Combis d.o.o.
Zagreb, Radnička 21

Combis Infrastructure Monitoring Service

COMBIS IMS
Infrastructure Monitoring Service

Tehničke značajke

14. 05. 2024.

COMBIS, usluge integracija informatičkih tehnologija, d.o.o.
Radnička cesta 21, 10000 Zagreb, Republika Hrvatska
T: +385 (0) 136 51222, F: +385 (0) 136 51251, E: combis@combis.hr, W: combis.hr
OIB: 91678676896, PDV identifikacijski broj: HR91678676896, MB: 3609103, Trgovački sud u Zagrebu, MBS: 060090126
Poslovna banka: Zagrebačka banka d.d., Zagreb IBAN: HR8723600001101227582 / SWIFT: ZABAHR2X
Temeljni kapital: 64.943.900,00 kn, uplaćen u cijelosti, Član Uprave: Goran Car

Sadržaj

I. INFORMACIJE O PONUĐAČU

Ponuđač:

COMBIS d.o.o.
Radnička cesta 21
10000 Zagreb
MB: 3609103
OIB: 91678676896

Kontakt podaci:

10000 Zagreb, Radnička cesta 21
Tel.:
mob: +
fax: +
e-mail:

Broj ponude:

Period valjanosti ponude:

Rok plaćanja:

1. Uvod

Combis predlaže vlastito nadzorno rješenje „Combis IMS“ (Infrastructure Monitoring Service) baziranog na Zabbix nadzornom sustavu s dodatnim modulima i popratim sustavima koji čine jednu integriranu cjelinu. U narednim poglavljima nalazi se opis našeg predloženog rješenja kao i opis funkcioniranja nadzornog sustava uz dodatne opcije koje se naknadno mogu implementirati, iskoristiti ili povezati s drugim sustavima.

2. Opis rješenja

2.1 O nadzornom sustavu

Sustav za nadzor omogućava jasnu sliku o radu i kapacitetu IT sustava i bolju koordinaciju i praćenje statusa rješavanja prepoznatih problema. Isto tako sustavnim nadzorom i praćenjem trendova Sustav za nadzor prepoznaje potencijalna područja strateškog razvoja IT infrastrukture i usluga na osnovu kojih mogu nastati kratkoročne i dugoročne preporuke za optimizaciju.

2.2 Komponente nadzornog rješenja

Za postizanje gore navedenih zahtjeva (2.1) predlažemo rješenje koje se sastoji od više komponenti integriranih u jedan sustav.

Cjelokupno rješenje sastoji se od:

- Combis IMS glavnog servera
- Baze podataka
- Servera za grafičko korisničko sučelje i ostale Combis module

3. Pregled Combis IMS nadzornog rješenja

Combis IMS (Infrastructure Monitoring Service) je moderno poslovno rješenje bazirano na Zabbix nadzornom sustavu otvorenog koda za praćenje mreže i nadgledanje aplikacija uključujući performanse i mogućnosti izvješćivanja za milijune metrika zajedno s nizom posebnih modula izrađenih od strane Combisa.

3.1. Skaliranje na velika okruženja

Zabbix je dizajniran za skaliranje od malih okruženja s nekoliko uređaja do velikih sustava s tisućama uređaja koji se nadziru. Postoje instalacije Zabbixa s preko 100.000 nadziranih uređaja, što pokazuje da sustav može obraditi više od 3.000.000 provjera u minuti koristeći lako dostupan hardver pri tome prikupljajući gigabajte povijesnih podataka dnevno. Ova razina skalabilnosti moguća je korištenjem inteligentnih i učinkovitih algoritama, koji iskorištavaju prednosti moderne hardverske i softverske modularnosti koja omogućuje pametnu raspodjelu zadataka što rezultira vrhunskim performansama.

Uz model jednog središnjeg poslužitelja, Combis IMS također nudi distribuirani nadzor sa proxy serverima koji se lako postavljaju i gotovo ne zahtijevaju posebno održavanje. Proxy služi korisnicima već dugi niz godina i vrlo je robusno rješenje.

Proxy se koristi u nadziranju velike količine uređaja i može se integrirati s različitim rješenjima za nadzor, a također se može pokrenuti na ugrađenom (embedded) hardveru za manja okruženja. Možemo unaprijed konfigurirati proxy server, poslati ga na udaljenu lokaciju da se priključi - i od tada nadalje upravljati svom proxy konfiguracijom sa središnjeg poslužitelja.

Osim što olakšavaju nadzor udaljenih lokacija, proxy također uvelike pomažu pri skaliranju za velika okruženja.

Combis IMS oslužitelj i proxy koriste različita rješenja za predmemoriju (cache) podataka, što im daje izvrsnu izvedbu i smanjuje opterećenje glavne baze podataka.

