



# jamk

## Open Source SOAR

Teo Häkkinen

Opinnäytetyö, AMK

Joulukuu 2021

Tekniikan ala

Insinööri (AMK), tieto- ja viestintätekniikka

**Häkkinen, Teo**

## **Open Source SOAR**

Jyväskylä: Jyväskylän ammattikorkeakoulu. Joulukuu 2021, 39 sivua. Liitteet 109 sivua.

Tekniikan ala. Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö, AMK.

Julkaisun kieli: suomi

Verkojulkaisulupa myönnetty: kyllä

## **Tiivistelmä**

Tietoteknisten uhkien kehittyessä, uhilta puolustautuvat tahot yrittävät niin ikään kehittyä ja tehostaa puolustautumisen tapoja vähemmän työtä vaativiksi. Ajateltuna paras tapa vähentämään manuaalista työtä on tietysti automatisointi, ja siihen juuri SOAR pyrkii. SOAR sitoo monet pienemmät sovellukset yhteen, mahdollistamalla niiden välisen tiedonjaon ja keskitetyn hallinnan yhdestä käyttöliittymästä. Tavoitteena olisi pienempiin ja vähäpätöisempiin uhkiin vastaaminen automatisoidusti.

Toimeksiantajan ollessa hyvin tietoturvakokeskeinen, kiinnostus automatisoituihin turvallisuustoimenpiteisiin on luonnollisesti suuri. Tavoitteena oli selvittää avoimen lähdekoodin SOAR toteutusten kypsyyttä, miten käyttökelpoisia ja toimivia avoimen lähdekoodin SOAR ratkaisut olisivat toimeksiantajalle potentiaalisina SOC-työkaluina. Työkalujen välinen vertailu kuului myös osaksi kokonaisuutta.

Tarkastelluista työkaluista valittiin valitsemisprosessin kautta yksi lähempää tarkastelua varten. Valinta tehtiin karsimalla sovelluksia asettamalla niille kriteereitä ja selvittämällä mitkä teknologioista täyttivät nämä kriteerit.

## **Avainsanat (asiasanat)**

Open Source, SOAR, Security, JYVSECTEC

## **Muut tiedot (salassa pidettävät liitteet)**

**Häkkinen, Teo**

### **Open Source SOAR**

Jyväskylä: JAMK University of Applied Sciences, December 2021, 39 pages. Attachments 109 pages.

Engineering and technology. Degree Programme in Information and Communication Technology. Bachelor's thesis.

Permission for web publication: Yes

Language of publication: Finnish

### **Abstract**

As cyber threats evolve, those who defend themselves against the threats are also trying to evolve and optimize their defense to less labor-intensive ways. In terms of thinking, the best way to reduce manual work is, of course, automation, and that's what SOAR is all about. SOAR binds many smaller applications together, enabling data sharing and centralized management from a single interface. The goal would be to respond automatically to smaller and minor threats.

As the client is very security-focused, there is naturally a great deal of interest in automated security measures. The aim was to find out the maturity of open source SOAR implementations, how useful and functional open source SOAR solutions would be as potential SOC tools for the client. The comparison between the tools was also part of the research.

One of the tools reviewed was selected through a selection process for further review. The selection was made by pruning applications, setting criteria for them, and finding out which technologies met these criteria.

### **Keywords/tags (subjects)**

Open Source, SOAR, Security, JYVSECTEC

### **Miscellaneous (Confidential information)**

## Sisältö

<b>1</b>	<b>Työn lähtökohdat</b> .....	<b>4</b>
1.1	Toimeksiantaja .....	4
1.2	Tutkimuskysymys ja tavoitteet .....	4
1.3	Tutkimusmenetelmä .....	4
<b>2</b>	<b>SOAR</b> .....	<b>5</b>
2.1	Toimintaperiaate ja rakenne .....	5
<b>3</b>	<b>Teknologiat</b> .....	<b>7</b>
3.1	Oracle VM VirtualBox .....	7
3.2	Ubuntu .....	7
3.3	Docker & Docker compose .....	7
<b>4</b>	<b>Tutkimustulokset</b> .....	<b>9</b>
4.1	Shuffle .....	10
4.1.1	Asennus .....	13
4.1.2	Käyttö .....	14
4.2	Cortex XSOAR (entinen Demisto) .....	25
4.3	PatrOwl .....	26
4.3.1	Asennus .....	28
4.4	CimSweep .....	30
4.5	GRR Rapid Response .....	30
4.5.1	Asennus .....	31
4.5.2	Toinen asennus .....	32
4.6	TheHive .....	33
4.6.1	Asennus .....	33
4.7	MIG .....	34
4.8	Johtopäätökset .....	35
<b>5</b>	<b>Pohdinta</b> .....	<b>36</b>
	<b>Lähteet</b> .....	<b>37</b>
	<b>Liitteet</b> .....	<b>40</b>
	Liite 1. Docker ja Docker-compose asennus .....	40
	Liite 2. PatrOwlManager asennus ennakkoon konfiguroitujen moottoreiden kanssa .....	44
	Liite 3. PatrOwlManager ja PatrOwlEngines erilliset asennukset .....	81
	Liite 4. GRR Rapid Response asennus .....	102
	Liite 5. TheHive asennus .....	120

Liite 6. Shuffle asennus.....	129
Liite 7. GRR Rapid Response asennus 2 .....	130

## Kuviot

Kuvio 1. Shuffle hinnasto .....	11
Kuvio 2. Shuffle Roadmap.....	13
Kuvio 3. Shufflen asennuksen aikana ilmennyt ongelma .....	14
Kuvio 4. Shuffle administrator-käyttäjän luonti .....	15
Kuvio 5. Shuffle ensinäkymä .....	15
Kuvio 6. Shuffle Apps-näkymä, lista applikaatioista .....	16
Kuvio 7. Shuffle Docs-näkymä, dokumentaatio.....	16
Kuvio 8. Shuffle ensimmäisen workflow:n luonti .....	17
Kuvio 9. Shuffle ensimmäinen workflow ja onnistunut hello world suoritus.....	18
Kuvio 10. Shuffle Repeater node .....	19
Kuvio 11. Shuffle Get_URL ja onnistunut suoritus.....	19
Kuvio 12. Shuffle My_IP ja onnistunut suoritus.....	20
Kuvio 13. Shuffle Schedule aikataulutus ja suoritukset.....	21
Kuvio 14. Shuffle Virustotal V3 luominen .....	22
Kuvio 15. Shuffle Virustotal V3 testi workflow ja suoritus .....	23
Kuvio 16. Shuffle Virustotal V3 osana kokonaisuutta ja onnistunut IP raportti .....	23
Kuvio 17. Shufflen TheHive docker-compose.yml .....	24
Kuvio 18. Shufflen TheHive autentikaatiovirhe Firefoxissa ja Chromessa .....	25
Kuvio 19. Shufflen TheHive syötteet ja yleisimpien virheiden korjauskomento .....	25
Kuvio 20. PatrOwlManager versiot.....	27
Kuvio 21. PatrOwl päänäkymä asennuksen jälkeen .....	29
Kuvio 22. PatrOwl ennakkoon konfiguroidut moottorit.....	29
Kuvio 23. PatrOwl-Censys asennuksen virheilmoitus .....	30
Kuvio 24. PatrOwl-owl_code asennuksen virheilmoitus .....	30
Kuvio 25. GRR Rapid Responseen asennuksen virheilmoitus.....	32
Kuvio 26. GRR client asennus.....	32
Kuvio 27. GRR client-lista tyhjä onnistuneesta asennuksesta huolimatta .....	33
Kuvio 28. TheHive perusnäkyminen asennuksen jälkeen.....	34
Kuvio 29. MIG kyvykkyydet .....	35

## Taulukot

Taulukko 1. SOAR-ratkaisut.....	9
Taulukko 2. Shufflen maksullisten versioiden ominaisuuserot .....	12

# 1 Työn lähtökohdat

## 1.1 Toimeksiantaja

Opinnäytetyön toimeksiantajana toimi JYVSECTEC, joka on itsenäinen kyberturvallisuutta tutkiva, kehittävä ja kouluttava keskus. JYVSECTEC toimii osana Jyväskylän ammattikorkeakoulun IT-instituuttia ja toimipaikka sijaitsee Jyväskylän Ammattikorkeakoulun Lutakon kampuksella, Dynamossa, osoitteessa Piippukatu 2. JYVSECTEC tarjoaa asiakkailleen koulutusta moderneista uhista pyrkimyksenä parantaa yritysten kyberuhkilta puolustautumista sekä ymmärrystä uusien teknologioiden käytöstä ja hyödyistä. Tarjottuja palveluita ovat muun muassa kyberharjoitukset, henkilöstökoulutus, ohjelmistotestaus ja yritysjohtamisen konsultointi. (Overview – JYVSECTEC. N.d.)

## 1.2 Tutkimuskysymys ja tavoitteet

Opinnäytetyön tutkimuskysymyksenä on: Ovatko avoimen lähdekoodin SOAR (Security Orchestration, Automation and Response) implementaatiot riittävän kypsiä ja käyttökelpoisia toimeksiantajalle harjoituskäyttöön SOC-työkaluna (Security Operations Center)? Tavoitteena on siis selvittää ja arvioida avoimen lähdekoodin SOAR implementaatioiden kypsyyttä kokonaisuutena, myös verrattuna saatavilla oleviin maksullisiin vastineisiin, sekä käyttökelpoisuutta toimeksiantajalle harjoituskäyttöön SOC-työkaluna. Erilaisten julkaisujen välillä olevien ominaisuuksien vertailu kuuluu osaksi vertailukokonaisuutta. Työkaluista valitaan yksi lähempää tutkiskelua varten, josta sitten laaditaan tarkempi arvio kyseisen ohjelman kypsyydestä ja toimintakelpoisuudesta mahdollisena SOC-työkaluna JYVSECTEC:lle.

## 1.3 Tutkimusmenetelmä

Opinnäytetyö on kartoitustutkimus, toteutettuna laadullisena tutkimuksena, jossa laadullisella tutkimusotteella pyrittiin ymmärtämään SOAR-tekniikoiden toimintaa sekä selvittämään Open Source SOAR implementaatioiden kypsyyttä ja käyttökelpoisuutta toimeksiantajalle. Kaikista implementaatioista valittiin yksi tarkempaa tutkimista varten. Valintaprosessissa otettiin huomioon tärkeimpiä osa-alueita mitä ohjelmistojen käyttöön liittyy. Tärkeysjärjestyksessä kriittisin ensin: aktiivisen kehityksen tila, riittävä määrä ilmaiseksi saatavia toimintoja täyttämään käyttötarkoitus sekä asennuksen onnistuminen. Osa-alueihin liittyen ohjelmia karsitui valintaprosessista pois, jos jokin näistä tärkeimmistä osa-alueista ei täyty.

## 2 SOAR

SOAR (Security Orchestration, Automation and Response) on alkujaan Gartnerin luoma termi, jota käytetään määrittelemään ja kuvaamaan kolmea tietotyypin ohjelmiston kykenevyyttä: uhkien ja haavoittuvuuksien hallinta, turvallisuustapahtumiin vastaaminen sekä turvallisuusoperaatioiden automaatio. Sen avulla yritykset voivat kerätä tietoja kohtaamistaan uhista lukuisista lähteistä ja automatisoida alhaisen tason uhkiin vastaamisen. SOAR-alustan perusidea on siis automaatiolla käsitellä tietoturvatapahtumia aikajänällisesti päästä päähän, eli tapahtumaa ennen, sen aikana ja sen jälkeen. SOAR-ohjelmistoilla kyetään helpottamaan tietoturvaoperaatioiden parissa työskentelevien työaikaa vähentämällä vaaditun manuaalisen työn määrää. Määrä vaihtelee yrityksen luonteesta, sekä kohdattujen uhkien määrästä ja vakavuudesta. Jos yritys kohtaa paljon lievempiä uhkia, automaatiolla voidaan saada aikaan suuri muutos. (Shea 2021; What is SOAR? Security definition | FireEye n.d.; Ødegårdstuen 2020a.)

SOAR:n käytöllä tavoitellaan fyysisten ja digitaalisten turvallisuusoperaatioiden tehostamista. Turvallisuusoperaatioiden automatisointi on kannattavaa, sillä se mahdollistaa tarkistusten laajamittaisemman, jatkuvan sekä tehokkaan suorittamisen vähentäen viivettä turvallisuustapahtumien havaitsemiseen ja korjaamiseen. Turvallisuuden parissa työskentelevien työtaakkaan ja uupumukseen SOAR-teknologioilla voi olla valtava vaikutus. Kun työntekijät jaksavat paremmin, myös manuaalista työtä vaativien operaatioiden suorittamisen taso pysyy korkealla ja tehokkaana.

### 2.1 Toimintaperiaate ja rakenne

Käytännössä SOAR-ohjelmisto kerää kaiken sille syötetyn datan, ilmoitukset ja hälytykset. Kyseiset tiedot käsitellään ja niiden pohjalta luodaan toistuvia, automatisoituja prosesseja korvaamaan manuaaliset prosessit. Analyttikoiden aiemmin suorittamat tehtävät, kuten esimerkiksi haavoittuvuuksien skannaus, lokien analysointi, tikettien läpikäynti sekä auditointi, kaikki voidaan standardisoida ja automatisoida SOAR alustalla. (Shea 2021.)

SOAR on rakenteeltaan ohjelmistopino, eli siihen sisältyy useita ohjelmia, joilla kaikilla on oma tehtävänsä, ja jotka yhdessä pystyvät suorittamaan jonkin isomman tarkoituksen tehtävän, mikä on tässä tapauksessa tietoturvatapahtumien automaatioitu käsittely päästä päähän keräämällä



tietoja turvallisuushista useista eri lähteistä ja reagoimalla alhaisen tason turvallisuustapahtumiin ilman ihmisen avustusta. Ihanteellisesti ohjelmat kommunikoivat ja jakavat jouhevasti tietoa toisilleen tehostaen uhkien tunnistamista ja torjumista. (Shea 2021.)

### 3 Teknologiat

SOAR-alustoja ajetaan pääasiassa Linux-pohjaisissa käyttöjärjestelmissä, joten niiden tutkiminen ja testaaminen Linux virtuaalikoneella oli optimaalinen ratkaisu. Virtuaalikoneita itsejään ajettiin Oraclen VirtualBoxilla Windows 10:llä, ja virtuaalikoneen käyttöjärjestelmäksi valikoitui laajimmassa jakelussa oleva, parhaimmin tuettu, Ubuntu.

#### 3.1 Oracle VM VirtualBox

Oraclen luoma VirtualBox on avoimen lähdekoodin virtualisoinnin ohjelmisto joka on aktiivisessa kehityksessä ja laajalti ilmaiseksi käytössä yritysmaailmassa kuin kodeissakin. Sillä voi tietokoneen komponenteista ja käyttöjärjestelmästä riippumatta suorittaa virtuaalikoneina periaatteessa rajattomasti valitsemiansa toisia käyttöjärjestelmiä. Rajoitteina ovat tietenkin välimuistin ja massamuistin riittävyys. VirtualBoxilla virtuaalikoneiden käyttö on tehokasta, helppoa ja vaivatonta. (VirtualBox User Manual – Chapter 1 n.d.)

#### 3.2 Ubuntu

Alunperin lokakuussa 2004 julkaistu Ubuntu on kaikista Linux julkaisuista kaikkein tunnetuin ja suosituin. Sillä on siten myös laaja tuki, ja kaikki SOAR-alustat tukevat tai jopa vaativat sitä. (About the Ubuntu project | Ubuntu n.d.)

Työssä pääasiallisessa käytössä oli Ubuntu 20.04 (Focal Fossa), mikä on luokiteltu LTS-julkaisuksi (Long-term support, pitkä tuki), tarkoittaen pidempiaikaista täyttä tukea käyttöjärjestelmälle päivitysten muodossa. Poikkeuksia oli vain jos jokin ohjelmisto oli eritoten suunniteltu jollekin muulle käyttöjärjestelmälle. Käyttöjärjestelmistä asennettiin minimalistinen asennus virtuaalikoneen suorituskyvyn parantamiseksi.

#### 3.3 Docker & Docker compose

Docker on alusta, jolla käyttäjä pystyy virtualisoinnin kautta suorittamaan ohjelmistoja paketeissa, niin kutsutuissa konteissa (container). Kontit ovat siitä käteviä, että niistä ohjelmistoja voi ajaa suoraan ja ohjelmistosta riippuen ne ovat myös jo enemmän tai vähemmän valmiiksi konfiguroituja. Kontit ovat myös erillään toisistaan, kansiorakenteessa ne sisällyttävät kaiken

tarvitsemansa omaan kansioonsa, eivätkä siten tarvitse tai vaikuta muihin kontteihin. (Docker frequently asked questions (FAQ) | Docker documentation n.d.; Empowering App Development for Developers | Docker n.d.)

Docker compose puolestaan on työkalu useamman kontin sisältävän Docker applikaation määrittämiseen ja suorittamiseen. Kaikki palvelut pystytään suorittamaan yhdellä komennolla suoraan konfiguraatiosta. (Overview of Docker Compose n.d.)

Tutkimuksessa Dockeria ja Docker composea hyödynnettiin runsaasti, sillä kontteihin perustuvat asennusmenetelmät ovat luotettavia ja suosittuja, eivätkä vaadi suurta määrää konfigurointia tai syötteitä asennuksen aikana tai sen jälkeen.

## 4 Tutkimustulokset

Tutkimuksen alussa tarkoituksena oli jakaa työkalut ilmaisiin ja maksullisiin. Sen aikana kuitenkin jo varhaisessa vaiheessa selvisi, että monet SOAR-implementaatiot, jotka aloittavat avoimen lähdekoodin ilmaisena alustana muuttuvat ajan myötä maksullisiksi, sulkien osan toiminnoista maksumuurin taakse. Tämän takia lähes kaikki avoimenkin lähdekoodin alustat voidaan luokitella samanaikaisesti maksullisiksi. Täysin maksullisia SOAR-alustoja ei ole, vaan jokaisella on olemassa enemmän tai vähemmän karsittu kokeiluversio. Näissä kokeiluversioissa tärkeimmät ja hyödyllisimmät ominaisuudet eivät ole käytettävissä.

Tutkittavien SOAR ratkaisujen joukosta valittiin yksi lähempää tutkimista varten. Valinta perustui ajantasaisuuteen eli aktiiviseen kehitystyöhön, riittäviin ilmaistoihin sekä asennuksen onnistumiseen. Valituksi tuli Shuffle. Eri SOAR-ratkaisujen tulokset ovat nähtävissä taulukosta 1.

Taulukko 1. SOAR-ratkaisut

Ohjelmisto	Aktiivisessa kehityksessä	Riittävät ilmaiset toiminnot	Onnistunut asennus
Shuffle	✓	✓	✓
Cortex XSOAR	✓	X	
PatrOwl	✓	✓	/
CimSweep	X		
GRR Rapid Response	✓	✓	X /
TheHive	✓	✓	✓
MIG	X		

CimSweep ja MIG ovat projekteina kehittäjiensä hylkäämiä, joiden kehitystyö on lopetettu, eikä niiden käyttöä voi siten myöskään suositella. Cortex XSOAR ei sisällä riittäviä ilmaistoihin. GRR Rapid Responserin asennus ei aluksi onnistunut, mutta toisella asennuskerralla onnistuminen oli osittaista. GRR Server asentui oikein ja toimi moitteettomasti, mutta kun GRR Client asennettiin, ei Server löytänyt Clientia noudattamalla asennusohjeita. PatrOwlin asennus ei myöskään onnistunut täysin. TheHive ja Shuffle asentuivat onnistuneesti, mutta Shufflen toimintojen sekä asennusprosessin ollessa parempi valikoitui se parhaimpana ehdokkaana. Shuffle pystyi lisäksi myös sisältämään itse TheHiven osaksi omaa kokonaisuuttaan, joten se voitiin tulkita

ominaisuuksiltaan kattavammaksi. Seuraavissa kappaleissa kaikki ohjelmistot käsitellään erikseen tarkemmin.

## 4.1 Shuffle

Shuffle, harrastusprojektina alkunsa vuonna 2019 saanut avoimen lähdekoodin tulkinta SOAR:sta vastauksena muutamiin huomiota vaativiin, automaatioon liittyviin ongelmiin CERT/SIRT yhteisöissä. Tarkoituksena on tarjota kaikki tarvittavat kyvykkyydet tiedonsiirtoon yrityksen läpi. Muut saatavilla olevat automaatoratkaisut yrittävät tehdä kaiken kerralla yhdessä alustassa, Shuffle puolestaan pyrkii rakentamaan parhaan ratkaisun yhdistämään kaikki käyttäjän käytössä olevat työkalut, seuraten Unixin filosofiaa: ”Tee yksi asia ja tee se hyvin”. Shuffle pyrkii ratkaisemaan valmiusväsymyksen antamalla analyytikoille työkalut useimpien hälytysten automatisointiin ja eliminoimalla turhan vähäpätöisten toimenpiteiden manuaalinen tekeminen. (Ødegårdstuen n.d.)

Shuffle hoitaa sovellusten integraation hyödyntämällä OpenAPI -verkko-ohjelmointirajapintaa, jonka ansiosta sovelluksia voi teoreettisesti yhdistellä sovelluksia lennosta, ilman tarvetta ohjelmoinnille. Tämä sovellusyhdistelmien rakentelu tapahtuu niin kutsutussa Workflow-käyttöliittymässä, jossa applikaatioita, suorittamisen aloittavia triggereitä ja toimintaa ohjaavia ja täsmentäviä variaabeleita voi hiirellä vetämällä yhdistellä toisiinsa. (Ødegårdstuen 2020.)

Ilmaisen version lisäksi Shufflesta tarjotaan myös maksullisia versioita, jotka tarjoavat lisäominaisuuksia ja niistä saaduilla tuotoilla tuotteen kehitystä voidaan jatkaa sulavammin. Eri versioiden kustannukset ovat nähtävissä kuviossa 1 ja ominaisuuserot on eritelty taulukossa 2. Ostettavien versioiden lisäksi kehitystiimi hyväksyy lahjoituksia, jos maksullisten versioiden tilaaminen ei ole mielekästä. (Early adopter Pricing n.d.)

Free	Hybrid	Enterprise	MSSP
Cloud access	Open Source X Cloud	For the inhouse SOC	Cross-Customer automation
\$0	\$258	\$1998	Custom
<b>Free</b>	<b>\$129</b>	<b>\$999</b>	<b>Custom</b>
Per month, billed yearly	Per month, billed yearly	Per month, billed yearly	Per month, billed yearly
<ul style="list-style-type: none"> <li>- Use any integration</li> <li>- Activate workflows</li> <li>- Share your usecases</li> <li>- Community support</li> </ul>	<ul style="list-style-type: none"> <li>- Custom Hybrid features</li> <li>- Includes onboarding</li> <li>- Community support</li> <li>- Extra executions</li> </ul>	<ul style="list-style-type: none"> <li>- Priority support</li> <li>- First access to features</li> <li>- Access to our security automation experts</li> </ul>	<ul style="list-style-type: none"> <li>- All previous tiers</li> <li>- Extra Customer control</li> <li>- Sub-organization access</li> <li>- Resell services through Shuffle</li> </ul>
Billed anually or monthly at 1.2x the cost	Billed anually or monthly at 1.2x the cost	Billed anually or monthly at 1.2x the cost	

Kuvio 1. Shuffle hinnasto

Taulukko 2. Shufflen maksullisten versioiden ominaisuuserot

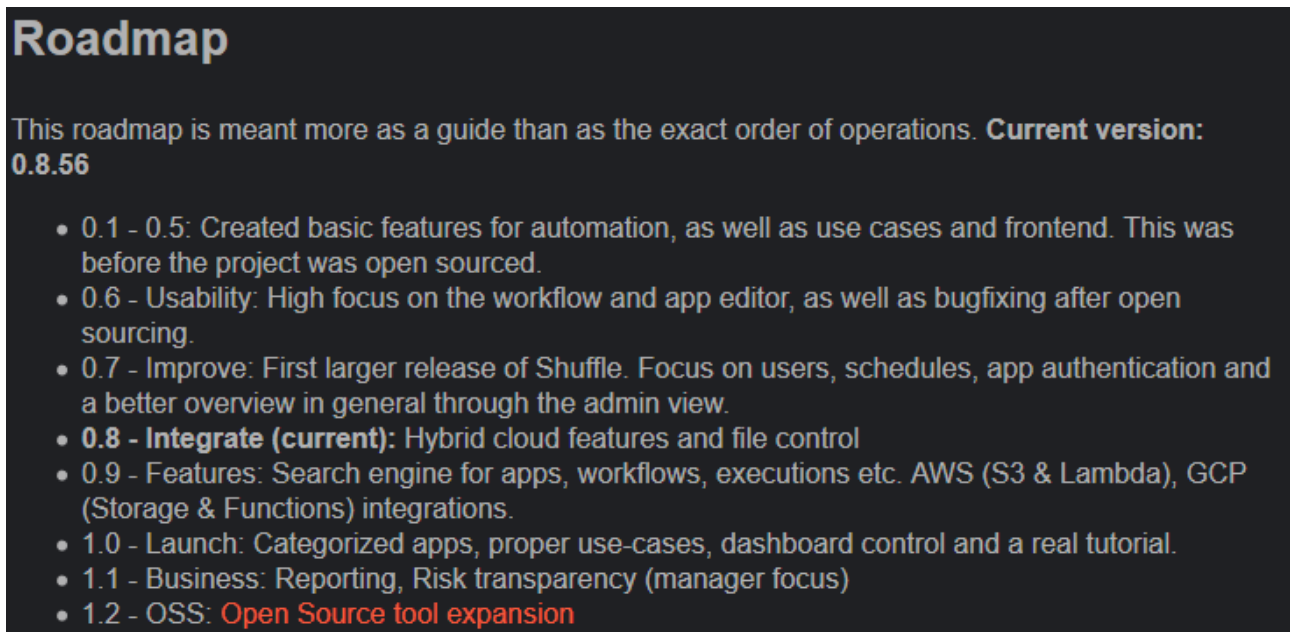
Orange = Not yet implemented	Free	Hybrid	Enterprise / MSSP
Community support	✓	✓	✓
Priority support	✗	✗	✓
Personal onboarding	✗	60min	✓
Users	No limit	No limit	No limit
Apps	No limit	No limit	No limit
Cloud Workflows	3	5	No limit
Workflow Action executions	1000 / month	2500 / month	150.000 / month
Workflow editor	✓	✓	✓
App editor	✓	✓	✓
Private Apps	✓	✓	✓
Default playbooks	✓	✓	✓
Discord support community	✓	✓	✓
Organization control	✓	✓	✓
Autocomplete features	✓	✓	✓
Shuffle creates integration	✗	✓	✓
Hybrid Webhook trigger	✗	✓	✓
Hybrid User Input trigger	✗	✓	✓
Shuffle SMS alerting	✗	✓	✓
Shuffle Email alerting	✗	✓	✓
Hybrid Email trigger	✗	✓	✓
Hybrid Schedule	✗	✓	✓
Hybrid Executions	✗	✓	✓
Uptime SLA	✗	✗	✓
Cloud backup	✗	✗	✓
Single sign-on	✓	✓	✓
Audit logging	✗	✗	✓
MSSP org overview	✗	✗	MSSP only
MSSP org control	✗	✗	MSSP only
Automatic Platform updates	✓	✓	✓
2-factor authentication	✓	✓	✓
Workflow recommendations	✓	✓	✓
Standardized app categories	✓	✓	✓
Mitre Att&ck integrations	✓	✓	✓
Detection Engineering framework	✓	✓	✓
Multiple Shuffle connectors	✗	✓	✓
Hybrid search engine	✗	✓	✓
Hybrid App synchronization	✗	✓	✓
Open Source account rollback	✗	✓	✓
Data LOCATION control	✗	✗	✓
Data RETENTION control	✗	✗	✓
Shuffle alerts	✗	✗	✓
Shuffle IoC search	✗	✗	✓
Controllable Reporting	✗	✗	✓
Management dashboard	✗	✗	✓
Risk based overview	✗	✗	✓
Compliance dashboard	✗	✗	✓

## Kehitystyö

Shuffle ei ole vielä saavuttanut ominaisuuksiltaan valmista julkaisuversiota. Nykyinen versio on 0.8.56, josta puuttuu vielä suuri määrä suunniteltuja toimintoja. Kehittäjät ovat julkaisseet viitteellisen roadmapin kehitystyön suunnittelusta kulusta, joka on nähtävissä kuviosta 2. Työkalun

oleellisimmat ja toiminnalta kriittisimmät toiminnot ovat siis jo valmiita ja käyttökelpoisia.

