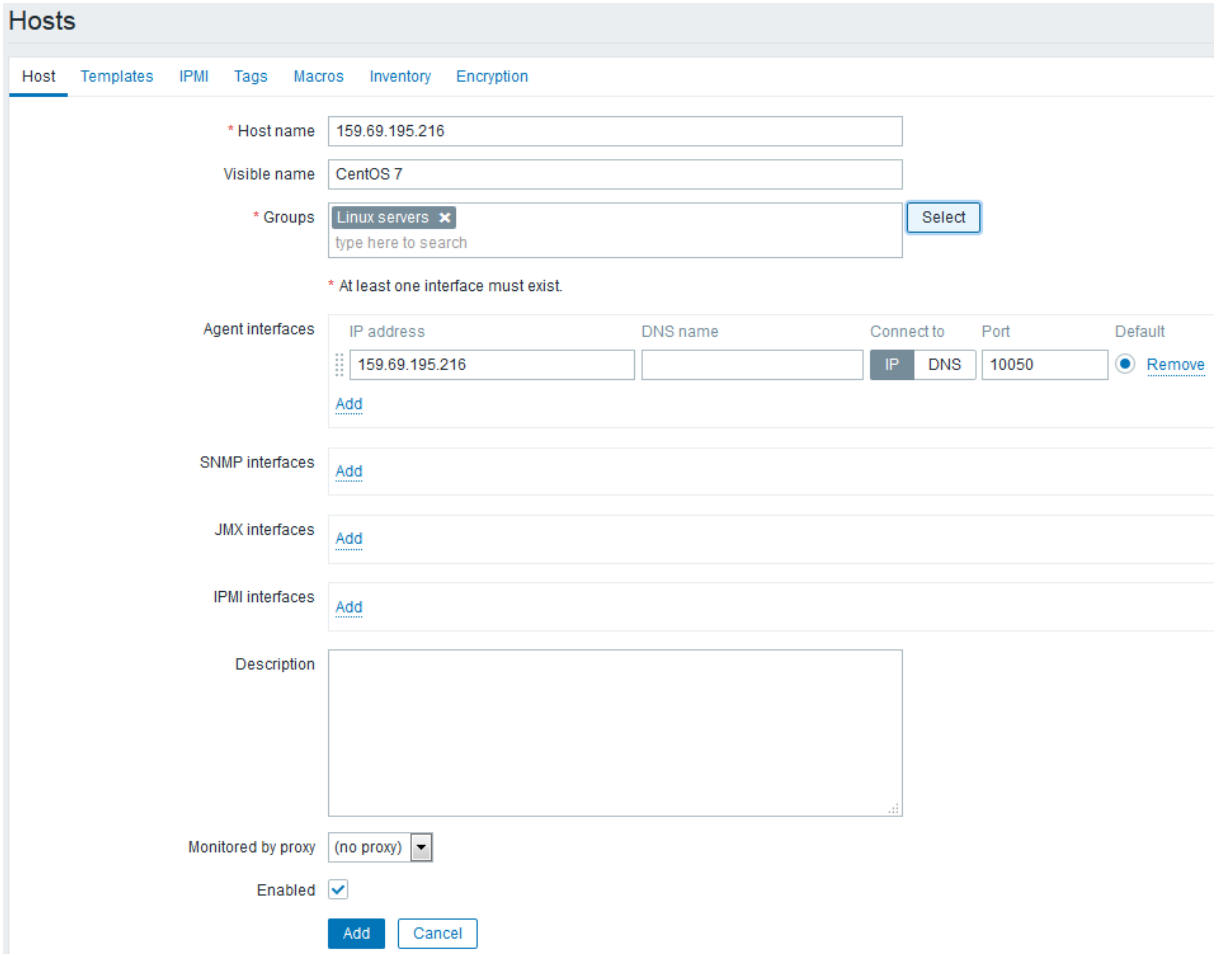
Korisničke grupe dostupne su kroz izbornik „Administration“ – „User groups“ (Slika 24.) te klikom na „Create group“ stvaramo novu korisničku grupu kojoj je moguće dodijeliti prava na izborniku „Permissions“, pri čemu je moguće definirati koji mrežni uređaji ili grupu će korisnik moći nadzirati. Na izborniku „Tag filter“ moguće je dodijeliti korisniku i uređaje sa određenom oznakom, primjerice „Windows serveri“.

4.1.4. Dodavanje mrežnih uređaja u Zabbix

Nakon učitavanja radne ploče (dashboard) možemo dodati mrežni uređaj klikom na izbornik „Configuration“, zatim „Hosts“ i „Create host“ (Slika 25.)

Od podataka potrebno je unijeti „Host name“, „Groups“ i „IP address“ pod „Agent interfaces“. Nakon toga na izborniku treba izabrati „Templates“ i pod „Link New Template“ upisati „Linux“ i zatim iz padajućeg izbornika odabrati „Linux OS template“ tj. onaj template koji odgovara mrežnom uređaju za nadzor, u našem slučaju radi se o Linux CentOS-u v7 (engl. *The Community ENTerprise Operating System*) (Slika 26.).

Slika 25. Dodavanja uređaja u Zabbix-u



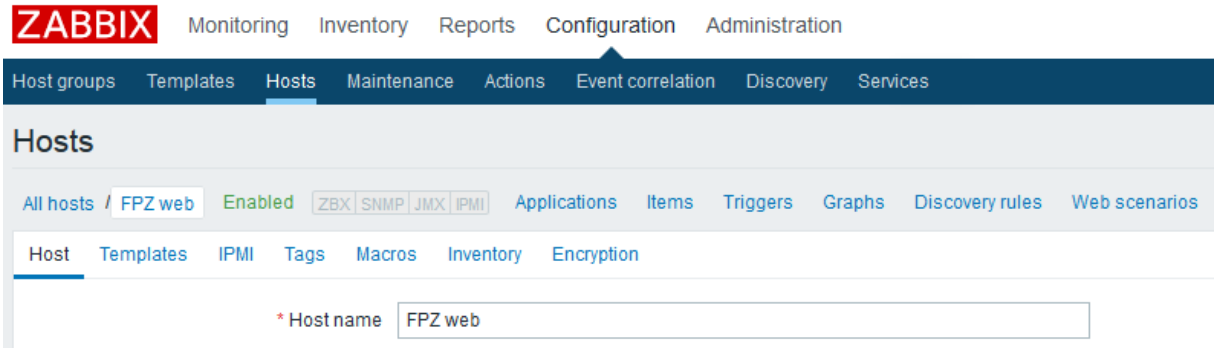
Slika 26. Parametri kod dodavanja novog uređaja (CentOS 7)

Potrebno je pričekati nekoliko minuta da Zabbix prikupi prve podatke o mrežnom uređaju kako bi se podaci počeli prikazivati na radnoj ploči.
Na isti način možemo dodati sve ostale uređaje u Zabbix nadzor kako bi se na radnoj ploči prikazala stanja svih potrebnih mrežnih uređaja.

Nadzor stanja web stranica Zabbix obavlja se provjerom HTTP statusnih odgovora s web stranice te je potrebno kreirati novi uređaj (Slika 25.), ali bez biranja predloška. Zatim je potrebno otvoriti taj novokreirani uređaj koji je u ovom slučaju nazvan „FPZ web“ (Slika 27.). Nastavno, potrebno je izabrati „Web scenario“ i kliknuti na „Create web scenario“ te pod „Name“ upisati proizvoljni naziv stranice. U ovom slučaju radi se o web stranici Fakulteta prometnih znanosti, stoga je upisana skraćenica „FPZ status“. Pod „Steps“ se definira naziv provjere „Name“, URL stranice koju želimo provjeravati „URL“ i status koji se očekuje „*Required status codes*“ koji je obično 200 što znači da je stranica dostupna.

U slučaju da je stranica preusmjerena zbog prelaska na novu domenu ili s nesigurnog protokola (HTTP) na sigurni protokol (HTTPS) tada je potrebno uključiti opciju praćenja redirekcije „*Follow redirects*“ što je bilo potrebno obzirom da smo unijeli sljedeće postavke: Name: Status, URL: https://www.fpz.unizg.hr, Follow redirects: uključeno, Required status codes: 200. Kako se stranica preusmjerava u

https://www.fpz.unizg.hr/web/naslovna/novosti javljat će statusni kod 301 u slučaju da se ne uključi opcija „*Follow redirects*“.



Slika 27. Kreiranje nadzora web stranice, Zabbix

Većinu mrežnih uređaja u Zabbix-u nadzirati ćemo pomoću agentskog programa koji je potrebno instalirati na nadzirani uređaj kako bi agent poslao tražene podatke Zabbix poslužitelju. Popis podržanih operativnih sustava vidljiv je tablici 2.

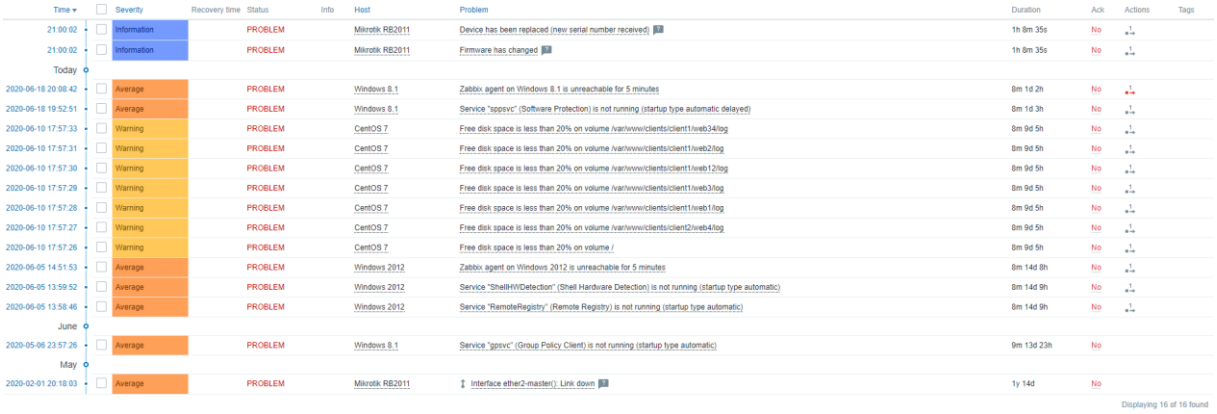
AIX	FreeBSD	Linux	OS X	OpenBSD	Windows	Solaris	HPUX	Tru64Unix

Tablica 2. Podržani operativni sustavi Zabbix agenta

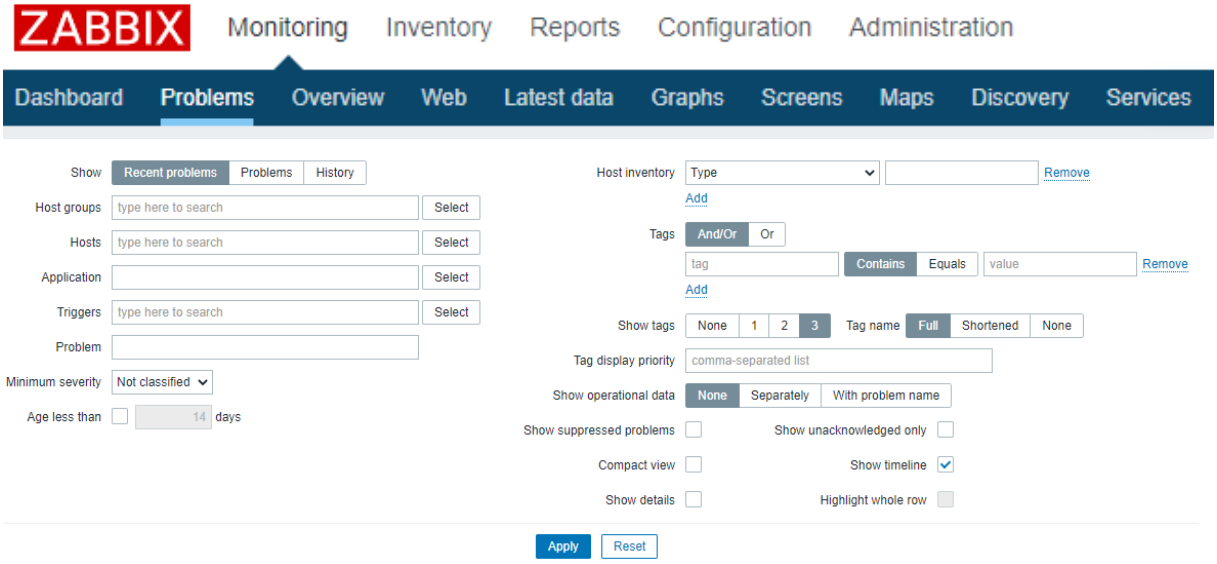
U slučaju kada nije moguće instalirati agent-a na operativni sustav koriste se dostupni protokoli poput SNMP-a, WMI, ICMP, SSH i sl, no bez agenta potrebna je dodatna konfiguracija i prilagodba nadziranog uređaja.

4.1.5. Detekcija i prikaz grešaka mrežnih uređaja - Zabbix

Osnovni prikaz stanja svih uređaja može se pratit putem nadzorne ploče tj. „*Dashbord*-a“ (Slika 22.), a pojedinačno stanje mrežnih uređaja moguće je vidjeti pod izbornikom Monitoring i zatim podizbornici „Dashboard“, „Problems, „Overview“, „Web“, „Latest Data“, „Graphs“, „Screens“ i „Maps“. Izbornik „Problems“ prikazuje sve dostupne greške (Slika 28.), a moguće ih je filtrirati po velikoj količini dostupnih parametara, a neki od njih naziv, vrsta greške, starost greške, oznaka, grupa i drugo (Slika 29.).