3.2. Optimizirano za visoke performanse

Protokoli mrežne komunikacije koji se koriste sa Combis IMS-om iznimno su učinkoviti s korištenjem računalnih resursa i propusnosti mreže, čak i u implementacijama velikih razmjera.

Jedna od ključnih komponenti za postizanje vrlo visokih performansi je pohranjivanje podataka u bazu podataka vremenskih serija kao što je TimescaleDB što po potrebi također može biti implementirano.

3.3. Jednostavno održavanje

U modernom poslovnom okruženju često susrećemo zastarjele sustave koji se ne mogu lako zamijeniti ili nadograditi. Izvršavanje prisilne nadogradnje nadzornih agenta samo zato što je glavni sustav za nadzor nadograđen nije prihvatljivo - stoga najnovija instanca sustava podržava sve prethodne verzije agenta sve do prvih izdanja, koja datiraju prije više od 10 godina.

Nadogradnja Combis IMS-a u granicama jedne veće verzije vrlo je jednostavna i ne zahtijeva nikakve promjene u pozadinskoj bazi podataka. Nadogradnja s jedne verzije na drugu je uvijek u potpunosti podržana i isporučeni su detaljni postupci za ispravnu nadogradnju baze podataka.

3.4. Sigurnost

Pristup Combis IMS sučelju može se izvršiti preko SSL zaštićene veze, čime se osigurava sigurnost između korisnika i poslužitelja. Osim toga, ima samozaštitu od „brute force" napada.

Sve Combis IMS komponente mogu raditi bez root prava – što je posebno važno za nadzorne agente. Štoviše, pokretanje Combis IMS servisa pod privilegiranim računom zahtijeva dodatne korake. Komponente međusobno komuniciraju i prihvaćaju samo veze s ovlaštenih IP adresa, ostale se veze automatski odbijaju.

S podrškom za enkripciju moguće je osigurati komunikaciju između zasebnih Combis IMS komponenti (kao što su Zabbix poslužitelj, proxy, Grafana, agenti i pomoćni programi iz naredbenog retka) korištenjem protokola Transport Layer Security (TLS) v.1.2 i v.1.3.

Podržana je enkripcija temeljena na certifikatima i unaprijed dijeljenim ključevima. Enkripcija je opcionalna i može se konfigurirati za pojedinačne komponente.

3.5. Jednostavna integracija

API nudi nevjerojatnu fleksibilnost za laku dvosmjernu integraciju s poslovnim aplikacijama. Automatizacija se može izvršiti pomoću skripti u različitim programskim jezicima kao što su Ruby, Python, Perl, PHP, Java ili shell skriptama.

Za Combis IMS grafičko sučelje, autentifikacija se može integrirati sa LDAP-om (uključujući Microsoft Active Directory) ili Radiusom, dopuštajući korisnicima da koriste istu lozinku za nadzorni sustav kao i svugdje drugdje.

3.6. IPv6 ready

Budući da IPv4 segmenti ponestaju prilično brzo, veći ISP-ovi sve više gledaju na IPv6.

Sve Combis IMS komponente podržavaju i IPv4 i IPv6, što omogućuje korištenje u mješovitom okruženju ili čistom IPv6 okruženju.

3.7. Prikaz i pristup podacima

Pratite status infrastrukture, aplikacija i poslovnih usluga pomoću Combis IMS nadzornih ploča. Upotrijebite širok raspon „widgeta" nadzorne ploče kako biste ne samo agregirali, transformirali i grafički prikazali svoje podatke, već i pratili krajnje točke na geografskim i mrežnim kartama, identificirali status najkritičnijih alarma, sortirali krajnje točke nadzora i još mnogo toga.

Osigurajte veze do i od vaših krajnjih točaka za praćenje pomoću certifikata ili unaprijed dijeljenog ključa. Stvorite jedinstvena prava za svoje korisnike kako biste kontrolirali pristup različitim Combis IMS elementima i značajkama. Iskoristite izvornu logiku dopuštenja za izolaciju krajnjih točaka nadzora između korisnika – svaki korisnik ima pristup do samo određenih nadzornih podatka kojima ima pristup.

3.8. Dostupnost usluge

Biti u mogućnosti pružati usluge nadzora 24/7 od vitalnog je značaja. Uvođenjem više Combis IMS poslužitelja i grafičkih sučelja možemo spriječiti kritičku točku kvara (single point of failure). Možemo poboljšati korisničko iskustvo postavljanjem servera blizu njihove lokacije. Combis IMS ne ograničava broj backend i frontend servera koji se mogu postaviti.