(Ødegårdstuen n.d.)



## Roadmap

This roadmap is meant more as a guide than as the exact order of operations. **Current version: 0.8.56**

- 0.1 - 0.5: Created basic features for automation, as well as use cases and frontend. This was before the project was open sourced.
- 0.6 - Usability: High focus on the workflow and app editor, as well as bugfixing after open sourcing.
- 0.7 - Improve: First larger release of Shuffle. Focus on users, schedules, app authentication and a better overview in general through the admin view.
- **0.8 - Integrate (current):** Hybrid cloud features and file control
- 0.9 - Features: Search engine for apps, workflows, executions etc. AWS (S3 & Lambda), GCP (Storage & Functions) integrations.
- 1.0 - Launch: Categorized apps, proper use-cases, dashboard control and a real tutorial.
- 1.1 - Business: Reporting, Risk transparency (manager focus)
- 1.2 - OSS: **Open Source tool expansion**

Kuvio 2. Shuffle Roadmap

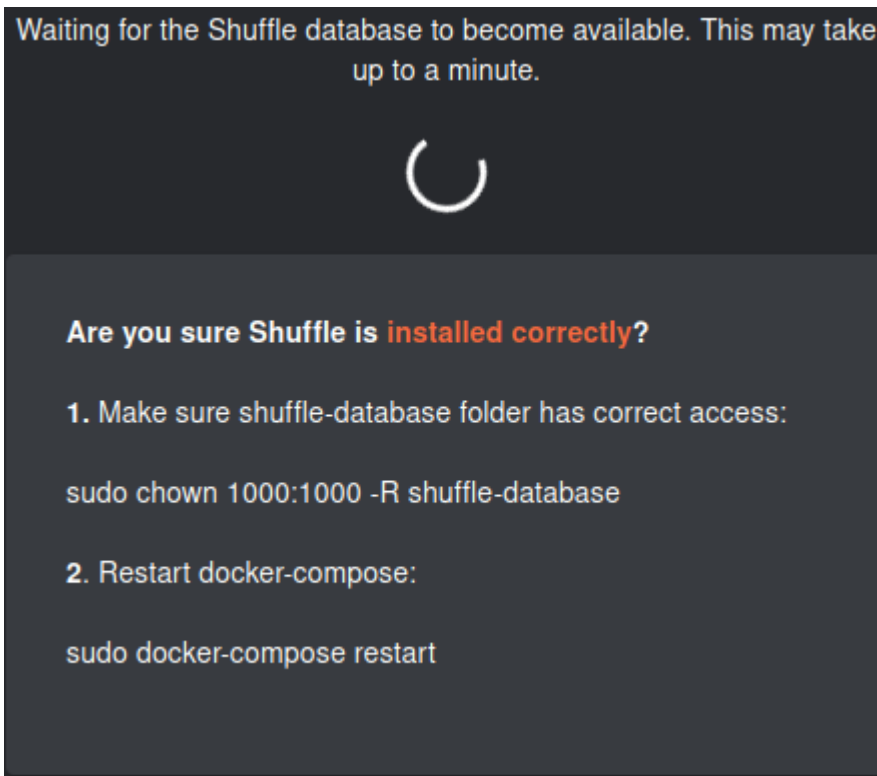
### 4.1.1 Asennus

Shufflen asennus suoritettiin github -repositorion ”Installation guide” -sivun ohjeilla. Asennus on mahdollista ainoastaan Dockerissa, joten ensiaskeleena olikin Dockerin ja Docker-composen asennukset. Docker-asennukset hoidettiin Dockerin omien dokumentaationsivujen asennusohjeiden avulla ja niihin liittyvät syötteet ovat nähtävissä liitteessä 1. (Install Docker Compose n.d.; Install Docker Engine n.d.; Ødegårdstuen 2021.)

Dockerin onnistuneen asennuksen jälkeen Shufflen asennus oli varsin lyhyt ja yksinkertainen prosessi. Shufflen asennukseen käytetyt syötteet löytyvät liitteestä 6. Huomattavaa on, että asennusohjeissa mainittu komento ”*sudo chown 1000:1000 -R shuffle-database*” ei toiminut kesken asennuksen, koska tietokantaan liittyvää kansiorakennetta ei oltu vielä luotu. Tästä johtuen ymmärrettävästi asennuksen jälkeisen Shufflen suorittamisen ja hallintasivulle (localhost:3001) pyrkimisen yhteydessä Shufflilla ei ollut pääsyä omaan tietokantaansa, joka johti kuviossa 3 nähtävissä olemaan näkymään. Oheisen ohjeistuksen avulla ongelma korjaantui vaivattomasti,



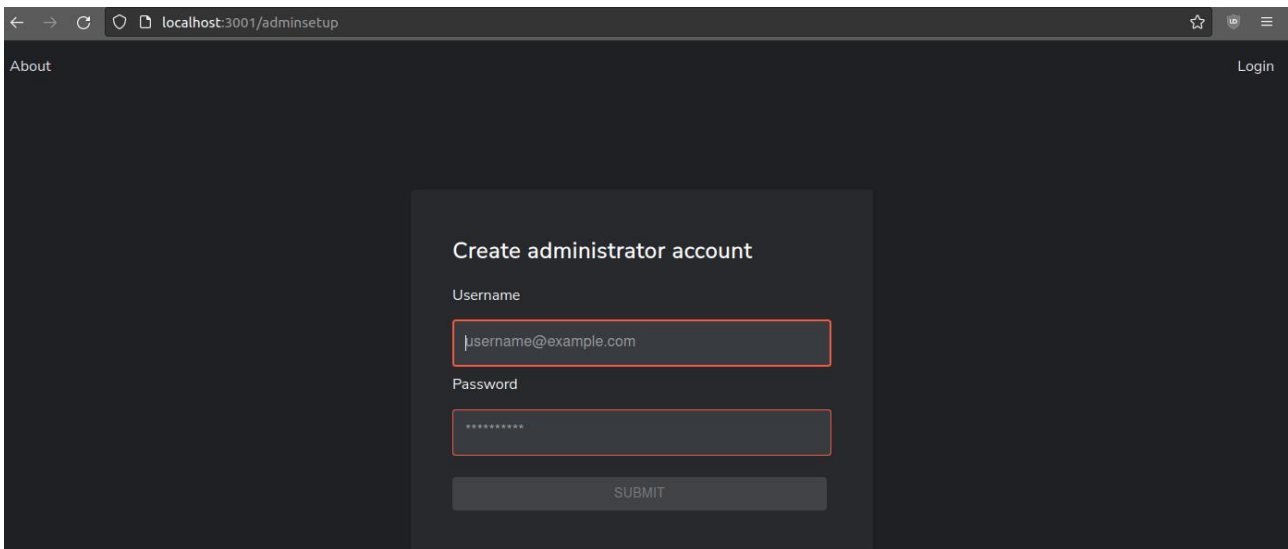
jonka jälkeen Shufflea pääsi käyttämään normaalisti ja asennus oli onnistunut. (Ødegårdstuen 2021.)



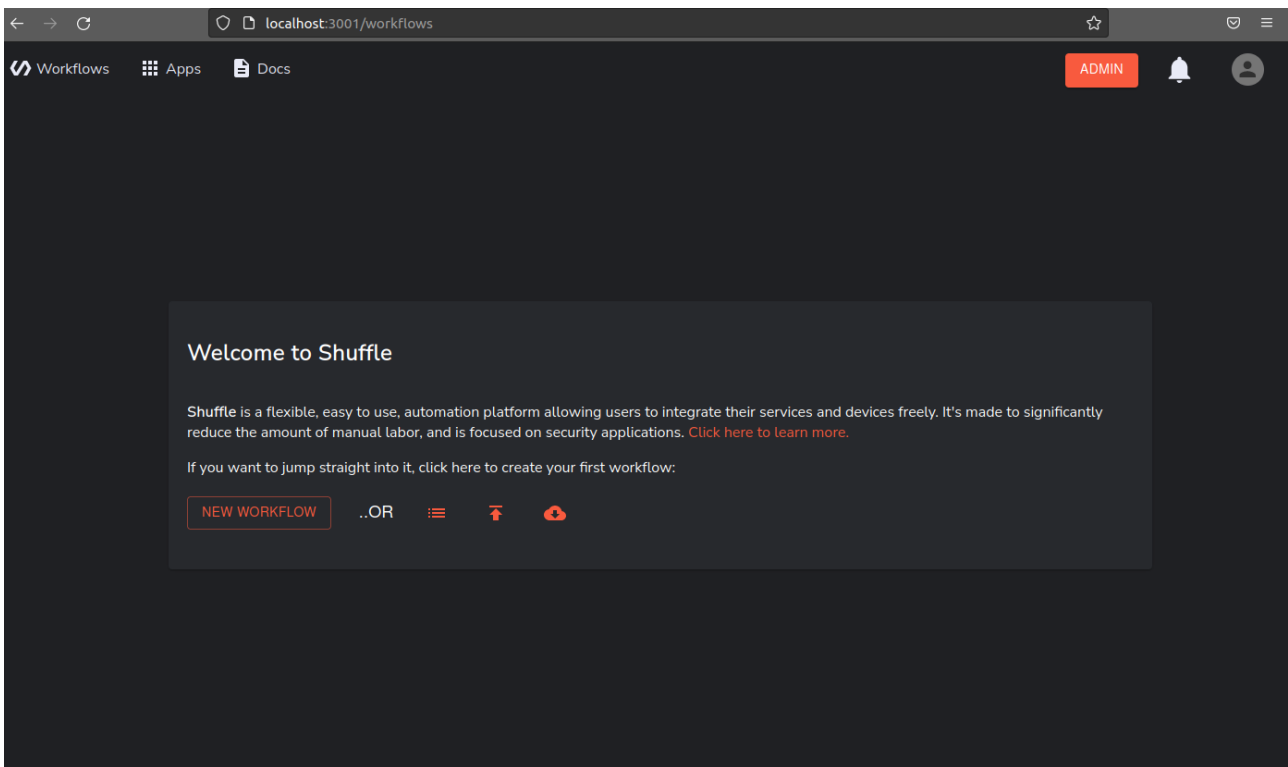
Kuvio 3. Shufflen asennuksen aikana ilmennyt ongelma

#### 4.1.2 Käyttö

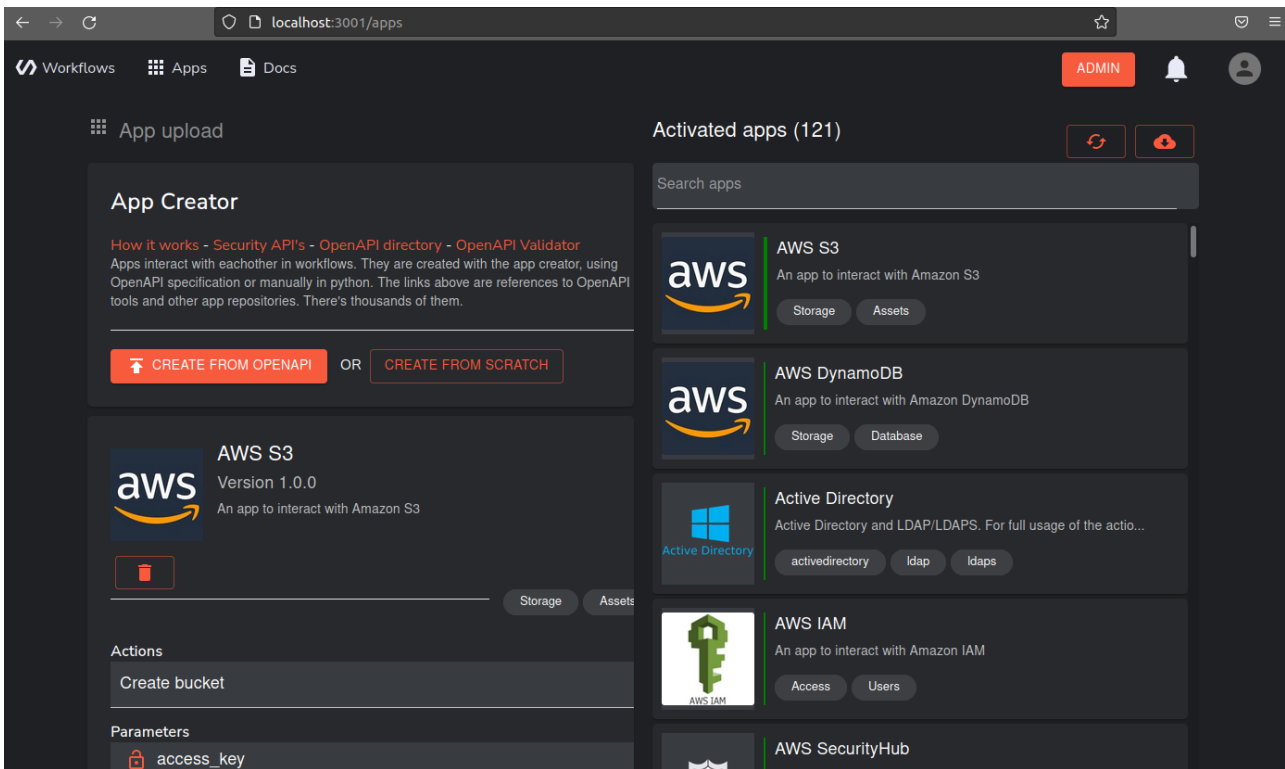
Shufflen käyttöliittymä on HTML-pohjainen ja sitä voi käyttää niin HTTP:n kuin myös HTTPS:n välityksellä. Välittömästi asennuksen jälkeen käyttäjää kehoitetaan luomaan administrator-käyttäjä (kuvion 4 näkymässä) hallinnointia varten. (Ødegårdstuen 2020b.) Luotuaan käyttäjän päästään Shufflen perusnäkömään, joka koostuu kolmesta eri osiosta. Workflows-osiosta, jossa voidaan hallinnoida itse ohjelman toimintaa ja eri sovellusten välistä yhteistyötä. Apps-osiosta on listattuna kaikki Shufflen tukemat yksittäiset ohjelmat ja sovellukset, joista voidaan tarvittaessa konfiguroida ja rakentaa omia versioita. Viimeinen osio on Shufflen oma dokumentaatio sivu, josta löytyy tietoa Shufflesta ja sen tekijöistä, sekä käyttöohjeistusta. Nämä eri näkymät ovat havainnollistettuina kuvioissa 5, 6 ja 7. Workflowien luomisen jälkeen kaikki workflowit listataan Workflows-osiosta, josta niitä kaikkia pääsee hallinnoimaan.



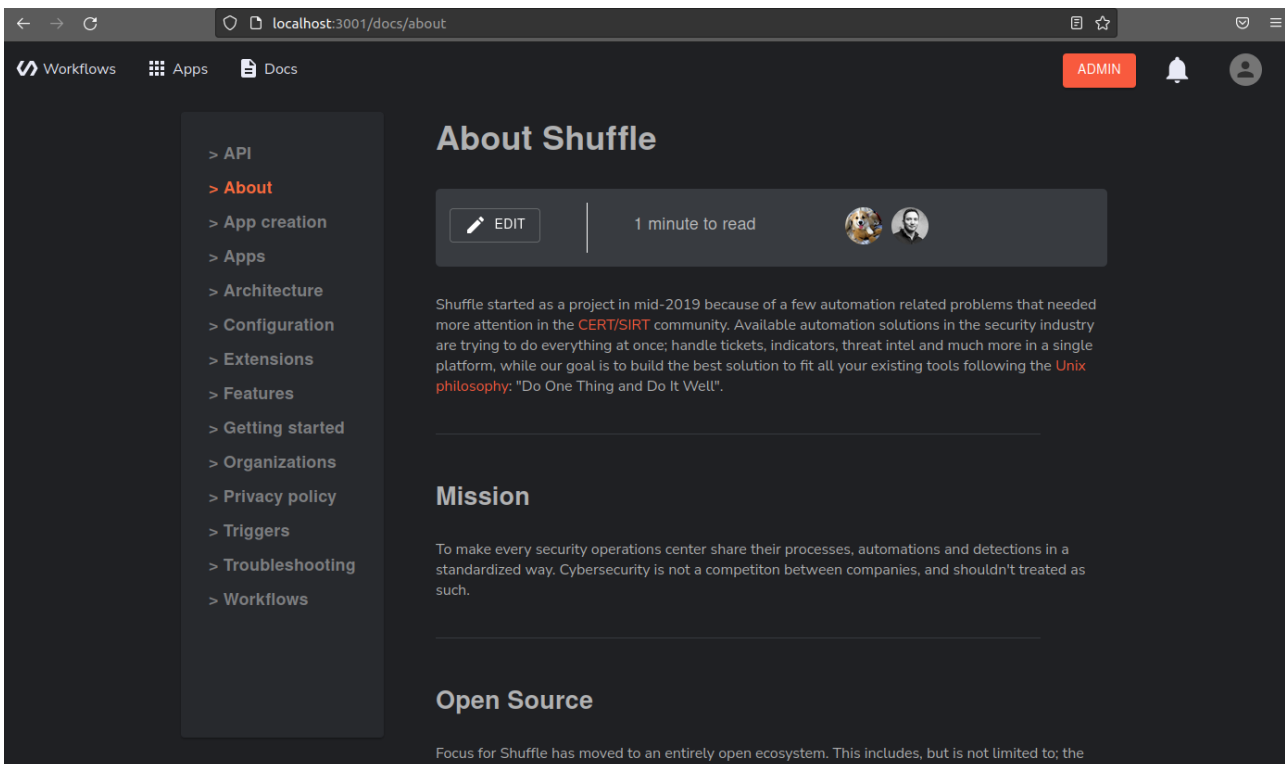
Kuvio 4. Shuffle administrator-käyttäjän luonti



Kuvio 5. Shuffle ensinäkymä

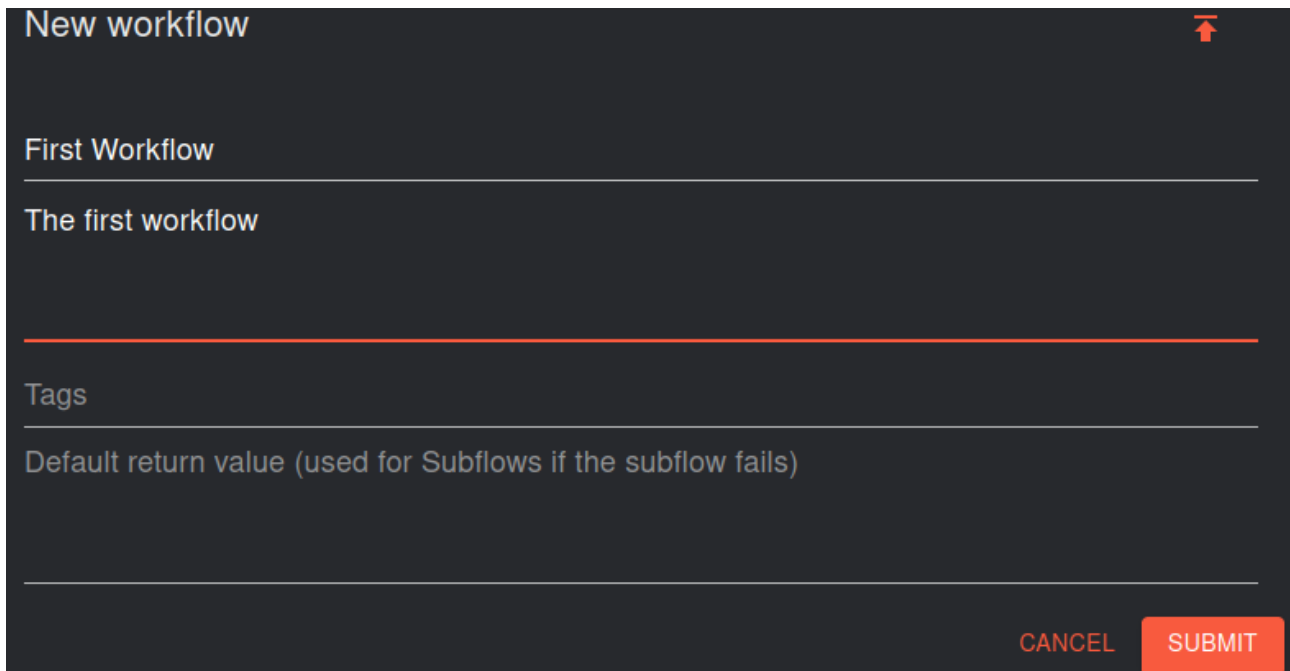


Kuvio 6. Shuffle Apps-näkymä, lista applikaatioista



Kuvio 7. Shuffle Docs-näkymä, dokumentaatio

Shuffleen tutustumisen ensiaskel on ensimmäisen workflow:n luonti, minkä näkymä on esitetty kuviossa 8. Luomisen yhteydessä ensimmäisessä workflow:ssa on havainnollistamista ja testaamista varten valmiiksi hello world-toiminto, jolla pystyy tutustumaan Shufflen workflowien toiminnan alkeisiin. (Ødegårdstuen 2020b.) Hello worldin suorittaminen toimi ongelmitta. (Kuvio 9)

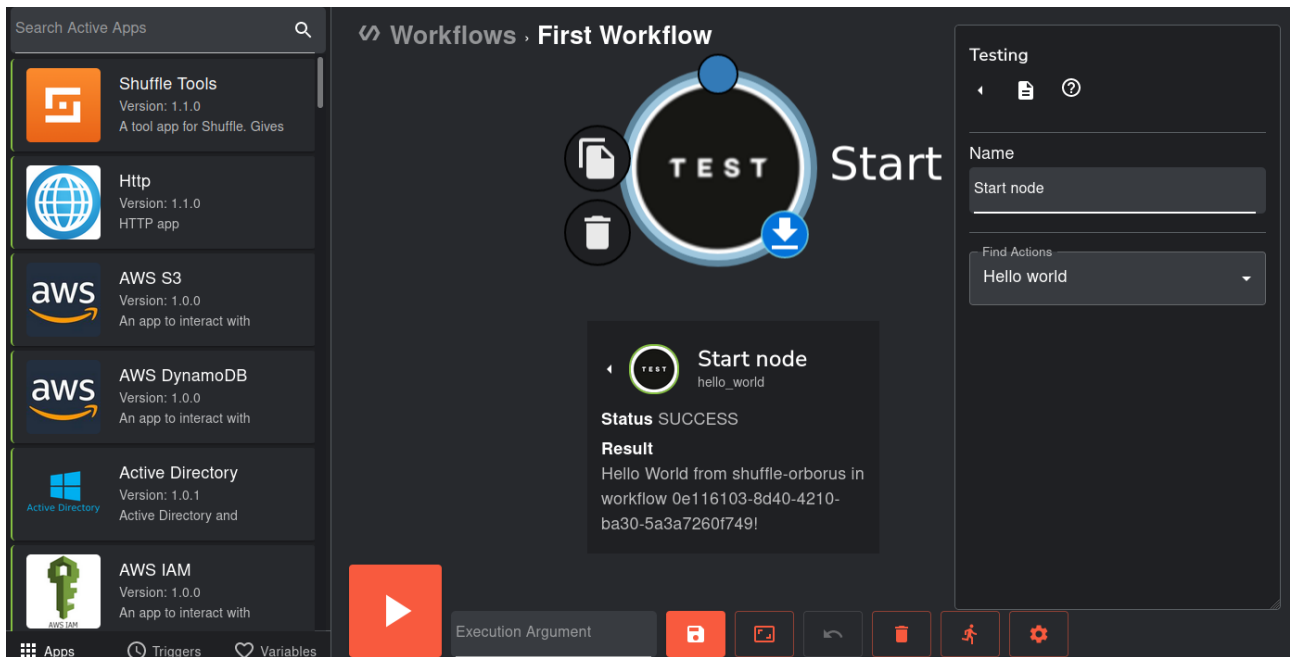


The image shows a dark-themed form titled "New workflow" with a red upward arrow icon in the top right corner. The form contains several input fields:

- A text input field labeled "First Workflow" with the placeholder text "The first workflow".
- A text input field labeled "Tags".
- A text input field labeled "Default return value (used for Subflows if the subflow fails)".

At the bottom right of the form, there are two buttons: "CANCEL" and "SUBMIT".

Kuvio 8. Shuffle ensimmäisen workflow:n luonti



Kuvio 9. Shuffle ensimmäinen workflow ja onnistunut hello world suoritus

Seuraavaksi on tarkoitus kokeilla lisätä workflowiin joitain uusia toimintoja hello worldin lisäksi. Ensimmäiseksi workflowiin lisätään repeater node (kuvio 10), joka toistaa hello worldin sisällön suorituslokiin, hakien tiedon suoraan hello world nodesta. Testausmielessä haluamme myös saada Shufflen avulla tietoomme oman julkisen IP-osoitteemme. Tätä varten tieto tarvitsee hakea ulkoisesta lähteestä, johon tässä yhteydessä käytetään palvelua verkko-osoitteessa <https://ip.seeip.org/jsonip>, joka palauttaa tiedon IP-osoitteesta json-muodossa Shuffleen. Tätä varten luodaan uusi Get\_URL-node, jonka ominaisuudet ja onnistunut suoritus ovat nähtävissä kuvioista 11. (Ødegårdstuen 2020b.)

The screenshot shows the 'Workflows · First Workflow' interface. On the left, a workflow diagram features a circular 'TEST' node labeled 'Hello\_world\_node' and a square 'TEST' node. On the right, the configuration panel for the 'Repeater\_node' is visible. The 'Name' field is set to 'Repeater\_node'. The 'Find Actions' dropdown is set to 'Repeat back to me'. Under the 'Parameters' section, the 'Call' field contains '\$hello\_world\_node'.