Slika 28. Prikaz problema svih mrežnih uređaja



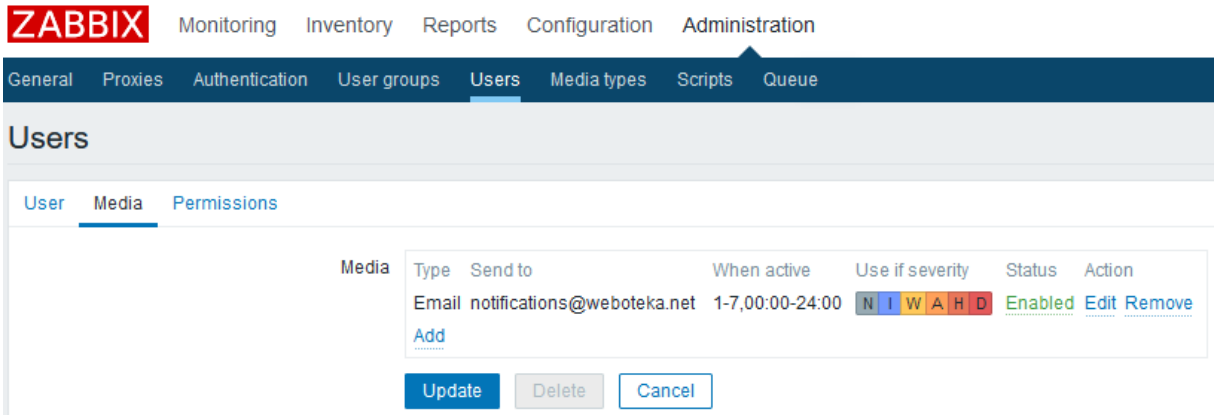
Slika 29. Dostupni parametri za filtraciju problema

Filteri su prikladni u situacijama kada je potrebno izdvojiti određeni mrežni uređaj u slučaju kada se nadzire stotine mrežnih uređaja i tisuće njihovih servisa ili je potrebno izolirati slučajeve ponavljanja određenog problema radi evidencije ili detekcije ponavljanja problema.

4.1.6. Slanje obavijesti o greškama – Zabbix

Najčešći način slanja obavijesti o greškama iz programske podrške je putem e-pošte. E-pošta može biti nepouzdana zbog toga što prolazi više mrežnih točaka koje ovise o drugim administratorima poput email servera, vatrozida, IPS (engl. *Intruder Prevention Systems*) sustava i drugih. Ipak, koristi se obzirom da za taj način slanja obavijesti nije potrebno plaćati nikakve naknade kao što se plaća kod slanja SMS-a, Viber-a, Messenger-a i sličnih komercijalnih društveno socijalnih računa, a danas svaki

mobilni uređaj kao i pametni sat ima mogućnost primanja email-ova. Zabbix podržava slanje notifikacija putem email-a, SMS-a i XMPP-a. Podešavanje načina slanja obavijesti se nalazi pod izbornikom „Administration“, „Users“ i zatim je pod tabom „Media“ kod svakog korisnika moguće podesiti željeni način slanja obavijesti kao i definirati u koje dane i vrijeme se šalju notifikacije određenog prioriteta (Slika 30.).



Slika 30. Podešavanje načina slanja obavijesti korisniku

Izgled i sadržaj notifikacija moguće je definirati putem predložaka, standardno se šalje notifikacija koja sadržava vrijeme problema (Date), naziv problema (Problem name), uređaj (Host), prioritet problema (Severity) te identifikacijsku oznaku (Original problem ID) (Slika 31.).

Problem has been resolved at 17:30:02 on 2021.02.15
Problem name: Interface ether5(): High bandwidth usage >90%
Host: Mikrotik RB2011
Severity: Warning

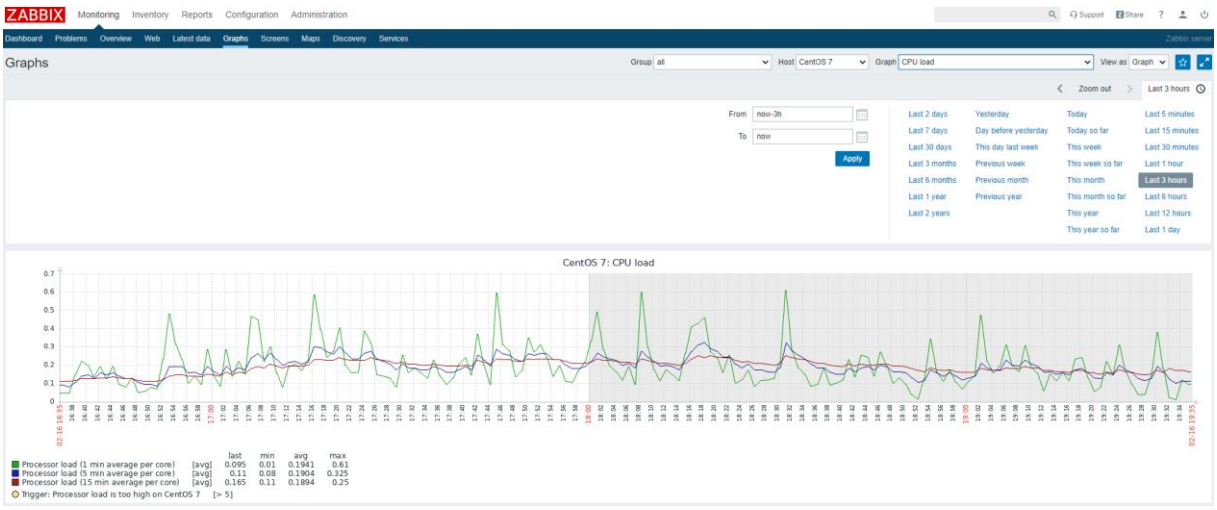
Original problem ID: 128476

Slika 31. Primjer standardne Zabbix notifikacije

Sadržaj notifikacija moguće je podesiti pod izbornikom „Configuration“, „Actions“, potrebno je izabrati akciju i zatim „Operation“ za podešavanje sadržaja problema, „Recovery operations“ za podeđavanje sadržaja oporavka od problema i „Update operations“ za podešavanje sadržaja kada se mijenja stanje problema.

4.1.7. Pregled i izrada izvještaja - Zabbix

Izrada izvještaja u PDF-u ili sličnom obliku u Zabbixu nije moguća, no kako postoji pregled stanja, dostupnosti i poslanih notifikacija za mrežne uređaje moguće je napraviti izvoz podataka o mrežnom uređaju preko print opcije Internet preglednika te na taj način napraviti izvještaj (Slika 32.).



Slika 32. Izrada izvještaja nadziranog uređaja u Zabbix-u

Postoje besplatni dodaci koji omogućuju generiranje periodičkih izvještaja no nisu podržani od strane Zabbix-a kao što i nije moguće dobiti podršku za iste. Kako se radi o otvorenom kodu, moguće je angažirati programera koji bi kreirao željene izvještaje. Izvještaji su najčešće potrebni ukoliko se nadziru mrežni uređaji trećih osoba primjerice unutar podatkovnog centra ili uprava želi pratiti stanje dostupnosti mrežnih servisa koji mogu utjecati na prihode tvrtke te na taj način utvrditi može li se poboljšati dostupnost mrežnih servisa kroz ulaganja u softversko ili hardversko sklopovlje. Ipak, barem osnovni izvoz u tekstualnu datoteku bi bio od velikog značaja radi lakšeg praćenja i evidencije potencijalnih poteškoća na mrežnim uređajima, što je jedan značajan nedostatak Zabbix-a.

4.1.8. Nadogradnja Zabbix-a

Kako je za potrebe ovog rada inicijalno instalirana verzija 4.2.4 Zabbix-a u međuvremenu je izdana manja nadogradnja v4.2.8 te potpuno nova inačica Zabbix-a v4.4.8. Za postupak nadogradnje na novo izdanje potrebno je potražiti upute na Zabbix službenim stranicama, dok se manja nadogradnja može obaviti standardnom sistemskom naredbom:

```
root@zabbix ~ $ yum update
```

Nakon izvršavanja navedene naredbe ponuditi će se nadogradnja paketa instaliranih na sustav, ali i nadogradnja zabbix paketa na v4.2.8 (Slika 33.) te je potrebno odgovorit sa „*yes*“ kako bi se nadogradio sustav. Nisu potrebne nikakve dodatne radnje te je potrebno samo osvježiti Internet preglednik sa Zabbix sučeljem kako bi promjena bila vidljiva.

```
zabbix-agent                                    x86_64                    4.2.8-1.el7
zabbix-release                                  noarch                    4.2-2.el7
zabbix-server-mysql                             x86_64                    4.2.8-1.el7
zabbix-web                                      noarch                    4.2.8-1.el7
zabbix-web-mysql                                noarch                    4.2.8-1.el7
```

Slika 33. Dostupno ažuriranje za Zabbix pakete

Nadogradnja na novu inačicu 4.4.8 nije značajno kompliciranija u odnosu na v4.2.8, jer također zahtjeva od administratora prijavu u konzolu i izvršavanje slijedećih naredbi koje su dostupne na Zabbix službenim stranicama.

```
root@zabbix ~ $ systemctl stop zabbix-server

root@zabbix ~ $ rpm -Uvh https://repo.zabbix.com/zabbix/4.4/rhel/7/x86_64/zabbix-release-4.4-1.el7.noarch.rpm

root@zabbix ~ $ yum upgrade zabbix-server-mysql zabbix-web-mysql zabbix-agent

root@zabbix ~ $ systemctl start zabbix-server
```

Mogućnost nadogradnje programske podrške za nadzor je iznimno važna kako bi se uvijek koristila zadnja dostupna verzija. Također novije verzije ispravljaju postojeće probleme i greške, optimiziraju rad aplikacije i ponekada donose poboljšanja i nove funkcionalnosti. Zabbix životni ciklus se može provjeriti na službenim stranicama Zabbix-a, a za verziju 4.x podrška će biti pružana do kraja 2023-e godine, nakon čega je poželjno nadograditi na iduću dostupnu verziju.

4.2. Nagios XI

Nagios je napravio Ethan Galstad 1999-te godine sa skupinom programera. Nakon inicijalnog izdanja uz pomoć brojne Nagios zajednice, tisuće različitih projekata za Nagios implementirano je u Nagios kakav poznajemo danas. Nagios-om je moguće nadzirati kompletne IT infrastrukture kako bi se osiguralo da sustavi, aplikacije, servisi i poslovni procesi ispravno rade na način da upozori tehničko osoblje na potencijalni problem kako bi mogli provjeriti i popraviti problem prije nego dođe do kvara i utjecaja na poslovnu okolinu [16]. Nagios XI je komercijalna nadogradnja na Nagios Core 4 sustav koji je u potpunosti besplatan no nije usporediv sa Zabbix-om zbog nedostatka web sučelja te je zbog toga izabran Nagios XI kako bi usporedba bila valjana. Unatoč tome što je komercijalan proizvod za potrebe ovog rada korištene su besplatne mogućnosti, iako su značajno ograničene, dovoljne su za nadzor nekoliko uređaja.

4.2.1. Mogućnosti Nagios XI-a

Kako bi mogao konkurirati svojem najvećem suparniku Zabbix-u, Nagios XI sadrži praktički iste mogućnosti, uz par dodatnih funkcionalnosti koje se mogu koristiti samo u plaćenoj verziji. U osnovnoj verziji moguće je nadzirati kompletnu informatičku infrastrukturu, komponente, aplikacije, operativne sustave, mrežne protokole, sistemsku metriku i mrežnu infrastrukturu. Dodatnu vrijednost pruža na stotine besplatnih dodataka drugih korisnika koji omogućavaju nadzor praktički svih aplikacija, servisa i sustava. Osnova Nagios XI-a je Nagios Core 4 nadzorni sustav koji korisnicima omogućava visokokvalitetni nadzor performansi nekog sustava pomoću vrlo dobro optimiziranih procesa koji omogućuju skalabilnost i efektivnost nadzora.

Pruža pregled cjelokupnog informatičkog sustava i poslovnih procesa sa centralnog mjesta putem Internet preglednika. Svaki korisnik si može prilagoditi radnu površinu sa podacima koje smatra korisnima.

Automatizirao integrirano grafičko praćenje smjera i kapacitiranja sustava omogućava poduzećima pravovremeno planiranje nadogradnju zastarjele i neefikasne infrastrukture. Notifikacije o problemima se šalju sistem administratorima, vlasnicima i krajnjim korisnicima putem email-a ili SMS poruka kako bi pravovremeno reagirali.

Grafičko sučelje dopušta prilagodbu izgleda i dizajna kao i opcija za svakog korisnika posebno čime se omogućava dodatna fleksibilnost.

Putem Internet preglednika administratori mogu kontrolirati konfiguraciju nadzora, sistemske postavke i još niz mogućnosti krajnjim korisnicima ili članovima tima.

Pomoću konfiguracijskih čarobnjaka korisnik dodaje nove uređaje, servise i aplikacije sve bez potrebe poznavanja kompleksnih koncepta nadzora.

Napredno korisničko sučelje omogućava klijentima da vide samo infrastrukturu koja je njima podešena i autorizirana. API omogućava jednostavnu integraciju sa drugima aplikacijama, a na tisuće besplatnih dodataka od strane Nagios zajednice proširuju mogućnosti nadziranja [17].