3.9. Report i audit

U Combis IMS-u se mogu implementirati unaprijed definirana automatska izvješća i slati dnevne, tjedne, mjesečne i godišnje reporte (izvještaje) nadgledanih infrastruktura i poslovnih usluga.

Pratite promjene izvršene na Combis IMS-u uz robusnu i detaljnu ugrađenu funkciju revizijskog zapisivanja svakog izvršenog koraka.

3.10. Combis IMS integracije

Combis IMS se može integrirati s rješenjima od trećih strana i proslijediti vaša upozorenja ITSM-u, helpdesku i sustavima za razmjenu poruka odabirom sa sve većeg popisa službenih Zabbix integracija. Čak i ako nije na popisu, integracija se može napraviti i prilagoditi pomoću različitih protokola i/ili pomoću API-ja. Combis IMS može obogatiti alarme i notifikacije dodatnim informacijama koje prikuplja i prilagoditi odlazne poruke prema vašim zahtjevima.

3.12 Visoka dostupnost

Combis IMS ima ugrađenu funkciju za visoku dostupnost. Visoka dostupnost (HA – High Availability) obično je potrebna u kritičnim infrastrukturama koje si ne mogu priuštiti gotovo nikakav zastoj. Dakle, za bilo koju uslugu koja bi mogla zakazati mora postojati opcija preusmjeravanja rada u slučaju da trenutna usluga zakaže.

Combis IMS nudi rješenje visoke dostupnosti koje se lako konfigurira i ne zahtijeva preveliku prethodnu stručnost za High Availability (HA). Izvorni Zabbix HA može biti koristan za dodatni sloj zaštite od kvarova softvera/hardvera Zabbix servera ili za manje prekide rada zbog održavanja.

U Combis IMS načinu visoke dostupnosti više Combis IMS poslužitelja se pokreće kao čvorovi u skupini. Dok je jedan Combis IMS poslužitelj u skupini aktivan, drugi su u stanju pripravnosti uvijek spremni preuzeti kada i ako je to potrebno.

3.13 API

Kako je Combis IMS baziran na Zabbixu koristi i njegov API. Zabbix API (Application Programming Interface) je sučelje koje korisnicima omogućuje programsku interakciju sa poslužiteljem, a ne putem grafičkog korisničkog sučelja. API omogućuje korisnicima automatizaciju različitih zadataka i integraciju Combis IMS-a s drugim sustavima i aplikacijama.

Zabbix API pruža RESTful API, što znači da koristi HTTP zahtjeve za komunikaciju sa poslužiteljem i vraćanje podataka u JSON (JavaScript Object Notation) formatu. API podržava različite HTTP metode kao što su GET, POST, PUT i DELETE, koje se mogu koristiti za stvaranje, čitanje, ažuriranje i brisanje različitih stavki na Zabbix poslužitelju, kao što su hostovi, metrike, alarmi i notifikacije.

API ima nekoliko krajnjih točaka kojima se može pristupiti, a svaka pruža različite funkcije:

- Provjera autentičnosti API korisnika i dobivanje tokena za provjeru autentičnosti, koji je potreban za buduće API zahtjeve
- Pristup raznim konfiguracijskim resursima na Combis IMS poslužitelju, kao što su hostovi, metrike, alarmi i predlošci nadzora
- Pristup različitim resursima za nadzor na Combis IMS poslužitelju, kao što su grafikoni, karte, ekrani i podaci koje prikuplja Zabbix poslužitelj.
- Pristup resursima koji se odnose na upozorenja (alarme) na Combis IMS poslužitelju, kao što su okidači, akcije i obavijesti.

Zabbix API je dobro dokumentiran i pruža širok raspon funkcionalnosti, što ga čini moćnim alatom za automatizaciju zadataka i integraciju s drugim sustavima i aplikacijama.

3.14 TimescaleDB

Koristeći dodatak „TimescaleDB" (Time-series uz PostgreSQL bazu) može dramatično poboljšati izvedbu upita za 100x ili više te smanjiti iskorištenost pohrane čak do 90%. Takve performanse omogućuje particioniranje podataka temeljeno na vremenu kada se koristi za vremenski orijentirane aplikacije.

3.15 Grafana

Grafana je alat za vizualizaciju otvorenog koda specijaliziran za bolju korelaciju između više izvora podataka. Omogućuje postavljanje upita, vizualizaciju, upozoravanje i razumijevanje mjernih podataka bez obzira gdje su pohranjeni.

4. Dimenzioniranje rješenja

4.1. Broj nadziranih uređaja

Da bismo znali skalirati nadzorni sustav potrebne su nam informacije o broju, tipu i vrsti uređaja

Točan broj različitih uređaja i tipova uređaja može utjecati na vrijeme konfiguracije i podešavanja svih uređaja u nadzoru.