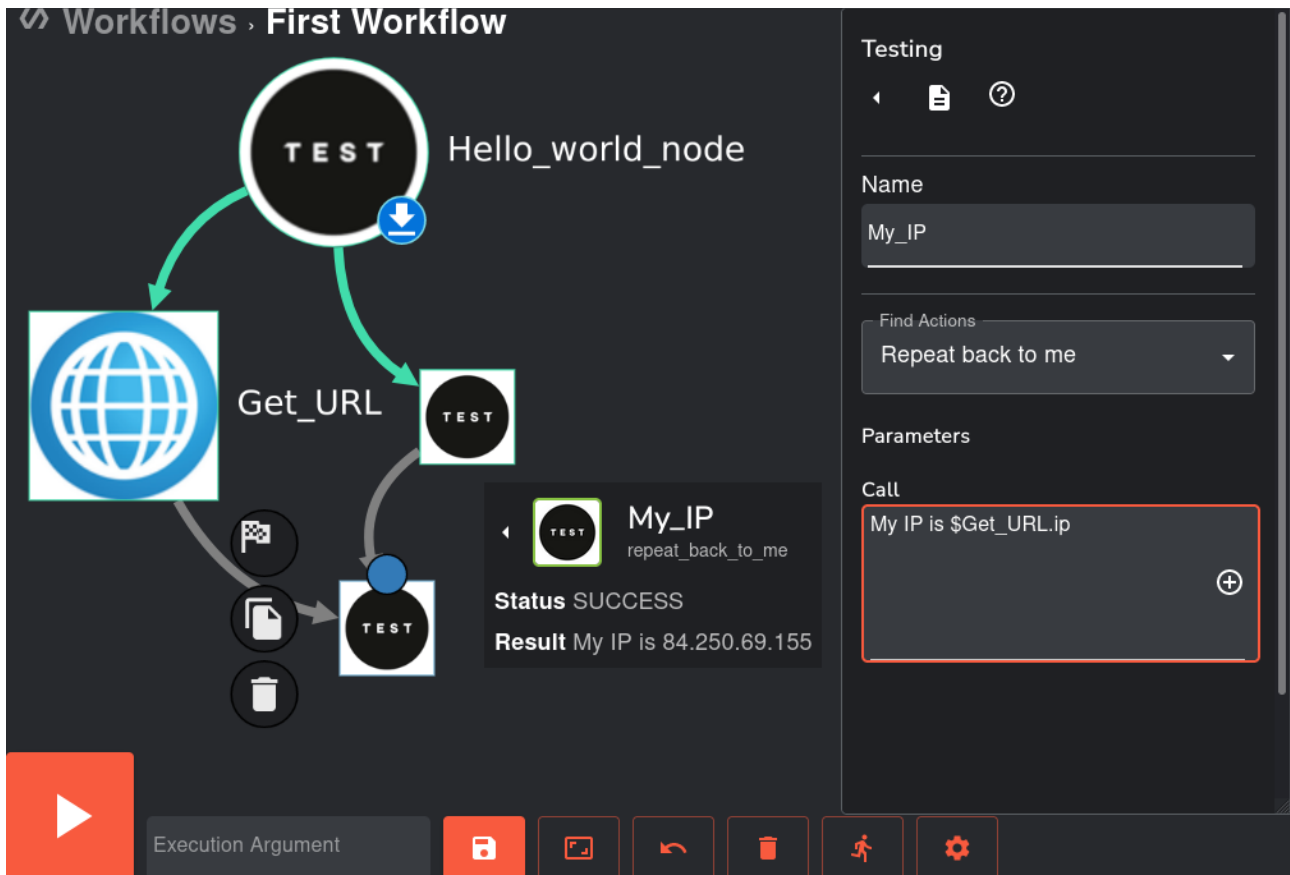
Kuvio 10. Shuffle Repeater node

The screenshot shows the workflow editor with the 'Hello\_world\_node' selected. The configuration panel for the 'Http' node is visible, showing the 'Name' as 'Get\_URL', the 'Method' as 'GET', and the 'Url' as 'http://ip.jsonest.com'. The 'Headers' section shows 'Authorization: Bearer asd' and 'Content-Type: application/json'. On the right, the execution results are displayed:

- Hello\_world\_node** (hello\_world): Status SUCCESS, Result: Hello World from shuffle-orborus in workflow 4ebb20c7-b4f4-490e-86a4-64ff0622920a!
- Repeater\_node** (repeat\_back\_to\_me): Status SUCCESS, Result: Hello World from shuffle-orborus in workflow 4ebb20c7-b4f4-490e-86a4-64ff0622920a!
- Get\_URL** (GET): Status SUCCESS, Results for Get\_URL: { 1 item, "ip": "84.250.69.155" }

Kuvio 11. Shuffle Get\_URL ja onnistunut suoritus

Get\_URL noden tuloste on kuitenkin käyttäjystävällisyydeltään epämieluisa, joten tulosteen muuttamiseksi miellyttävämpään muotoon lukea, luodaan My\_IP node, jonka ainut tarkoitus on toistaa tulos vapaasti kirjoitettavassa muodossa, noutaen IP-osoitteen suoraan Get\_URL-nodesta. (Kuvio 12) (Ødegårdstuen 2020b.)



Kuvio 12. Shuffle My\_IP ja onnistunut suoritus

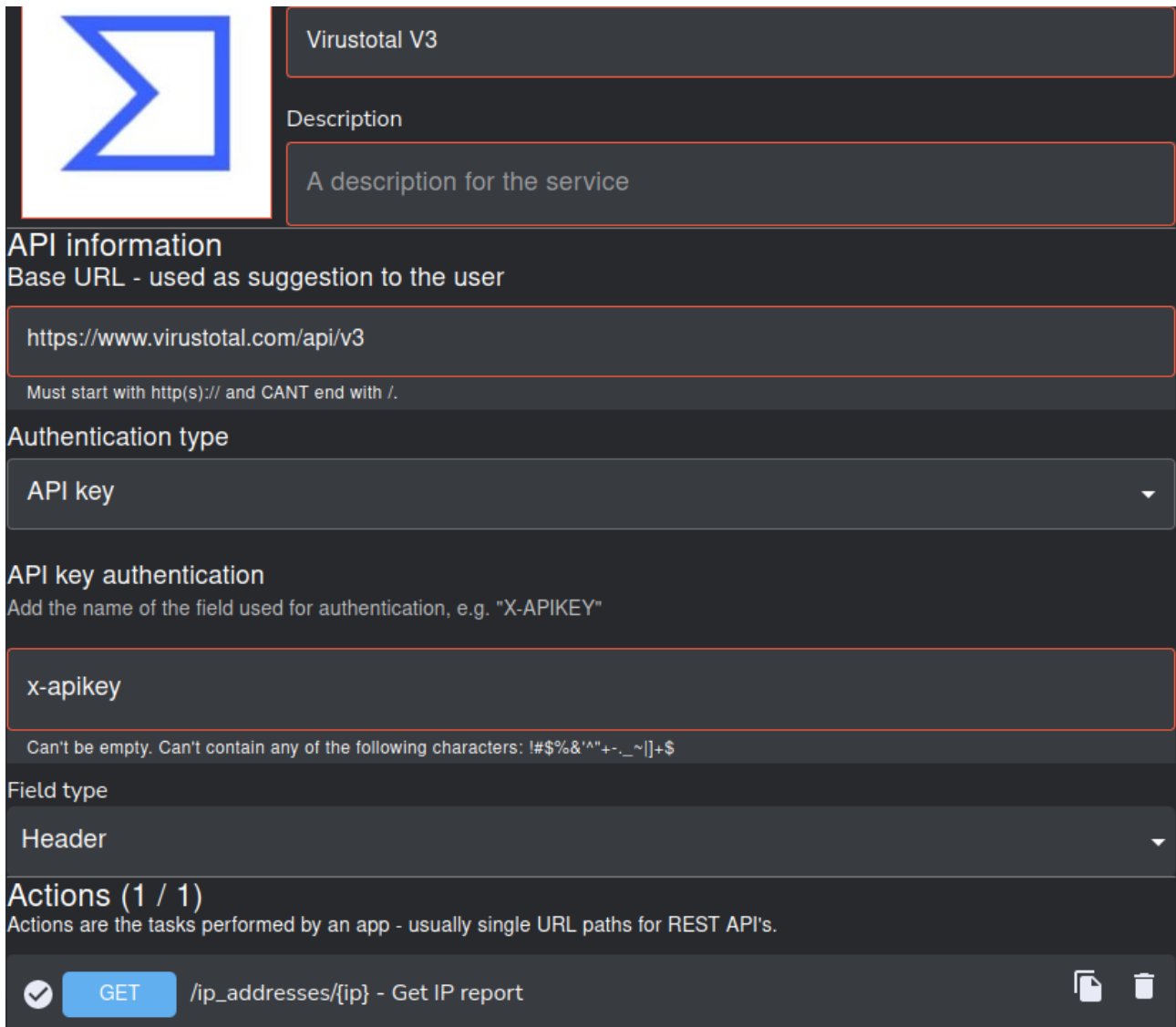
Shufflessa toimintoja voi aikatauluttaa tapahtumaan määriteltyjen väliaikojen tiheydellä toistuvasti. Sitäkin varten on oma node, Schedule, jota ajamalla suorituslokiin ilmestyy erilaiset merkinnät, kuten havainnollistettu kuviossa 13. Lokin listaamissa suorituskerroissa on kaikissa jokaisen noden suorituksen tiedot, eli kaikki nodet ajetaan määritellyn aikataulun mukaan. (Ødegårdstuen 2020b.)

The screenshot displays the Shuffle workflow management interface. At the top, a workflow diagram titled "First Workflow" shows a sequence of steps: "Schedule\_1" (a clock icon), "Hello\_world" (a circle with "TEST"), "Get\_URL" (a globe icon), and two "TEST" nodes. Below the diagram is the "All Executions" section, which includes a "REFRESH EXECUTIONS" button and a list of four execution records, each with a timestamp and a progress indicator (0/4). On the right, a configuration panel for "Schedule: running" shows the name "Schedule\_1", environment "onprem", and parameters for "Interval (UTC)" set to 5 and "Execution argument" set to {"url": "http://ip.jsonest.com"}. At the bottom, there is a red play button and a row of icons for workflow management.

Kuvio 13. Shuffle Schedule aikataulus ja suoritukset

IP-osoitteen pohjalta voi myös saada yksityiskohtaisemman raportin, josta esimerkkinä käytetään tässä tapauksessa Virustotalia. Virustotalista on jo valmiiksi rakennettuna applikaatio versio 2, mutta Shufflen dokumentaatiossa on ohjeet Virustotal version 3 käytöstä, jota varten sovellus täytyy konfiguroida uudelleen ja luoda siten tavallaan kokonaan uusi appi Shufflen listaukseen. Virustotal V3:n luontiin käyteyt tiedot nähtävissä kuviosta 14. Virustotalin käyttö Shufflessa vaatii myös API-avaimen, eli käyttäjäkohtaisen avaimen käyttörajapinnan hyödyntämiseen. Tätä varten täytyi luoda tunnukset Virustotalin palveluun. (Ødegårdstuen 2020c.)





**Virustotal V3**

Description

A description for the service

**API information**  
Base URL - used as suggestion to the user

`https://www.virustotal.com/api/v3`

Must start with http(s):// and CANT end with /.

**Authentication type**

API key

**API key authentication**  
Add the name of the field used for authentication, e.g. "X-APIKEY"

x-apikey

Can't be empty. Can't contain any of the following characters: !#\$%&'^"+-.\_~[]+\$\$

**Field type**

Header


**Actions (1 / 1)**  
Actions are the tasks performed by an app - usually single URL paths for REST API's.


✓ GET /ip\_addresses/{ip} - Get IP report

Kuvio 14. Shuffle Virustotal V3 luominen

Applikaation luomisen jälkeen sen toimivuutta testattiin ensin uudessa workflow:ssa. Vaikka testin tulos näyttää sisäisen IP-osoitteen, testi lasketaan silti onnistuneeksi, koska virheilmoituksia ei tullut ja applikaatio suoritti tehtävänsä onnistuneesti, kuten kuvioista 15 on huomattavissa. Toimivuuden varmistuttua Virustotal V3:n pystyi liittämään osaksi ensimmäisenä luotua workflowia. Siellä tuloksena saatiin asianmukaisesti raportti ulkoisesta IP-osoitteesta yksityiskohtaisempine tietoineen. (Kuvio 16) (Ødegårdstuen 2020c.)

Workflows · Virustotal test

 Virustotal\_V3\_1

 Virustotal\_V3\_1  
get\_ip\_report

Status SUCCESS

```

"Results for Virustotal_V3_1"
:
{
  1 item
  -> "data" : { 4 items
    -> "attributes" : { ... }
    14 items
    "type" : "ip_address"
    "id" : "122.0.0.28"
    -> "links" : { ... } 1 item
  }
}

```

Execution Argument

Virustotal V3

Name  
Virustotal\_V3\_1

+ AUTHENTICATE VIRUSTOTAL\_V3

Find Actions  
Get ip report

Parameters

Apikey  
.....

Url  
https://www.virustotal.com

Ip

Kuvio 15. Shuffle Virustotal V3 testi workflow ja suoritus

Workflows · First workflow

Schedule

TEST Hello\_world\_node

Get\_URL

TEST

TEST

Virustotal\_V

Name  
Virustotal\_V3\_1

+ AUTHENTICATE VIRUSTOTAL\_V3

Find Actions  
Get ip report

Parameters

Apikey  
.....

Url  
https://www.virustotal.com

Ip  
\$get\_url.ip

Headers  
Content-Type=application/json

Status SUCCESS

```

"Results for Get_URL" : { ... }
1 item

```

TEST My\_IP  
repeat\_back\_to\_me

Status SUCCESS

Result My IP is 84.250.69.155

Virustotal\_V3\_1  
get\_ip\_report

Status SUCCESS

```

"Results for Virustotal_V3_1"
:
{
  1 item
  -> "data" : { 4 items
    -> "attributes" : { ... }
    12 items
    "type" : "ip_address"
    "id" : "84.250.69.155"
    -> "links" : { ... } 1 item
  }
}

```

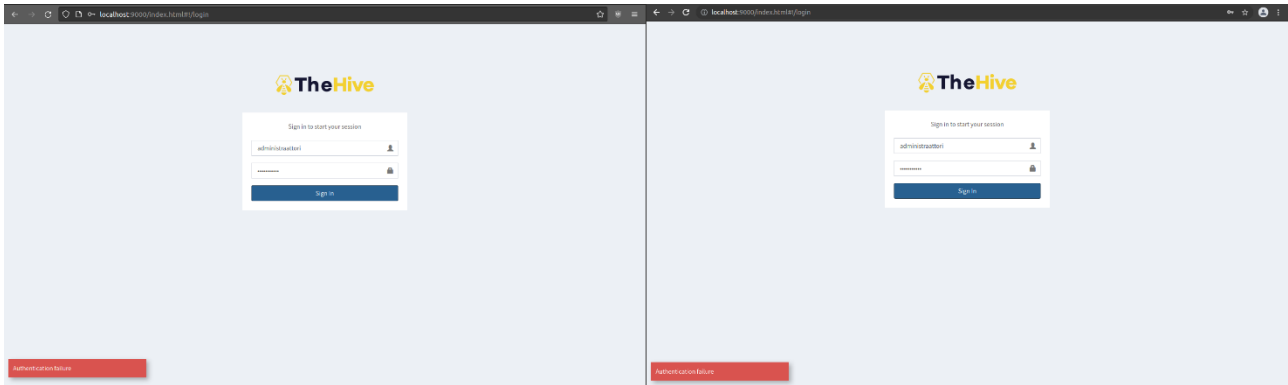
Execution Argument

Kuvio 16. Shuffle Virustotal V3 osana kokonaisuutta ja onnistunut IP raportti

Virustotalin jälkeen vuorossa olisi ollut TheHiven liittäminen osaksi kokonaisuutta, mutta tämä ei onnistunut. Dokumentaation ohjeistuksessa oli annettu TheHiven pikaista pystyttämistä varten Docker-composen .yaml-skripti (kuvio 17), jonka suorittaminen itsessään onnistui, mutta hallinnoimista varten tarkoitetun tunnuksen luomisen ja tietokannan päivittämisen jälkeen kirjautumisyhteyden yhteydessä vastaan tuli autentikaatiovirhe (kuvio 18), joka ei korjaantunut ohjeissa annetulla toisella komennollakaan (kuvio 19), jonka tarkoitus olisi ollut ohittaa/korjata yleisimmät vastaantulevat ongelmat. Siltä varalta, että kyseessä olisi ollut ongelma liittyen käytössä olleeseen selaimen, yritettiin kirjautumista Ubuntu mukana tulleen Firefoxin lisäksi myös Google Chromella, mutta tulos oli sama. (Ødegårdstuen 2020c.)

```
GNU nano 4.8 docker-compose.yml
version: "2"
services:
  elasticsearch:
    image: elasticsearch:6.8.8
    environment:
      - http.host=0.0.0.0
      - discovery.type=single-node
    ulimits:
      nofile:
        soft: 65536
        hard: 65536
  cortex:
    image: thehiveproject/cortex:latest
    depends_on:
      - elasticsearch
    ports:
      - "0.0.0.0:9001:9001"
  thehive:
    image: thehiveproject/thehive:latest
    depends_on:
      - elasticsearch
      - cortex
    ports:
      - "0.0.0.0:9000:9000"
    command: --cortex-port 9001
```

Kuvio 17. Shufflen TheHive docker-compose.yaml



Kuvio 18. Shufflen TheHive autentikaativirhe Firefoxissa ja Chromessa

```

2@z:~/TheHive$ docker-compose up -d
Creating network "thehive_default" with the default driver
Creating thehive_elasticsearch_1 ... done
Creating thehive_cortex_1 ... done
Creating thehive_thehive_1 ... done
2@z:~/TheHive$ docker exec -u 0 -it thehive_elasticsearch_1 curl -XPUT -H "Content-Type: application/json" http://localhost:9200/_cluster/settings -d '{ "transient": { "cluster.routing.allocation.disk.threshold_enabled": false } }'; curl -XPUT -H "Content-Type: application/json" http://localhost:9200/_all/_settings -d '{"index.blocks.read_only_allow_delete": null}'
{"acknowledged":true,"persistent":{},"transient":{"cluster":{"routing":{"allocation":{"disk":{"threshold_enabled":"false"}}}}}curl: (7) Failed to connect to localhost port 9200: Connection refused
2@z:~/TheHive$ docker-compose restart
Restarting thehive_thehive_1 ... done
Restarting thehive_cortex_1 ... done
Restarting thehive_elasticsearch_1 ... done

```

Kuvio 19. Shufflen TheHive syötteet ja yleisempien virheiden korjauskomento

## 4.2 Cortex XSOAR (entinen Demisto)

Cortex XSOAR (entiseltä nimeltään Demisto) on Palo Alto Networksin kehittämä turvallisuuden orkestroinnin, automaation ja reagoinnin alusta, joka yhdistää täyden turvallisuustapahtuman hallinnan, turvallisuuden automaation sekä orkestroinnin ja reaaliaikaisen yhteistyön turvallisuusoperaatioiden tehokkuuden parantamiseksi myös tapahtumiin reagoinnissa. Ohjelmisto on sisällöltään varsin laaja, sisältäen yli 750 integraatiota sekä yli 680 sisältöpakettia erilaisiin turvallisuuteen liittyviin käyttötarkoituksiin. (Security Automation (SOAR) for Everyone – Palo Alto Networks n.d.)

Cortex XSOAR:sta tarjotaan kahta eri versiota. Maksullista, kaikki ominaisuudet kattavaa versiota, sekä ilmaista yhteisöllistä versiota, jossa on 30 päivän pituisen kokeiluajanjakson ajan kaikki toiminnot käytettävissä. Ilmaisenkin version käyttö vaatii rekisteröitymisen. Kokeiluajanjakson päätyttyä version pyyntöjen määrään asetetaan seuraavat rajoitteet: 166 päivittäistä automaatiokomentoa, rullaava 30 päivän tapahtumahistoria, 5 aktiivista feediä / 100 indikaattoria

per feed, tapahtuman päätökseensaattamisen raportti. (Cortex XSOAR Community Edition FAQ 2020.)

### 4.3 PatrOwl

PatrOwl on alusta turvallisuusoperaatioiden automatisointiin tehokkaan resurssien puolustamisen saavuttamiseksi. Se tarjoaa jatkuvan turvallisuusyleisnäkymän IP:stä dataan ja on kustannustehokas. Mahdollisia orkestroitavia turvallisuusoperaatioita ovat muun muassa penetraatiotestaus, haavoittuvuusarviot, koodin arviointi, sekä SOC ja DFIR operaatiot. (Patrowl.io – Patrowl n.d.)

Työkalusta on saatavilla sekä avoimen lähdekoodin julkaisu, joka on tarkoitettu lähinnä henkilökohtaiseen kokeiluun tai koulutukselliseen käyttöön, sekä maksullisia versioita yrityksille, turvallisuustiimeille ja -keskuksille. Kehitystyö on vielä kesken, maksullisten versioiden kaikkia toimintoja ei ole saatu vielä implementoitua, eivätkä kaikki PatrOwlEnginesin moottorit ole toimintakelpoisia. PatrOwlin kotisivulla listatut eri versiot havainnollistettuina kuviossa 20. (Patrowl.io – PatrowlManager n.d.)

The screenshot displays the pricing page for PatrOwlManager, categorized under 'PATROWLMANAGER'. It features four pricing tiers, each with a list of features and a 'CONTACT SALES' button. The 'Starter SaaS' tier is highlighted with an orange border and labeled 'Recommended'.

Edition	Target Audience	Price	Key Features	Action
Starter SaaS	For small teams with security concerns	199 € /month	<ul style="list-style-type: none"> <li>Users: 1</li> <li>Unlimited scans</li> <li>Assets: Up to 25</li> <li>Engines: Up to 5 connectors</li> <li>Team sharing &amp; RBAC</li> </ul>	CONTACT SALES >
Professional SaaS	For security teams and MSSP	- € /month	<ul style="list-style-type: none"> <li>Users: Up to 50</li> <li>Unlimited scans</li> <li>Assets: view quantity</li> <li>Engines: Up to 15 connectors</li> <li>Team sharing &amp; RBAC</li> </ul>	CONTACT SALES >
Community Edition	For testing and educational purposes	- € /month	<ul style="list-style-type: none"> <li>Unlimited users</li> <li>Unlimited scans</li> <li>Unlimited assets</li> <li>Unlimited engines</li> <li>Team sharing &amp; RBAC</li> </ul>	GITHUB >
Professional Edition	For savvy security teams	- € /month	<ul style="list-style-type: none"> <li>Unlimited users</li> <li>Unlimited scans</li> <li>Unlimited assets</li> <li>Unlimited engines</li> <li>Team sharing &amp; RBAC</li> </ul>	CONTACT SALES >

Kuvio 20. PatrOwlManager versiot

## Rakenne

PatrOwl on jaettu kahteen komponenttiosaan. Ensimmäinen, suurempi osa, on PatrOwlManager, joka on kojelauta front-end applikaatio PatrOwlin hallintaan, riskien reaaliaikaiseen tarkkailuun, operaatioiden (skannaukset, haut, ohjelmointirajapintojen kutsut) orkestroimiseen, tulosten yhteenvetoon sekä varoitusten välittämiseen kolmansille osapuolille. (TheHive, SIEM tai muu vastaava Incident Response ohjelmisto) (Patrowl.io – Patrowl n.d.)

Toinen osa PatrOwlista on PatrowlEngines, mikä puolestaan on moottoriviitekehys ja ylläpidetty lista operaatioita ajallaan suorittavista moottoreista. Moottorit ovat PatrOwlin työmyyriä jotka suorittavat erilaisia tehtäviä saavuttaakseen tietoturvatapahtumien päästä päähän käsittelyn. (GitHub – Patrowl/PatrowlEngines 2020.)

PatrOwliin sisältyvät ilmaiset moottorit ovat: NMAP, Nessus, OpenVAS, Censys, Dependency-check, arachni, certstream, Qualys, Pastebin, VirusTotal, TheHive ja Cortex. Maksullisia premium

moottoreita ovat sonarqube, OWASP, Nikto sekä Microsoft Cloud App Security. (Patrowl.io – Patrowl n.d.)

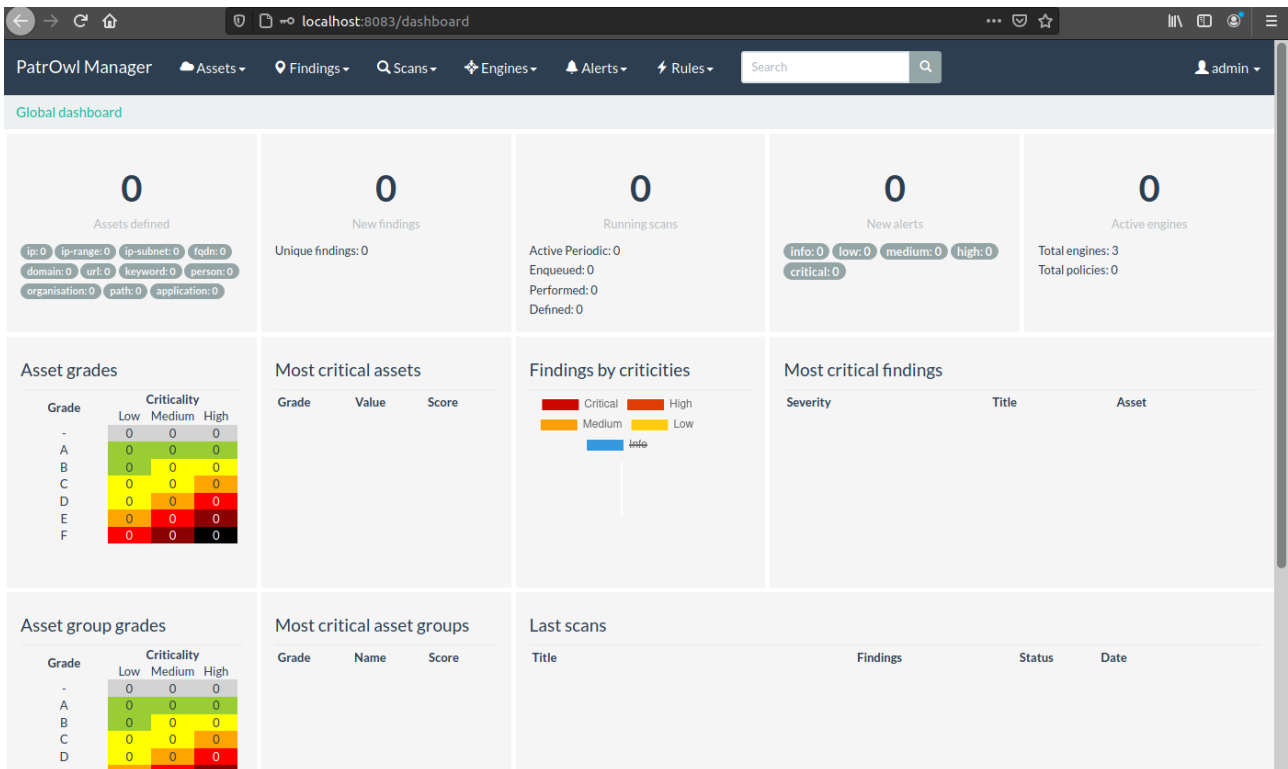
## **Kehitystyö**

PatrOwlin kehitystyö on aktiivista ja PatrowlManager, eli työkalun käyttörajapinta ja hallintatyökalu on käyttökelpoisessa kunnossa. PatrOwlEnginesin eli työkalun moottorit ovat vielä varsin keskeneräisiä ja Github-repositorion build on määritelty epäonnistuneeksi, mikä tarkoittaa julkaisun olevan epäkypsä käytettäväksi. Asennus ei onnistu ilman vakavia virheilmoituksia. (GitHub – Patrowl/PatrowlEngines 2020.; GitHub – Patrowl/PatrowlManager 2020.)