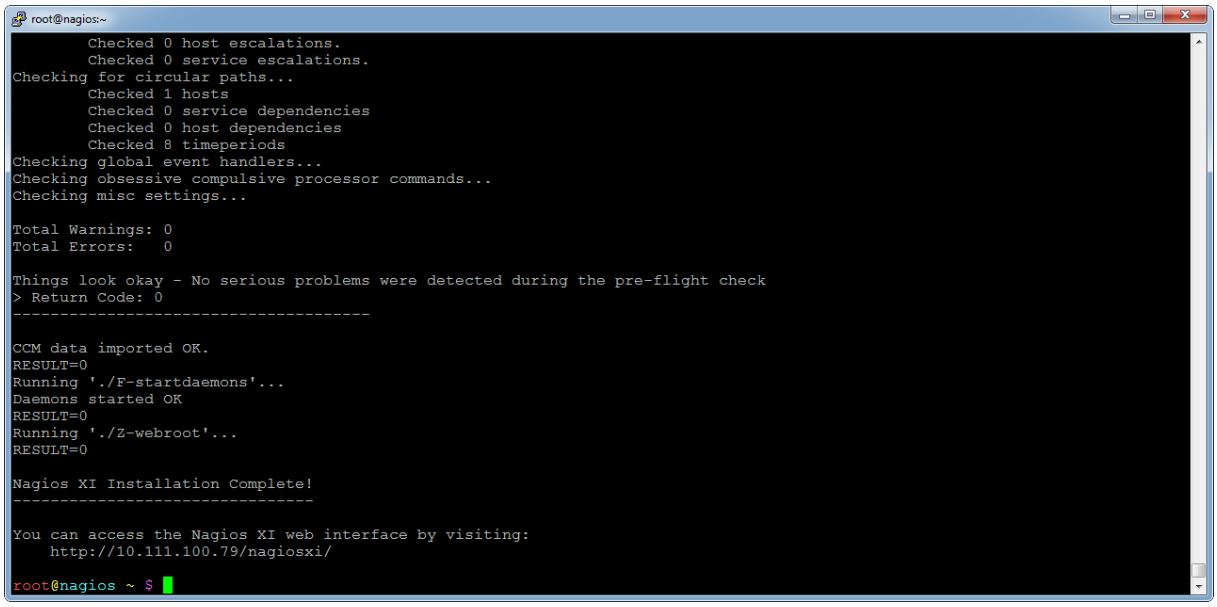
4.2.2. Instalacija Nagios-a

Kao i kod Zabbixa, instalacija je moguća samo na Linux/Unix operativne sustave te se i u ovom slučaju koristio CentOS operativni sustav [15], dok je za bazu kod novih instalacija moguće koristiti samo MySQL/MariaDB ili PostgreSQL ukoliko se nadograđuje postojeća verzija Nagios-a sa PostgreSQL bazom [19].

Nakon prijave u CentOS kao root potrebno je pokrenuti slijedeću naredbu i pričekati da instalacija završi:

```
root@nagios ~ $ curl https://assets.nagios.com/downloads/nagiosxi/install.sh | sh
```

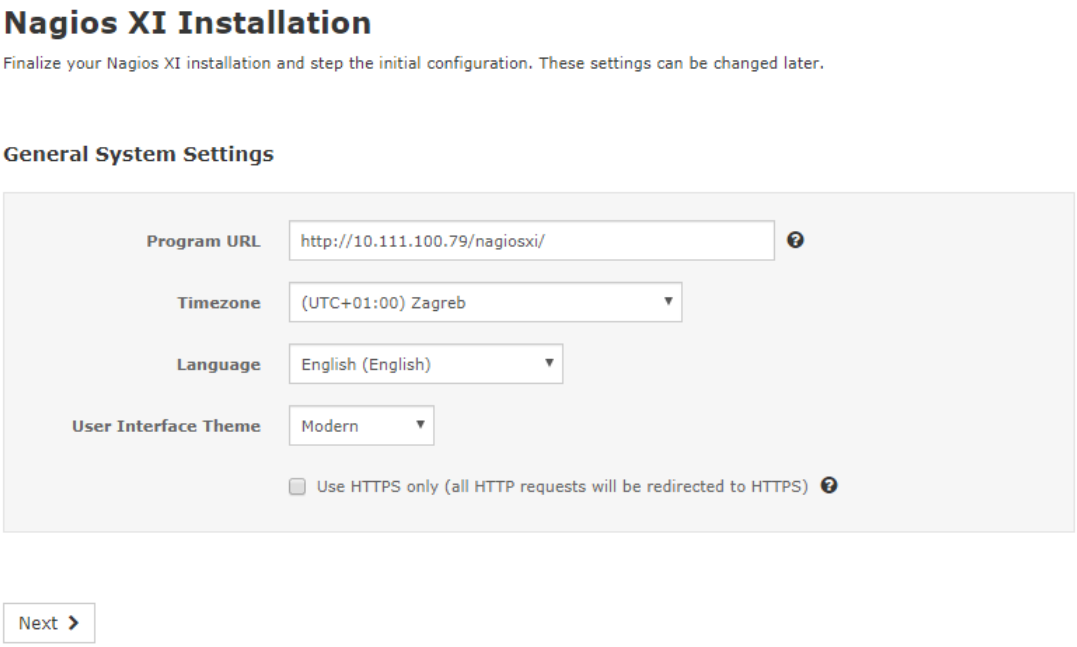
Na kraju će se pojaviti poruka da je instalacija Nagios XI-a dovršena (Slika 34.) i da se možemo prijaviti putem Internet preglednika obzirom da se kao i kod Zabbix-a konfiguracija i upravljanje obavlja preko web sučelja. Iako je potrebno čekati desetak minuta da instalacija završi, instalacija je puno jednostavnija od Zabbix-a i ne iziskuje dodatno konfiguriranje već se sve odrađuje automatski.



Slika 34. Instalacija Nagios-a

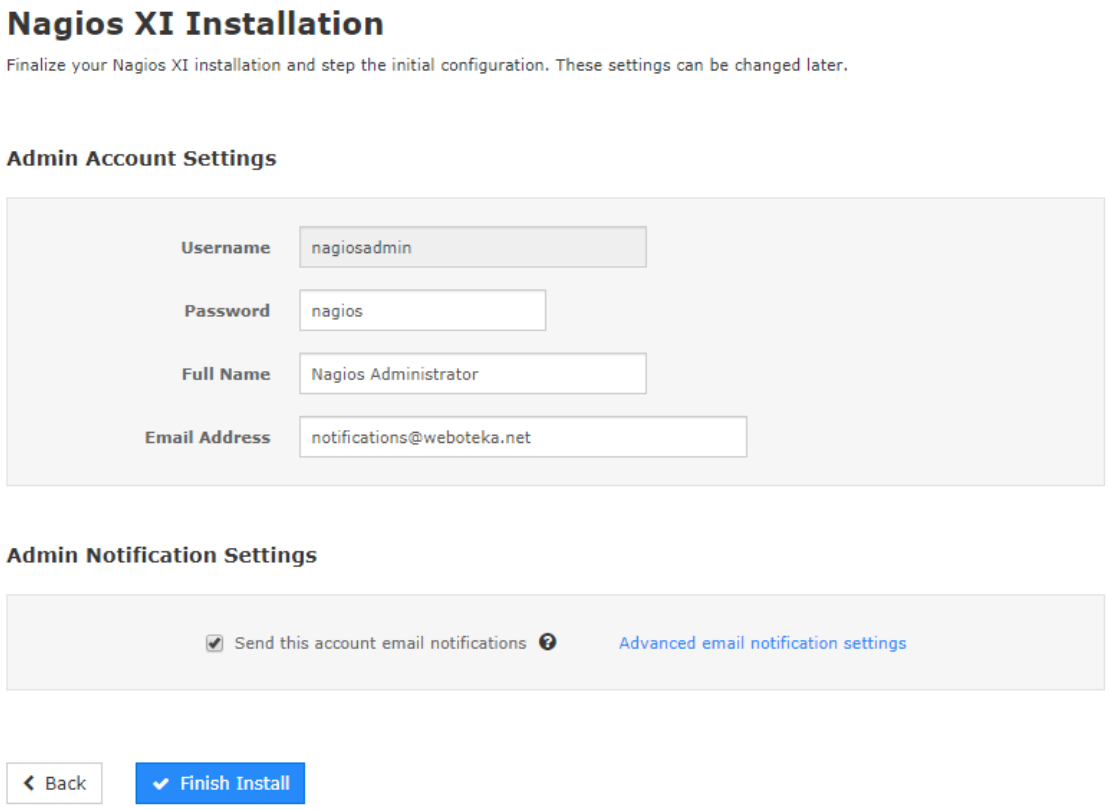
Preostalu konfiguraciju Nagios XI servera kao i dodavanje mrežnih obavlja se putem Internet preglednika te je u njemu potrebno otvoriti lokacijsku adresu na kojoj smo instalirali Nagios XI server, što je u ovom slučaju: http://10.111.100.79/nagiosxi/ i zatim proći kroz završni dio instalacije.

Nakon učitavanja pojaviti će se Nagios XI ekran dobrodošlice što znači da je instalacija uspješno obavljena (Slika 35.) i obzirom da su sve postavke ispravno definirane dovoljno je kliknuti „Next“ (Slika 36.).

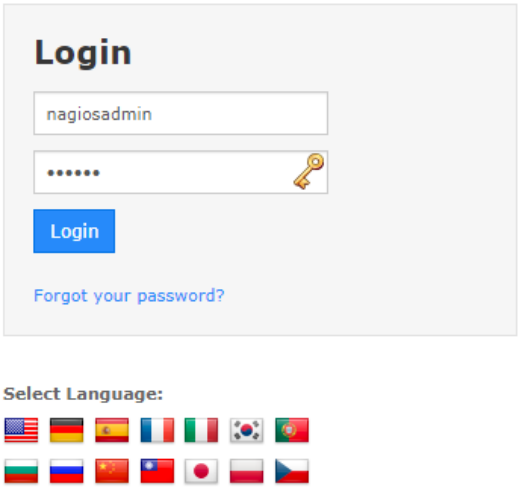


Slika 35. Početna stranica finalne konfiguracije Nagios XI servera.

Na drugoj stranici predefiniranom administratorskom računu „nagiosadmin“ podesiti ćemo pristupnu šifru „nagios“, a za email adresu unijeti „notifications@weboteka.net“ email adresu na koju će dolaziti sve obavijesti vezane uz Nagios XI nadzor, ali će se koristiti i kod Zabbix-a. Za kraj je potrebno kliknuti „Finish Install“, nakon čega će se prikazati ekran za inicijalnu prijavu (Slika 37.).

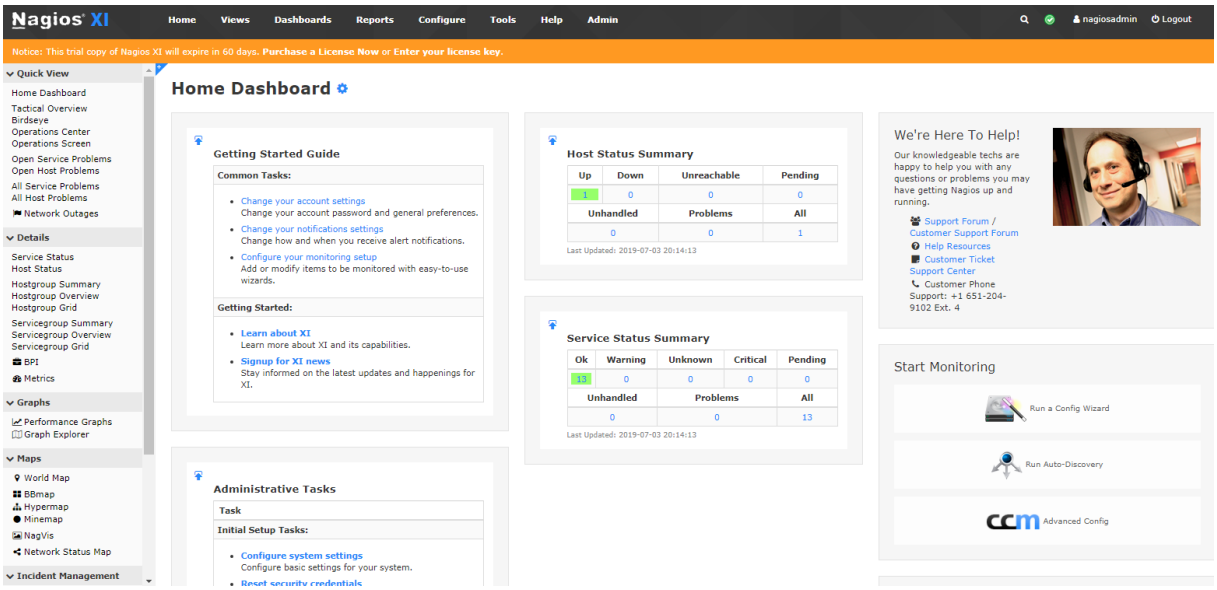


Slika 36. Druga stranica konfiguracije Nagios XI servera



Slika 37. Nagios XI inicijalna prijava.