4.2. Tehnički preduvjeti za Combis IMS

Korisnik mora osigurati fizičke ili virtualne servere za rad nadzornog sustava. Cijeli sustav može biti instaliran u zatvorenu ICT mrežu korisnika ili se u mrežu korisnika može postaviti samo kolektor (proxy).
Sve Combis IMS komponente sustava izvršavaju se u Linux okruženju uz preporuku za korištenje RHEL ili Ubuntu server distribucija. Ovisno o količini nadziranih uređaja i funkcionalnosti potrebna su nam minimalno 2 virtualna ili fizička servera. Osim odabira OS-a i backup sustava od strane korisnika, nisu potrebne nikakve posebne licence za funkcioniranje cjelokupnog nadzornog rješenja.

4.3. Combis IMS server

Combis IMS poslužitelj središnji je proces Combis IMS sustava.

Poslužitelj vrši anketiranje i hvatanje podataka, izračunava vrijednosti za alarmiranje, šalje obavijesti korisnicima. To je središnja komponenta kojoj agenti dostavljaju podatke o dostupnosti i integritetu sustava i koji prikuplja podatke svih udaljenih mrežnih uređaja. Poslužitelj može sam daljinski provjeravati mrežne usluge (kao što su web poslužitelji i poslužitelji e-pošte) koristeći jednostavne provjere usluga.

Zabbix server je središnji repozitorij u kojem se pohranjuju svi konfiguracijski, statistički i operativni podaci, a to je entitet u Combis IMS-u koji će aktivno upozoravati administratore kada se pojave problemi u bilo kojem od nadziranih sustava.

Funkcioniranje osnovnog Combis IMS-a podijeljeno je u nekoliko različitih komponenti:

- Zabbix backend poslužitelj
- Web grafičko sučelje
- Baza podataka

- SNMP trap kolektor
- Topology mape

Sve konfiguracijske informacije za Combis IMS pohranjene su u bazi podataka s kojom su u interakciji i poslužitelj i web sučelje. Na primjer, kada stvorite novu stavku pomoću web sučelja (ili API-ja), ona se dodaje u tablicu stavki u bazi podataka. Zatim će otprilike jednom u minuti poslužitelj tražiti tablicu stavki za popis stavki koje su aktivne, a zatim ih pohraniti u predmemoriju unutar Zabbix poslužitelja.

Neke komponente Combis IMS sustava (ovisno o potrebama korisnika) pokreću se iz zasebnih Docker containera a neke su instalirane direktno na OS poslužitelja.

4.6 Combis IMS grafičko sučelje

Za jednostavan pristup Combis IMS-u s bilo kojeg mjesta i s bilo koje platforme, osigurano je web sučelje.

Web sučelje dizajnirano je tako da bude jednostavno za korištenje s modernim i responzivnim sučeljem.

Sučelje je podijeljeno u nekoliko odjeljaka, od kojih svaki pruža različite funkcionalnosti:

- Nadzorna ploča: Nadzorna ploča je početna stranica Combis IMS sučelja, koja pruža sažetak ukupnog stanja i performansi nadziranog okruženja.
- Nadzor: Odjeljak za nadzor (Monitoring) je mjesto gdje možete vidjeti podatke koje je prikupio Combis IMS poslužitelj, uključujući grafikone, karte i ostalo. Omogućuje detaljnu analizu određenih stavki, okidača, hostova i grupa kako biste vidjeli detaljne informacije.
- Konfiguracija: Konfiguracijski odjeljak je mjesto gdje možete konfigurirati Combis IMS server, uključujući dodavanje hostova, stavki, okidača i predložaka. Također omogućuje pristup raznim postavkama i opcijama za Combis IMS server.
- Administracija: Odjeljak za administraciju je mjesto gdje možete upravljati korisnicima sustava, dozvolama, vrstama medija za obavještavanja i drugim postavkama cijelog sustava.

Sveukupno, Combis IMS sučelje pruža sveobuhvatno i moćno rješenje za nadzor s modernim sučeljem prilagođenim korisniku koje olakšava korištenje i navigaciju.

4.7 Zabbix agenti

Za nadziranje Linux i Windows poslužitelja ili računala potrebno je koristiti Zabbix Agent. Agent se instalira na svaki server koji je potrebno nadzirati uz konfiguracijski dokument u kojem je napisana destinacija proxy ili glavnog servera. Iako se za virtualne servere osnovne

informacije mogu pročitati spajanjem na njihov hipervizor, najtočnija informacija dobiva se preko instaliranog agenta te se time otvara niz ostalih opcija nadziranja na tom serveru kao i mogućnosti automatskog oporavka problema. Agent ne troši puno resursa i može raditi u aktivnom ili pasivnom načinu rada. Drugim riječima može koristi Pull ili Push metodu za slanje podataka, tj. komunikaciju između Combis IMS servera i nadziranog servera.