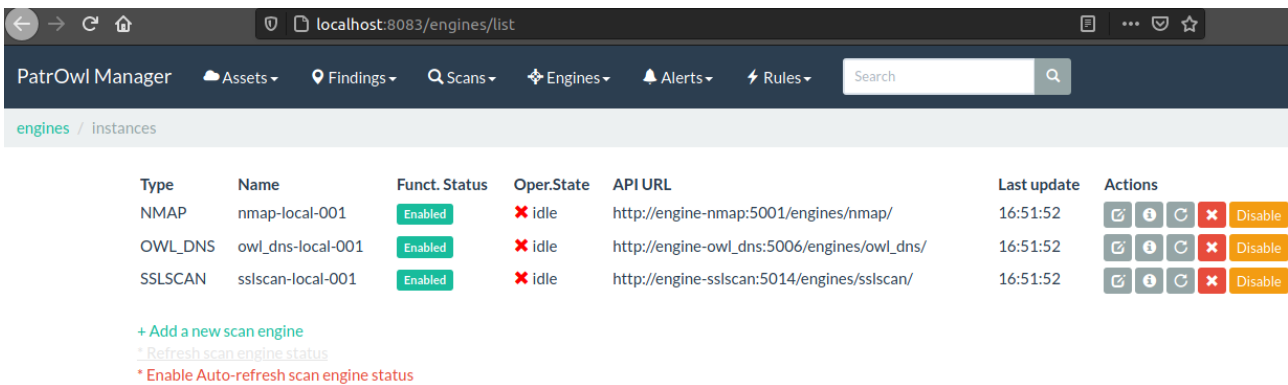
### **4.3.1 Asennus**

PatrOwlin yhteisöversion asentamiseen laaditut asennusohjeet löytyvät PatrOwlin dokumentaatiota varten luodusta Github-repositoriosta. (PatrowlDocs/installation-guide.md 2020.) Suositeltu asennustapa on Dockerin ja Docker Comosen kautta. Dockerin asennukselle on omat ohjeensa. (Install Docker Compose n.d.; Install Docker Engine n.d.) Dockerin asennus onnistui ilman ongelmia. Dockerin asennuksen syötteen on dokumentoitu liitteeseen 1.

PatrOwlManagerin asennuksessa on mahdollista suorittaa skripti (docker-compose.with-engines.yml), joka asentaa valmiiksi konfiguroidut moottorit. (PatrowlDocs/installation-guide.md 2020.) Skriptin suorittamalla PatrOwl asentaa 3 moottoria, joiden asennuksessa ei tule ongelmia vastaan. Kyseiset moottorit ovat NMAP, OWL\_DNS sekä SSLSCAN. Tämän tyyppisen asennuksen jälkeen PatrOwlManager näyttää kuvion 21 kaltaiselta ja sisältää kuviossa 22 näkyvät ennalta konfiguroidut moottorit. PatrOwlManagerin asennuksessa ei ilmene ongelmia. PatrOwlManagerin asennukseen



Kuvio 21. PatrOwl päänäkymä asennuksen jälkeen



Kuvio 22. PatrOwl ennakkoon konfiguroidut moottorit

Ennakkoon konfiguroitujen moottoreiden asennus on kuitenkin toissijaista, koska pääasiallisena tavoitteena olisi saada kaikki ilmaiseksi saatavilla olevat moottorit asennettua. Ensisijainen asennusohje sisältää erillisen osion PatrOwlEnginesin asennukseen, jota seuraamalla kaikki moottorit ensin rakennetaan (build-docker-engines.sh) ja sitten suoritetaan (start-docker-engines.sh). (PatrowlDocs/installation-guide.md 2020.) Rakennusvaiheessa kuitenkin ilmeni ongelmia, sillä kahden moottorin asennus epäonnistui virheilmoituksiin. Kyseiset moottorit ovat



patrowl-censys (virheilmoitus kuviossa 23) ja patrowl-owl\_code (virheilmoitus kuviossa 24). Molempien moottoreiden kohdalla asennus päättyi virheilmoituksen kohdalla.

```
ERROR: unable to select packages:
python (no such package):
  required by: world[python]
python-dev (no such package):
  required by: world[python-dev]
The command '/bin/sh -c apk add --update linux-headers build-base libffi-dev openssl-dev python python-dev py3-pip && rm -rf /var/cache/apk/*' returned a non-zero code: 2
```

Kuvio 23. PatrOwl-Censys asennuksen virheilmoitus

```
--2021-05-12 12:11:52-- https://dl.bintray.com/jeremy-long/owasp/dependency-check-6.0.3-release.zip
Resolving dl.bintray.com (dl.bintray.com)... 3.66.199.110, 18.193.131.58
Connecting to dl.bintray.com (dl.bintray.com)|3.66.199.110|:443... connected.
HTTP request sent, awaiting response... 403 Forbidden
2021-05-12 12:11:52 ERROR 403: Forbidden.
```

Kuvio 24. PatrOwl-owl\_code asennuksen virheilmoitus

## 4.4 CimSweep

CimSweep on kokoelma työkaluja tietoturvatapahtumiin vastaamiseen liittyviin operaatioihin etänä kaikille Windows versioille. Ydintoimintoina se kykenee etäisesti hankkimaan tiedot Windows-käyttöjärjestelmän: rekisteristä, tiedostoista, tapahtumalokeista, palveluista ja prosesseista. (GitHub – PowerShellMafia/CimSweep 2017.)

CimSweepin viimeisin versio (0.6.1.1) julkaistiin kesäkuun 8. 2017. Projekti on vanhentunut ja kehitystyö lopetettu. Käyttöä ei voi suositella, eikä työkaluun tästä syystä keskitytä tarkemmin. (GitHub – PowerShellMafia/CimSweep 2017.)

## 4.5 GRR Rapid Response

Googlen kehittämä GRR Rapid Response on etänä tietoturvatapahtumiin vastaamiseen reaaliaikaisella forensiikalla keskittyvä viitekehys. Tavoite on tukea forensiikkaa sekä tutkimuksia nopealla, skaalattavalla tavalla mahdollistaakseen analyttikoiden nopean hyökkäysten luokittelun ja analyysin suorittamisen etänä. GRR:n avulla analyttikoiden on mahdollista tehokkaasti kerätä ja prosessoida dataa suureltakin määrältä päätteitä. Työkalu erottuu edukseen kilpailijoistaan siten,

että se on täysin avoin, eikä GRR:stä ole saatavilla erillisiä maksullisia julkaisuversioita. (What is GRR? – GRR documentation n.d)

## Rakenne

GRR koostuu kahdesta Pythonilla tehdystä osasta: päätteestä (client) sekä serveristä.

GRR-pääte (client) asennetaan järjestelmille jotka mahdollisesti halutaan tutkia. Jokaisella vastaavalla järjestelmällä GRR-pääte tietyin väliajoin lähettää kyselyn GRR serverille mahdollisista tehtävistä. Tehtävillä tarkoitetaan jonkin tietyn toiminnon suorittamista: tiedoston tai rekisteritiedon lataamista, hakemiston listaamista, muistin analyysia, komponenttien monitorointia ja niin edelleen. (What is GRR? – GRR documentation n.d)

GRR-serverin infrastruktuuri koostuu useista komponenteista (etupäätteistä, workereista, käyttöliittymäservereistä) ja toimittaa verkkopohjaisia graafisia käyttöliittymiä sekä -rajapintoja, jotka mahdollistavat analyttikoiden asettaa ajastettuja tehtäviä päätteille, sekä nähdä ja prosessoida kerättyä dataa. (What is GRR? – GRR documentation n.d)

### 4.5.1 Asennus

GRR Rapid Responseen asennusohjeet löytyvät dokumentaationsivulta. Asennustapoja on useampia, mutta tässä tapauksessa niistä valittiin suositeltu vaihtoehto, eli "release deb" -julkaisu. Ohjeessa kerrotaan GRR serverin olevan rakennettu Ubuntu 18.04 Bionic Beaveria varten, joten ohjetta mukailleen kyseinen käyttöjärjestelmä valittiin käyttöön tätä varten. (Installing from a release server deb (recommended) n.d.)

Ohjetta seuraamalla asennus ei onnistunut. Asennuksen aikana ilmeni ongelma joka pysäytti asennusprosessin kokonaan, eikä asennusta voinut jatkaa. Virheilmoitus on nähtävissä kuvioista 25 sekä koko syöteketju liitteestä 5.

```

Could not find platform independent libraries <prefix>
Could not find platform dependent libraries <exec_prefix>
Consider setting $PYTHONHOME to <prefix>[:<exec_prefix>]
Fatal Python error: Py_Initialize: Unable to get the locale encoding
ModuleNotFoundError: No module named 'encodings'

Current thread 0x00007f32dc4d4740 (most recent call first):
/usr/bin/grr_config_updater: line 34: 4806 Aborted                (core dumped) "${GRR_PREFIX}/bin/${NAME}" "${GRR_EXTRA_ARGS[@]}" "${@}"
dpkg: error processing package grr-server (--configure):
 installed grr-server package post-installation script subprocess returned error exit status 134
Processing triggers for libc-bin (2.33-0ubuntu5) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for install-info (6.7.0.dfsg.2-6) ...
Errors were encountered while processing:
 grr-server
E: Download is performed unsandboxed as root as file '/home/z/grr-server_3.4.2-4_amd64.deb' couldn't be accessed by user '_apt'. - pkgAcquire::Run (13: Permission denied)
E: Sub-process /usr/bin/dpkg returned an error code (1)

```

Kuvio 25. GRR Rapid Responsen asennuksen virheilmoitus

## 4.5.2 Toinen asennus

GRR:n ollen Googlen kehittämä, usko sovelluksen tulevaisuudesta ja toimivuudesta on vahva. Asennusta yritettiin siis uudelleen myöhemmin, kun GRR:stä oli julkaistu uusia versioita. Tällä kerralla asennus onnistui osittain seuraamalla ohjeita samasta lähteestä kuin ensimmäiselläkin kerralla. Asennuksen jälkeen GRR server ei havainnut clientia, vaikka clientin asennus onnistui ongelmitta, ilman minkäänlaisia virheitä. (Kuviot 26 ja 27) GRR toisen asennuksen syötteen nähtävissä liitteestä 7.



Kuvio 26. GRR client asennus

<input type="checkbox"/>	Online	Subject	Host	OS Version	MAC	Usernames	First Seen	Client version	Labels	Last Checkin	OS Install Date

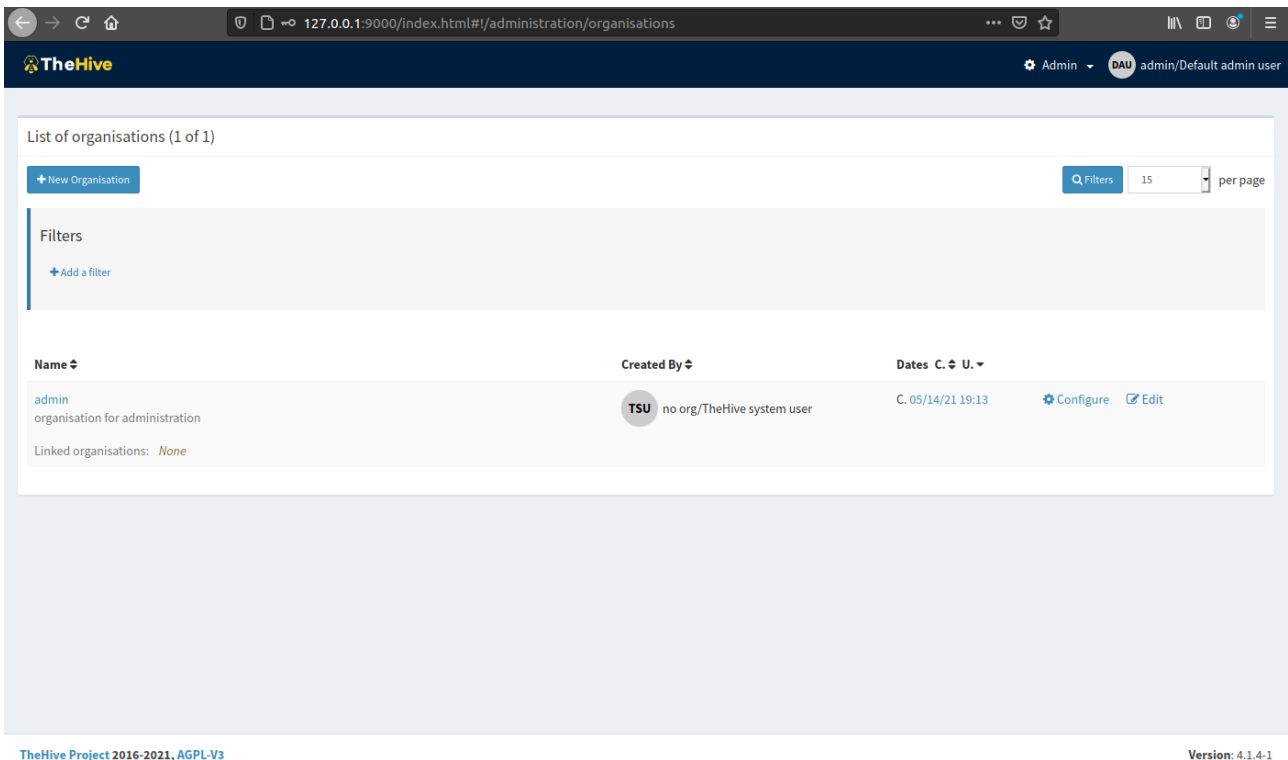
Kuvio 27. GRR client-lista tyhjä onnistuneesta asennuksesta huolimatta

## 4.6 TheHive

TheHive projekti on ilmainen, skaalattava sekä avoimella lähdekoodilla tuotettu turvallisuustapahtumiin vastaamisen alusta. Se on tiiviisti integroitu MISP:iin. (Malware Information Sharing Platform) ja on suunniteltu helpottamaan tietoturva harjoittavien elämää käsittelemällä turvallisuustapahtumia nopeasti. (TheHive Project n.d.)

### 4.6.1 Asennus

Asennusohjeita seuraamalla asennus onnistui ongelmitta. (Installation Guide on Debian-based OS 2021.) Tietojentallennukseen liittyvistä valinnoista tälle asennukselle valikoitui suositeltu Cassandra-tietokanta, sekä valinta koskien TheHiveen lähetettyjä tietoja: tiedot talletetaan paikalliseen tietokantaan. Suoraan asennuksen jälkeen TheHiven päänäkyvä näyttää kuvion 28 kaltaiselta.



Kuvio 28. TheHive perusnäkyä asennuksen jälkeen

## 4.7 MIG

MIG (Mozilla InvestiGator) on Mozillan kehittämä digitaalisen forensiikan ja tutkimuksen alusta. Se koostuu agenteista, jotka asennetaan kaikille infrastruktuurin järjestelmille joiden tietojärjestelmiä, verkon tilaa, muistia tai päätteiden konfiguraatiota halutaan tarkkailla reaaliajassa. Kyvykkyydeltään MIG on parhaimmillaan Linuxilla, jolla se pystyy tiedostojen, verkon sekä muistin tarkastamiseen ja haavoittuvuuksien hallintaan. (Kuvio 29) (MIG: Mozilla InvestiGator n.d.)

Capability	Linux	MacOS	Windows
file inspection	✓	✓	✓
network inspection	✓	✓	(partial)
memory inspection	✓	✓	✓
vuln management	✓	(planned)	(planned)
system auditing	(planned)	(planned)	(planned)

Kuvio 29. MIG kyvykkydet

Alustan kehitystyö on lopetettu, eikä Mozilla siten enää ylläpidä projektia. Viimeisimmäksi jäänyt päivitys projektin Github-repositorioon tehtiin 14. syyskuuta 2019. Repositorio on sittemmin asetettu vain-luku tilaan. (GitHub – Mozilla/mig 2019.)

#### 4.8 Johtopäätökset

Tutkimustulosten pohjalta on todettavissa, miten SOAR teknologia on varsin tuore ilmiö, ja siten saatavilla olevat tuotteet ovat enemmän tai vähemmän raakileita. SOC-työkaluiksi käyttökelpoisia toteutuksia ei ole vielä tässä vaiheessa saatavilla, ainakaan ilmaiseksi. Näin ollen, tällä hetkellä toimeksiantajalle ei voi suositella SOAR-työkaluja käytettäväksi ainakaan vielä tällä ajankohdalla. Aktiivisen kehitystyön ansiosta tilanne tulee varmasti muuttumaan parempaan lähivuosien aikana. On mahdollista että jo parin tai muutaman vuoden sisällä osa työkaluista on saavuttanut täyden julkaisun, joiden toimivuus on jo riittävän varmaa.

## 5 Pohdinta

Tutkimuksen lähtökohdat huomioiden on pettymys, etteivät SOAR-työkalut olleet riittävän kypsiä tai toimintakelpoisia SOC-työkaluiksi. Olisi ollut toivottavaa saada edes yksi kelvollinen tulos toimeksiantajalle, jota olisi voinut kyseiseen käyttötarkoitukseen hyödyntää. Tämän tutkimuksen aikana tutkitut avoimen lähdekoodin ilmaiset SOAR-julkaisut eivät olleet riittävän kypsiä tai toimintakelpoisia täyttämään SOARin määrittelemät vaatimukset ja edistyksen tietoturvallisuuden liittyvien alhaisen tason operaatioiden automaatiassa.

Aihe vaatii tulevaisuudessa lisätutkimusta teknologioiden kehittyessä ja valikoiman kasvaessa. Tietoturvaoperaatioiden automatisointi on varmasti tulevaisuudessa yhä enemmän ja enemmän läsnä, ja siten siitä tullaan varmasti saamaan enemmän kilpailevia ryhmiä ja yrityksiä, joilla kullakin on omat versionsa. Käytön yleistyessä myös käyttöön ja käyttökokemuksiin liittyvää dataa tullaan saamaan paljon enemmän ja SOAR tulee leviämään laajempaan tietouteen, mikä tulee helpottamaan vastaavia lisätutkimuksia tulevaisuudessa.

Tutkimus laadittiin ja suoritettiin noudattaen Jyväskylän ammattikorkeakoulun eettisiä periaatteita ja tietosuojaa.

## Lähteet

About the Ubuntu project | Ubuntu. N.d. Viitattu 1.12.2021. <https://ubuntu.com/about>.

Cortex XSOAR Community Edition FAQ. 2020. Tietoa ilmaisesta Cortex XSOARista. Viitattu 21.5.2021. [https://start.paloaltonetworks.com/rs/531-OCS-018/images/Cortex\\_XSOAR\\_Community\\_Edition\\_FAQ.pdf](https://start.paloaltonetworks.com/rs/531-OCS-018/images/Cortex_XSOAR_Community_Edition_FAQ.pdf).

Docker frequently asked questions (FAQ) | Docker documentation. N.d. Viitattu 6.12.2021. <https://docs.docker.com/engine/faq/>.

Early adopter Pricing. N.d. Shufflen hinnasto ja eri versioiden erot. Viitattu 30.11.2021. <https://shuffler.io/pricing>.

Empowering App Development for Developers | Docker. N.d. Dockerin kotisivu. Viitattu 6.12.2021. <https://www.docker.com>.

GitHub – mozilla/mig. 2019. Mozilla InvestiGatorin GitHub repositorio. Viitattu 14.4.2021. <https://github.com/mozilla/mig>.

GitHub – Patrowl/PatrowlEngines. 2020. PatrowlEnginesin GitHub repositorio. Viitattu 21.10.2020. <https://github.com/Patrowl/PatrowlEngines>.

GitHub – Patrowl/PatrowlManager. 2020. PatrowlManagerin Github repositorio. Viitattu 21.10.2020. <https://github.com/Patrowl/PatrowlManager>.

GitHub – PowerShellMafia/CimSweep. 2017. Viitattu 14.4.2021. <https://github.com/PowerShellMafia/CimSweep>.

Install Docker Compose. N.d. Docker Compose asennusohjeet Linuxille. Viitattu 22.11.2021. <https://docs.docker.com/compose/install/>.

Install Docker Engine on Ubuntu. N.d. Docker Enginen asennusohjeet Ubuntulle. Viitattu 22.11.2021. <https://docs.docker.com/engine/install/ubuntu/>.

Installation Guide on Debian-based OS. 2021. TheHive 4 asennusohjeet Debian-pohjaiselle järjestelmälle. Viitattu 12.2.2021. [https://github.com/TheHive-Project/TheHiveDocs/blob/master/TheHive4/Installation/Install\\_deb.md](https://github.com/TheHive-Project/TheHiveDocs/blob/master/TheHive4/Installation/Install_deb.md).

Installing from a release server deb (recommended). N.d. GRR serverin asennusohje. Viitattu 6.12.2021. <https://grr-doc.readthedocs.io/en/latest/installing-grr-server/from-release-deb.html>.

Installing GRR clients on Linux. N.d. GRR clientin asennusohje Linuxille. Viitattu 6.12.2021. <https://grr-doc.readthedocs.io/en/latest/deploying-grr-clients/on-linux.html>.

MIG: Mozilla InvestiGator. N.d. Viitattu 14.4.2021. <http://mozilla.github.io/mig/>.



- Ødegårdstuen, F. 2020a. Introducing Shuffle – an Open Source SOAR platform part 1. Shufflen esittelyartikkeli. Viitattu 14.4.2021. <https://medium.com/shuffle-automation/introducing-shuffle-an-open-source-soar-platform-part-1-58a529de7d12>.
- Ødegårdstuen, F. 2020b. Getting started with Shuffle – an Open Source SOAR platform part 2. Shufflen käyttönoton ohjeistusta. Viitattu 22.11.2021. <https://medium.com/shuffle-automation/getting-started-with-shuffle-an-open-source-soar-platform-part-2-1d7c67a64244>.
- Ødegårdstuen, F. 2020c. Integrating Shuffle with Virustotal and TheHive – Open Source SOAR part 3. Shufflen integraatio Virustotaliin ja TheHiveen ohjeistusta. <https://medium.com/shuffle-automation/integrating-shuffle-with-virustotal-and-thehive-open-source-soar-part-3-8e2e0d3396a9>.
- Ødegårdstuen, F. 2021. Shuffle Installation Guide. Shufflen asennusohjeet. Viitattu 22.11.2021. <https://github.com/frikky/shuffle/blob/master/.github/install-guide.md>.
- Ødegårdstuen, F. N.d. About Shuffle -dokumentaatio sivu Shufflestä. Viitattu 14.4.2021. <https://shuffler.io/docs/about>.
- Overview – JYVSECTEC. N.d. Viitattu 21.8.2021. <https://jyvsectec.fi/about/overview/>.
- Overview of Docker Compose. N.d. Yleiskatsaus Docker composeen. Viitattu 6.12.2021. <https://docs.docker.com/compose/>.
- Patrowl.io – Patrowl. N.d. Patrowlin kotisivu. Viitattu 21.10.2020. <https://patrowl.io/patrowl>.
- Patrowl.io – PatrowlManager. N.d. PatrowlManagerin kotisivu. Viitattu 21.10.2020. <https://patrowl.io/products/manager>.
- PatrowlDocs/installation-guide.md. 2020. Patrowlin asennusohjeet. Viitattu 21.10.2020. <https://github.com/Patrowl/PatrowlDocs/blob/master/installation/installation-guide.md>.
- Security Automation (SOAR) for Everyone – Palo Alto Networks. N.d. Cortex XSOARin verkkosivu. Viitattu 21.5.2021. <https://www.paloaltonetworks.com/cortex/cortex-xsoar>.
- Shea, S. 2021. What is SOAR (Security Orchestration, Automation and Response)? A definition from WhatIs.com. TechTarget SearchSecurity artikkeli. Viitattu 14.4.2021. <https://searchsecurity.techtarget.com/definition/SOAR>.
- TheHive Project. N.d. TheHive kotisivu. Viitattu 12.2.2021. <https://thehive-project.org>.
- VirtualBox User Manual – Chapter 1. N.d. Viitattu 30.11.2021. <https://www.virtualbox.org/manual/ch01.html>.
- What is GRR? – GRR documentation. N.d. GRR tietoa dokumentaatioissa. Viitattu 27.10.2021. <https://grr-doc.readthedocs.io/en/latest/what-is-grr.html>.

What is SOAR? Security definition | FireEye. N.d. Viitattu 21.8.2021.  
<https://www.fireeye.com/products/helix/what-is-soar.html>.

## Liitteet

Liitteiden sisältämät syötteet ovat varsin pitkiä ja mahdollisesti vaikealukuisia. Sen vuoksi syötteet on liitetty myös kätevästi avattavan tekstitiedoston muodossa.

### Liite 1. Docker ja Docker-compose asennus



Docker +  
Docker-compose ins

```

z@z:~$ sudo apt-get update
Hit:1 http://fi.archive.ubuntu.com/ubuntu hirsute InRelease
Hit:2 http://fi.archive.ubuntu.com/ubuntu hirsute-updates InRelease
Hit:3 http://fi.archive.ubuntu.com/ubuntu hirsute-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu hirsute-security InRelease
Reading package lists... Done
z@z:~$ sudo apt-get install \
  apt-transport-https \
  ca-certificates \
  curl \
  gnupg \
  lsb-release -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ca-certificates is already the newest version (20210119build1).
ca-certificates set to manually installed.
gnupg is already the newest version (2.2.20-1ubuntu3).
gnupg set to manually installed.
lsb-release is already the newest version (11.1.0ubuntu2).
lsb-release set to manually installed.
The following NEW packages will be installed:
  apt-transport-https curl
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 172 kB of archives.
After this operation, 596 kB of additional disk space will be used.
Get:1 http://fi.archive.ubuntu.com/ubuntu hirsute/universe amd64 apt-transport-https all 2.2.3
[1 704 B]
Get:2 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 curl amd64 7.74.0-1ubuntu2 [170
kB]
Fetched 172 kB in 0s (969 kB/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 127257 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_2.2.3_all.deb ...