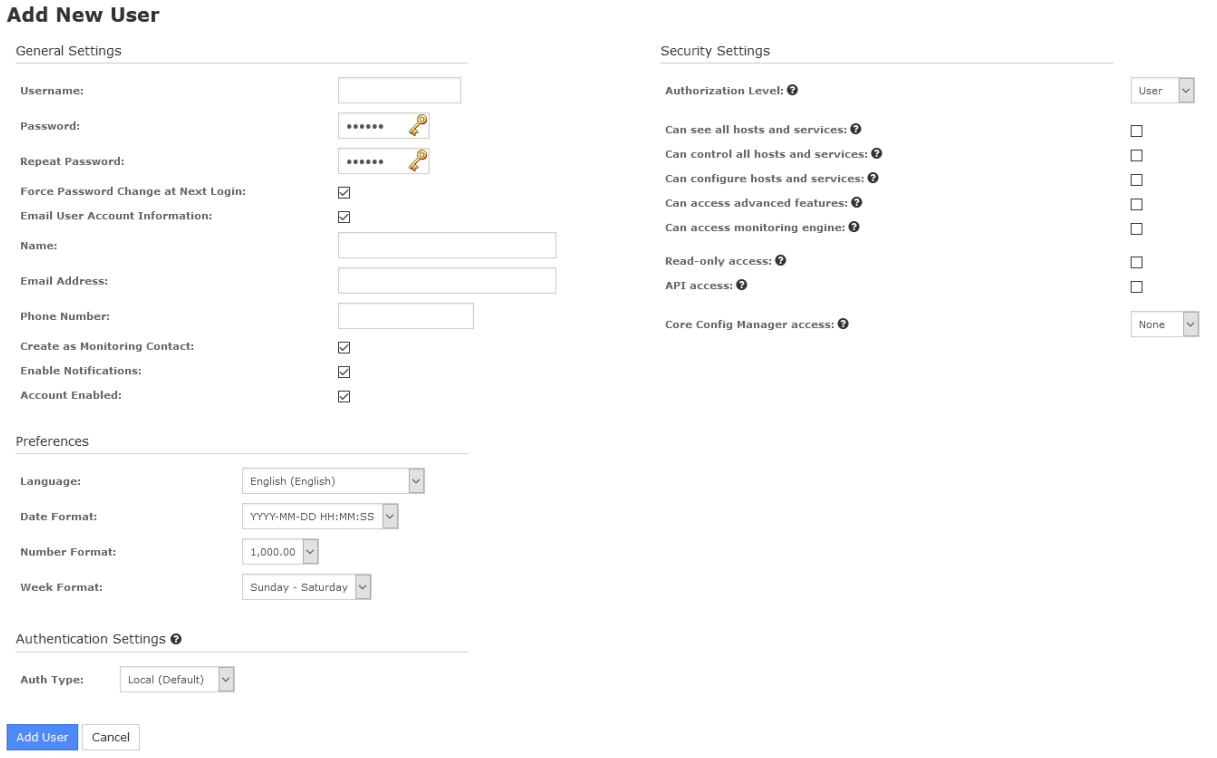
Nakon prijave u Nagios XI otvara se prihvat licenčnih uvjeta i zatim se prikazuje radna ploča na koju je potrebno dodati mrežne uređaje za nadzor, kao i kod Zabbix-a inicijalno se nadzire samo poslužitelj na kojem je Nagios instaliran (Slika 38.)



Slika 38. Nagios XI radna ploča

4.2.3. Administracija Nagios korisnika

Korisnike u Nagios-u možemo kreirati lokalno ili povezati lokalne korisnike sa AD ili LDAP bazom i na prvi pogled vidljivo je da kod kreiranja korisnika imamo nešto više dostupnih opcija u odnosu na kreiranje Zabbix korisnika (Slika 39.)



Slika 39. Dodavanje novog Nagios korisnika

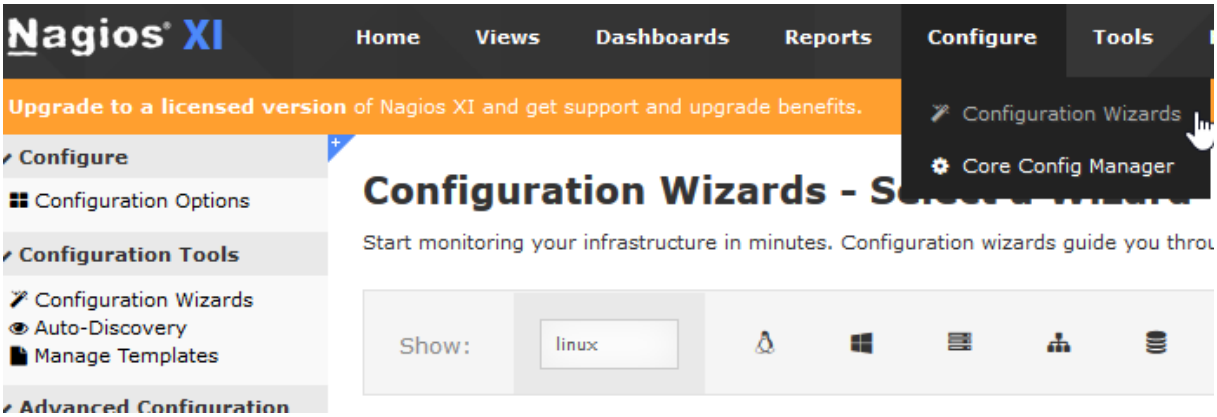
Kreiranju korisnika se pristupa putem izbornika „Admin“ i zatim „Add New Users“, no nema mogućnosti definiranje grupe korisnika, primjerice ako imamo korisnike koji imaju omogućen samo pristup određenim kategorijama uređaja. Nagios

podržava slanje notifikacija i kreiranje grupa za određenu grupu mrežnih uređaja, no nema podršku za administraciju grupnih korisnike unutar samog Nagios-a što smatramo nedostatkom radi lakšeg upravljanja korisnicima i dozvolama trećih osoba.

Od zanimljivih značajki kod kreiranja novog korisnika je mogućnost izmjene pristupne šifre kod iduće prijave kao i niz dodatnih personalizacija poput datuma, formatiranja, broja telefona, fino podešavanje sigurnosnih postavki i sl.. Vizualno je sve pregledno na jednoj strani u odnosu na Zabbix te pridonosi razumljivosti podešavanju postavki korisnika. U odnosu na Zabbix, Nagios ne nudi HTTP pristup putem Internet poslužitelja, ali to i nije veliki nedostatak.

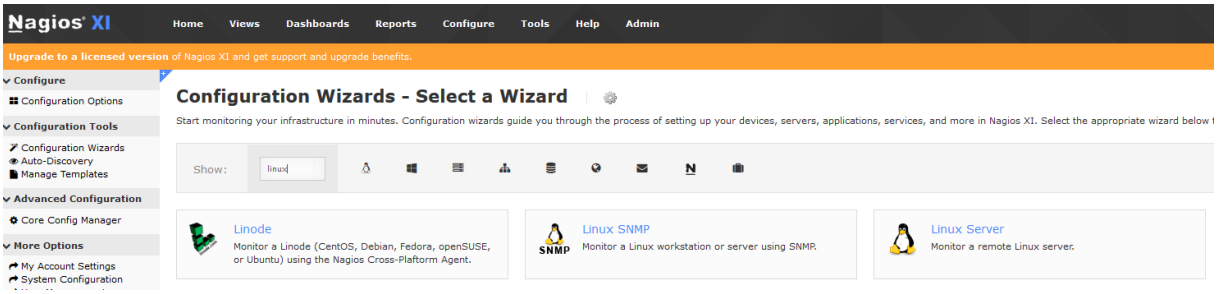
4.2.4. Postupak dodavanje mrežnih uređaja u Nagios

Dodavanje mrežnih uređaja je jednostavno te se obavlja pomoću konfiguracijskog čarobnjaka izborom opcije „Configure“ na glavnom izborniku te zatim klikom na „Configuration Wizards“ u padajućem izborniku (Slika 40.).



Slika 40. Nagios: dodavanje mrežnog uređaja

Da bismo dodali Linux server potrebno je upisati „linux“ unutar „Show“ kućice za pretraživanje kako bi se prikazao prikaz opcije za nadzor mrežnih uređaja baziranih na Linux-u i zatim odabrati „Linux Server“ (Slika 41.).



Slika 41. Filtriranje predefiniranih konfiguracija po nazivu „linux“

Nakon izbora ponuđenog „Linux Server“-a pojaviti će se prozor za unos detalja o mrežnom poslužitelju kojeg želimo nadzirati te je potrebno unijeti IP adresu ili naziv domene kao i vrstu Linux distribucije koja će se nadzirati (Slika 42.).

Slika 42. Nagios: unos detalja o Linux mrežnom uređaju

Kada su dodani svi mrežni uređaji koji će se nadzirati u Nagios-u potrebno je pričekati nekoliko minuta da Nagios prikupi inicijalne podatke i prikaže eventualne probleme o mrežnim uređajima na početnoj stranici. Windows mrežni uređaji se u Nagiosu nadziru putem WMI-a obzirom da Nagios nativno podržava WMI bez dodatne konfiguracije i instalacije agenta. Popis podržanih operativnih sustava vidljiv je tablici 3.

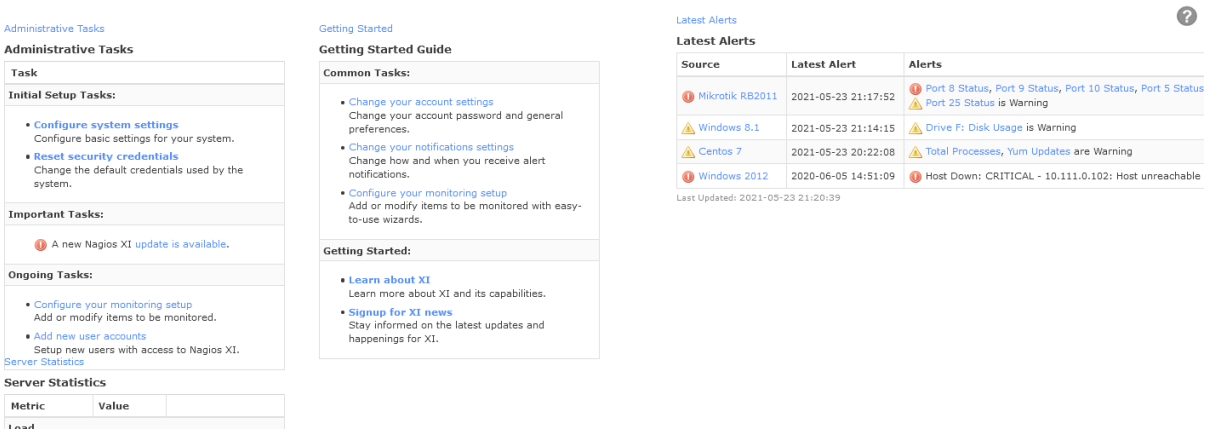
AIX	FreeBSD	Linux	OS X	OpenBSD	Windows	Solaris

Tablica 3. Podržani operativni sustavi NCPA agenta

Iz tablice je vidljivo da Nagios XI može agentskim programom nadzirati sve značajnije operativne sustave kao i kod konkurentske programske podrške Zabbix, no također zahtjeva dodatnu konfiguraciju i prilagodbu nadziranog uređaja.

4.2.5. Detekcija i prikaz grešaka mrežnih uređaja u Nagios-u

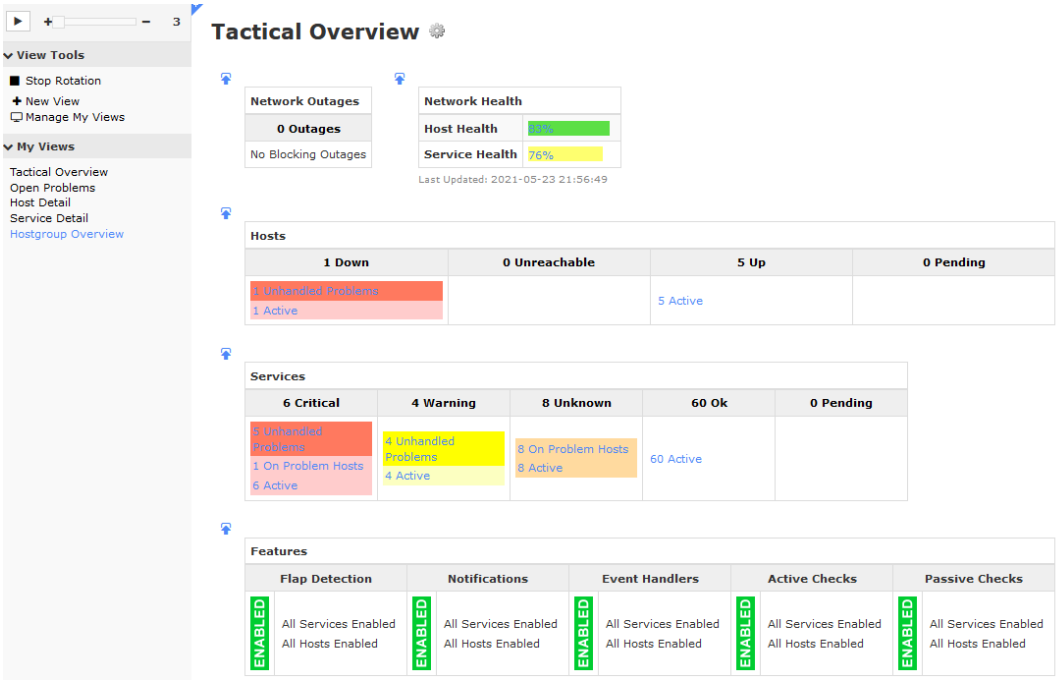
Centralni nadzor putem „*Dashboard*-a“ nam nudi cjelokupan prikaz svih problema s mrežnim uređajima, ali i potrebne aktivnosti koje se mogu provesti na Nagios sustavu poput dostupne nadogradnje, status opterećenja procesora i potrošnje memorije Nagios servera pa do uputa kako podesiti korisnički račun, notifikacije, nadzor i općenite upute za korištenje Nagios-a (Slika 43.).