Svakom instaliranom agentu moguće je ograničiti prava kojim dijelovima sustava smije pristupiti. Pravilno podešen agent može pročitati gotovo sve podatke kao da administrator uživo radi na tom serveru.

Instalaciju agenta moraju odraditi administratori svakog servera.

4.7 Fizički ili virtualni serveri

Konfiguracija i količina servera za svakog korisnika može biti drugačija, a najviše utječe:

- Učestalost prikupljanja informacija kao i njezina količina
- Ukupno vrijeme čuvanja sirovih podataka kao i kalkuliranih podataka
- Kompleksnosti transformacije podataka i naprednih kalkulacija u realnom vremenu
- Broj istovremenih korisnika i kompleksnosti izrađenih nadzornih ploča i vizualizacija.

Preporuka (ali ne i osnovni uvjet) je da svi serveri za backend, bazu podataka pa čak i frontend budu odvojeni fizički serveri. Razlog za to je taj što u slučaju problema, npr. hipervizora postoji mogućnost da nadzorni alat to neće moći registrirati i/ili dojaviti jer je afektiran tim istim problemom. Odvojednim serverom, nadzorni alat nije afektiran redovitim patchiranjem ili bilo kojim drugim radovima, već se radovi za nadzorni sustav planiraju posebno. Sve to služi odnosno pomaže kako bi se uvijek prikupljali podaci o nadziranim uređajima te lakše i brže pronašli stvarni uzrok problema i odmah krenuli u njegovo rješavanje.

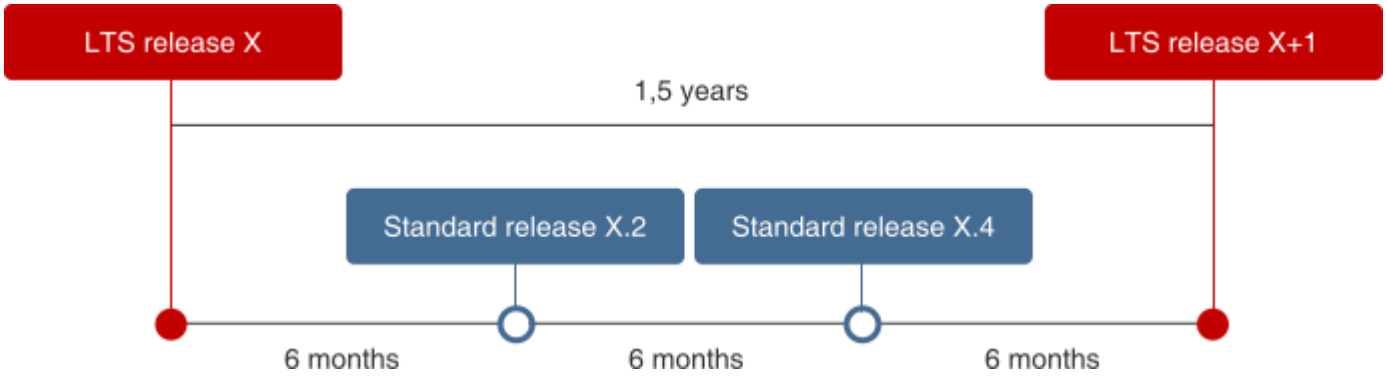
5. Politika životnog ciklusa softvera i izlazak novih verzija

5.1. Opće informacije

Kako bismo osigurali da Zabbix na kojem je izgrađen Combis IMS svojim korisnicima i kupcima nudi proizvod očekivane kvalitete i podršku koja se lako planira, svako novo izdanje Zabbix softvera podliježe standardnom životnom ciklusu i datumu isteka.

5.2. Program planiranih izdanja Zabbixa

Zabbix tim predan je novom programu planiranih izdanja na šestomjesečnoj osnovi. Svakih šest (6) mjeseci Zabbix će objaviti novu stabilnu verziju.



Kontinuirana učestalost novih Zabbix izdanja

Tijekom svake godine i pol (1,5) Zabbix će izdati:

- Zabbix LTS (Long Term Support - dugoročna podrška) izdanje. Zabbix LTS izdanja podržana su za Zabbix korisnike tijekom pet (5) godina tj. 3 godine pune podrške (opća, kritična i sigurnosna podrška) i 2 dodatne godine ograničene podrške (kritična i sigurnosna podrška). Izdanje Zabbix LTS verzije rezultirat će promjenom prvog broja verzije.
- Izdanja Zabbix Standard release. Standardna izdanja Zabbixa podržana su za korisnike Zabbixa tijekom šest (6) mjeseci pune podrške (opća, kritična i sigurnosna podrška) do sljedećeg stabilnog izdanja Zabbixa, plus jedan (1) dodatni mjesec ograničene podrške (samo kritična i sigurnosna podrška). Izdanje verzije Zabbix Standard release rezultirat će promjenom drugog broja verzije.