```

```

Unpacking apt-transport-https (2.2.3) ...
Selecting previously unselected package curl.
Preparing to unpack .../curl_7.74.0-1ubuntu2_amd64.deb ...
Unpacking curl (7.74.0-1ubuntu2) ...
Setting up apt-transport-https (2.2.3) ...
Setting up curl (7.74.0-1ubuntu2) ...
Processing triggers for man-db (2.9.4-2) ...
z@z:~$ curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o
/usr/share/keyrings/docker-archive-keyring.gpg
z@z:~$ echo \
"deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://down-
load.docker.com/linux/ubuntu \
$(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
z@z:~$ sudo apt-get update
Hit:1 http://fi.archive.ubuntu.com/ubuntu hirsute InRelease
Hit:2 http://fi.archive.ubuntu.com/ubuntu hirsute-updates InRelease
Hit:3 http://fi.archive.ubuntu.com/ubuntu hirsute-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu hirsute-security InRelease
Get:5 https://download.docker.com/linux/ubuntu hirsute InRelease [28,3 kB]
Get:6 https://download.docker.com/linux/ubuntu hirsute/stable amd64 Packages [2 406 B]
Fetched 30,7 kB in 1s (40,7 kB/s)
Reading package lists... Done
z@z:~$ sudo apt-get install docker-ce docker-ce-cli containerd.io -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  docker-ce-rootless-extras docker-scan-plugin git git-man liberror-perl libslirp0 pigz slirp4netns
Suggested packages:
  aufs-tools cgroupfs-mount | cgroup-lite git-daemon-run | git-daemon-sysvinit git-doc git-el git-
email git-gui gitk gitweb git-cvs git-mediawiki
  git-svn
The following NEW packages will be installed:
  containerd.io docker-ce docker-ce-cli docker-ce-rootless-extras docker-scan-plugin git git-man
liberror-perl libslirp0 pigz slirp4netns
0 upgraded, 11 newly installed, 0 to remove and 0 not upgraded.
Need to get 112 MB of archives.
After this operation, 496 MB of additional disk space will be used.
Get:1 http://fi.archive.ubuntu.com/ubuntu hirsute/universe amd64 pigz amd64 2.6-1 [63,6 kB]
Get:2 https://download.docker.com/linux/ubuntu hirsute/stable amd64 containerd.io amd64
1.4.4-1 [28,3 MB]
Get:3 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 liberror-perl all 0.17029-1 [26,5
kB]
Get:4 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 git-man all 1:2.30.2-1ubuntu1
[931 kB]
Get:5 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 git amd64 1:2.30.2-1ubuntu1
[3 457 kB]
Get:6 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 libslirp0 amd64 4.4.0-1 [55,9 kB]

```

```
Get:7 http://fi.archive.ubuntu.com/ubuntu hirsute/universe amd64 slirp4netns amd64 1.0.1-1
[33,1 kB]
Get:8 https://download.docker.com/linux/ubuntu hirsute/stable amd64 docker-ce-cli amd64
5:20.10.6~3-0~ubuntu-hirsute [41,4 MB]
Get:9 https://download.docker.com/linux/ubuntu hirsute/stable amd64 docker-ce amd64
5:20.10.6~3-0~ubuntu-hirsute [24,8 MB]
Get:10 https://download.docker.com/linux/ubuntu hirsute/stable amd64 docker-ce-rootless-ex-
tras amd64 5:20.10.6~3-0~ubuntu-hirsute [9 061 kB]
Get:11 https://download.docker.com/linux/ubuntu hirsute/stable amd64 docker-scan-plugin
amd64 0.7.0~ubuntu-hirsute [3 885 kB]
Fetched 112 MB in 10s (11,2 MB/s)
Selecting previously unselected package pigz.
(Reading database ... 127268 files and directories currently installed.)
Preparing to unpack .../00-pigz_2.6-1_amd64.deb ...
Unpacking pigz (2.6-1) ...
Selecting previously unselected package containerd.io.
Preparing to unpack .../01-containerd.io_1.4.4-1_amd64.deb ...
Unpacking containerd.io (1.4.4-1) ...
Selecting previously unselected package docker-ce-cli.
Preparing to unpack .../02-docker-ce-cli_5%3a20.10.6~3-0~ubuntu-hirsute_amd64.deb ...
Unpacking docker-ce-cli (5:20.10.6~3-0~ubuntu-hirsute) ...
Selecting previously unselected package docker-ce.
Preparing to unpack .../03-docker-ce_5%3a20.10.6~3-0~ubuntu-hirsute_amd64.deb ...
Unpacking docker-ce (5:20.10.6~3-0~ubuntu-hirsute) ...
Selecting previously unselected package docker-ce-rootless-extras.
Preparing to unpack .../04-docker-ce-rootless-extras_5%3a20.10.6~3-0~ubuntu-hir-
sute_amd64.deb ...
Unpacking docker-ce-rootless-extras (5:20.10.6~3-0~ubuntu-hirsute) ...
Selecting previously unselected package docker-scan-plugin.
Preparing to unpack .../05-docker-scan-plugin_0.7.0~ubuntu-hirsute_amd64.deb ...
Unpacking docker-scan-plugin (0.7.0~ubuntu-hirsute) ...
Selecting previously unselected package liberror-perl.
Preparing to unpack .../06-liberror-perl_0.17029-1_all.deb ...
Unpacking liberror-perl (0.17029-1) ...
Selecting previously unselected package git-man.
Preparing to unpack .../07-git-man_1%3a2.30.2-1ubuntu1_all.deb ...
Unpacking git-man (1:2.30.2-1ubuntu1) ...
Selecting previously unselected package git.
Preparing to unpack .../08-git_1%3a2.30.2-1ubuntu1_amd64.deb ...
Unpacking git (1:2.30.2-1ubuntu1) ...
Selecting previously unselected package libslirp0:amd64.
Preparing to unpack .../09-libslirp0_4.4.0-1_amd64.deb ...
Unpacking libslirp0:amd64 (4.4.0-1) ...
Selecting previously unselected package slirp4netns.
Preparing to unpack .../10-slirp4netns_1.0.1-1_amd64.deb ...
Unpacking slirp4netns (1.0.1-1) ...
Setting up docker-scan-plugin (0.7.0~ubuntu-hirsute) ...
Setting up liberror-perl (0.17029-1) ...
Setting up containerd.io (1.4.4-1) ...
```

```

Created symlink /etc/systemd/system/multi-user.target.wants/containerd.service → /lib/systemd/system/containerd.service.
Setting up docker-ce-cli (5:20.10.6~3-0~ubuntu-hirsute) ...
Setting up libslirp0:amd64 (4.4.0-1) ...
Setting up pigz (2.6-1) ...
Setting up git-man (1:2.30.2-1ubuntu1) ...
Setting up docker-ce-rootless-extras (5:20.10.6~3-0~ubuntu-hirsute) ...
Setting up slirp4netns (1.0.1-1) ...
Setting up docker-ce (5:20.10.6~3-0~ubuntu-hirsute) ...
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service → /lib/systemd/system/docker.service.
Created symlink /etc/systemd/system/sockets.target.wants/docker.socket → /lib/systemd/system/docker.socket.
Setting up git (1:2.30.2-1ubuntu1) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for libc-bin (2.33-0ubuntu5) ...
z@z:~$ sudo usermod -aG docker $USER
z@z:~$ sudo curl -L "https://github.com/docker/compose/releases/download/1.29.1/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose
% Total    % Received % Xferd Average Speed   Time    Time     Time  Current
           Dload  Upload  Total   Spent    Left     Speed
100 633    100 633    0    0 3014    0 --:--:-- --:--:-- --:--:-- 3014
100 12.1M 100 12.1M    0    0 7447k    0 0:00:01 0:00:01 --:--:-- 10.6M
z@z:~$ sudo chmod +x /usr/local/bin/docker-compose

```

## Liite 2. PatrOwlManager asennus ennakkoon konfiguroitujen moottoreiden kanssa



PatrOwl.txt

```

z@z:~$ git clone https://github.com/Patrowl/PatrowlManager.git
Cloning into 'PatrowlManager'...
remote: Enumerating objects: 4292, done.
remote: Counting objects: 100% (110/110), done.
remote: Compressing objects: 100% (76/76), done.
remote: Total 4292 (delta 55), reused 51 (delta 32), pack-reused 4182
Receiving objects: 100% (4292/4292), 2.15 MiB | 3.34 MiB/s, done.
Resolving deltas: 100% (3149/3149), done.
z@z:~$ cd PatrowlManager
z@z:~/PatrowlManager$
z@z:~/PatrowlManager$ docker-compose build --force-rm
rabbitmq uses an image, skipping
db uses an image, skipping
nginx uses an image, skipping
Building web
Sending build context to Docker daemon 7.223MB
Step 1/14 : FROM python:3.7-slim
3.7-slim: Pulling from library/python
f7ec5a41d630: Pull complete
6f318b7b4c32: Pull complete
af3fa3eb7bae: Pull complete
4e08e182f49d: Pull complete
16277d8ed69c: Pull complete
Digest: sha256:5375725c3c0a0215279c1c5ddb33f91d31f0eb37010140397e5c7e5530073d2c
Status: Downloaded newer image for python:3.7-slim
---> e7d86653f62f
Step 2/14 : MAINTAINER Patrowl.io "getsupport@patrowl.io"
---> Running in 27821344f0b3
Removing intermediate container 27821344f0b3
---> e6511a1ea884
Step 3/14 : LABEL Name="PatrowlManager" Version="1.6.15"
---> Running in 8294d80ec6f1
Removing intermediate container 8294d80ec6f1
---> edc2eb3a2211
Step 4/14 : ENV PYTHONUNBUFFERED 1
---> Running in f6c00b9ee82c
Removing intermediate container f6c00b9ee82c
---> 9a167747bef7
Step 5/14 : RUN mkdir -p /opt/patrowl-manager/
---> Running in 54f308d0f8ea
Removing intermediate container 54f308d0f8ea

```

```

---> 836d8aee8d0e
Step 6/14 : WORKDIR /opt/patrowl-manager/
---> Running in fc316104884e
Removing intermediate container fc316104884e
---> a9e1a3ca6dba
Step 7/14 : RUN apt-get update -yq      && apt-get install -yq --no-install-recommends apt-utils
python3 python3-pip libmagic-dev python3-dev gcc  && apt-get purge -y --auto-remove -o
APT::AutoRemove::RecommendsImportant=false      && rm -rf /var/lib/apt/lists/* /tmp/*
/var/tmp/*
---> Running in 970d197c1ab5
Get:1 http://security.debian.org/debian-security buster/updates InRelease [65.4 kB]
Get:2 http://deb.debian.org/debian buster InRelease [121 kB]
Get:3 http://deb.debian.org/debian buster-updates InRelease [51.9 kB]
Get:4 http://security.debian.org/debian-security buster/updates/main amd64 Packages [285 kB]
Get:5 http://deb.debian.org/debian buster/main amd64 Packages [7907 kB]
Get:6 http://deb.debian.org/debian buster-updates/main amd64 Packages [10.9 kB]
Fetched 8441 kB in 3s (3297 kB/s)
Reading package lists...
Reading package lists...
Building dependency tree...
Reading state information...
The following additional packages will be installed:
 apt binutils binutils-common binutils-x86-64-linux-gnu cpp cpp-8 dh-python
 gcc-8 libapt-inst2.0 libasan5 libatomic1 libbinutils libc-dev-bin libc6-dev
 libcc1-0 libexpat1-dev libgcc-8-dev libgomp1 libisl19 libitm1 liblsan0
 libmagic-mgc libmagic1 libmpc3 libmpdec2 libmpfr6 libmpx2 libpython3-dev
 libpython3-stdlib libpython3.7 libpython3.7-dev libpython3.7-minimal
 libpython3.7-stdlib libquadmath0 libtsan0 libubsan1 linux-libc-dev
 mime-support python-pip-whl python3-distutils python3-lib2to3
 python3-minimal python3.7 python3.7-dev python3.7-minimal
Suggested packages:
 apt-doc aptitude | synaptic | wajig dpkg-dev gnupg | gnupg2 | gnupg1
 powermgmt-base binutils-doc cpp-doc gcc-8-locales libdpkg-perl gcc-multilib
 make manpages-dev autoconf automake libtool flex bison gdb gcc-doc
 gcc-8-multilib gcc-8-doc libgcc1-dbg libgomp1-dbg libitm1-dbg libatomic1-dbg
 libasan5-dbg liblsan0-dbg libtsan0-dbg libubsan1-dbg libmpx2-dbg
 libquadmath0-dbg glibc-doc file python3-doc python3-tk python3-venv
 python3.7-venv python3.7-doc binfmt-support
Recommended packages:
 manpages manpages-dev bzip2 file xz-utils build-essential python3-setuptools
 python3-wheel
The following NEW packages will be installed:
 apt-utils binutils binutils-common binutils-x86-64-linux-gnu cpp cpp-8
 dh-python gcc gcc-8 libapt-inst2.0 libasan5 libatomic1 libbinutils
 libc-dev-bin libc6-dev libcc1-0 libexpat1-dev libgcc-8-dev libgomp1 libisl19
 libitm1 liblsan0 libmagic-dev libmagic-mgc libmagic1 libmpc3 libmpdec2
 libmpfr6 libmpx2 libpython3-dev libpython3-stdlib libpython3.7
 libpython3.7-dev libpython3.7-minimal libpython3.7-stdlib libquadmath0
 libtsan0 libubsan1 linux-libc-dev mime-support python-pip-whl python3

```



python3-dev python3-distutils python3-lib2to3 python3-minimal python3-pip  
python3.7 python3.7-dev python3.7-minimal

The following packages will be upgraded:

apt

1 upgraded, 50 newly installed, 0 to remove and 1 not upgraded.

Need to get 92.0 MB of archives.

After this operation, 256 MB of additional disk space will be used.

Get:1 <http://deb.debian.org/debian> buster-updates/main amd64 apt amd64 1.8.2.3 [1418 kB]

Get:2 <http://deb.debian.org/debian> buster/main amd64 libpython3.7-minimal amd64 3.7.3-2+deb10u3 [589 kB]

Get:3 <http://deb.debian.org/debian> buster/main amd64 python3.7-minimal amd64 3.7.3-2+deb10u3 [1737 kB]

Get:4 <http://deb.debian.org/debian> buster/main amd64 python3-minimal amd64 3.7.3-1 [36.6 kB]

Get:5 <http://deb.debian.org/debian> buster/main amd64 mime-support all 3.62 [37.2 kB]

Get:6 <http://deb.debian.org/debian> buster/main amd64 libmpdec2 amd64 2.4.2-2 [87.2 kB]

Get:7 <http://deb.debian.org/debian> buster/main amd64 libpython3.7-stdlib amd64 3.7.3-2+deb10u3 [1734 kB]

Get:8 <http://deb.debian.org/debian> buster/main amd64 python3.7 amd64 3.7.3-2+deb10u3 [330 kB]

Get:9 <http://deb.debian.org/debian> buster/main amd64 libpython3-stdlib amd64 3.7.3-1 [20.0 kB]

Get:10 <http://deb.debian.org/debian> buster/main amd64 python3 amd64 3.7.3-1 [61.5 kB]

Get:11 <http://deb.debian.org/debian> buster-updates/main amd64 libapt-inst2.0 amd64 1.8.2.3 [204 kB]

Get:12 <http://deb.debian.org/debian> buster-updates/main amd64 apt-utils amd64 1.8.2.3 [421 kB]

Get:13 <http://deb.debian.org/debian> buster/main amd64 binutils-common amd64 2.31.1-16 [2073 kB]

Get:14 <http://deb.debian.org/debian> buster/main amd64 libbinutils amd64 2.31.1-16 [478 kB]

Get:15 <http://deb.debian.org/debian> buster/main amd64 binutils-x86-64-linux-gnu amd64 2.31.1-16 [1823 kB]

Get:16 <http://deb.debian.org/debian> buster/main amd64 binutils amd64 2.31.1-16 [56.8 kB]

Get:17 <http://deb.debian.org/debian> buster/main amd64 libisl19 amd64 0.20-2 [587 kB]

Get:18 <http://deb.debian.org/debian> buster/main amd64 libmpfr6 amd64 4.0.2-1 [775 kB]

Get:19 <http://deb.debian.org/debian> buster/main amd64 libmpc3 amd64 1.1.0-1 [41.3 kB]

Get:20 <http://deb.debian.org/debian> buster/main amd64 cpp-8 amd64 8.3.0-6 [8914 kB]

Get:21 <http://deb.debian.org/debian> buster/main amd64 cpp amd64 4:8.3.0-1 [19.4 kB]

Get:22 <http://deb.debian.org/debian> buster/main amd64 python3-lib2to3 all 3.7.3-1 [76.7 kB]

Get:23 <http://deb.debian.org/debian> buster/main amd64 python3-distutils all 3.7.3-1 [142 kB]

Get:24 <http://deb.debian.org/debian> buster/main amd64 dh-python all 3.20190308 [99.3 kB]

Get:25 <http://deb.debian.org/debian> buster/main amd64 libcc1-0 amd64 8.3.0-6 [46.6 kB]

Get:26 <http://deb.debian.org/debian> buster/main amd64 libgomp1 amd64 8.3.0-6 [75.8 kB]

Get:27 <http://deb.debian.org/debian> buster/main amd64 libitm1 amd64 8.3.0-6 [27.7 kB]

Get:28 <http://deb.debian.org/debian> buster/main amd64 libatomic1 amd64 8.3.0-6 [9032 B]

Get:29 <http://deb.debian.org/debian> buster/main amd64 libasan5 amd64 8.3.0-6 [362 kB]

Get:30 <http://deb.debian.org/debian> buster/main amd64 liblsan0 amd64 8.3.0-6 [131 kB]

Get:31 <http://deb.debian.org/debian> buster/main amd64 libtsan0 amd64 8.3.0-6 [283 kB]

Get:32 <http://deb.debian.org/debian> buster/main amd64 libubsan1 amd64 8.3.0-6 [120 kB]

Get:33 <http://deb.debian.org/debian> buster/main amd64 libmpx2 amd64 8.3.0-6 [11.4 kB]

Get:34 <http://deb.debian.org/debian> buster/main amd64 libquadmath0 amd64 8.3.0-6 [133 kB]

Get:35 http://deb.debian.org/debian buster/main amd64 libgcc-8-dev amd64 8.3.0-6 [2298 kB]  
Get:36 http://deb.debian.org/debian buster/main amd64 gcc-8 amd64 8.3.0-6 [9452 kB]  
Get:37 http://deb.debian.org/debian buster/main amd64 gcc amd64 4:8.3.0-1 [5196 B]  
Get:38 http://deb.debian.org/debian buster/main amd64 libc-dev-bin amd64 2.28-10 [275 kB]  
Get:39 http://deb.debian.org/debian buster/main amd64 linux-libc-dev amd64 4.19.181-1 [1441 kB]  
Get:40 http://deb.debian.org/debian buster/main amd64 libc6-dev amd64 2.28-10 [2691 kB]  
Get:41 http://deb.debian.org/debian buster/main amd64 libexpat1-dev amd64 2.2.6-2+deb10u1 [153 kB]  
Get:42 http://deb.debian.org/debian buster/main amd64 libmagic-mgc amd64 1:5.35-4+deb10u2 [242 kB]  
Get:43 http://deb.debian.org/debian buster/main amd64 libmagic1 amd64 1:5.35-4+deb10u2 [118 kB]  
Get:44 http://deb.debian.org/debian buster/main amd64 libmagic-dev amd64 1:5.35-4+deb10u2 [130 kB]  
Get:45 http://deb.debian.org/debian buster/main amd64 libpython3.7 amd64 3.7.3-2+deb10u3 [1498 kB]  
Get:46 http://deb.debian.org/debian buster/main amd64 libpython3.7-dev amd64 3.7.3-2+deb10u3 [48.4 MB]  
Get:47 http://deb.debian.org/debian buster/main amd64 libpython3-dev amd64 3.7.3-1 [20.1 kB]  
Get:48 http://deb.debian.org/debian buster/main amd64 python-pip-whl all 18.1-5 [1591 kB]  
Get:49 http://deb.debian.org/debian buster/main amd64 python3.7-dev amd64 3.7.3-2+deb10u3 [510 kB]  
Get:50 http://deb.debian.org/debian buster/main amd64 python3-dev amd64 3.7.3-1 [1264 B]  
Get:51 http://deb.debian.org/debian buster/main amd64 python3-pip all 18.1-5 [171 kB]  
debconf: delaying package configuration, since apt-utils is not installed  
Fetched 92.0 MB in 9s (10.3 MB/s)  
(Reading database ... 6840 files and directories currently installed.)  
Preparing to unpack .../archives/apt\_1.8.2.3\_amd64.deb ...  
Unpacking apt (1.8.2.3) over (1.8.2.2) ...  
Setting up apt (1.8.2.3) ...  
Selecting previously unselected package libpython3.7-minimal:amd64.  
(Reading database ... 6840 files and directories currently installed.)  
Preparing to unpack .../libpython3.7-minimal\_3.7.3-2+deb10u3\_amd64.deb ...  
Unpacking libpython3.7-minimal:amd64 (3.7.3-2+deb10u3) ...  
Selecting previously unselected package python3.7-minimal.  
Preparing to unpack .../python3.7-minimal\_3.7.3-2+deb10u3\_amd64.deb ...  
Unpacking python3.7-minimal (3.7.3-2+deb10u3) ...  
Setting up libpython3.7-minimal:amd64 (3.7.3-2+deb10u3) ...  
Setting up python3.7-minimal (3.7.3-2+deb10u3) ...  
Selecting previously unselected package python3-minimal.  
(Reading database ... 7081 files and directories currently installed.)  
Preparing to unpack .../0-python3-minimal\_3.7.3-1\_amd64.deb ...  
Unpacking python3-minimal (3.7.3-1) ...  
Selecting previously unselected package mime-support.  
Preparing to unpack .../1-mime-support\_3.62\_all.deb ...  
Unpacking mime-support (3.62) ...  
Selecting previously unselected package libmpdec2:amd64.  
Preparing to unpack .../2-libmpdec2\_2.4.2-2\_amd64.deb ...

Unpacking libmpdec2:amd64 (2.4.2-2) ...  
Selecting previously unselected package libpython3.7-stdlib:amd64.  
Preparing to unpack .../3-libpython3.7-stdlib\_3.7.3-2+deb10u3\_amd64.deb ...  
Unpacking libpython3.7-stdlib:amd64 (3.7.3-2+deb10u3) ...  
Selecting previously unselected package python3.7.  
Preparing to unpack .../4-python3.7\_3.7.3-2+deb10u3\_amd64.deb ...  
Unpacking python3.7 (3.7.3-2+deb10u3) ...  
Selecting previously unselected package libpython3-stdlib:amd64.  
Preparing to unpack .../5-libpython3-stdlib\_3.7.3-1\_amd64.deb ...  
Unpacking libpython3-stdlib:amd64 (3.7.3-1) ...  
Setting up python3-minimal (3.7.3-1) ...  
Selecting previously unselected package python3.  
(Reading database ... 7518 files and directories currently installed.)  
Preparing to unpack .../00-python3\_3.7.3-1\_amd64.deb ...  
Unpacking python3 (3.7.3-1) ...  
Selecting previously unselected package libapt-inst2.0:amd64.  
Preparing to unpack .../01-libapt-inst2.0\_1.8.2.3\_amd64.deb ...  
Unpacking libapt-inst2.0:amd64 (1.8.2.3) ...  
Selecting previously unselected package apt-utils.  
Preparing to unpack .../02-apt-utils\_1.8.2.3\_amd64.deb ...  
Unpacking apt-utils (1.8.2.3) ...  
Selecting previously unselected package binutils-common:amd64.  
Preparing to unpack .../03-binutils-common\_2.31.1-16\_amd64.deb ...  
Unpacking binutils-common:amd64 (2.31.1-16) ...  
Selecting previously unselected package libbinutils:amd64.  
Preparing to unpack .../04-libbinutils\_2.31.1-16\_amd64.deb ...  
Unpacking libbinutils:amd64 (2.31.1-16) ...  
Selecting previously unselected package binutils-x86-64-linux-gnu.  
Preparing to unpack .../05-binutils-x86-64-linux-gnu\_2.31.1-16\_amd64.deb ...  
Unpacking binutils-x86-64-linux-gnu (2.31.1-16) ...  
Selecting previously unselected package binutils.  
Preparing to unpack .../06-binutils\_2.31.1-16\_amd64.deb ...  
Unpacking binutils (2.31.1-16) ...  
Selecting previously unselected package libisl19:amd64.  
Preparing to unpack .../07-libisl19\_0.20-2\_amd64.deb ...  
Unpacking libisl19:amd64 (0.20-2) ...  
Selecting previously unselected package libmpfr6:amd64.  
Preparing to unpack .../08-libmpfr6\_4.0.2-1\_amd64.deb ...  
Unpacking libmpfr6:amd64 (4.0.2-1) ...  
Selecting previously unselected package libmpc3:amd64.  
Preparing to unpack .../09-libmpc3\_1.1.0-1\_amd64.deb ...  
Unpacking libmpc3:amd64 (1.1.0-1) ...  
Selecting previously unselected package cpp-8.  
Preparing to unpack .../10-cpp-8\_8.3.0-6\_amd64.deb ...  
Unpacking cpp-8 (8.3.0-6) ...  
Selecting previously unselected package cpp.  
Preparing to unpack .../11-cpp\_4%3a8.3.0-1\_amd64.deb ...  
Unpacking cpp (4:8.3.0-1) ...  
Selecting previously unselected package python3-lib2to3.

Preparing to unpack .../12-python3-lib2to3\_3.7.3-1\_all.deb ...  
Unpacking python3-lib2to3 (3.7.3-1) ...  
Selecting previously unselected package python3-distutils.  
Preparing to unpack .../13-python3-distutils\_3.7.3-1\_all.deb ...  
Unpacking python3-distutils (3.7.3-1) ...  
Selecting previously unselected package dh-python.  
Preparing to unpack .../14-dh-python\_3.20190308\_all.deb ...  
Unpacking dh-python (3.20190308) ...  
Selecting previously unselected package libcc1-0:amd64.  
Preparing to unpack .../15-libcc1-0\_8.3.0-6\_amd64.deb ...  
Unpacking libcc1-0:amd64 (8.3.0-6) ...  
Selecting previously unselected package libgomp1:amd64.  
Preparing to unpack .../16-libgomp1\_8.3.0-6\_amd64.deb ...  
Unpacking libgomp1:amd64 (8.3.0-6) ...  
Selecting previously unselected package libitm1:amd64.  
Preparing to unpack .../17-libitm1\_8.3.0-6\_amd64.deb ...  
Unpacking libitm1:amd64 (8.3.0-6) ...  
Selecting previously unselected package libatomic1:amd64.  
Preparing to unpack .../18-libatomic1\_8.3.0-6\_amd64.deb ...  
Unpacking libatomic1:amd64 (8.3.0-6) ...  
Selecting previously unselected package libasan5:amd64.  
Preparing to unpack .../19-libasan5\_8.3.0-6\_amd64.deb ...  
Unpacking libasan5:amd64 (8.3.0-6) ...  
Selecting previously unselected package liblsan0:amd64.  
Preparing to unpack .../20-liblsan0\_8.3.0-6\_amd64.deb ...  
Unpacking liblsan0:amd64 (8.3.0-6) ...  
Selecting previously unselected package libtsan0:amd64.  
Preparing to unpack .../21-libtsan0\_8.3.0-6\_amd64.deb ...  
Unpacking libtsan0:amd64 (8.3.0-6) ...  
Selecting previously unselected package libubsan1:amd64.  
Preparing to unpack .../22-libubsan1\_8.3.0-6\_amd64.deb ...  
Unpacking libubsan1:amd64 (8.3.0-6) ...  
Selecting previously unselected package libmpx2:amd64.  
Preparing to unpack .../23-libmpx2\_8.3.0-6\_amd64.deb ...  
Unpacking libmpx2:amd64 (8.3.0-6) ...  
Selecting previously unselected package libquadmath0:amd64.  
Preparing to unpack .../24-libquadmath0\_8.3.0-6\_amd64.deb ...  
Unpacking libquadmath0:amd64 (8.3.0-6) ...  
Selecting previously unselected package libgcc-8-dev:amd64.  
Preparing to unpack .../25-libgcc-8-dev\_8.3.0-6\_amd64.deb ...  
Unpacking libgcc-8-dev:amd64 (8.3.0-6) ...  
Selecting previously unselected package gcc-8.  
Preparing to unpack .../26-gcc-8\_8.3.0-6\_amd64.deb ...  
Unpacking gcc-8 (8.3.0-6) ...  
Selecting previously unselected package gcc.  
Preparing to unpack .../27-gcc\_4%3a8.3.0-1\_amd64.deb ...  
Unpacking gcc (4:8.3.0-1) ...  
Selecting previously unselected package libc-dev-bin.  
Preparing to unpack .../28-libc-dev-bin\_2.28-10\_amd64.deb ...