Slika 43. Nagios centralni prikaz stanja svih sustava

Vizualni prikaz „Dashboard“-a je moguće personalizirati za svakog korisnika i podesiti prema vlastitim željama dodajući „Dashlet“-e po želji kao i kod Zabbix-a što bitno pridonosi funkcionalnosti obzirom da različiti korisnici mogu nadzirati potpuno različite mrežne uređaje.

„Dashlet“-i su prozorčići u kojim se mogu prikazivati informacije po želji, a u odnosu na Zabbix, Nagios nudi nešto veći izbor, a od značajnih vrijedi istaknuti prikaz URL-a po želji čime primjerice možemo prikazati nadzor nekog nepodržanog uređaja, ali kojem se može pristupiti putem URL-a, prikaz mrežnog prometa po lokacijama radi bržeg uočavanja slabije propusnosti i zagušenosti, dostupnost Nagios nadogradnje, Google Map koji će na karti prikazati status mrežnih uređaja ukoliko postoji više udaljenih lokacija, prikaz problematičnih portova sa SANS (engl. *SysAdmin, Audit, Network, and Security*) podatkovnog poslužitelja kao izvor potencijalnih izvora zaraze i propusta koji mogu ukazati na potrebne provjere, RSS vijesti i druge.

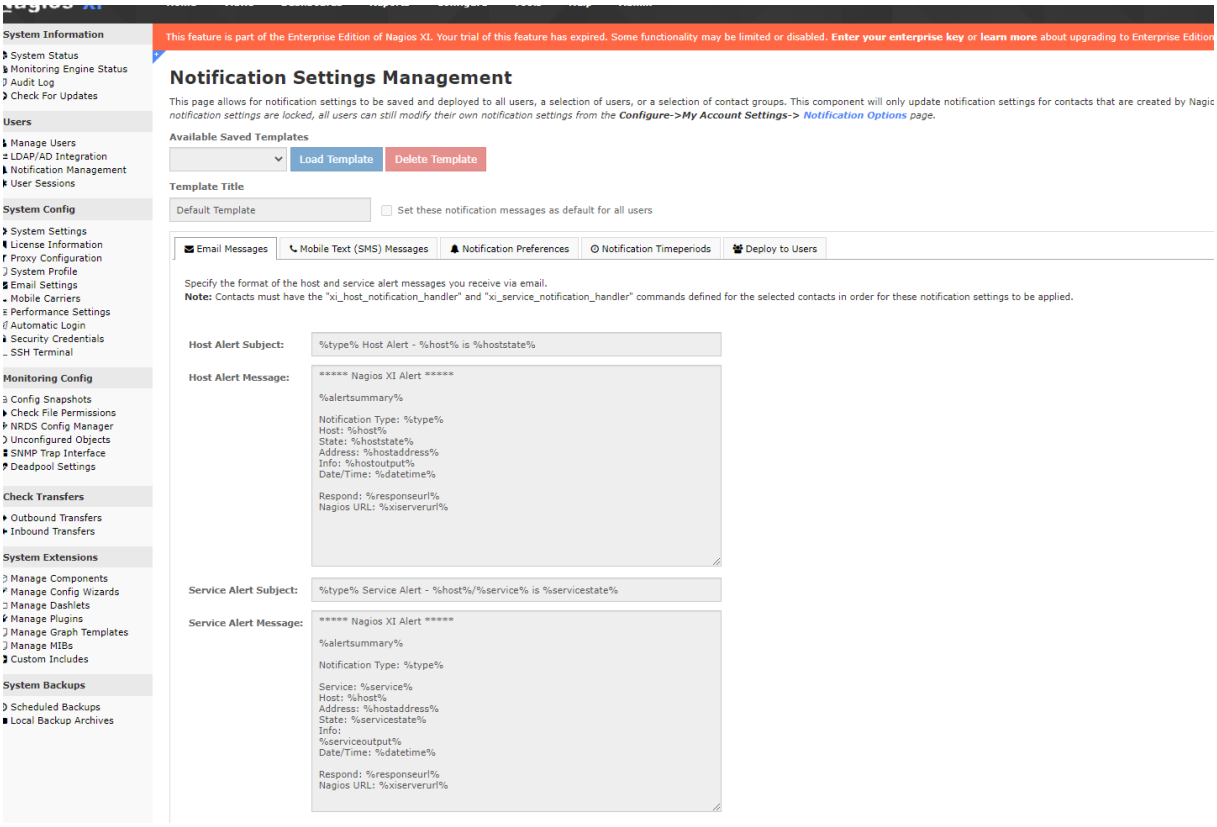


Slika 44. Nagios: prikaz različitih pregleda poteškoća

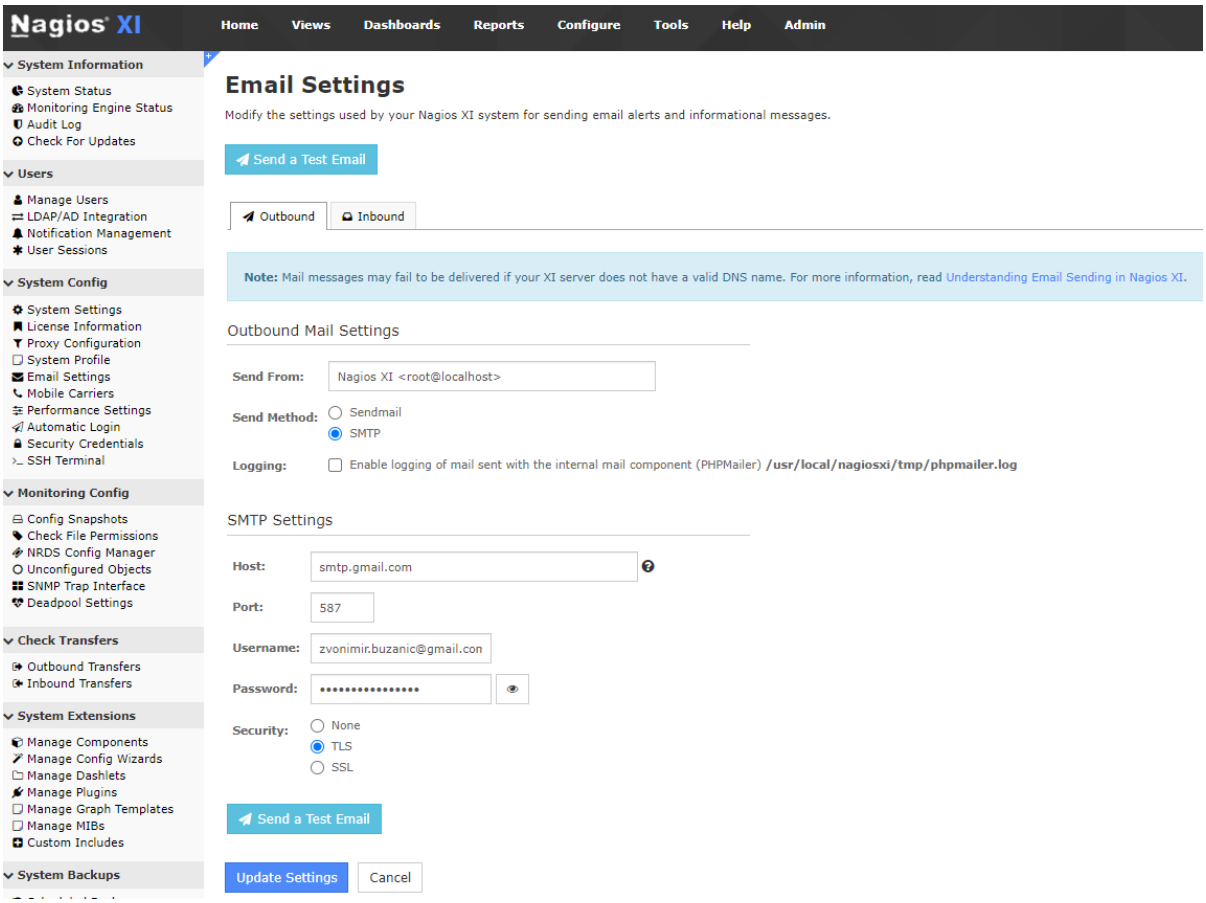
Osim centralnog pregleda postoji pregled mrežnih uređaja pod „Views“ gdje je definirano pet različitih pregleda. „*Tactical Overview*“ prikazuje cjelokupno stanje sustava, mrežnih uređaja i servisa te je moguće na svako od tih stanja kliknuti i dobiti detaljnije stanje. „Open Problems“ prikazuje trenutne probleme svih mrežnih uređaja kao i sumarni prikaz svih uređaja i servisa na koje je također moguće kliknuti za detaljniji prikaz. „Host detail“ prikazuje detalje pojedinačnih mrežnih uređaja, stanje, zadnji upit, trajanje nadzora, graf performansi i slično. „Service Detail“ prikazuje popis stanja svih servisa svakog mrežnog uređaja, također sa prikazom zadnjeg upita, trajanja nadzora, graf i sl.. Zadnji „Hostgroup overview“ omogućuje grupirani prikaz mrežnih uređaja. Većinu navedenih prikaza i statusa moguće je dodati na „Dashboard“. Poput Zabbixa prikazi problema su jasni, ali je ovdje moguće lakše identificirati poteškoću te je vizualno vrlo jasno kada i gdje postoji poteškoća sa mrežnim uređajem i servisom čime u ovom slučaju prednost ima Nagios (Slika 44.).

4.2.6. Slanje obavijesti o greškama u Nagios-u

Notifikacije su dio plaćene verzije Nagios-a te je iste moguće isprobati samo za vrijeme testnog perioda Enterprise verzije (Slika 45.). Podržano je slanje putem email-a, ali i putem SMS-a, kao i podešavanje predložaka za obje vrste notifikacija. Također je moguće podesiti kojim korisnicima i u koje vrijeme će se slati određene notifikacije ili grupa notifikacija vezana uz uređaje. Za upotrebu Email notifikacija je potrebno predefinirati postavke mail servera kako bi iste ispravno radile, u našem slučaju podešen je *Google* besplatni račun i radio je bez poteškoća (Slika 46.).



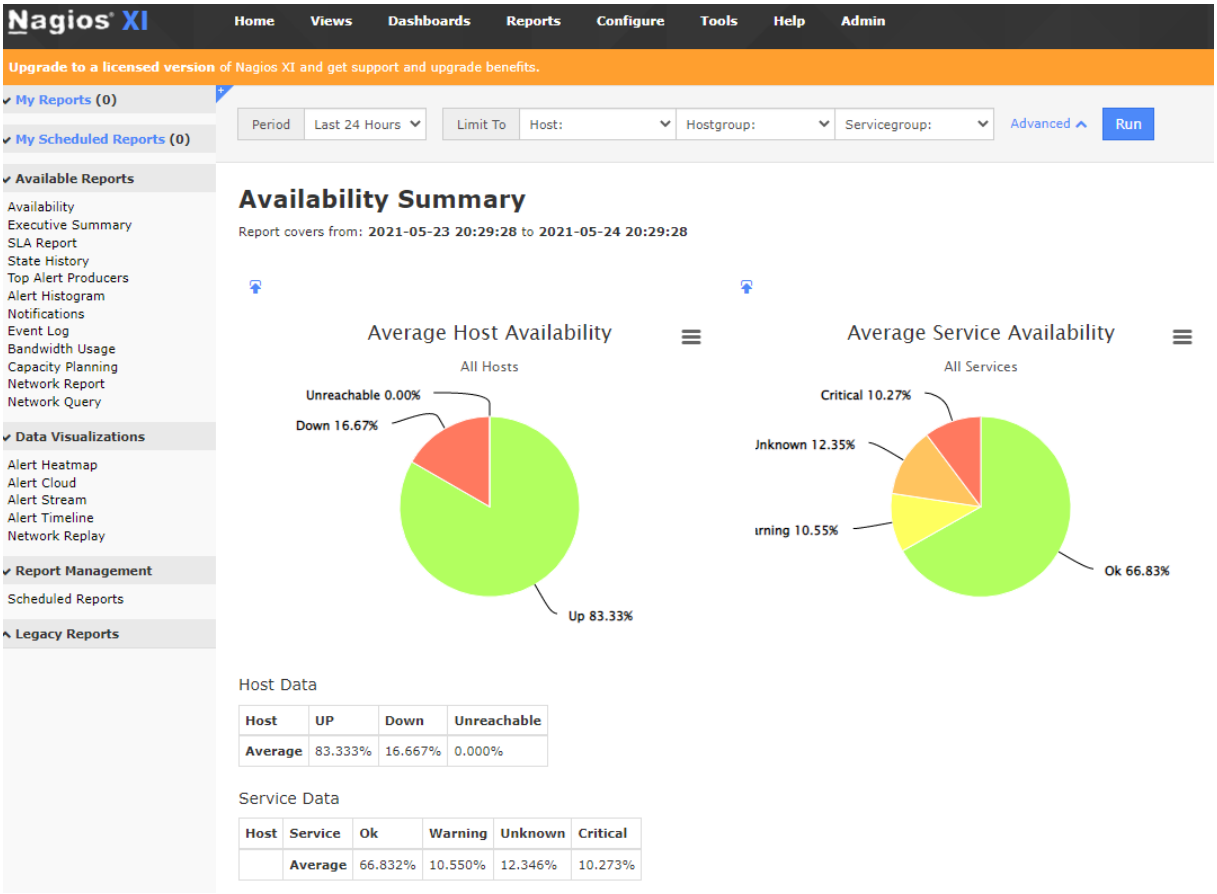
Slika 45. Notifikacijske mogućnosti Nagios XI-a



Slika 46. Podešavanje e-pošte

4.2.7. Pregled i izrada izvještaja u Nagios-u

Direktnim klikom na izbornik „Reports“ Nagios XI nativno podržava kreiranje i periodičko slanje izvještaja koje je dostupno samo u plaćenoj verziji na željene destinacije radi praćenja dostupnosti sustava [20] (Slika 47.). Moguće je izabrati predefinirane vremenske periode kao što su dan, tjedan, mjesec, godina, ali i korisnički definirane vremenske periode za željeni nadzirani mrežni uređaj ili uređaje. Osim općenite dostupnosti, nude se SLA (engl. *Service Level Agreement*) izvještaji (plaćena verzija), zatim povijest grešaka, povijest notifikacija, potrošnje podatkovnog prometa nekog mrežnog uređaja i planiranje kapaciteta (plaćena verzija) radi vizualnog utvrđivanja postoji li potreba za povećanjem resursa nekog sustava ili njegovih dijelova.