5.3. Long Term Support

LTS je skraćenica za "Long Term Support (dugoročna podrška)". Zabbix LTS verzija izlazi svake godine i pol (1,5) i nudi Zabbix korisnicima usluge podrške za pet (5) godina

Za Zabbix LTS verziju nema dodatne naknade ili skrivene naknade, tj. to je izdanje softvera 100% otvorenog koda dostupno svima.

Zabbix LTS specifičnosti:

- Dulja usluga podrške, tj. ažuriranja za potencijalne sigurnosne probleme i greške
- Bolja kvaliteta i nove mogućnosti
- Otklanjanje nepredvidivih grešaka
- Puno lakše planiranje i upravljanje u smislu nadogradnje verzija u odnosu na „Standard Release".

5.4. Sigurnosna politika

Combis i Zabbix slijede strogi proces pri razvoju novih verzija softvera prema Zabbix životnom ciklusu i politici izdavanja. Svi zadaci podliježu strogim standardima koje nameće Zabbix:

- Svi Combis i Zabbix programeri pridržavaju se smjernica za kodiranje projekta
- Svi Combis inženjeri koji rade na održavanju Combis IMS sustava su certificirani od strane Zabbixa
- Sav kod pregledava viši programer prije nego što se spoji u Zabbix bazu koda
- Sve zadatke testiraju inženjeri za osiguranje kvalitete
- Kada se izda glavna verzija Zabbixa, Zabbix Security tim prolazi kroz internu sigurnosnu reviziju.

Combis i Zabbix imaju ISO/IEC 27001:2013 certifikat. Ovaj certifikat jamči da Zabbix štiti sve svoje podatke unutar najviših međunarodno priznatih sigurnosnih standarda. Ovaj certifikat je izdan za četiri Zabbix ureda: Zabbix LLC (SAD), Zabbix SIA (Latvija), Zabbix Japan LLC (Japan) i Zabbix Servicos de Software LTDA (LATAM Brazil). Iako je razvojni proces osmišljen tako da eliminira svaku mogućnost sigurnosnih problema, ipak je moguće da se otkriju nove ranjivosti. Zabbix tretira sigurnosna pitanja u održavanim verzijama kao visoki prioritet. Imajte na umu da Zabbix i Combis ne rješavaju sigurnosne probleme u verzijama koje više nisu podržane. U slučaju da je to potrebno na nepodržanim verzijama – zakrpe se izrađuju po narudžbi koja se naplaćuje po satu.

6. Sigurnost

6.1. Kriptirana komunikacija između Combis IMS komponenti

Combis IMS podržava šifriranje bilo kojeg komunikacijskog toka između različitih Combis IMS komponenti:

- Sve komunikacije između različitih komponenti (kao što su poslužitelj, proxy, agenti i programi naredbenog retka) podržavaju TLS protokol
- Podrška za rad sa certifikatima i unaprijed dijeljenog ključa
- Enkripcija je izborna i može se konfigurirati za pojedinačne komponente.

6.2. Korisnička prava

Combis IMS pruža fleksibilnu shemu prava (Multi-tenant) koja se može učinkovito koristiti za upravljanje korisničkim dopuštenjima unutar jedne Combis IMS instalacije ili u distribuiranom okruženju.

Mogu se definirati tri razine dopuštenja:

- Read-write – pristup za čitanje-pisanje
- Read-only – pristup samo za čitanje
- Deny – pristup odbijen.

Tipovi korisnika (user types) koriste se za definiranje pristupa administrativnim funkcijama i za određivanje zadanih dopuštenja:

- „Korisnik" ima dopuštenja samo za čitanje prikupljenih podataka i događaja
- „Administratori" mogu upravljati konfiguracijom nadzora i čitati prikupljene podatke i događaje
- „Super administratori" sposobni su upravljati konfiguracijom Combis IMS instance, osim što imaju Combis IMS administratorska dopuštenja.

6.3. Korisničke uloge

Korisničke uloge (User roles) također omogućuju skrivanje ili prikazivanje UI elemenata kako bi odgovarali potrebama poslovanja.

Pomoću korisničkih uloga možete:

- Ograničiti pristup određenim elementima korisničkog sučelja
- Ograničiti pristup izvođenju određenih radnji u korisničkom sučelju (UI)

- Napraviti popis dopuštenih ili zabranjenih API metoda.