Unpacking libc-dev-bin (2.28-10) ...  
Selecting previously unselected package linux-libc-dev:amd64.  
Preparing to unpack .../29-linux-libc-dev\_4.19.181-1\_amd64.deb ...  
Unpacking linux-libc-dev:amd64 (4.19.181-1) ...  
Selecting previously unselected package libc6-dev:amd64.  
Preparing to unpack .../30-libc6-dev\_2.28-10\_amd64.deb ...  
Unpacking libc6-dev:amd64 (2.28-10) ...  
Selecting previously unselected package libexpat1-dev:amd64.  
Preparing to unpack .../31-libexpat1-dev\_2.2.6-2+deb10u1\_amd64.deb ...  
Unpacking libexpat1-dev:amd64 (2.2.6-2+deb10u1) ...  
Selecting previously unselected package libmagic-mgc.  
Preparing to unpack .../32-libmagic-mgc\_1%3a5.35-4+deb10u2\_amd64.deb ...  
Unpacking libmagic-mgc (1:5.35-4+deb10u2) ...  
Selecting previously unselected package libmagic1:amd64.  
Preparing to unpack .../33-libmagic1\_1%3a5.35-4+deb10u2\_amd64.deb ...  
Unpacking libmagic1:amd64 (1:5.35-4+deb10u2) ...  
Selecting previously unselected package libmagic-dev:amd64.  
Preparing to unpack .../34-libmagic-dev\_1%3a5.35-4+deb10u2\_amd64.deb ...  
Unpacking libmagic-dev:amd64 (1:5.35-4+deb10u2) ...  
Selecting previously unselected package libpython3.7:amd64.  
Preparing to unpack .../35-libpython3.7\_3.7.3-2+deb10u3\_amd64.deb ...  
Unpacking libpython3.7:amd64 (3.7.3-2+deb10u3) ...  
Selecting previously unselected package libpython3.7-dev:amd64.  
Preparing to unpack .../36-libpython3.7-dev\_3.7.3-2+deb10u3\_amd64.deb ...  
Unpacking libpython3.7-dev:amd64 (3.7.3-2+deb10u3) ...  
Selecting previously unselected package libpython3-dev:amd64.  
Preparing to unpack .../37-libpython3-dev\_3.7.3-1\_amd64.deb ...  
Unpacking libpython3-dev:amd64 (3.7.3-1) ...  
Selecting previously unselected package python-pip-whl.  
Preparing to unpack .../38-python-pip-whl\_18.1-5\_all.deb ...  
Unpacking python-pip-whl (18.1-5) ...  
Selecting previously unselected package python3.7-dev.  
Preparing to unpack .../39-python3.7-dev\_3.7.3-2+deb10u3\_amd64.deb ...  
Unpacking python3.7-dev (3.7.3-2+deb10u3) ...  
Selecting previously unselected package python3-dev.  
Preparing to unpack .../40-python3-dev\_3.7.3-1\_amd64.deb ...  
Unpacking python3-dev (3.7.3-1) ...  
Selecting previously unselected package python3-pip.  
Preparing to unpack .../41-python3-pip\_18.1-5\_all.deb ...  
Unpacking python3-pip (18.1-5) ...  
Setting up mime-support (3.62) ...  
Setting up libmagic-mgc (1:5.35-4+deb10u2) ...  
Setting up binutils-common:amd64 (2.31.1-16) ...  
Setting up libmagic1:amd64 (1:5.35-4+deb10u2) ...  
Setting up linux-libc-dev:amd64 (4.19.181-1) ...  
Setting up libmagic-dev:amd64 (1:5.35-4+deb10u2) ...  
Setting up libgomp1:amd64 (8.3.0-6) ...  
Setting up libapt-inst2.0:amd64 (1.8.2.3) ...  
Setting up libasan5:amd64 (8.3.0-6) ...

```

Setting up libmpfr6:amd64 (4.0.2-1) ...
Setting up libquadmath0:amd64 (8.3.0-6) ...
Setting up libmpc3:amd64 (1.1.0-1) ...
Setting up libatomic1:amd64 (8.3.0-6) ...
Setting up libmpx2:amd64 (8.3.0-6) ...
Setting up libubsan1:amd64 (8.3.0-6) ...
Setting up libisl19:amd64 (0.20-2) ...
Setting up python-pip-whl (18.1-5) ...
Setting up libmpdec2:amd64 (2.4.2-2) ...
Setting up libbinutils:amd64 (2.31.1-16) ...
Setting up cpp-8 (8.3.0-6) ...
Setting up libc-dev-bin (2.28-10) ...
Setting up libcc1-0:amd64 (8.3.0-6) ...
Setting up liblsan0:amd64 (8.3.0-6) ...
Setting up libitm1:amd64 (8.3.0-6) ...
Setting up binutils-x86-64-linux-gnu (2.31.1-16) ...
Setting up libtsan0:amd64 (8.3.0-6) ...
Setting up libpython3.7-stdlib:amd64 (3.7.3-2+deb10u3) ...
Setting up apt-utils (1.8.2.3) ...
Setting up libpython3.7:amd64 (3.7.3-2+deb10u3) ...
Setting up binutils (2.31.1-16) ...
Setting up libgcc-8-dev:amd64 (8.3.0-6) ...
Setting up cpp (4:8.3.0-1) ...
Setting up libc6-dev:amd64 (2.28-10) ...
Setting up libpython3-stdlib:amd64 (3.7.3-1) ...
Setting up python3.7 (3.7.3-2+deb10u3) ...
Setting up gcc-8 (8.3.0-6) ...
Setting up python3 (3.7.3-1) ...
running python rtupdate hooks for python3.7...
running python post-rtupdate hooks for python3.7...
Setting up gcc (4:8.3.0-1) ...
Setting up libexpat1-dev:amd64 (2.2.6-2+deb10u1) ...
Setting up python3-lib2to3 (3.7.3-1) ...
Setting up python3-distutils (3.7.3-1) ...
Setting up dh-python (3.20190308) ...
Setting up libpython3.7-dev:amd64 (3.7.3-2+deb10u3) ...
Setting up python3.7-dev (3.7.3-2+deb10u3) ...
Setting up python3-pip (18.1-5) ...
Setting up libpython3-dev:amd64 (3.7.3-1) ...
Setting up python3-dev (3.7.3-1) ...
Processing triggers for libc-bin (2.28-10) ...
Reading package lists...
Building dependency tree...
Reading state information...
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
Removing intermediate container 970d197c1ab5
--> 7886ca0d37be
Step 8/14 : ADD ./requirements.txt /root/
--> 9faca43d7ffb

```

```

Step 9/14 : RUN python --version      && pip3 install virtualenv && virtualenv env3      &&
/opt/patrowl-manager/env3/bin/pip3 install --no-cache-dir -r /root/requirements.txt
---> Running in b35d991133d3
Python 3.7.10
Collecting virtualenv
  Downloading virtualenv-20.4.6-py2.py3-none-any.whl (7.2 MB)
Collecting distlib<1,>=0.3.1
  Downloading distlib-0.3.1-py2.py3-none-any.whl (335 kB)
Collecting six<2,>=1.9.0
  Downloading six-1.16.0-py2.py3-none-any.whl (11 kB)
Collecting importlib-metadata>=0.12
  Downloading importlib_metadata-4.0.1-py3-none-any.whl (16 kB)
Collecting filelock<4,>=3.0.0
  Downloading filelock-3.0.12-py3-none-any.whl (7.6 kB)
Collecting appdirs<2,>=1.4.3
  Downloading appdirs-1.4.4-py2.py3-none-any.whl (9.6 kB)
Collecting zipp>=0.5
  Downloading zipp-3.4.1-py3-none-any.whl (5.2 kB)
Collecting typing-extensions>=3.6.4
  Downloading typing_extensions-3.10.0.0-py3-none-any.whl (26 kB)
Installing collected packages: zipp, typing-extensions, six, importlib-metadata, filelock, distlib, ap-
pdirs, virtualenv
Successfully installed appdirs-1.4.4 distlib-0.3.1 filelock-3.0.12 importlib-metadata-4.0.1 six-1.16.0
typing-extensions-3.10.0.0 virtualenv-20.4.6 zipp-3.4.1
WARNING: Running pip as root will break packages and permissions. You should install packages
reliably by using venv: https://pip.pypa.io/warnings/venv
created virtual environment CPython3.7.10.final.0-64 in 1023ms
  creator CPython3Posix(dest=/opt/patrowl-manager/env3, clear=False, no_vcs_ignore=False,
global=False)
  seeder FromAppData(download=False, pip=bundle, setuptools=bundle, wheel=bundle, via=copy,
app_data_dir=/root/.local/share/virtualenv)
  added seed packages: pip==21.1.1, setuptools==56.0.0, wheel==0.36.2
  activators BashActivator,CShellActivator,FishActivator,PowerShellActivator,PythonActivator,Xon-
shActivator
Collecting amqp==2.5.1
  Downloading amqp-2.5.1-py2.py3-none-any.whl (49 kB)
Collecting Babel==2.4.0
  Downloading Babel-2.4.0-py2.py3-none-any.whl (6.8 MB)
Collecting backports-abc==0.5
  Downloading backports_abc-0.5-py2.py3-none-any.whl (5.2 kB)
Collecting billiard==3.6.1.0
  Downloading billiard-3.6.1.0-py3-none-any.whl (89 kB)
Collecting celery==4.4.0rc3
  Downloading celery-4.4.0rc3-py2.py3-none-any.whl (417 kB)
Collecting certifi==2017.4.17
  Downloading certifi-2017.4.17-py2.py3-none-any.whl (375 kB)
Collecting chardet==3.0.4
  Downloading chardet-3.0.4-py2.py3-none-any.whl (133 kB)
Collecting coreapi==2.3.3

```

Downloading coreapi-2.3.3-py2.py3-none-any.whl (25 kB)  
Collecting coreschema==0.0.4  
  Downloading coreschema-0.0.4.tar.gz (10 kB)  
Collecting Django==2.2.19  
  Downloading Django-2.2.19-py3-none-any.whl (7.5 MB)  
Collecting django-celery-beat==2.0.0  
  Downloading django\_celery\_beat-2.0.0-py2.py3-none-any.whl (37 kB)  
Collecting django-celery-results==1.1.2  
  Downloading django\_celery\_results-1.1.2-py2.py3-none-any.whl (18 kB)  
Collecting django-cursor-pagination==0.1.4  
  Downloading django\_cursor\_pagination-0.1.4-py3-none-any.whl (5.6 kB)  
Collecting django-datetime-widget==0.9.3  
  Downloading django-datetime-widget-0.9.3.tar.gz (37 kB)  
Collecting django-debug-toolbar==2.0  
  Downloading django\_debug\_toolbar-2.0-py3-none-any.whl (198 kB)  
Collecting django-extensions==2.1.9  
  Downloading django\_extensions-2.1.9-py2.py3-none-any.whl (223 kB)  
Collecting django-rest-swagger==2.2.0  
  Downloading django\_rest\_swagger-2.2.0-py2.py3-none-any.whl (495 kB)  
Collecting django-timezone-field==4.0  
  Downloading django\_timezone\_field-4.0-py3-none-any.whl (7.6 kB)  
Collecting djangorestframework>=3.11.2  
  Downloading djangorestframework-3.12.4-py3-none-any.whl (957 kB)  
Collecting flower==0.9.2  
  Downloading flower-0.9.2.tar.gz (1.3 MB)  
Collecting future==0.16.0  
  Downloading future-0.16.0.tar.gz (824 kB)  
Collecting futures==3.1.1  
  Downloading futures-3.1.1-py3-none-any.whl (2.8 kB)  
Collecting gunicorn==20.0.4  
  Downloading gunicorn-20.0.4-py2.py3-none-any.whl (77 kB)  
Collecting idna==2.5  
  Downloading idna-2.5-py2.py3-none-any.whl (55 kB)  
Collecting importlib-metadata==0.23  
  Downloading importlib\_metadata-0.23-py2.py3-none-any.whl (28 kB)  
Collecting itypes==1.1.0  
  Downloading itypes-1.1.0.tar.gz (2.2 kB)  
Collecting Jinja2==2.11.3  
  Downloading Jinja2-2.11.3-py2.py3-none-any.whl (125 kB)  
Collecting jsonfield==2.0.2  
  Downloading jsonfield-2.0.2-py2.py3-none-any.whl (13 kB)  
Collecting kombu==4.6.4  
  Downloading kombu-4.6.4-py2.py3-none-any.whl (182 kB)  
Collecting libmagic==1.0  
  Downloading libmagic-1.0.tar.gz (3.7 kB)  
Collecting MarkupSafe==1.1.0  
  Downloading MarkupSafe-1.1.0-cp37-cp37m-manylinux1\_x86\_64.whl (27 kB)  
Collecting meld3==1.0.2  
  Downloading meld3-1.0.2-py2.py3-none-any.whl (24 kB)



Collecting more-itertools==7.2.0  
 Downloading more\_itertools-7.2.0-py3-none-any.whl (57 kB)  
Collecting netaddr==0.7.19  
 Downloading netaddr-0.7.19-py2.py3-none-any.whl (1.6 MB)  
Collecting openapi-codec==1.3.2  
 Downloading openapi-codec-1.3.2.tar.gz (6.3 kB)  
Collecting psycpg2-binary==2.7.5  
 Downloading psycpg2\_binary-2.7.5-cp37-cp37m-manylinux1\_x86\_64.whl (2.7 MB)  
Collecting python-crontab==2.3.6  
 Downloading python-crontab-2.3.6.tar.gz (44 kB)  
Collecting python-dateutil==2.8.0  
 Downloading python\_dateutil-2.8.0-py2.py3-none-any.whl (226 kB)  
Collecting python-magic==0.4.15  
 Downloading python\_magic-0.4.15-py2.py3-none-any.whl (5.5 kB)  
Collecting python-memcached==1.59  
 Downloading python\_memcached-1.59-py2.py3-none-any.whl (16 kB)  
Collecting pytz==2019.2  
 Downloading pytz-2019.2-py2.py3-none-any.whl (508 kB)  
Collecting requests==2.22.0  
 Downloading requests-2.22.0-py2.py3-none-any.whl (57 kB)  
Collecting simplejson==3.16.0  
 Downloading simplejson-3.16.0.tar.gz (81 kB)  
Collecting singledispatch==3.4.0.3  
 Downloading singledispatch-3.4.0.3-py2.py3-none-any.whl (12 kB)  
Collecting six==1.10.0  
 Downloading six-1.10.0-py2.py3-none-any.whl (10 kB)  
Collecting sqlparse==0.3.0  
 Downloading sqlparse-0.3.0-py2.py3-none-any.whl (39 kB)  
Collecting supervisor==4.2.1  
 Downloading supervisor-4.2.1-py2.py3-none-any.whl (738 kB)  
Collecting thehive4py==1.4.3  
 Downloading thehive4py-1.4.3-py2.py3-none-any.whl (11 kB)  
Collecting tornado==5.1  
 Downloading tornado-5.1.tar.gz (516 kB)  
Collecting tzlocal==1.5.1  
 Downloading tzlocal-1.5.1.tar.gz (16 kB)  
Collecting uritemplate==3.0.0  
 Downloading uritemplate-3.0.0-py2.py3-none-any.whl (10 kB)  
Collecting urllib3==1.25.9  
 Downloading urllib3-1.25.9-py2.py3-none-any.whl (126 kB)  
Collecting vine==1.3.0  
 Downloading vine-1.3.0-py2.py3-none-any.whl (14 kB)  
Collecting Werkzeug==0.15.3  
 Downloading Werkzeug-0.15.3-py2.py3-none-any.whl (327 kB)  
Collecting zipp==0.6.0  
 Downloading zipp-0.6.0-py2.py3-none-any.whl (4.1 kB)  
Collecting django-filter==2.4.0  
 Downloading django\_filter-2.4.0-py3-none-any.whl (73 kB)  
Collecting django-cors-headers==3.2.0

Downloading django\_cors\_headers-3.2.0-py3-none-any.whl (14 kB)  
 Collecting django-rest-framework-simplejwt==4.4.0  
 Downloading django-rest-framework-simplejwt-4.4.0-py3-none-any.whl (29 kB)  
 Collecting django-health-check==3.12.1  
 Downloading django\_health\_check-3.12.1-py2.py3-none-any.whl (25 kB)  
 Collecting psutil==5.7.0  
 Downloading psutil-5.7.0.tar.gz (449 kB)  
 Collecting django-organizations==1.1.2  
 Downloading django\_organizations-1.1.2-py2.py3-none-any.whl (56 kB)  
 Collecting django-annoying==0.10.6  
 Downloading django\_annoying-0.10.6-py2.py3-none-any.whl (9.5 kB)  
 Collecting django-reset-migrations  
 Downloading django\_reset\_migrations-0.4.0-py3-none-any.whl (8.0 kB)  
 Collecting django-dbconn-retry  
 Downloading django\_dbconn\_retry-0.1.5-py3-none-any.whl (8.6 kB)  
 Requirement already satisfied: setuptools>=3.0 in ./env3/lib/python3.7/site-packages (from gunicorn==20.0.4->r /root/requirements.txt (line 24)) (56.0.0)  
 Collecting pyjwt  
 Downloading PyJWT-2.1.0-py3-none-any.whl (16 kB)  
 Building wheels for collected packages: coreschema, django-datetime-widget, flower, future, itypes, libmagic, openapi-codec, python-crontab, simplejson, tornado, tzlocal, psutil  
 Building wheel for coreschema (setup.py): started  
 Building wheel for coreschema (setup.py): finished with status 'done'  
 Created wheel for coreschema: filename=coreschema-0.0.4-py3-none-any.whl size=15031 sha256=31f04df19b6dd95fa460f9835d3e5ebd79c94a76102e97f91dd5c34cd6bf608e  
 Stored in directory: /tmp/pip-ephem-wheel-cache-tb16rge8/wheels/29/28/77/73539fe0ce161da7a571cd8278a9296adbda257406bb6f100d  
 Building wheel for django-datetime-widget (setup.py): started  
 Building wheel for django-datetime-widget (setup.py): finished with status 'done'  
 Created wheel for django-datetime-widget: filename=django\_datetime\_widget-0.9.3-py3-none-any.whl size=55480 sha256=cde48e2144cf01156d8a61f11821b83db4d9c68a62ccb6c96b7643640bb6f2b9  
 Stored in directory: /tmp/pip-ephem-wheel-cache-tb16rge8/wheels/c2/1a/ea/1bc6eb473fe391682592bf5eb0b178098f020ef06e5bead42a  
 Building wheel for flower (setup.py): started  
 Building wheel for flower (setup.py): finished with status 'done'  
 Created wheel for flower: filename=flower-0.9.2-py2.py3-none-any.whl size=455328 sha256=33d99fc36035be7b45f6dce06586da160f464752c8717e51988e8012cb945b59  
 Stored in directory: /tmp/pip-ephem-wheel-cache-tb16rge8/wheels/f4/9b/c6/38f40eb6b98ab9819317b03c892a94423dec8d056e8dc83eba  
 Building wheel for future (setup.py): started  
 Building wheel for future (setup.py): finished with status 'done'  
 Created wheel for future: filename=future-0.16.0-py3-none-any.whl size=487798 sha256=18fa10646ec1e5d2e843587f7f2b51dcd3f8a42ecaa950bbd23c748f6f129fdd  
 Stored in directory: /tmp/pip-ephem-wheel-cache-tb16rge8/wheels/7c/09/6f/dfd31fb2ebe951aefbee461a0dfce1bdc2e4b2c1016e85d233  
 Building wheel for itypes (setup.py): started  
 Building wheel for itypes (setup.py): finished with status 'done'

Created wheel for itypes: filename=itypes-1.1.0-py3-none-any.whl size=2311  
sha256=a6069bc21cc87c332aff172acebb271476d4ecb2cb7a63d77f1b16686cb252a7  
Stored in directory: /tmp/pip-ephem-wheel-cache-  
tb16rge8/wheels/a5/92/71/4ee11d4146fae4155e5585d0d7261463943c36380c87395899  
Building wheel for libmagic (setup.py): started  
Building wheel for libmagic (setup.py): finished with status 'done'  
Created wheel for libmagic: filename=libmagic-1.0-py3-none-any.whl size=4287  
sha256=795941a0468070499003ccddb3f9ee10990d584322c910dbaed01835bc9a451  
Stored in directory: /tmp/pip-ephem-wheel-cache-  
tb16rge8/wheels/1f/09/8f/b428f254d5cdeb8b9b158355f5bc10119dc4914e0b22852aaa  
Building wheel for openapi-codec (setup.py): started  
Building wheel for openapi-codec (setup.py): finished with status 'done'  
Created wheel for openapi-codec: filename=openapi\_codec-1.3.2-py3-none-any.whl size=7307  
sha256=07c1d15da93529bcfef71b12499d45f8c55ac7ead6fd5f158a8e3fa43fd1c9a  
Stored in directory: /tmp/pip-ephem-wheel-cache-  
tb16rge8/wheels/90/4f/a2/0cef56e55966463564e594a0fcd8ff1a858917fe7c1585cc6d  
Building wheel for python-crontab (setup.py): started  
Building wheel for python-crontab (setup.py): finished with status 'done'  
Created wheel for python-crontab: filename=python\_crontab-2.3.6-py3-none-any.whl  
size=24893 sha256=d71b5e56348abaeb2ba8e22a27f4ac8cbdc175bfa4ea73701eddb21340d5d7fb  
Stored in directory: /tmp/pip-ephem-wheel-cache-tb16rge8/wheels/21/06/e4/c12ad-  
ffcb4876a05e4ace2bf90a390323007708964fe9101a2  
Building wheel for simplejson (setup.py): started  
Building wheel for simplejson (setup.py): finished with status 'done'  
Created wheel for simplejson: filename=simplejson-3.16.0-cp37-cp37m-linux\_x86\_64.whl  
size=74378 sha256=0a9b1a1a43f192aabdddec2c6b696d53d5714c9f84a4a1da0c455ee4e3c1887ab  
Stored in directory: /tmp/pip-ephem-wheel-cache-  
tb16rge8/wheels/00/6f/29/109ee3b85a9f9861d4294b05e4597363d5ad3c9dfaccc78787  
Building wheel for tornado (setup.py): started  
Building wheel for tornado (setup.py): finished with status 'done'  
Created wheel for tornado: filename=tornado-5.1-cp37-cp37m-linux\_x86\_64.whl size=451545  
sha256=f5194de3278915b4e7d87c1b837022b54dfc00d4bed91b97f26c98f4624bc936  
Stored in directory: /tmp/pip-ephem-wheel-cache-  
tb16rge8/wheels/8e/53/de/6a6860ebf6d2958e20a9a8337f25b0369f1666002ade0ce284  
Building wheel for tzlocal (setup.py): started  
Building wheel for tzlocal (setup.py): finished with status 'done'  
Created wheel for tzlocal: filename=tzlocal-1.5.1-py3-none-any.whl size=17541  
sha256=3c7326828b3f7581442649e4a0e80752bcea1b6c6e3b00806c459d9fb852c13c  
Stored in directory: /tmp/pip-ephem-wheel-cache-  
tb16rge8/wheels/6a/76/b4/f97e26f8f60b5b2b1287415f1202e2b34a97775cead74072be  
Building wheel for psutil (setup.py): started  
Building wheel for psutil (setup.py): finished with status 'done'  
Created wheel for psutil: filename=psutil-5.7.0-cp37-cp37m-linux\_x86\_64.whl size=217145  
sha256=5edc81d8a50e3119a26de0772e3223e176273a0a1420695f1c04819dfcdb22ca  
Stored in directory: /tmp/pip-ephem-wheel-cache-  
tb16rge8/wheels/b6/e7/50/aee9cc966163d74430f13f208171dee22f11efa4a4a826661c  
Successfully built coreshema django-datetime-widget flower future itypes libmagic openapi-co-  
dec python-crontab simplejson tornado tzlocal psutil

Installing collected packages: more-itertools, MarkupSafe, zipp, vine, urllib3, Jinja2, idna, chardet, certifi, uritemplate, sqlparse, six, requests, pytz, itypes, importlib-metadata, coreschema, amqp, python-dateutil, kombu, Django, coreapi, billiard, tornado, simplejson, python-magic, python-crontab, pyjwt, openapi-codec, future, django-rest-framework, django-timezone-field, celery, Babel, Werkzeug, tzlocal, thehive4py, supervisor, singledispatch, python-memcached, pycpg2-binary, psutil, netaddr, meld3, libmagic, jsonfield, gunicorn, futures, flower, django-rest-framework-simplejwt, django-rest-swagger, django-reset-migrations, django-organizations, django-health-check, django-filter, django-extensions, django-debug-toolbar, django-dbconn-retry, django-datetime-widget, django-cursor-pagination, django-cors-headers, django-celery-results, django-celery-beat, django-annoying, backports-abc

Successfully installed Babel-2.4.0 Django-2.2.19 Jinja2-2.11.3 MarkupSafe-1.1.0 Werkzeug-0.15.3 amqp-2.5.1 backports-abc-0.5 billiard-3.6.1.0 celery-4.4.0rc3 certifi-2017.4.17 chardet-3.0.4 coreapi-2.3.3 coreschema-0.0.4 django-annoying-0.10.6 django-celery-beat-2.0.0 django-celery-results-1.1.2 django-cors-headers-3.2.0 django-cursor-pagination-0.1.4 django-datetime-widget-0.9.3 django-dbconn-retry-0.1.5 django-debug-toolbar-2.0 django-extensions-2.1.9 django-filter-2.4.0 django-health-check-3.12.1 django-organizations-1.1.2 django-reset-migrations-0.4.0 django-rest-swagger-2.2.0 django-timezone-field-4.0 django-rest-framework-3.12.4 django-rest-framework-simplejwt-4.4.0 flower-0.9.2 future-0.16.0 futures-3.1.1 gunicorn-20.0.4 idna-2.5 importlib-metadata-0.23 itypes-1.1.0 jsonfield-2.0.2 kombu-4.6.4 libmagic-1.0 meld3-1.0.2 more-itertools-7.2.0 netaddr-0.7.19 openapi-codec-1.3.2 psutil-5.7.0 pycpg2-binary-2.7.5 pyjwt-2.1.0 python-crontab-2.3.6 python-dateutil-2.8.0 python-magic-0.4.15 python-memcached-1.59 pytz-2019.2 requests-2.22.0 simplejson-3.16.0 singledispatch-3.4.0.3 six-1.10.0 sqlparse-0.3.0 supervisor-4.2.1 thehive4py-1.4.3 tornado-5.1 tzlocal-1.5.1 uritemplate-3.0.0 urllib3-1.25.9 vine-1.3.0 zipp-0.6.0  
Removing intermediate container b35d991133d3

---> f2ad2c37fd09

Step 10/14 : COPY ./opt/patrowl-manager/

---> 2f93ac71c35b

Step 11/14 : COPY app/settings.py.sample /opt/patrowl-manager/app/settings.py

---> b6bb81d8f185

Step 12/14 : EXPOSE 8003

---> Running in 16c818b4ccb4

Removing intermediate container 16c818b4ccb4

---> 158a287f70c7

Step 13/14 : ENTRYPOINT ["/opt/patrowl-manager/docker-entrypoint.sh"]

---> Running in 99805ca8f377

Removing intermediate container 99805ca8f377

---> 4dd9010a21d3

Step 14/14 : CMD ["run"]

---> Running in 151ad6bac825

Removing intermediate container 151ad6bac825

---> c9f886be6d26

Successfully built c9f886be6d26

Successfully tagged patrowl/patrowl-manager-community-edition:latest

z@z:~/PatrowlManager\$ docker-compose -f docker-compose.with-engines.yml up

Creating network "patrowlmanager\_default" with the default driver

Pulling rabbitmq (rabbitmq:3-alpine)...