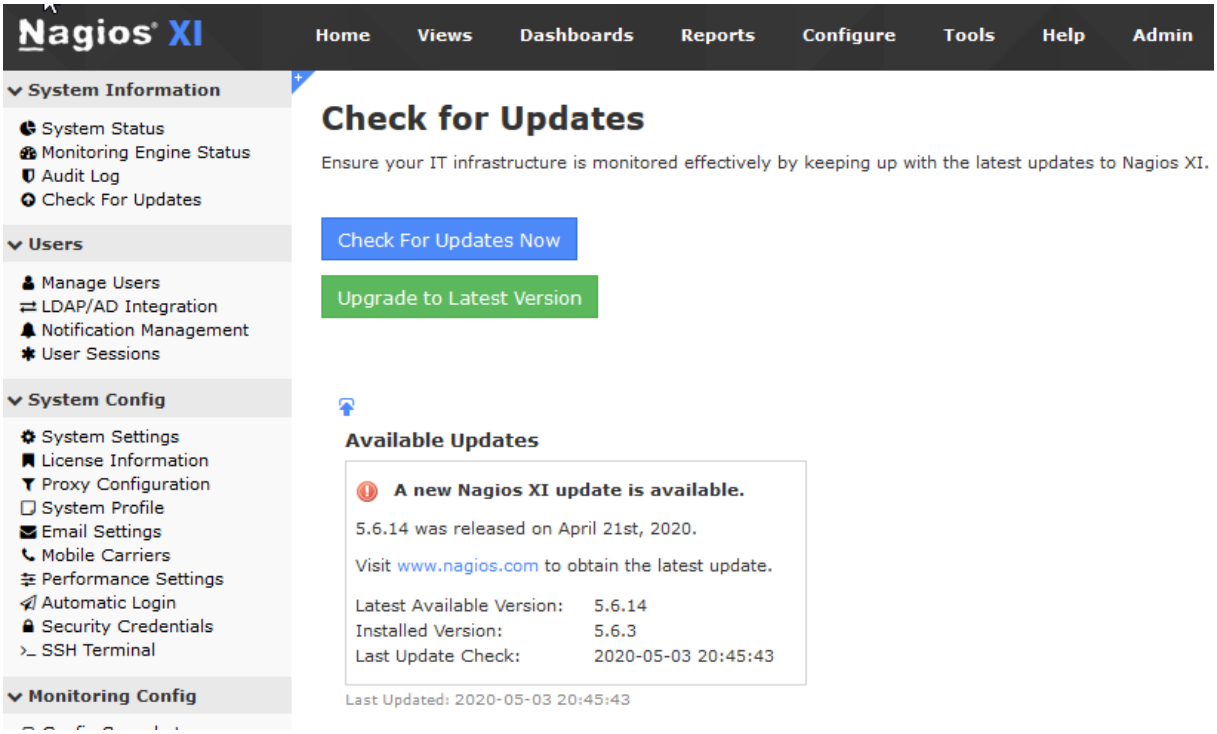
Slika 47. Generiranje izvještaja dostupnosti u Nagios XI

Vizualni pregled dostupnosti se najčešće koristi za kreiranje periodičkih izvještaja po potrebi, ali i lakšeg praćenja dostupnosti određenog mrežnog uređaja ili skupine mrežnih uređaja koje pripadaju nekom segmentu mreže.

4.2.8. Nadogradnja Nagios-a

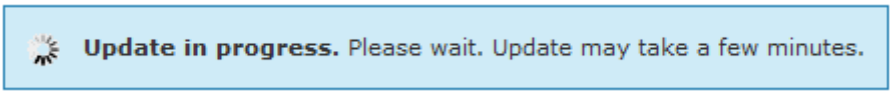
Nadogradnja Nagios-a je iznimno jednostavna, točnije, u odnosu na nadogradnju Zabbix-a je značajno jednostavnija. Potrebno je otvoriti Nagios

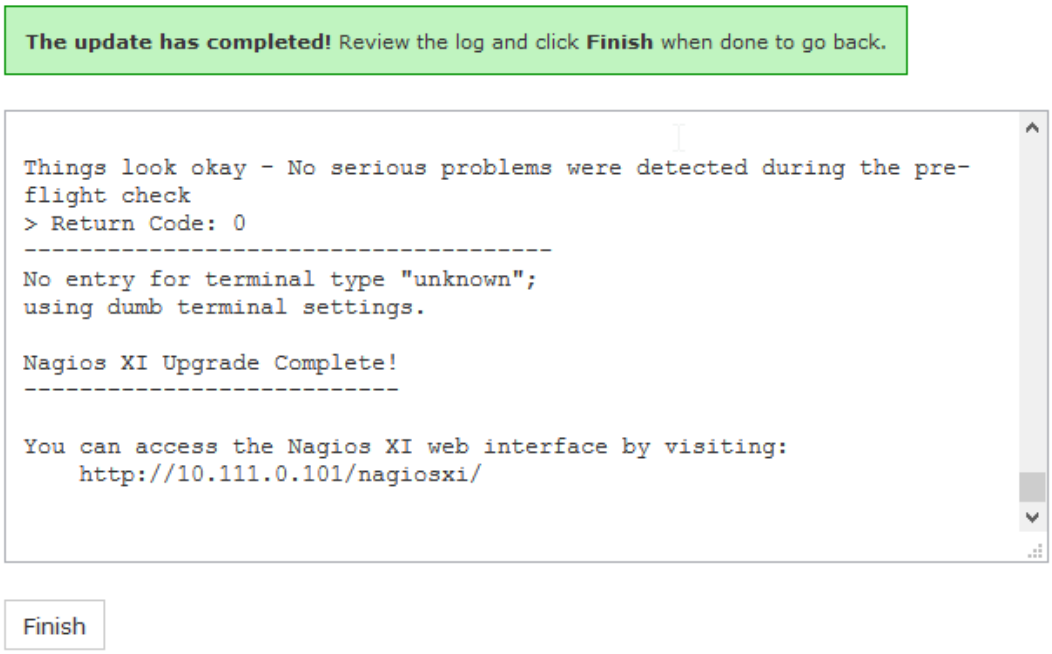
administraciju te kliknuti „Admin“, zatim „Check For Updates“ i zatim „Check For Updates Now“ (Slika 48.).



Slika 48. Nadogradnja Nagios-a kroz web sučelje

Nakon provjere, ukoliko je dostupna nova verzija, pojaviti će se informacija koja verzija je dostupna, kada je izdana kao i gumb za nadogradnju. Jednostavnim klikom na „Upgrade to Latest Version“ Nagios će automatski obaviti nadogradnju na zadnju dostupnu verziju 5.6.14 sa verzije 5.6.3 (Slika 49).





Slika 49. Tijek nadogradnje Nagios-a na zadnju dostupnu verziju

Potrebno je pričekati nekoliko minuta i bez dodatne interakcije sa korisnikom nadogradnja će biti izvršena, u slučaju problema nadogradnja će biti obustavljena i ukoliko postoje ispisat će se greške, a zatim vratiti sustav na prijašnju verziju.

5. Usporedba programske podrške za nadzor mrežnih uređaja

Kod usporedbe programske podrške Nagios i Zabbix koristile su se funkcionalnosti bitne za nadzor mrežnih uređaja kao što su kompatibilnost mrežnih uređaja s programskom podrškom za nadzor tj. podržava li programska podrška nadzor mrežnog uređaja bez potrebe za instalacijom agentske aplikacije na nadzirani uređaj, detekciju greške ili nepravilnosti rada mrežnog uređaja, slanje obavijesti nakon detekcije greške tj. nepravilnosti i izvještaje iz kojih je moguće vidjeti koliko često i u koje vrijeme su se greške događale kako bi bilo moguće napraviti preventivne radnje čime bi se te greške u budućnosti otklonile ili smanjio njihov broj, također kod usporedbe će se prikazati mogućnosti programske podrške za nadzor poput broja uređaja, protokola, operativnih sustava, jednostavnosti instalacije i konfiguracije i slično. Nadzirani uređaji (CentOS 7, Windows 2012, Mikrotik RB2011, Canon TS5050, Microsoft IIS) su u oba slučaja bili podržani i bez ikakvih poteškoća praćeni te su pravodobno stizale informacije o problemima, greškama ili nedostupnošću uređaja te su se oba nadzorna sustava pokazala iznimno stabilnim.

Detekcija problema na promatranim sustavima se na obje programske podrške obavljala u vrlo sličnim vremenskim razdobljima tj. oba bi detektirala problem unutar pet minuta i poslala notifikaciju o problemu. Na CentOS 7 stroju, Nagios je detektirao

pad Apache Web servera (HTTPS), nadogradnje operativnog sustava „Yum updates“, preveliki broj pokrenutih procesa i problem sa diskovnim prostorom (Slika 50.):

Host	Service	Status	Duration	Attempt	Last Check	Status Information
Centos 7	Apache Web Server	Critical	1m 31s	5/5	2022-01-30 22:46:16	inactive
	Yum Updates	Warning	6h 18m 49s	5/5	2022-01-30 22:44:03	YUM WARNING: O/S requires an update.
	Total Processes	Warning	5d 17h 4m 47s	5/5	2022-01-30 22:42:55	PROCS WARNING: 153 processes
	/ Disk Usage	Warning	6d 8h 50m 51s	5/5	2022-01-30 22:46:52	DISK WARNING - free space: / 5684 MiB (15.44% inode=89%):

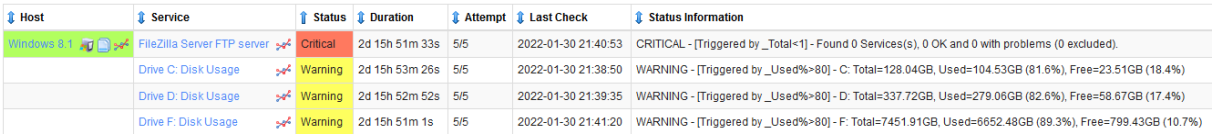
Slika 50: Detektirani problemi na CentOS 7 operativnom sustavu (Nagios XI)

Zabbix na istom sustavu slično, ali na malo drugačiji način prikazuje probleme. Detektirao je pad HTTPS servisa tj. Apache Web servera i problem sa diskovnim prostorom (Slika 51.). Može se primijetiti da nedostaje nadogradnja operativnog sustava, broj pokrenutih procesa se može zanemariti jer je u današnje vrijeme očekivano da na sustavu bude pokrenuto i preko 200 mikroservisa što je manji minus za Nagios XI. Nedostatak prikaza potrebnih nadogradnji kod Zabbix-a je dosta značajan obzirom da su sigurnosne nadogradnje operativnog sustava iznimno važne i vrlo je bitno nadograditi operativni sustav na vrijeme kako bi spriječili potencijalne upade na server ili onemogućavanje rada sustava zbog propusta u starijoj verziji nekog vitalnog servisa. Pregledom stranice Zabbix službene podrške, dostupna je konfiguracija za nadzor nadogradnji CentOS 7 sustava [21], no nije dio službenog Zabbix servera, niti je podržana kao službena konfiguracija. Dodatna kritika na račun Zabbix-a je što je pad HTTP servisa okarakterizirao kao „*Average*“, a obzirom da bez HTTP servera stranica ne može posluživati klijente, trebalo bi svakako važnost greške postaviti na kritično „*Critical*“. Kako je moguće po želji u konfiguraciji *template*-a, ali i konfiguraciji pojedinačnog uređaja mijenjati važnost greške, može se smatrati manjim nedostatkom.