6.4. Autentifikacija korisnika

Combis IMS se može integrirati s vašim postojećim mehanizmima provjere autentičnosti.

Combis IMS podržava razne metode provjere autentičnosti:

- Interne prijave
- HTTP provjera autentičnosti
- Podrška za autentifikaciju s više faktora (multi-factor authentication)
- Definirajte vlastite zahtjeve za složenost lozinke
- LDAP autentifikacija
- SAML autentifikacija
- Single sign-on autentifikacija
- Integracija s Active Directoryjem.

S podrškom za HTTP, LDAP i SAML provjeru autentičnosti možete pružiti dodatni sloj sigurnosti i poboljšati korisničko iskustvo tijekom rada s Combis IMS-om.

6.5. Revizija i kontrola promjena (Audit log)

Combis IMS prati sve promjene i korake u sustavu korištenjem Audit log-a:

- Saznajte koji je korisnik napravio izmjene na Combis IMS entitetima
- Prati IP adresu s koje se korisnik prijavio
- Filtrirajte audit log i pratite promjene koje je izvršio određeni korisnik na određenom resursu
- Izvoz cijelog ili filtriranog dnevnika revizije putem API-ja za daljnju analizu.

7. Upravljanje događajima/alarmima

7.1. Pametni pragovi problema (Smart thresholds)

Combis IMS može automatski detektirati stanja problema unutar dolaznog toka metrike:

- Zasebni problemi i uvjeti za rješavanje problema
- Velik broj Severity razina alarma
- Root-cause analiza
- Zaštita od „Flappanja"
- Detekcija anomalije
- Predikcije trendova
- Otkriveni problemi mogu se klasificirati pomoću oznaka za pametnije upozoravanje (Tags)
- Izvoz otkrivenih problematičnih događaja u stvarnom vremenu u sustave treće strane (Elastic, Splunk, itd.)
- Ručno suzbijanje problema na neodređeno vrijeme ili do određenog trenutka u vremenu.

Combis IMS svojim korisnicima pruža vrlo fleksibilne, inteligentne opcije definiranja thresholda. Dok prag za okidač može biti jednostavan kao "veći od x", moguće je iskoristiti svu moć podržanih funkcija i operatora za statističku analizu povijesnih podataka.

7.2. Predikcije trendova

Iako je lijepo imati thresholde za otkrivanje problema, učinkovitije je proaktivno reagirati na probleme. Combis IMS prediktivne funkcije mogu pomoći u postizanju tog cilja koristeći:

- Predviđanje vrijednosti za rano upozorenje (Forecasting)
- Predviđanje vremena preostalog do dostizanja thresholda.

7.3. Machine learning

Ručno definiranje thresholda problema nije uvijek najučinkovitiji pristup. U dinamičnim okruženjima gdje se osnovne vrijednosti mogu povremeno mijenjati važno je automatski izračunati referentnu točku prema kojoj će se izračunati threshold. Combis IMS Baseline monitoring omogućuje vam upravo to - otkrivanje anomalije na temelju analize povijesnih podataka u stvarnom vremenu koristeći metode strojnog učenja.

7.4. Notifikacije i prosljeđivanje eventa

Upotrijebite više kanala za razmjenu poruka kako biste obavijestili odgovornu osobu ili osobe o različitim vrstama događaja koji se događaju u vašem okruženju:

Alerting sustavi:

- VictorOPS
- Opsgenie
- Pagerduty
- SIGNL4
- And more
- Email
- SMS (USB modem)
- Online SMS gateway.

Komunikacijske platforme:

- Slack
- MS Teams
- Telegram
- Express.ms
- Rocket.chat
- I ostali…

Webhooks, SOAP, REST i slične metode za integraciju s vanjskim sustavima za razmjenu poruka, ITSM ili ticketing sustavima.

7.5. Vlastiti oblik notifikacija

Definirajte različite poruke za različite kanale slanja poruka. Možete upotrijebiti zadane predloške poruka ili izraditi i prilagoditi vlastiti predložak poruka:

- Prilagodite poruke na temelju vrste problema i uloge primatelja
- Obogatite poruke svim informacijama o vremenu izvođenja i inventaru
- Slanje planiranih PDF izvještaja na uvid i dugoročnu analitiku.

7.6. Scenariji eskalacija

Combis IMS ima mogućnost definiranja scenarija eskalacije različite složenosti ovisno o potrebnom tijeku rada. Od jednostavnih obavijesti i eskalacija različitim korisnicima do odgođenih obavijesti i automatskog rješavanja problema:

- Obavještavanje korisnika o novim problemima
- Proaktivno izvršavanje udaljenih skripti
- Ponavljanje obavijesti dok se problem ne riješi
- Odgađanje obavijesti i daljinske naredbe
- Eskaliranje problema drugim skupinama korisnika
- Automatska promjena eskalacijske rute
- Pošaljite poruku za oporavak svim uključenim stranama

- Neograničen broj koraka eskalacije.