3-alpine: Pulling from library/rabbitmq

540db60ca938: Pull complete

28043b0246d1: Pull complete

357d43553933: Pull complete  
5e29f96505bc: Pull complete  
a2ffa83a2499: Pull complete  
86b6ff74a244: Pull complete  
db682261b173: Pull complete  
374b79da3a0c: Pull complete  
Digest: sha256:db965b78f81597106d9c5d0a3f62fda483ac855a00539f37bb24d25e0db9639e  
Status: Downloaded newer image for rabbitmq:3-alpine  
Pulling db (postgres:11-alpine)...  
11-alpine: Pulling from library/postgres  
540db60ca938: Already exists  
a3cb73039552: Pull complete  
39855706e49a: Pull complete  
71553cacf6c5: Pull complete  
c74391ac460b: Pull complete  
91f3d9ec56e6: Pull complete  
5d8f64be1896: Pull complete  
4b29fd570404: Pull complete  
c6ebc7224b03: Pull complete  
Digest: sha256:be3abb1a355d74adf6f33517d7a4770c39ec32438be0375c0700428a1c15f2cc  
Status: Downloaded newer image for postgres:11-alpine  
Pulling nginx (nginx:stable-alpine)...  
stable-alpine: Pulling from library/nginx  
540db60ca938: Already exists  
3b88e9e9a17d: Pull complete  
3019f265923a: Pull complete  
fd39c3601fe1: Pull complete  
4d0e0e4dee17: Pull complete  
f81ca69df58f: Pull complete  
Digest: sha256:e015192ec74937149dce3aa1feb8af016b7cce3a2896246b623cfd55c14939a6  
Status: Downloaded newer image for nginx:stable-alpine  
Pulling engine-nmap (patrowl/engine-nmap)...  
latest: Pulling from patrowl/engine-nmap  
540db60ca938: Already exists  
2dafc937c833: Pull complete  
af01fc82ff08: Pull complete  
436c5c0edbd7: Pull complete  
e125e323d49d: Pull complete  
2daba5b09356: Pull complete  
b449ab3b77c0: Pull complete  
750a55ec9267: Pull complete  
9aa8a67a3b33: Pull complete  
49137ecfa5fb: Pull complete  
29aa1c4fec3d: Pull complete  
914fc3a3aaf2: Pull complete  
ac8d80d6d85d: Pull complete  
88e3d691f1e6: Pull complete  
Digest: sha256:fd88654f17b70f28e10d3b47d2397cf1403b62ec0e863c741ee50385d09b695b  
Status: Downloaded newer image for patrowl/engine-nmap:latest

```
Pulling engine-sslsan (patrowl/engine-sslsan):...
latest: Pulling from patrowl/engine-sslsan
540db60ca938: Already exists
57aac026a592: Pull complete
6d05eb4bb17a: Pull complete
6fd4e26b0685: Pull complete
21939cdbe007: Pull complete
172a1a8ec8f3: Pull complete
cdd697564057: Pull complete
1abc74789958: Pull complete
81bedff90b93: Pull complete
a52294eb97ff: Pull complete
be91e4a695b4: Pull complete
a6da6f7b43b7: Pull complete
Digest: sha256:0b0b16e736173d2aa60bb06404bc84326c2699fa55d4025acb32c7e4d3c07c7a
Status: Downloaded newer image for patrowl/engine-sslsan:latest
Pulling engine-owl_dns (patrowl/engine-owl_dns):...
latest: Pulling from patrowl/engine-owl_dns
345e3491a907: Pull complete
57671312ef6f: Pull complete
5e9250ddb7d0: Pull complete
3641a63256e8: Pull complete
e97eb3a8d425: Pull complete
456dc2b1a014: Pull complete
26bef2632788: Pull complete
5bf8280481a6: Pull complete
305f1ad04226: Pull complete
484ef0eb3fe5: Pull complete
4bf89eff8075: Pull complete
c04353e4231d: Pull complete
185906cd7b7d: Pull complete
0924d959cb55: Pull complete
0ddcaa9bbfbc: Pull complete
ab6598a44a1e: Pull complete
4aed8cfa4cfe: Pull complete
e2179ccfbd90: Pull complete
188de9913505: Pull complete
Digest: sha256:1ea4a38d47d1b541d6afbb04fde1b5d72702754454b886c12679862d93ab395c
Status: Downloaded newer image for patrowl/engine-owl_dns:latest
Creating patrowl-rabbitmq ... done
Creating patrowl-sslsan ... done
Creating patrowl-owl_dns ... done
Creating patrowl-nmap ... done
Creating patrowl-postgres ... done
Creating patrowl-django ... done
Creating patrowl-nginx ... done
Attaching to patrowl-postgres, patrowl-owl_dns, patrowl-sslsan, patrowl-nmap, patrowl-rab-
bitmq, patrowl-django, patrowl-nginx
patrowl-django | [+] Wait for DB availability
```

```

patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 9: /dev/tcp/db/5432: Connection re-
fused
patrowl-nginx | /docker-entrypoint.sh: /docker-entrypoint.d/ is not empty, will attempt to per-
form configuration
patrowl-nginx | /docker-entrypoint.sh: Looking for shell scripts in /docker-entrypoint.d/
patrowl-nginx | /docker-entrypoint.sh: Launching /docker-entrypoint.d/10-listen-on-ipv6-by-
default.sh
patrowl-nginx | 10-listen-on-ipv6-by-default.sh: info: Getting the checksum of
/etc/nginx/conf.d/default.conf
patrowl-owl_dns | [2021-05-10 14:07:35 +0000] [1] [INFO] Starting gunicorn 20.0.4
patrowl-owl_dns | [2021-05-10 14:07:35 +0000] [1] [INFO] Listening at: http://0.0.0.0:5006 (1)
patrowl-owl_dns | [2021-05-10 14:07:35 +0000] [1] [INFO] Using worker: threads
patrowl-owl_dns | [2021-05-10 14:07:35 +0000] [8] [INFO] Booting worker with pid: 8
patrowl-postgres | The files belonging to this database system will be owned by user "postgres".
patrowl-postgres | This user must also own the server process.
patrowl-postgres |
patrowl-postgres | The database cluster will be initialized with locale "en_US.utf8".
patrowl-postgres | The default database encoding has accordingly been set to "UTF8".
patrowl-postgres | The default text search configuration will be set to "english".
patrowl-postgres |
patrowl-postgres | Data page checksums are disabled.
patrowl-postgres |
patrowl-postgres | fixing permissions on existing directory /var/lib/postgresql/data ... ok
patrowl-postgres | creating subdirectories ... ok
patrowl-postgres | selecting default max_connections ... 100
patrowl-postgres | selecting default shared_buffers ... 128MB
patrowl-sslscan | [2021-05-10 14:07:37 +0000] [1] [INFO] Starting gunicorn 20.0.4
patrowl-sslscan | [2021-05-10 14:07:37 +0000] [1] [INFO] Listening at: http://0.0.0.0:5014 (1)
patrowl-sslscan | [2021-05-10 14:07:37 +0000] [1] [INFO] Using worker: sync
patrowl-sslscan | [2021-05-10 14:07:37 +0000] [8] [INFO] Booting worker with pid: 8
patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 9: /dev/tcp/db/5432: Connection re-
fused
patrowl-nginx | 10-listen-on-ipv6-by-default.sh: info: /etc/nginx/conf.d/default.conf differs from
the packaged version
patrowl-nginx | /docker-entrypoint.sh: Launching /docker-entrypoint.d/20-envsubst-on-tem-
plates.sh
patrowl-nginx | /docker-entrypoint.sh: Launching /docker-entrypoint.d/30-tune-worker-pro-
cesses.sh
patrowl-nginx | /docker-entrypoint.sh: Configuration complete; ready for start up
patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 9: /dev/tcp/db/5432: Connection re-
fused
patrowl-nginx | 2021/05/10 14:07:49 [notice] 1#1: using the "epoll" event method
patrowl-nginx | 2021/05/10 14:07:49 [notice] 1#1: nginx/1.20.0
patrowl-nginx | 2021/05/10 14:07:49 [notice] 1#1: built by gcc 10.2.1 20201203 (Alpine
10.2.1_pre1)
patrowl-nginx | 2021/05/10 14:07:49 [notice] 1#1: OS: Linux 5.11.0-16-generic

```

```

patrowl-nginx | 2021/05/10 14:07:49 [notice] 1#1: getrlimit(RLIMIT_NOFILE): 1048576:1048576
patrowl-nginx | 2021/05/10 14:07:49 [notice] 1#1: start worker processes
patrowl-nginx | 2021/05/10 14:07:49 [notice] 1#1: start worker process 31
patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 9: /dev/tcp/db/5432: Connection re-
fused
patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 9: /dev/tcp/db/5432: Connection re-
fused
patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 9: /dev/tcp/db/5432: Connection re-
fused
patrowl-nmap | [2021-05-10 14:07:52 +0000] [1] [INFO] Starting gunicorn 20.0.4
patrowl-nmap | [2021-05-10 14:07:52 +0000] [1] [INFO] Listening at: http://0.0.0.0:5001 (1)
patrowl-nmap | [2021-05-10 14:07:52 +0000] [1] [INFO] Using worker: sync
patrowl-nmap | [2021-05-10 14:07:52 +0000] [8] [INFO] Booting worker with pid: 8
patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 9: /dev/tcp/db/5432: Connection re-
fused
patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 9: /dev/tcp/db/5432: Connection re-
fused
patrowl-postgres | selecting default timezone ... UTC
patrowl-postgres | selecting dynamic shared memory implementation ... posix
patrowl-postgres | creating configuration files ... ok
patrowl-postgres | running bootstrap script ... ok
patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 9: /dev/tcp/db/5432: Connection re-
fused
patrowl-postgres | performing post-bootstrap initialization ... sh: locale: not found
patrowl-postgres | 2021-05-10 14:07:55.489 UTC [30] WARNING: no usable system locales were
found
patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 9: /dev/tcp/db/5432: Connection re-
fused
patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 9: /dev/tcp/db/5432: Connection re-
fused
patrowl-postgres | ok
patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 9: /dev/tcp/db/5432: Connection re-
fused
patrowl-rabbitmq | Configuring logger redirection
patrowl-postgres | syncing data to disk ... ok
patrowl-postgres |
patrowl-postgres | WARNING: enabling "trust" authentication for local connections
patrowl-postgres | You can change this by editing pg_hba.conf or using the option -A, or
patrowl-postgres | --auth-local and --auth-host, the next time you run initdb.
patrowl-postgres |

```



```

patrowl-postgres | Success. You can now start the database server using:
patrowl-postgres |
patrowl-postgres | pg_ctl -D /var/lib/postgresql/data -l logfile start
patrowl-postgres |
patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 9: /dev/tcp/db/5432: Connection re-
fused
patrowl-postgres | waiting for server to start....2021-05-10 14:07:58.981 UTC [35] LOG: listening
on Unix socket "/var/run/postgresql/.s.PGSQL.5432"
patrowl-postgres | 2021-05-10 14:07:59.029 UTC [36] LOG: database system was shut down at
2021-05-10 14:07:57 UTC
patrowl-postgres | 2021-05-10 14:07:59.032 UTC [35] LOG: database system is ready to accept
connections
patrowl-postgres | done
patrowl-postgres | server started
patrowl-postgres | CREATE DATABASE
patrowl-postgres |
patrowl-postgres |
patrowl-postgres | /usr/local/bin/docker-entrypoint.sh: running /docker-entrypoint-in-
itdb.d/init_db.sql
patrowl-postgres | ALTER ROLE
patrowl-postgres | ALTER ROLE
patrowl-postgres | ALTER ROLE
patrowl-postgres | GRANT
patrowl-postgres |
patrowl-postgres |
patrowl-postgres | 2021-05-10 14:07:59.914 UTC [35] LOG: received fast shutdown request
patrowl-postgres | waiting for server to shut down....2021-05-10 14:07:59.916 UTC [35] LOG:
aborting any active transactions
patrowl-postgres | 2021-05-10 14:07:59.921 UTC [35] LOG: background worker "logical replica-
tion launcher" (PID 42) exited with exit code 1
patrowl-postgres | 2021-05-10 14:07:59.922 UTC [37] LOG: shutting down
patrowl-postgres | 2021-05-10 14:07:59.946 UTC [35] LOG: database system is shut down
patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 9: /dev/tcp/db/5432: Connection re-
fused
patrowl-postgres | done
patrowl-postgres | server stopped
patrowl-postgres |
patrowl-postgres | PostgreSQL init process complete; ready for start up.
patrowl-postgres |
patrowl-postgres | 2021-05-10 14:08:00.076 UTC [1] LOG: listening on IPv4 address "0.0.0.0",
port 5432
patrowl-postgres | 2021-05-10 14:08:00.077 UTC [1] LOG: listening on IPv6 address ":::", port
5432
patrowl-postgres | 2021-05-10 14:08:00.079 UTC [1] LOG: listening on Unix socket
"/var/run/postgresql/.s.PGSQL.5432"
patrowl-postgres | 2021-05-10 14:08:00.145 UTC [51] LOG: database system was shut down at
2021-05-10 14:07:59 UTC

```

```

patrowl-postgres | 2021-05-10 14:08:00.148 UTC [1] LOG: database system is ready to accept
connections
patrowl-django | [+] Wait for RabbitMQ availability
patrowl-postgres | 2021-05-10 14:08:00.961 UTC [58] LOG: incomplete startup packet
patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 12: /dev/tcp/rabbitmq/5672: Connec-
tion refused
patrowl-rabbitmq | Using deprecated config parameter 'log_levels'. Please update your configura-
tion file according to https://rabbitmq.com/logging.html2021-05-10 14:08:01.757 [debug]
<0.288.0> Lager installed handler error_logger_lager_h into error_logger
patrowl-rabbitmq | 2021-05-10 14:08:01.795 [debug] <0.291.0> Lager installed handler lager_for-
warder_backend into error_logger_lager_event
patrowl-rabbitmq | 2021-05-10 14:08:01.795 [debug] <0.294.0> Lager installed handler lager_for-
warder_backend into rabbit_log_lager_event
patrowl-rabbitmq | 2021-05-10 14:08:01.795 [debug] <0.297.0> Lager installed handler lager_for-
warder_backend into rabbit_log_channel_lager_event
patrowl-rabbitmq | 2021-05-10 14:08:01.795 [debug] <0.300.0> Lager installed handler lager_for-
warder_backend into rabbit_log_connection_lager_event
patrowl-rabbitmq | 2021-05-10 14:08:01.795 [debug] <0.303.0> Lager installed handler lager_for-
warder_backend into rabbit_log_feature_flags_lager_event
patrowl-rabbitmq | 2021-05-10 14:08:01.795 [debug] <0.306.0> Lager installed handler lager_for-
warder_backend into rabbit_log_federation_lager_event
patrowl-rabbitmq | 2021-05-10 14:08:01.795 [debug] <0.309.0> Lager installed handler lager_for-
warder_backend into rabbit_log_ldap_lager_event
patrowl-rabbitmq | 2021-05-10 14:08:01.795 [debug] <0.312.0> Lager installed handler lager_for-
warder_backend into rabbit_log_mirroring_lager_event
patrowl-rabbitmq | 2021-05-10 14:08:01.795 [debug] <0.315.0> Lager installed handler lager_for-
warder_backend into rabbit_log_prelaunch_lager_event
patrowl-rabbitmq | 2021-05-10 14:08:01.795 [debug] <0.318.0> Lager installed handler lager_for-
warder_backend into rabbit_log_queue_lager_event
patrowl-rabbitmq | 2021-05-10 14:08:01.795 [debug] <0.321.0> Lager installed handler lager_for-
warder_backend into rabbit_log_ra_lager_event
patrowl-rabbitmq | 2021-05-10 14:08:01.795 [debug] <0.324.0> Lager installed handler lager_for-
warder_backend into rabbit_log_shovel_lager_event
patrowl-rabbitmq | 2021-05-10 14:08:01.795 [debug] <0.327.0> Lager installed handler lager_for-
warder_backend into rabbit_log_upgrade_lager_event
patrowl-rabbitmq | 2021-05-10 14:08:01.914 [info] <0.44.0> Application lager started on node
rabbit@e86669c920ed
patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 12: /dev/tcp/rabbitmq/5672: Connec-
tion refused
patrowl-rabbitmq | 2021-05-10 14:08:02.220 [info] <0.44.0> Application mnesia started on node
rabbit@e86669c920ed
patrowl-rabbitmq | 2021-05-10 14:08:02.220 [info] <0.273.0>
patrowl-rabbitmq | Starting RabbitMQ 3.8.16 on Erlang 23.3.3
patrowl-rabbitmq | Copyright (c) 2007-2021 VMware, Inc. or its affiliates.
patrowl-rabbitmq | Licensed under the MPL 2.0. Website: https://rabbitmq.com
patrowl-rabbitmq |
patrowl-rabbitmq | ## ## RabbitMQ 3.8.16

```

```

patrowl-rabbitmq | ## ##
patrowl-rabbitmq | ##### Copyright (c) 2007-2021 VMware, Inc. or its affiliates.
patrowl-rabbitmq | ##### ##
patrowl-rabbitmq | ##### Licensed under the MPL 2.0. Website: https://rabbitmq.com
patrowl-rabbitmq |
patrowl-rabbitmq | Doc guides: https://rabbitmq.com/documentation.html
patrowl-rabbitmq | Support: https://rabbitmq.com/contact.html
patrowl-rabbitmq | Tutorials: https://rabbitmq.com/getstarted.html
patrowl-rabbitmq | Monitoring: https://rabbitmq.com/monitoring.html
patrowl-rabbitmq |
patrowl-rabbitmq | Logs: <stdout>
patrowl-rabbitmq |
patrowl-rabbitmq | Config file(s): /etc/rabbitmq/rabbitmq.conf
patrowl-rabbitmq | /etc/rabbitmq/conf.d/management_agent.disable_metrics_collec-
patrowl-rabbitmq | tor.conf
patrowl-rabbitmq |
patrowl-rabbitmq | Starting broker...2021-05-10 14:08:02.223 [info] <0.273.0>
patrowl-rabbitmq | node      : rabbit@e86669c920ed
patrowl-rabbitmq | home dir  : /var/lib/rabbitmq
patrowl-rabbitmq | config file(s) : /etc/rabbitmq/rabbitmq.conf
patrowl-rabbitmq | : /etc/rabbitmq/conf.d/management_agent.disable_metrics_collec-
patrowl-rabbitmq | tor.conf
patrowl-rabbitmq | cookie hash : jqz0dWsW2ePo90TXSAYx/w==
patrowl-rabbitmq | log(s)      : <stdout>
patrowl-rabbitmq | database dir : /var/lib/rabbitmq/mnesia/rabbit@e86669c920ed
patrowl-rabbitmq | 2021-05-10 14:08:02.252 [debug] <0.284.0> Lager installed handler la-
patrowl-rabbitmq | ger_backend_throttle into lager_event
patrowl-rabbitmq | 2021-05-10 14:08:02.666 [info] <0.273.0> Feature flags: list of feature flags
patrowl-rabbitmq | found:
patrowl-rabbitmq | 2021-05-10 14:08:02.666 [info] <0.273.0> Feature flags: [] drop_unrou-
patrowl-rabbitmq | table_metric
patrowl-rabbitmq | 2021-05-10 14:08:02.667 [info] <0.273.0> Feature flags: []
patrowl-rabbitmq | empty_basic_get_metric
patrowl-rabbitmq | 2021-05-10 14:08:02.667 [info] <0.273.0> Feature flags: [] implici-
patrowl-rabbitmq | t_default_bindings
patrowl-rabbitmq | 2021-05-10 14:08:02.667 [info] <0.273.0> Feature flags: [] mainte-
patrowl-rabbitmq | nance_mode_status
patrowl-rabbitmq | 2021-05-10 14:08:02.668 [info] <0.273.0> Feature flags: [] quorum_queue
patrowl-rabbitmq | 2021-05-10 14:08:02.668 [info] <0.273.0> Feature flags: [] user_limits
patrowl-rabbitmq | 2021-05-10 14:08:02.668 [info] <0.273.0> Feature flags: [] vir-
patrowl-rabbitmq | tual_host_metadata
patrowl-rabbitmq | 2021-05-10 14:08:02.669 [info] <0.273.0> Feature flags: feature flag states
patrowl-rabbitmq | written to disk: yes
patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 12: /dev/tcp/rabbitmq/5672: Connec-
patrowl-django | tion refused
patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 12: /dev/tcp/rabbitmq/5672: Connec-
patrowl-django | tion refused

```

```

patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 12: /dev/tcp/rabbitmq/5672: Connection refused
patrowl-rabbitmq | 2021-05-10 14:08:05.153 [info] <0.273.0> Running boot step pre_boot defined by app rabbit
patrowl-rabbitmq | 2021-05-10 14:08:05.153 [info] <0.273.0> Running boot step rabbit_core_metrics defined by app rabbit
patrowl-rabbitmq | 2021-05-10 14:08:05.155 [info] <0.273.0> Running boot step rabbit_alarm defined by app rabbit
patrowl-rabbitmq | 2021-05-10 14:08:05.168 [info] <0.355.0> Memory high watermark set to 1570 MiB (1647240806 bytes) of 3927 MiB (4118102016 bytes) total
patrowl-rabbitmq | 2021-05-10 14:08:05.171 [info] <0.357.0> Enabling free disk space monitoring
patrowl-rabbitmq | 2021-05-10 14:08:05.171 [info] <0.357.0> Disk free limit set to 50MB
patrowl-rabbitmq | 2021-05-10 14:08:05.178 [info] <0.273.0> Running boot step code_server_cache defined by app rabbit
patrowl-rabbitmq | 2021-05-10 14:08:05.179 [info] <0.273.0> Running boot step file_handle_cache defined by app rabbit
patrowl-rabbitmq | 2021-05-10 14:08:05.179 [info] <0.360.0> Limiting to approx 1048479 file handles (943629 sockets)
patrowl-rabbitmq | 2021-05-10 14:08:05.179 [info] <0.361.0> FHC read buffering: OFF
patrowl-rabbitmq | 2021-05-10 14:08:05.179 [info] <0.361.0> FHC write buffering: ON
patrowl-rabbitmq | 2021-05-10 14:08:05.194 [info] <0.273.0> Running boot step worker_pool defined by app rabbit
patrowl-rabbitmq | 2021-05-10 14:08:05.194 [info] <0.347.0> Will use 1 processes for default worker pool
patrowl-rabbitmq | 2021-05-10 14:08:05.194 [info] <0.347.0> Starting worker pool 'worker_pool' with 1 processes in it
patrowl-rabbitmq | 2021-05-10 14:08:05.195 [info] <0.273.0> Running boot step database defined by app rabbit
patrowl-rabbitmq | 2021-05-10 14:08:05.195 [info] <0.273.0> Node database directory at /var/lib/rabbitmq/mnesia/rabbit@e86669c920ed is empty. Assuming we need to join an existing cluster or initialise from scratch...
patrowl-rabbitmq | 2021-05-10 14:08:05.195 [info] <0.273.0> Configured peer discovery backend: rabbit_peer_discovery_classic_config
patrowl-rabbitmq | 2021-05-10 14:08:05.195 [info] <0.273.0> Will try to lock with peer discovery backend rabbit_peer_discovery_classic_config
patrowl-rabbitmq | 2021-05-10 14:08:05.196 [info] <0.273.0> Peer discovery backend does not support locking, falling back to randomized delay
patrowl-rabbitmq | 2021-05-10 14:08:05.196 [info] <0.273.0> Peer discovery backend rabbit_peer_discovery_classic_config does not support registration, skipping randomized startup delay.
patrowl-rabbitmq | 2021-05-10 14:08:05.196 [info] <0.273.0> All discovered existing cluster peers:
patrowl-rabbitmq | 2021-05-10 14:08:05.196 [info] <0.273.0> Discovered no peer nodes to cluster with. Some discovery backends can filter nodes out based on a readiness criteria. Enabling debug logging might help troubleshoot.
patrowl-rabbitmq | 2021-05-10 14:08:05.198 [info] <0.44.0> Application mnesia exited with reason: stopped

```

```

patrowl-rabbitmq | 2021-05-10 14:08:05.198 [info] <0.44.0> Application mnesia exited with reason: stopped
patrowl-rabbitmq | 2021-05-10 14:08:05.243 [info] <0.44.0> Application mnesia started on node rabbit@e86669c920ed
patrowl-rabbitmq | 2021-05-10 14:08:05.329 [info] <0.273.0> Waiting for Mnesia tables for 30000 ms, 9 retries left
patrowl-rabbitmq | 2021-05-10 14:08:05.330 [info] <0.273.0> Successfully synced tables from a peer
patrowl-rabbitmq | 2021-05-10 14:08:05.366 [info] <0.273.0> Waiting for Mnesia tables for 30000 ms, 9 retries left
patrowl-rabbitmq | 2021-05-10 14:08:05.366 [info] <0.273.0> Successfully synced tables from a peer
patrowl-rabbitmq | 2021-05-10 14:08:05.366 [info] <0.273.0> Feature flag `drop_unroutable_metric`: supported, attempt to enable...
patrowl-rabbitmq | 2021-05-10 14:08:05.366 [info] <0.273.0> Feature flag `drop_unroutable_metric`: mark as enabled=state_changing
patrowl-rabbitmq | 2021-05-10 14:08:05.371 [info] <0.273.0> Feature flags: list of feature flags found:
patrowl-rabbitmq | 2021-05-10 14:08:05.373 [info] <0.273.0> Feature flags: [~] drop_unroutable_metric
patrowl-rabbitmq | 2021-05-10 14:08:05.373 [info] <0.273.0> Feature flags: []
empty_basic_get_metric
patrowl-rabbitmq | 2021-05-10 14:08:05.374 [info] <0.273.0> Feature flags: [] implicit_default_bindings
patrowl-rabbitmq | 2021-05-10 14:08:05.374 [info] <0.273.0> Feature flags: [] maintenance_mode_status
patrowl-rabbitmq | 2021-05-10 14:08:05.375 [info] <0.273.0> Feature flags: [] quorum_queue
patrowl-rabbitmq | 2021-05-10 14:08:05.376 [info] <0.273.0> Feature flags: [] user_limits
patrowl-rabbitmq | 2021-05-10 14:08:05.376 [info] <0.273.0> Feature flags: [] virtual_host_metadata
patrowl-rabbitmq | 2021-05-10 14:08:05.376 [info] <0.273.0> Feature flags: feature flag states written to disk: yes
patrowl-rabbitmq | 2021-05-10 14:08:05.400 [info] <0.273.0> Feature flag `drop_unroutable_metric`: mark as enabled=true
patrowl-rabbitmq | 2021-05-10 14:08:05.412 [info] <0.273.0> Feature flags: list of feature flags found:
patrowl-rabbitmq | 2021-05-10 14:08:05.416 [info] <0.273.0> Feature flags: [x] drop_unroutable_metric
patrowl-rabbitmq | 2021-05-10 14:08:05.417 [info] <0.273.0> Feature flags: []
empty_basic_get_metric
patrowl-rabbitmq | 2021-05-10 14:08:05.417 [info] <0.273.0> Feature flags: [] implicit_default_bindings
patrowl-rabbitmq | 2021-05-10 14:08:05.417 [info] <0.273.0> Feature flags: [] maintenance_mode_status
patrowl-rabbitmq | 2021-05-10 14:08:05.417 [info] <0.273.0> Feature flags: [] quorum_queue
patrowl-rabbitmq | 2021-05-10 14:08:05.417 [info] <0.273.0> Feature flags: [] user_limits
patrowl-rabbitmq | 2021-05-10 14:08:05.417 [info] <0.273.0> Feature flags: [] virtual_host_metadata