Time	Severity	Recovery time	Status	Info	Host	Problem
22:41:58	Average		PROBLEM		CentOS 7	HTTPS service is down on CentOS 7
22:33:21	Warning		PROBLEM		CentOS 7	Free disk space is less than 20% on volume /var/www/clients/client1/web12/log
22:33:20	Warning		PROBLEM		CentOS 7	Free disk space is less than 20% on volume /var/www/clients/client1/web1/log
22:33:19	Warning		PROBLEM		CentOS 7	Free disk space is less than 20% on volume /var/www/clients/client2/web4/log
22:33:18	Warning		PROBLEM		CentOS 7	Free disk space is less than 20% on volume /var/www/clients/client1/web3/log
22:33:17	Warning		PROBLEM		CentOS 7	Free disk space is less than 20% on volume /var/www/clients/client1/web2/log
22:33:16	Warning		PROBLEM		CentOS 7	Free disk space is less than 20% on volume /var/www/clients/client1/web34/log
22:33:15	Warning		PROBLEM		CentOS 7	Free disk space is less than 20% on volume /

Slika 51: Detektirani problemi na CentOS 7 operativnom sustavu (Zabbix)

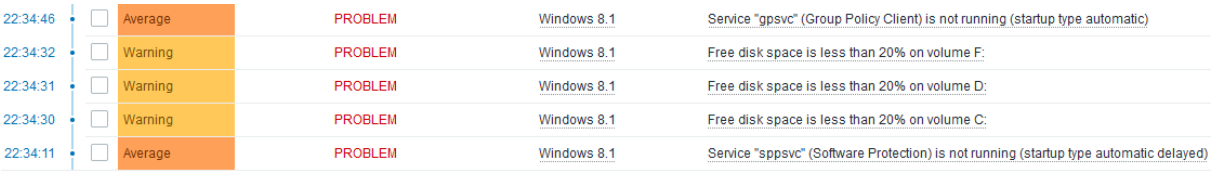
Nagios XI je na operativnom sustavu Windows 8.1 detektirao problem sa softverom Filezilla Server FTP, no iz greške nije jasno o kakvom se točno problemu radi (Slika 52.). Na sustavu je pokrenut navedeni servis, no nisu uočene nikakve poteškoće s njegovim radom te je provjerom utvrđeno da se radi o pogrešno detektiranoj grešci jer Nagios XI pretpostavlja da servis mora biti nazvan „Filezilla Server“ što na ovom sustavu nije bio slučaj. Osim navedenog, detektirao je i problem sa prostorom na tri tvrda diska, C:, D: i F:



Host	Service	Status	Duration	Attempt	Last Check	Status Information
Windows 8.1	FileZilla Server FTP server	Critical	2d 15h 51m 33s	5/5	2022-01-30 21:40:53	CRITICAL - [Triggered by _Total<1] - Found 0 Services(s), 0 OK and 0 with problems (0 excluded).
	Drive C: Disk Usage	Warning	2d 15h 53m 26s	5/5	2022-01-30 21:38:50	WARNING - [Triggered by _Used%>80] - C: Total=128.04GB, Used=104.53GB (81.6%), Free=23.51GB (18.4%)
	Drive D: Disk Usage	Warning	2d 15h 52m 52s	5/5	2022-01-30 21:39:35	WARNING - [Triggered by _Used%>80] - D: Total=337.72GB, Used=279.06GB (82.6%), Free=58.67GB (17.4%)
	Drive F: Disk Usage	Warning	2d 15h 51m 1s	5/5	2022-01-30 21:41:20	WARNING - [Triggered by _Used%>80] - F: Total=7451.91GB, Used=6652.48GB (89.3%), Free=799.43GB (10.7%)

Slika 52. Detektirani problemi na Windows 8.1 operativnom sustavu (Nagios XI)

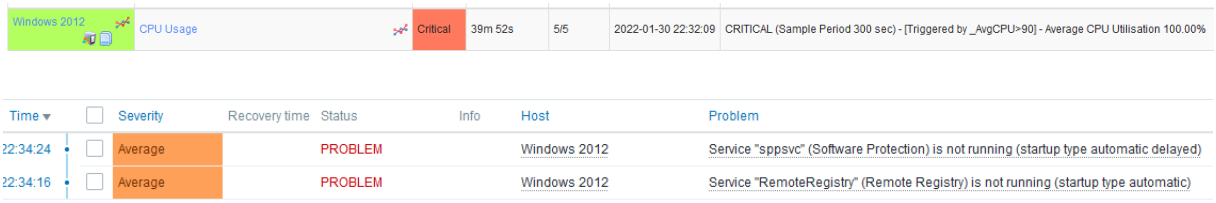
Kao i kod CentOS 7 operativnog sustava, Zabbix uredno detektira probleme s diskovnim prostorom te uredno javlja da FTP server radi. Dodatno nadzire i servise operativnog sustava Windows te je prijavio problem sa „Group Policy Client“ i „Software protection“ servisima (Slika 53.). Provjerom na sustavu, servisi su bili nedostupni, no nisu od značajne važnosti, te se pokreću automatski kada su potrebni, što je i naznačeno u Zabbixu kao prosječno važna greška „Average“.



22:34:46	Average	PROBLEM	Windows 8.1	Service "gpsvc" (Group Policy Client) is not running (startup type automatic)
22:34:32	Warning	PROBLEM	Windows 8.1	Free disk space is less than 20% on volume F:
22:34:31	Warning	PROBLEM	Windows 8.1	Free disk space is less than 20% on volume D:
22:34:30	Warning	PROBLEM	Windows 8.1	Free disk space is less than 20% on volume C:
22:34:11	Average	PROBLEM	Windows 8.1	Service "sppsvc" (Software Protection) is not running (startup type automatic delayed)

Slika 53. Detektirani problemi na Windows 8.1 operativnom sustavu (Zabbix)

Treći nadzirani sustav Windows Server 2012 imao je pokrenuti program koji je 100% opterećivao CPU i otprilike je trošio 80% memorije sustava, no Nagios XI je detektirao da je problematičan samo CPU, dok Zabbix uopće nije detektirao problem niti sa CPU-om niti memorijom (Slika 54.)!

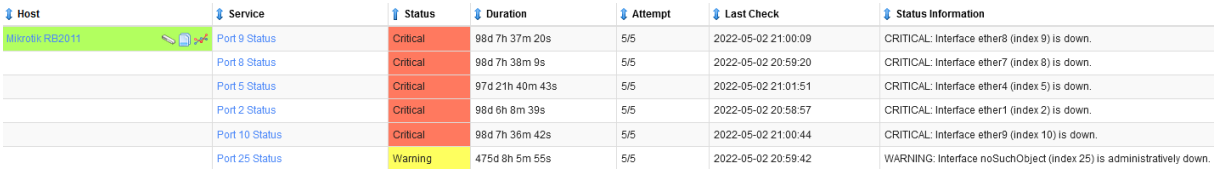


Host	Service	Status	Duration	Attempt	Last Check	Status Information
Windows 2012	CPU Usage	Critical	39m 52s	5/5	2022-01-30 22:32:09	CRITICAL (Sample Period 300 sec) - [Triggered by _AvgCPU>90] - Average CPU Utilisation 100.00%

Time	Severity	Recovery time	Status	Info	Host	Problem
22:34:24	Average		PROBLEM		Windows 2012	Service "sppsvc" (Software Protection) is not running (startup type automatic delayed)
22:34:16	Average		PROBLEM		Windows 2012	Service "RemoteRegistry" (Remote Registry) is not running (startup type automatic)

Slika 54. Razlika detektiranih problema na Windows Server 2012 (Zabbix)

Kod mrežnog preklopnika tj. usmjerivača Mikrotik RB2011 Nagios XI je sve neiskorištene mrežne priključke detektirao kao kritičan problem (Slika 55.). Iz sigurnosnih razloga takva detekcija je vrlo korisna informacija za mrežnog administratora kako bi onemogućio korištenje tih mrežnih priključaka od neovlaštenih osoba i to tako da ne mogu spojiti svoj mrežni uređaj na slobodni priključak i neovlašteno pristupati podacima sa mreže bez ometanja ostalih mrežnih uređaja. Zabbix ne detektira mrežne priključke koji nisu aktivni na mrežnom uređaju već je obavijestio administratora da je nadograđen operativni sustav Mikrotik uređaja tj. „firmware“.



Host	Service	Status	Duration	Attempt	Last Check	Status Information
Mikrotik RB2011	Port 9 Status	Critical	98d 7h 37m 20s	5/5	2022-05-02 21:00:09	CRITICAL: Interface ether8 (index 9) is down.
	Port 8 Status	Critical	98d 7h 38m 9s	5/5	2022-05-02 20:59:20	CRITICAL: Interface ether7 (index 8) is down.
	Port 5 Status	Critical	97d 21h 40m 43s	5/5	2022-05-02 21:01:51	CRITICAL: Interface ether4 (index 5) is down.
	Port 2 Status	Critical	98d 6h 8m 39s	5/5	2022-05-02 20:58:57	CRITICAL: Interface ether1 (index 2) is down.
	Port 10 Status	Critical	98d 7h 36m 42s	5/5	2022-05-02 21:00:44	CRITICAL: Interface ether9 (index 10) is down.
	Port 25 Status	Warning	475d 8h 5m 55s	5/5	2022-05-02 20:59:42	WARNING: Interface noSuchObject (index 25) is administratively down.

Slika 55. Detektirani problemi na mrežnom uređaju Mikrotik RB2011 (Nagios XI)

Time	Severity	Recovery time	Status	Info	Host	Problem
21:00:02	Information		PROBLEM		Mikrotik RB2011	Firmware has changed

Slika 56. Zabbix nije detektirao poteškoće osim nadogradnje Mikrotik sustava

Nagios XI se pokazao kao puno pouzdaniji prilikom detekcije mrežnih uređaja i problema, no za bežični mrežni printer nadziran putem SNMPv1 ili v3 nismo automatikom uspjeli dodati niti jednu stavku poput statusa signala ili statusa boje osim same mrežne dostupnosti uređaja Canon TS5050 (Slika 57.).

Canon TS5050	Uptime	Ok	N/A	1/5	2022-05-02 22:06:10	SNMP OK - 334000

Slika 57. Nagios XI je detektirao samo mrežnu prisutnost

Ipak, ni Zabbix nije detektirao ništa više od mrežne dostupnosti Canon TS5050 uređaja, pa su time oboje izjednačeni u nemogućnosti nadzora navedenog uređaja.
U slučaju da administrator preuzme dodatne pakete i/ili konfiguracijske module sa Nagios ili Zabbix stranica, nadzor uređaja će biti točniji te će sadržavati značajno više informacija kao što je navedeni status bežične mreže tj. kvaliteta i jačina bežičnog signala, status pojedine boje, broj ispisanih stranica i slične informacije.

Programske podrške Nagios i Zabbix bez poteškoća su pratile stanje dostupnosti Microsoft IIS web servera stranice Fakulteta prometnih znanosti te nisu uočeni problemi. Za postavljanje nadzora navedene web stranice kod Zabbix-a je bilo potrebno proučiti dokumentaciju kao i savjete za nadzor sa Zabbix foruma, dok je kod Nagios-a dodavanje web stranice u nadzor bilo trivijalno.

Programska podrška za nadzor	Nagios Core (XI)	Zabbix
Podržani operativni sustavi	RHEL 7/8 CentOS 7 & Stream 8 Oracle Linux 7/8 Debian 9/10/11 Ubuntu 16/18/20 (LTS)	Linux IBM AIX FreeBSD NetBSD OpenBSD HP-UX Mac OS X Solaris
Podržane baze podataka	MySQL/MariaDB PostgreSQL	MySQL/MariaDB Oracle PostgreSQL IBM DB2 SQLite
Podržani protokoli	TCP/IP, SNMP, WMI, Agent, Email	TCP/IP, SNMP, WMI, Agent
Broj podržanih uređaja	Neograničeno (7 u demo verziji)	Neograničeno
Automatska detekcija mrežnih uređaja	Da	Da
Jednostavna instalacija programske podrške za nadzor	Da	Da, potrebno znanje Linux-a
Mogućnost nadogradnje programske podrške	Da, direktno iz aplikacije	Da, putem nadogradnje operativnog sustava
Jednostavna konfiguracija uređaja	Da	Da
Podržani sustavi za agentsku aplikaciju	AIX FreeBSD Linux OS X OpenBSD Windows Solaris	AIX FreeBSD Linux OS X OpenBSD Windows Solaris HP-UX Tru64Unix
Slanje obavijesti o greškama	Email, SMS, IM	Email, SMS, IM
Povijest grešaka i stanja sustava	Da	Da
Grafički prikaz stanja sustava	Da	Da
Generiranje i slanje izvještaja	Da, automatsko slanje se plaća	Da, nije moguće slati
SLA izvještaji	Da, plaćena verzija	Da
Automatska detekcija novih nadogradnji za operativni sustav nadziranog uređaja	Da	Ne
Nadzor web stranica	Da	Da

Tablica 4. Usporedba mogućnosti programske podrške za nadzor

6. Zaključak

Nagios XI programska podrška kao i Zabbix razvijani su preko dvadeset godina i međusobna su konkurencija obzirom da su oba otvorenog koda te ih je moguće koristiti bez naknade, ali zahtijevaju inicijalno konfiguriranje koje mora biti kvalitetno odrađeno. Nagios XI se vremenom orijentirao na plaćenu podršku prije svega za web sučelje jer se u počecima podešavao isključivo preko konfiguracijskih datoteka, što ne znači da nije upotrebljiv bez plaćanja, no tek sa plaćenom licencom ukidaju se ograničenja nadzora što je jedini veći nedostatak Nagios-a. Dugi niz godina na tržištu te malena prednost koju je Nagios XI imao u odnosu na Zabbix učinile su ga jednim od najpoznatijih u programskoj podršci za nadzor. Zabbix je pak u potpunosti besplatan i ne postoje ograničenja, a moguće je angažirati profesionalnu (plaćenu) podršku i to mu daje malu prednost kod izbora.

Instalaciju programske podrške moguće je izvršiti pomoću uputa od strane administratora/informatičara i ne zahtjeva predznanje ili poznavanje Linuxa, no Nagios instalacijska skripta značajno olakšava cijelu proceduru te ga čini dostupnijim običnim korisnicima, dok je kod Zabbix-a poželjno osnovno poznavanje Linux-a/BSD-a.

Nadogradnje programske podrške za nadzor mrežnih uređaja su redovite i poželjne, a kao i kod instalacije, nadogradnja Nagios XI-a ne zahtijeva poznavanje rada na Linux-u već se jednostavno pokreće iz web sučelja.