7.7. Automatski oporavak

Uz Combis IMS možete ne samo primiti obavijest o problemu, već ga i automatski riješiti. Skripta ili naredba za popravak može se izvršiti kako bi se pokušao riješiti problem:

Neki primjeri skripti za automatski oporavak:

- Ponovno pokretanje servisa
- Upravljanje resursima u oblaku
- Automatsko skaliranje resursa
- Izvršavanje bilo koje druge prilagođene logike.

8. Monitoring

8.1. Prikupljanje i automatsko otkrivanje metrika

Combis IMS omogućuje automatsko otkrivanje te prikupljanje metričkih podataka s poznatih sustava:

- Mrežni uređaji
- Cloud servisi, containeri, virtualni serveri
- Praćenje operacijskog sustava
- Hipervizori i virtualne mašine
- Log datoteke
- Baze podataka
- Aplikacije
- Servisi i procesi
- Telemetrijski podaci
- IoT senzori i ostali digitalni uređaji
- Web page monitoring
- HTTP/HTTPS endpoint monitoring
- Aktivni nadzor iz korisničke perspektive
- Prikupljanje podataka s udaljenih uređaja (kopiranje konfiguracija) i sl.
- Podrška za cijeli niz industrijskih standardnih protokola
- Prikupljanje podataka s vanjskih API krajnjih točaka

Prikupljanje podataka može se lako proširiti implementacijom prilagođenih metoda prikupljanja podataka:

- CLI utility
- Externe skripte napisane na bilo kojem skriptnom jeziku
- Pluginovi za agente napisanu u Go-u ili moduli napisani u C-u
- Nadzor WEB i HTTP scenarija simulirajući rad korisnika

8.2. Prikupljanje većih podataka

Combis IMS podržava pull i push metode za prikupljanje podataka.

Prikupljanje podataka visokog intenziteta:

- Minimalni interval prozivanja je 1 sekunda
- Zakazivanje prikupljanja metričkih podataka prema naprednom rasporedu
- Mogućnost povećavanja intervala prikupljanja za određena vremenska razdoblja

- Data throttling.

Prikupite podatke bilo koje vrste:

- Numerički
- Tekst
- Binarno
- Strukturirani JSON, XML, CSV i drugi formati podataka.

Log file monitoring:

- Prikupljanje i obrada logova
- Prikupljanje i obrada Windows eventlog zapisa
- Dohvaćanje ukupnog broja odgovarajućih zapisa u logu.

Integracija sa sustavima kao Kafka, Prometheus i Elastic Search također se može koristiti za prikupljanje podataka.

8.3 Obrada/transformacija podataka

Combis IMS može prikupiti i optimizirati podatke korištenjem opcija za transformaciju podataka.

Standardizirajte i transformirajte bilo koju vrstu podataka prije pohranjivanja:

- Nestrukturirani tekst s rubovima, funkcijama zamjene i regularnim izrazima
- JSONPath, XPath expressions i CSV u JSON transformacija
- Računanje delte između vrijednosti
- Izvršavanje izračuna s numeričkim vrijednostima
- Transformacije brojevnog sustava
- Provjera validnosti podataka odnosno je li primljena vrijednost u određenom rasponu vrijednosti ili sadrži li pogreške
- Transformacija podataka koristeći JavaScript
- Odbacivanje ponavljajuće vrijednosti.

Prikupljanje „bulk" podataka i korištenje tih informacija za dopunjavanje više zasebnih metrika:

- Transformirajte i izdvajajte samo potrebne podatke
- Smanjite broj veza/upita/poziva prema krajnjoj točki
- Smanjite propusnost mreže grupnim prikupljanjem i transformiranjem metrika
- Odbacite početne „bulk" podatke i pohranite samo već obrađene metrike.

9. Reference monitoring rješenja

Tablica nekih od nedavnih Combis nadzornih projekta.

Customer	Year
HT Mostar	2020
ZagrebŠped	2020
Valamar	2021
FinaGS	2021
Carinska uprava Republike Hrvatske	2022
Poliklinika Medikol	2022
Croatia osiguranje	2022
Weidmann	2022
KBC Split	2022
HEP Telekomunikacije	2022
Croatia banka	2022
ENNA PPD	2022
Arriva	2023
Ministarstvo kulture	2023
Arsano Medical Group	2023
Addiko banka	2024
Hrvatske ceste	2024
Datex	2024