Administracija korisnika, dodavanje mrežnih uređaja i detekcija servisa su kod Nagios-a bile nešto jednostavnije i brže, te je glavni nedostatak Zabbix-a što je potrebno preuzeti dodatnu konfiguraciju određenog mrežnog uređaja sa Zabbix stranica i u tom slučaju je potrebno poznavati što i kako želimo nadzirati.

Izrada izvještaja u Zabbix-u nije dostupna u smislu generiranja periodičnog stanja ali je dostupna putem web sučelja i na taj način se može pohraniti kao PDF dokument. Automatsko generiranje izvještaja kao u slučaju Nagios-a je poželjno, uz napomenu da je potrebno imati Nagios licencu za automatsko generiranje standardnih ili SLA izvještaja, ručno generiranje je dostupno i u besplatnoj inačici.

Za profesionalnu upotrebu radi što kvalitetnijeg nadzora sustava poželjno je angažirati stručnjaka koji je upoznat sa radom izabrane programske podrške radi što veće dostupnosti i uporabljivosti cijelog sustava bez obzira o kojoj podršci se radilo.
Važno je napraviti plan nadzora i definirati koje mrežne točke ili servisi imaju prioritet kako nadzorni sustav ne bi nepotrebno opterećivao mrežni sustav i slao nepotrebne i brojne notifikacije administratorima zbog čega administrator zbog količine informacija neće reagirati pravovremeno i u konačnici provjeriti stanje sustava što je uočeno kod obje programske podrške kada se konfiguriraju po standardnim postavkama zbog čega će sustavi za nadzor poslati na tisuće nepotrebnih i neželjenih upozorenja.

U konačnici Nagios XI djeluje kao ozbiljniji izbor, ali Zabbix sigurno preuzima dio Nagios tržišta iz vrlo jednostavnog razloga, a to je cijena korištenja. Prije odabira bilo kojeg od programske podrške potrebno je dobro proučiti zahtjeve i mogućnosti, zatim podesiti programsku podršku za nadzor te se nakon testnog perioda odlučiti na željeni sustav jer dostupnost mrežnog sustava i njegovih servisa nemaju cijenu.

Popis literature

[1] Hallberg B. *Networking, a Beginner's Guid, 6th edition*. New York: McGraw-Hill Education; 2014.

[2] Tanenbaum A.S., Wetherall D.J. *Computer networks, 5th edition*. Seattle: Prentice Hall; 2011. https://www.mbit.edu.in/wp-content/uploads/2020/05/Computer-Networks-5th-Edition.pdf

[3] Mikalsen A, Borgesen P. *Local Area Network Managment, Design and Security*. Chichester: , John Wiley & Sons Ltd, Baffins Lane; 2002.

[4] Begović M. *Održavanje tehničkih sustava*. Zagreb: Sveučilište u Zagrebu, Fakultet prometnih znanosti; 2003.

[5] Mauro D., Schmidt K. *Essential SNMP, 2nd edition.* O'Reilly Media, Inc.: 2005. https://www.oreilly.com/library/view/essential-snmp-2nd/0596008406/

[6] Miller M.A. *Managing Internetworks with SNMP, 2nd edition*. M & T Books; 1997.

[7] White S., Sharkey K., Coulter D., Batchelor D., Jacobs M., Satran M. *Windows Management Instrumentation*. Microsoft; 2021. Preuzeto s https://docs.microsoft.com/en-us/windows/desktop/WmiSdk [Pristupljeno: 17. travnja 2021.]

[8] Stemp G., Tsaltas D., Wells B., Wilansky E. *Microsoft Windows 2000 Scripting Guide*. Redmond: Microsoft Press; 2003.

[9] Case J., Fedor M., Schoffstall M., Davin J. *A Simple Network Management Protocol (SNMP)*. Network Working Group; 1990. Preuzeto s https://tools.ietf.org/html/rfc1157 [Pristupljeno: 17. travnja 2019.]

[10] Warrier U., Besaw L. *The Common Management Information Services and Protocol over TCP/IP (CMOT)*. Network Working Group; 1989. Preuzeto s https://tools.ietf.org/html/rfc1095 [Pristupljeno: 17. travnja 2019.]

[11] McCloghrie K., Rose M. *Structure and Identification of Management Information*. Network Working Group; 1988. Preuzeto s https://tools.ietf.org/html/rfc1065 [Pristupljeno: 17. travnja 2019.]

McCloghrie K., Rose M. *Management Information Base for Network Management of TCP/IP-based internets*. Network Working Group; 1988. Preuzeto s https://tools.ietf.org/html/rfc1066 [Pristupljeno: 17. travnja 2019.]

[12] Postel J. *Internet Control Message Protocol*. Network Working Group; 1981. Preuzeto s https://tools.ietf.org/html/rfc792 [Pristupljeno: 17. travnja 2019.]

[13] Hollenbeck S., Rose M., Masinter L. *Guidelines for the Use of Extensible Markup Language (XML) within IETF Protocols*. Network Working Group; 2003. Preuzeto s https://tools.ietf.org/html/rfc3470 [Pristupljeno: 17. travnja 2019.]

[14] Morris S.B. *Network Management, MIBs and MPLS: Principles, Design and Implementation*. Pearson; 2003.
https://www.oreilly.com/library/view/network-management-mibs/0131011138/

[15] Brehm T. *The Perfect Server CentOS 7.6 with Apache, PHP 7.2, Postfix, Dovecot, Pure-FTPD, BIND and ISPConfig 3.1*. HowtoForge.
Preuzeto s https://www.howtoforge.com/tutorial/perfect-server-centos-7-apache-mysql-php-pureftpd-postfix-dovecot-and-ispconfig/ [Pristupljeno: 15. svibnja 2019.]

[16] *About Nagios. What is Nagios?.* Preuzeto s https://www.nagios.org/about/ [Pristupljeno: 3. srpnja 2019.]

[17] *Nagios XI benefits*. Nagios. Preuzeto s https://www.nagios.com/products/nagios-xi/#benefits [Pristupljeno 5. lipnja 2020.]

[18] *Zabbix hardware and software requirements*. Zabbix SIA. Preuzeto s https://www.zabbix.com/documentation/4.0/en/manual/installation/requirements
[Pristupljeno 25. siječnja 2022.]

[19] Nagios XI features. Nagios. reuzeto s https://www.nagios.com/products/nagios-xi/ [Pristupljeno 25. siječnja 2022.]

[20] *Generating Reports With Nagios XI*. Nagios; 2018. Preuzeto s https://assets.nagios.com/downloads/nagiosxi/docs/Generating-Reports-With-Nagios-XI.pdf [Pristupljeno 25. siječnja 2022.]

[21] *CentOS 7 yum update info*. Preuzeto s https://share.zabbix.com/yum-update-info [Pristupljeno 30. siječanj 2022.]

Popis ilustracija

Slika 1. Struktura mreže: klijent-poslužitelj, Izvor: [1]..... 8
Slika 2. Struktura mreže: klijent-klijent, Izvor: [1] 9
Slika 3. Aktivni način rada..... 10
Slika 4. Aktivno-pasivni način rada 10
Slika 5. Slojevi OSI modela i komunikacija između njih, Izvor: [3] 11
Slika 6. Slojevi TCP/IP modela i komunikacija između njih, Izvor: [3]. 13
Slika 7. Usporedba OSI i TCP/IP referentnih modela, Izvor: [2], [3]. 14
Slika 8. SMI arhitektura [5]..... 16
Slika 9. CMOT arhitektura [6] 17
Slika 10. Arhitektura SNMP-a, Izvor [6] 18
Slika 11. Primjer informacija koju pruža Linux *ping* naredba 19
Slika 12: WMI arhitektura, [8]..... 20
Slika 13. WMI repozitorij, [8] 21
Slika 14. Primjer nadzora mrežnih uređaja bez unificiranog rješenja, [14] 24
Slika 15: Primjer centralnog nadzora lokalnih i udaljenih mrežnih uređaja, [14] 24
Slika 16. Početna stranica inicijalne konfiguracije Zabbix servera 29
Slika 17. Provjera PHP i HTTPD konfiguracije 29
Slika 18. Podešavanje pristupnih podataka MySQL tj. MariaDB baze..... 30
Slika 19. Unos naziva servera i porta, te imena Zabbix servera 30
Slika 20. Završna stranica inicijalne konfiguracije Zabbix servera 31
Slika 21. Inicijalna prijava na Zabbix. 31
Slika 22. Zabbix radna ploča 32
Slika 23. Kreiranje korisnika 32
Slika 24. Korisničke grupe 33
Slika 25. Dodavanja uređaja u Zabbix-u 33
Slika 26. Parametri kod dodavanja novog uređaja (CentOS 7) 34
Slika 27. Kreiranje nadzora web stranice, Zabbix 35
Slika 28. Prikaz problema svih mrežnih uređaja 36
Slika 29. Dostupni parametri za filtraciju problema 36
Slika 30. Podešavanje načina slanja obavijesti korisniku 37
Slika 31. Primjer standardne Zabbix notifikacije 37
Slika 32. Izrada izvještaja nadziranog uređaja u Zabbix-u..... 38
Slika 33. Dostupno ažuriranje za Zabbix pakete..... 38
Slika 34. Instalacija Nagios-a..... 41
Slika 35. Početna stranica finalne konfiguracije Nagios XI servera. 41
Slika 36. Druga stranica konfiguracije Nagios XI servera 42
Slika 37. Nagios XI inicijalna prijava. 42
Slika 38. Nagios XI radna ploča..... 43
Slika 39. Dodavanje novog Nagios korisnika..... 43
Slika 40. Nagios: dodavanje mrežnog uređaja 44
Slika 41. Filtriranje predefiniranih konfiguracija po nazivu „linux“ 44

Slika 42. Nagios: unos detalja o Linux mrežnom uređaju 45
Slika 43. Nagios centralni prikaz stanja svih sustava 46
Slika 44. Nagios: prikaz različitih pregleda poteškoća 46
Slika 45. Notifikacijske mogućnosti Nagios XI-a 48
Slika 46. Podešavanje e-pošte 48
Slika 47. Generiranje izvještaja dostupnosti u Nagios XI 49
Slika 48. Nadogradnja Nagios-a kroz web sučelje 50
Slika 49. Tijek nadogradnje Nagios-a na zadnju dostupnu verziju 51
Slika 50: Detektirani problemi na CentOS 7 operativnom sustavu (Nagios XI) 52
Slika 51: Detektirani problemi na CentOS 7 operativnom sustavu (Zabbix) 52
Slika 52. Detektirani problemi na Windows 8.1 operativnom sustavu (Nagios XI) 53
Slika 53. Detektirani problemi na Windows 8.1 operativnom sustavu (Zabbix) 53
Slika 54. Razlika detektiranih problema na Windows Server 2012 (Zabbix) 53
Slika 55. Detektirani problemi na mrežnom uređaju Mikrotik RB2011 (Nagios XI) ... 54
Slika 56. Zabbix nije detektirao poteškoće osim nadogradnje Mikrotik sustava 54
Slika 57. Nagios XI je detektirao samo mrežnu prisutnost 54

Popis tablica

Tablica 1. Popis nadziranih mrežnih uređaja 25
Tablica 2. Podržani operativni sustavi Zabbix agenta 35
Tablica 3. Podržani operativni sustavi NCPA agenta 45
Tablica 4. Usporedba mogućnosti programske podrške za nadzor 55

Popis kratica

AD - Active Directory
API - Application Programming Interface
ASCE - Association Control Service Element
CIM - Common Information Model
CLI - Command Line Interface
CMIP - Common Management Information Protocol
CMIS - Common Management Information Service
CMISE - Common Management Information Service Element
COM – Component Object Model
DMTF - Distributed Management Task Force
DMZ – Demilitarized Zone
DNS - Domain Network Server
EOL - End of Life
FTP – File Transfer protocol
GUI - Graphical User Interface
HTTP(S) – Hypertext Transfer Protocol (Secure)
IAB - Internet Architect Bord
ICMP – Internet Control Message Protocol
IMAP – Internet Message Access Protocol
IP – Internet Protocol
IPS - Intrusion Prevention Systems
IPsec – Internet Protocol Security
IPX – Internetwork Packet Exchange
ISO - International Organization for Standardization
JMX – Java Managment Extensions
LAN – Local Area Network
LDAP - Lightweight Directory Access Protocol
LLC – Low Level Control
MAC – Media Access Control
MIB – Managment Information Base
OSI – Open System Interconnection
PHP - PHP: Hypertext Preprocessor
POP – Post Office Protocol
RFC - Request for Comments
ROSE - Remote Operation Service Element
RPC - Remote Procedure
RSS - Really Simple Syndication
SANS - SysAdmin, Audit, Network, and Security
SLA - Service-level agreement
SMI - Structure of Management Information
SMS - Short Message Service

SMTP – Simple Mail Transfer protocol
SNMP – Simple Network Managment Protocol
SOAP - Simple Object Access Protocol
SQL - Structured Query Language
SSH – Secure Shell
TCP – Transmission Control Protocol
UDP - User Datagram Protocol
VPN – Virtual Private Network
WAN – Wide Area Network
WBEM – Web-Based Enterprise Managment
WDM - Windows Driver Model
WMI – Windows Managment Instrumentation
XML - Extendible Message Language
XMPP - Extensible Messaging and Presence Protocol

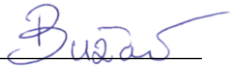
Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je završni rad
(*vrsta rada*)
isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom "Usporedna analiza programske podrške za nadzor mrežnih uređaja" , u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 15.06.2022. Zvonimir Bužanić, 
(ime i prezime, *potpis*)