```

```

patrowl-rabbitmq | 2021-05-10 14:08:05.417 [info] <0.273.0> Feature flags: feature flag states
written to disk: yes
patrowl-rabbitmq | 2021-05-10 14:08:05.441 [info] <0.273.0> Feature flag
`empty_basic_get_metric`: supported, attempt to enable...
patrowl-rabbitmq | 2021-05-10 14:08:05.448 [info] <0.273.0> Feature flag
`empty_basic_get_metric`: mark as enabled=state_changing
patrowl-rabbitmq | 2021-05-10 14:08:05.456 [info] <0.273.0> Feature flags: list of feature flags
found:
patrowl-rabbitmq | 2021-05-10 14:08:05.456 [info] <0.273.0> Feature flags: [x] drop_unrouta-
ble_metric
patrowl-rabbitmq | 2021-05-10 14:08:05.457 [info] <0.273.0> Feature flags: [~]
empty_basic_get_metric
patrowl-rabbitmq | 2021-05-10 14:08:05.457 [info] <0.273.0> Feature flags: [] implicit_de-
fault_bindings
patrowl-rabbitmq | 2021-05-10 14:08:05.457 [info] <0.273.0> Feature flags: [] mainte-
nance_mode_status
patrowl-rabbitmq | 2021-05-10 14:08:05.457 [info] <0.273.0> Feature flags: [] quorum_queue
patrowl-rabbitmq | 2021-05-10 14:08:05.458 [info] <0.273.0> Feature flags: [] user_limits
patrowl-rabbitmq | 2021-05-10 14:08:05.459 [info] <0.273.0> Feature flags: [] vir-
tual_host_metadata
patrowl-rabbitmq | 2021-05-10 14:08:05.459 [info] <0.273.0> Feature flags: feature flag states
written to disk: yes
patrowl-rabbitmq | 2021-05-10 14:08:05.479 [info] <0.273.0> Feature flag
`empty_basic_get_metric`: mark as enabled=true
patrowl-rabbitmq | 2021-05-10 14:08:05.499 [info] <0.273.0> Feature flags: list of feature flags
found:
patrowl-rabbitmq | 2021-05-10 14:08:05.499 [info] <0.273.0> Feature flags: [x] drop_unrouta-
ble_metric
patrowl-rabbitmq | 2021-05-10 14:08:05.499 [info] <0.273.0> Feature flags: [x]
empty_basic_get_metric
patrowl-rabbitmq | 2021-05-10 14:08:05.499 [info] <0.273.0> Feature flags: [] implicit_de-
fault_bindings
patrowl-rabbitmq | 2021-05-10 14:08:05.499 [info] <0.273.0> Feature flags: [] mainte-
nance_mode_status
patrowl-rabbitmq | 2021-05-10 14:08:05.499 [info] <0.273.0> Feature flags: [] quorum_queue
patrowl-rabbitmq | 2021-05-10 14:08:05.500 [info] <0.273.0> Feature flags: [] user_limits
patrowl-rabbitmq | 2021-05-10 14:08:05.500 [info] <0.273.0> Feature flags: [] vir-
tual_host_metadata
patrowl-rabbitmq | 2021-05-10 14:08:05.500 [info] <0.273.0> Feature flags: feature flag states
written to disk: yes
patrowl-rabbitmq | 2021-05-10 14:08:05.519 [info] <0.273.0> Feature flag `implicit_default_bind-
ings`: supported, attempt to enable...
patrowl-rabbitmq | 2021-05-10 14:08:05.526 [info] <0.273.0> Feature flag `implicit_default_bind-
ings`: mark as enabled=state_changing
patrowl-rabbitmq | 2021-05-10 14:08:05.535 [info] <0.273.0> Feature flags: list of feature flags
found:
patrowl-rabbitmq | 2021-05-10 14:08:05.535 [info] <0.273.0> Feature flags: [x] drop_unrouta-
ble_metric

```

patrowl-rabbitmq | 2021-05-10 14:08:05.536 [info] <0.273.0> Feature flags: [x] empty\_basic\_get\_metric

patrowl-rabbitmq | 2021-05-10 14:08:05.537 [info] <0.273.0> Feature flags: [~] implicit\_default\_bindings

patrowl-rabbitmq | 2021-05-10 14:08:05.537 [info] <0.273.0> Feature flags: [] maintenance\_mode\_status

patrowl-rabbitmq | 2021-05-10 14:08:05.537 [info] <0.273.0> Feature flags: [] quorum\_queue

patrowl-rabbitmq | 2021-05-10 14:08:05.537 [info] <0.273.0> Feature flags: [] user\_limits

patrowl-rabbitmq | 2021-05-10 14:08:05.537 [info] <0.273.0> Feature flags: [] virtual\_host\_metadata

patrowl-rabbitmq | 2021-05-10 14:08:05.538 [info] <0.273.0> Feature flags: feature flag states written to disk: yes

patrowl-rabbitmq | 2021-05-10 14:08:05.563 [info] <0.273.0> Waiting for Mnesia tables for 30000 ms, 0 retries left

patrowl-rabbitmq | 2021-05-10 14:08:05.566 [info] <0.273.0> Successfully synced tables from a peer

patrowl-rabbitmq | 2021-05-10 14:08:05.566 [info] <0.273.0> Feature flag `implicit\_default\_bindings`: mark as enabled=true

patrowl-rabbitmq | 2021-05-10 14:08:05.580 [info] <0.273.0> Feature flags: list of feature flags found:

patrowl-rabbitmq | 2021-05-10 14:08:05.580 [info] <0.273.0> Feature flags: [x] drop\_unroutable\_metric

patrowl-rabbitmq | 2021-05-10 14:08:05.581 [info] <0.273.0> Feature flags: [x] empty\_basic\_get\_metric

patrowl-rabbitmq | 2021-05-10 14:08:05.585 [info] <0.273.0> Feature flags: [x] implicit\_default\_bindings

patrowl-rabbitmq | 2021-05-10 14:08:05.585 [info] <0.273.0> Feature flags: [] maintenance\_mode\_status

patrowl-rabbitmq | 2021-05-10 14:08:05.585 [info] <0.273.0> Feature flags: [] quorum\_queue

patrowl-rabbitmq | 2021-05-10 14:08:05.585 [info] <0.273.0> Feature flags: [] user\_limits

patrowl-rabbitmq | 2021-05-10 14:08:05.585 [info] <0.273.0> Feature flags: [] virtual\_host\_metadata

patrowl-rabbitmq | 2021-05-10 14:08:05.585 [info] <0.273.0> Feature flags: feature flag states written to disk: yes

patrowl-rabbitmq | 2021-05-10 14:08:05.604 [info] <0.273.0> Feature flag `maintenance\_mode\_status`: supported, attempt to enable...

patrowl-rabbitmq | 2021-05-10 14:08:05.613 [info] <0.273.0> Feature flag `maintenance\_mode\_status`: mark as enabled=state\_changing

patrowl-rabbitmq | 2021-05-10 14:08:05.619 [info] <0.273.0> Feature flags: list of feature flags found:

patrowl-rabbitmq | 2021-05-10 14:08:05.619 [info] <0.273.0> Feature flags: [x] drop\_unroutable\_metric

patrowl-rabbitmq | 2021-05-10 14:08:05.624 [info] <0.273.0> Feature flags: [x] empty\_basic\_get\_metric

patrowl-rabbitmq | 2021-05-10 14:08:05.625 [info] <0.273.0> Feature flags: [x] implicit\_default\_bindings

patrowl-rabbitmq | 2021-05-10 14:08:05.625 [info] <0.273.0> Feature flags: [~] maintenance\_mode\_status

patrowl-rabbitmq | 2021-05-10 14:08:05.625 [info] <0.273.0> Feature flags: [] quorum\_queue

```

patrowl-rabbitmq | 2021-05-10 14:08:05.625 [info] <0.273.0> Feature flags: [ ] user_limits
patrowl-rabbitmq | 2021-05-10 14:08:05.625 [info] <0.273.0> Feature flags: [ ] virtual_host_metadata
patrowl-rabbitmq | 2021-05-10 14:08:05.625 [info] <0.273.0> Feature flags: feature flag states written to disk: yes
patrowl-rabbitmq | 2021-05-10 14:08:05.648 [info] <0.273.0> Creating table rabbit_node_maintenance_states for feature flag `maintenance_mode_status`
patrowl-rabbitmq | 2021-05-10 14:08:05.677 [info] <0.273.0> Feature flag `maintenance_mode_status`: mark as enabled=true
patrowl-rabbitmq | 2021-05-10 14:08:05.686 [info] <0.273.0> Feature flags: list of feature flags found:
patrowl-rabbitmq | 2021-05-10 14:08:05.687 [info] <0.273.0> Feature flags: [x] drop_unroutable_metric
patrowl-rabbitmq | 2021-05-10 14:08:05.687 [info] <0.273.0> Feature flags: [x] empty_basic_get_metric
patrowl-rabbitmq | 2021-05-10 14:08:05.687 [info] <0.273.0> Feature flags: [x] implicit_default_bindings
patrowl-rabbitmq | 2021-05-10 14:08:05.687 [info] <0.273.0> Feature flags: [x] maintenance_mode_status
patrowl-rabbitmq | 2021-05-10 14:08:05.688 [info] <0.273.0> Feature flags: [ ] quorum_queue
patrowl-rabbitmq | 2021-05-10 14:08:05.688 [info] <0.273.0> Feature flags: [ ] user_limits
patrowl-rabbitmq | 2021-05-10 14:08:05.688 [info] <0.273.0> Feature flags: [ ] virtual_host_metadata
patrowl-rabbitmq | 2021-05-10 14:08:05.688 [info] <0.273.0> Feature flags: feature flag states written to disk: yes
patrowl-rabbitmq | 2021-05-10 14:08:05.708 [info] <0.273.0> Feature flag `quorum_queue`: supported, attempt to enable...
patrowl-rabbitmq | 2021-05-10 14:08:05.716 [info] <0.273.0> Feature flag `quorum_queue`: mark as enabled=state_changing
patrowl-rabbitmq | 2021-05-10 14:08:05.721 [info] <0.273.0> Feature flags: list of feature flags found:
patrowl-rabbitmq | 2021-05-10 14:08:05.721 [info] <0.273.0> Feature flags: [x] drop_unroutable_metric
patrowl-rabbitmq | 2021-05-10 14:08:05.722 [info] <0.273.0> Feature flags: [x] empty_basic_get_metric
patrowl-rabbitmq | 2021-05-10 14:08:05.728 [info] <0.273.0> Feature flags: [x] implicit_default_bindings
patrowl-rabbitmq | 2021-05-10 14:08:05.729 [info] <0.273.0> Feature flags: [x] maintenance_mode_status
patrowl-rabbitmq | 2021-05-10 14:08:05.729 [info] <0.273.0> Feature flags: [~] quorum_queue
patrowl-rabbitmq | 2021-05-10 14:08:05.729 [info] <0.273.0> Feature flags: [ ] user_limits
patrowl-rabbitmq | 2021-05-10 14:08:05.729 [info] <0.273.0> Feature flags: [ ] virtual_host_metadata
patrowl-rabbitmq | 2021-05-10 14:08:05.729 [info] <0.273.0> Feature flags: feature flag states written to disk: yes
patrowl-rabbitmq | 2021-05-10 14:08:05.748 [info] <0.273.0> Waiting for Mnesia tables for 30000 ms, 9 retries left
patrowl-rabbitmq | 2021-05-10 14:08:05.755 [info] <0.273.0> Successfully synced tables from a peer

```



patrowl-rabbitmq | 2021-05-10 14:08:05.755 [info] <0.273.0> Feature flag `quorum\_queue`: migrating Mnesia table rabbit\_queue...

patrowl-rabbitmq | 2021-05-10 14:08:05.773 [info] <0.273.0> Feature flag `quorum\_queue`: migrating Mnesia table rabbit\_durable\_queue...

patrowl-rabbitmq | 2021-05-10 14:08:05.796 [info] <0.273.0> Feature flag `quorum\_queue`: Mnesia tables migration done

patrowl-rabbitmq | 2021-05-10 14:08:05.796 [info] <0.273.0> Feature flag `quorum\_queue`: mark as enabled=true

patrowl-rabbitmq | 2021-05-10 14:08:05.803 [info] <0.273.0> Feature flags: list of feature flags found:

patrowl-rabbitmq | 2021-05-10 14:08:05.805 [info] <0.273.0> Feature flags: [x] drop\_unroutable\_metric

patrowl-rabbitmq | 2021-05-10 14:08:05.806 [info] <0.273.0> Feature flags: [x] empty\_basic\_get\_metric

patrowl-rabbitmq | 2021-05-10 14:08:05.807 [info] <0.273.0> Feature flags: [x] implicit\_default\_bindings

patrowl-rabbitmq | 2021-05-10 14:08:05.807 [info] <0.273.0> Feature flags: [x] maintenance\_mode\_status

patrowl-rabbitmq | 2021-05-10 14:08:05.807 [info] <0.273.0> Feature flags: [x] quorum\_queue

patrowl-rabbitmq | 2021-05-10 14:08:05.807 [info] <0.273.0> Feature flags: [ ] user\_limits

patrowl-rabbitmq | 2021-05-10 14:08:05.808 [info] <0.273.0> Feature flags: [ ] virtual\_host\_metadata

patrowl-rabbitmq | 2021-05-10 14:08:05.808 [info] <0.273.0> Feature flags: feature flag states written to disk: yes

patrowl-rabbitmq | 2021-05-10 14:08:05.829 [info] <0.273.0> Feature flag `user\_limits`: supported, attempt to enable...

patrowl-rabbitmq | 2021-05-10 14:08:05.836 [info] <0.273.0> Feature flag `user\_limits`: mark as enabled=state\_changing

patrowl-rabbitmq | 2021-05-10 14:08:05.847 [info] <0.273.0> Feature flags: list of feature flags found:

patrowl-rabbitmq | 2021-05-10 14:08:05.847 [info] <0.273.0> Feature flags: [x] drop\_unroutable\_metric

patrowl-rabbitmq | 2021-05-10 14:08:05.847 [info] <0.273.0> Feature flags: [x] empty\_basic\_get\_metric

patrowl-rabbitmq | 2021-05-10 14:08:05.847 [info] <0.273.0> Feature flags: [x] implicit\_default\_bindings

patrowl-rabbitmq | 2021-05-10 14:08:05.847 [info] <0.273.0> Feature flags: [x] maintenance\_mode\_status

patrowl-rabbitmq | 2021-05-10 14:08:05.847 [info] <0.273.0> Feature flags: [x] quorum\_queue

patrowl-rabbitmq | 2021-05-10 14:08:05.848 [info] <0.273.0> Feature flags: [~] user\_limits

patrowl-rabbitmq | 2021-05-10 14:08:05.848 [info] <0.273.0> Feature flags: [ ] virtual\_host\_metadata

patrowl-rabbitmq | 2021-05-10 14:08:05.848 [info] <0.273.0> Feature flags: feature flag states written to disk: yes

patrowl-rabbitmq | 2021-05-10 14:08:05.870 [info] <0.273.0> Waiting for Mnesia tables for 30000 ms, 9 retries left

patrowl-rabbitmq | 2021-05-10 14:08:05.873 [info] <0.273.0> Successfully synced tables from a peer

```

patrowl-rabbitmq | 2021-05-10 14:08:05.891 [info] <0.273.0> Feature flag `user_limits`: mark as
enabled=true
patrowl-rabbitmq | 2021-05-10 14:08:05.899 [info] <0.273.0> Feature flags: list of feature flags
found:
patrowl-rabbitmq | 2021-05-10 14:08:05.904 [info] <0.273.0> Feature flags: [x] drop_unrou-
table_metric
patrowl-rabbitmq | 2021-05-10 14:08:05.905 [info] <0.273.0> Feature flags: [x]
empty_basic_get_metric
patrowl-rabbitmq | 2021-05-10 14:08:05.905 [info] <0.273.0> Feature flags: [x] implicit_de-
fault_bindings
patrowl-rabbitmq | 2021-05-10 14:08:05.905 [info] <0.273.0> Feature flags: [x] mainte-
nance_mode_status
patrowl-rabbitmq | 2021-05-10 14:08:05.905 [info] <0.273.0> Feature flags: [x] quorum_queue
patrowl-rabbitmq | 2021-05-10 14:08:05.905 [info] <0.273.0> Feature flags: [x] user_limits
patrowl-rabbitmq | 2021-05-10 14:08:05.906 [info] <0.273.0> Feature flags: [ ] vir-
tual_host_metadata
patrowl-rabbitmq | 2021-05-10 14:08:05.906 [info] <0.273.0> Feature flags: feature flag states
written to disk: yes
patrowl-rabbitmq | 2021-05-10 14:08:05.923 [info] <0.273.0> Feature flag `vir-
tual_host_metadata`: supported, attempt to enable...
patrowl-rabbitmq | 2021-05-10 14:08:05.934 [info] <0.273.0> Feature flag `vir-
tual_host_metadata`: mark as enabled=state_changing
patrowl-rabbitmq | 2021-05-10 14:08:05.940 [info] <0.273.0> Feature flags: list of feature flags
found:
patrowl-rabbitmq | 2021-05-10 14:08:05.944 [info] <0.273.0> Feature flags: [x] drop_unrou-
table_metric
patrowl-rabbitmq | 2021-05-10 14:08:05.945 [info] <0.273.0> Feature flags: [x]
empty_basic_get_metric
patrowl-rabbitmq | 2021-05-10 14:08:05.945 [info] <0.273.0> Feature flags: [x] implicit_de-
fault_bindings
patrowl-rabbitmq | 2021-05-10 14:08:05.945 [info] <0.273.0> Feature flags: [x] mainte-
nance_mode_status
patrowl-rabbitmq | 2021-05-10 14:08:05.945 [info] <0.273.0> Feature flags: [x] quorum_queue
patrowl-rabbitmq | 2021-05-10 14:08:05.945 [info] <0.273.0> Feature flags: [x] user_limits
patrowl-rabbitmq | 2021-05-10 14:08:05.945 [info] <0.273.0> Feature flags: [~] vir-
tual_host_metadata
patrowl-rabbitmq | 2021-05-10 14:08:05.945 [info] <0.273.0> Feature flags: feature flag states
written to disk: yes
patrowl-rabbitmq | 2021-05-10 14:08:05.968 [info] <0.273.0> Waiting for Mnesia tables for 30000
ms, 9 retries left
patrowl-rabbitmq | 2021-05-10 14:08:05.971 [info] <0.273.0> Successfully synced tables from a
peer
patrowl-django | ./docker-entrypoint.with-engines.sh: connect: Connection refused
patrowl-django | ./docker-entrypoint.with-engines.sh: line 12: /dev/tcp/rabbitmq/5672: Connec-
tion refused
patrowl-rabbitmq | 2021-05-10 14:08:05.998 [info] <0.273.0> Feature flag `vir-
tual_host_metadata`: mark as enabled=true
patrowl-rabbitmq | 2021-05-10 14:08:06.007 [info] <0.273.0> Feature flags: list of feature flags
found:

```

patrowl-rabbitmq | 2021-05-10 14:08:06.011 [info] <0.273.0> Feature flags: [x] drop\_unrouteable\_metric

patrowl-rabbitmq | 2021-05-10 14:08:06.011 [info] <0.273.0> Feature flags: [x] empty\_basic\_get\_metric

patrowl-rabbitmq | 2021-05-10 14:08:06.011 [info] <0.273.0> Feature flags: [x] implicit\_default\_bindings

patrowl-rabbitmq | 2021-05-10 14:08:06.011 [info] <0.273.0> Feature flags: [x] maintenance\_mode\_status

patrowl-rabbitmq | 2021-05-10 14:08:06.011 [info] <0.273.0> Feature flags: [x] quorum\_queue

patrowl-rabbitmq | 2021-05-10 14:08:06.012 [info] <0.273.0> Feature flags: [x] user\_limits

patrowl-rabbitmq | 2021-05-10 14:08:06.012 [info] <0.273.0> Feature flags: [x] virtual\_host\_metadata

patrowl-rabbitmq | 2021-05-10 14:08:06.012 [info] <0.273.0> Feature flags: feature flag states written to disk: yes

patrowl-rabbitmq | 2021-05-10 14:08:06.033 [info] <0.273.0> Waiting for Mnesia tables for 30000 ms, 9 retries left

patrowl-rabbitmq | 2021-05-10 14:08:06.036 [info] <0.273.0> Successfully synced tables from a peer

patrowl-rabbitmq | 2021-05-10 14:08:06.066 [info] <0.273.0> Waiting for Mnesia tables for 30000 ms, 9 retries left

patrowl-rabbitmq | 2021-05-10 14:08:06.067 [info] <0.273.0> Successfully synced tables from a peer

patrowl-rabbitmq | 2021-05-10 14:08:06.067 [info] <0.273.0> Peer discovery backend rabbit\_peer\_discovery\_classic\_config does not support registration, skipping registration.

patrowl-rabbitmq | 2021-05-10 14:08:06.068 [info] <0.273.0> Running boot step database\_sync defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.068 [info] <0.273.0> Running boot step feature\_flags defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.068 [info] <0.273.0> Running boot step codec\_correctness\_check defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.069 [info] <0.273.0> Running boot step external\_infrastructure defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.069 [info] <0.273.0> Running boot step rabbit\_registry defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.070 [info] <0.273.0> Running boot step rabbit\_auth\_mechanism\_cr\_demo defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.073 [info] <0.273.0> Running boot step rabbit\_queue\_location\_random defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.073 [info] <0.273.0> Running boot step rabbit\_event defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.074 [info] <0.273.0> Running boot step rabbit\_auth\_mechanism\_amqplain defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.074 [info] <0.273.0> Running boot step rabbit\_auth\_mechanism\_plain defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.074 [info] <0.273.0> Running boot step rabbit\_exchange\_type\_direct defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.075 [info] <0.273.0> Running boot step rabbit\_exchange\_type\_fanout defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.075 [info] <0.273.0> Running boot step rabbit\_exchange\_type\_headers defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.076 [info] <0.273.0> Running boot step rabbit\_exchange\_type\_topic defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.076 [info] <0.273.0> Running boot step rabbit\_mirror\_queue\_mode\_all defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.077 [info] <0.273.0> Running boot step rabbit\_mirror\_queue\_mode\_exactly defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.077 [info] <0.273.0> Running boot step rabbit\_mirror\_queue\_mode\_nodes defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.078 [info] <0.273.0> Running boot step rabbit\_priority\_queue defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.080 [info] <0.273.0> Priority queues enabled, real BQ is rabbit\_variable\_queue

patrowl-rabbitmq | 2021-05-10 14:08:06.080 [info] <0.273.0> Running boot step rabbit\_queue\_location\_client\_local defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.081 [info] <0.273.0> Running boot step rabbit\_queue\_location\_min\_masters defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.081 [info] <0.273.0> Running boot step kernel\_ready defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.081 [info] <0.273.0> Running boot step rabbit\_sysmon\_minder defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.081 [info] <0.273.0> Running boot step rabbit\_epmd\_monitor defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.082 [info] <0.617.0> epmd monitor knows us, inter-node communication (distribution) port: 25672

patrowl-rabbitmq | 2021-05-10 14:08:06.082 [info] <0.273.0> Running boot step guid\_generator defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.097 [info] <0.273.0> Running boot step rabbit\_node\_monitor defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.097 [info] <0.621.0> Starting rabbit\_node\_monitor

patrowl-rabbitmq | 2021-05-10 14:08:06.098 [info] <0.273.0> Running boot step delegate\_sup defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.099 [info] <0.273.0> Running boot step rabbit\_memory\_monitor defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.099 [info] <0.273.0> Running boot step core\_initialized defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.099 [info] <0.273.0> Running boot step upgrade\_queues defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.128 [info] <0.273.0> message\_store upgrades: 1 to apply

patrowl-rabbitmq | 2021-05-10 14:08:06.128 [info] <0.273.0> message\_store upgrades: Applying rabbit\_variable\_queue:move\_messages\_to\_vhost\_store

patrowl-rabbitmq | 2021-05-10 14:08:06.128 [info] <0.273.0> message\_store upgrades: No durable queues found. Skipping message store migration

patrowl-rabbitmq | 2021-05-10 14:08:06.128 [info] <0.273.0> message\_store upgrades: Removing the old message store data

patrowl-rabbitmq | 2021-05-10 14:08:06.130 [info] <0.273.0> message\_store upgrades: All upgrades applied successfully

patrowl-rabbitmq | 2021-05-10 14:08:06.157 [info] <0.273.0> Running boot step channel\_tracking defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.165 [info] <0.273.0> Setting up a table for channel tracking on this node: tracked\_channel\_on\_node\_rabbit@e86669c920ed

patrowl-rabbitmq | 2021-05-10 14:08:06.171 [info] <0.273.0> Setting up a table for channel tracking on this node: tracked\_channel\_table\_per\_user\_on\_node\_rabbit@e86669c920ed

patrowl-rabbitmq | 2021-05-10 14:08:06.171 [info] <0.273.0> Running boot step rabbit\_channel\_tracking\_handler defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.171 [info] <0.273.0> Running boot step connection\_tracking defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.175 [info] <0.273.0> Setting up a table for connection tracking on this node: tracked\_connection\_on\_node\_rabbit@e86669c920ed

patrowl-rabbitmq | 2021-05-10 14:08:06.178 [info] <0.273.0> Setting up a table for per-vhost connection counting on this node: tracked\_connection\_per\_vhost\_on\_node\_rabbit@e86669c920ed

patrowl-rabbitmq | 2021-05-10 14:08:06.184 [info] <0.273.0> Setting up a table for per-user connection counting on this node: tracked\_connection\_table\_per\_user\_on\_node\_rabbit@e86669c920ed

patrowl-rabbitmq | 2021-05-10 14:08:06.184 [info] <0.273.0> Running boot step rabbit\_connection\_tracking\_handler defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.184 [info] <0.273.0> Running boot step rabbit\_exchange\_parameters defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.185 [info] <0.273.0> Running boot step rabbit\_mirror\_queue\_misc defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.185 [info] <0.273.0> Running boot step rabbit\_policies defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.186 [info] <0.273.0> Running boot step rabbit\_policy defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.186 [info] <0.273.0> Running boot step rabbit\_queue\_location\_validator defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.186 [info] <0.273.0> Running boot step rabbit\_quorum\_memory\_manager defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.187 [info] <0.273.0> Running boot step rabbit\_vhost\_limit defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.187 [info] <0.273.0> Running boot step rabbit\_mgmt\_db\_handler defined by app rabbitmq\_management\_agent

patrowl-rabbitmq | 2021-05-10 14:08:06.187 [info] <0.273.0> Management plugin: using rates mode 'basic'

patrowl-rabbitmq | 2021-05-10 14:08:06.188 [info] <0.273.0> Running boot step recovery defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.189 [info] <0.273.0> Running boot step empty\_db\_check defined by app rabbit

patrowl-rabbitmq | 2021-05-10 14:08:06.189 [info] <0.273.0> Will seed default virtual host and user...

patrowl-rabbitmq | 2021-05-10 14:08:06.190 [info] <0.273.0> Adding vhost '/' (description: 'Default virtual host', tags: [])

patrowl-rabbitmq | 2021-05-10 14:08:06.204 [info] <0.680.0> Making sure data directory '/var/lib/rabbitmq/mnesia/rabbit@e86669c920ed/msg\_stores/vhosts/628WB79CIFYO9LJI6DKMI09L' for vhost '/' exists

```

patrowl-rabbitmq | 2021-05-10 14:08:06.208 [info] <0.680.0> Starting message stores for vhost '/'
patrowl-rabbitmq | 2021-05-10 14:08:06.209 [info] <0.684.0> Message store
"628WB79CIFDYO9LJI6DKMI09L/msg_store_transient": using rabbit_msg_store_ets_index to provide index
patrowl-rabbitmq | 2021-05-10 14:08:06.211 [info] <0.680.0> Started message store of type transient for vhost '/'
patrowl-rabbitmq | 2021-05-10 14:08:06.211 [info] <0.688.0> Message store
"628WB79CIFDYO9LJI6DKMI09L/msg_store_persistent": using rabbit_msg_store_ets_index to provide index
patrowl-rabbitmq | 2021-05-10 14:08:06.212 [warning] <0.688.0> Message store
"628WB79CIFDYO9LJI6DKMI09L/msg_store_persistent": rebuilding indices from scratch
patrowl-rabbitmq | 2021-05-10 14:08:06.213 [info] <0.680.0> Started message store of type persistent for vhost '/'
patrowl-rabbitmq | 2021-05-10 14:08:06.227 [info] <0.273.0> Created user 'guest'
patrowl-rabbitmq | 2021-05-10 14:08:06.229 [info] <0.273.0> Successfully set user tags for user 'guest' to [administrator]
patrowl-rabbitmq | 2021-05-10 14:08:06.230 [info] <0.273.0> Successfully set permissions for 'guest' in virtual host '/' to '.*', '.*', '.*'
patrowl-rabbitmq | 2021-05-10 14:08:06.230 [info] <0.273.0> Running boot step rabbit_looking_glass defined by app rabbit
patrowl-rabbitmq | 2021-05-10 14:08:06.230 [info] <0.273.0> Running boot step rabbit_core_metrics_gc defined by app rabbit
patrowl-rabbitmq | 2021-05-10 14:08:06.230 [info] <0.273.0> Running boot step background_gc defined by app rabbit
patrowl-rabbitmq | 2021-05-10 14:08:06.231 [info] <0.273.0> Running boot step routing_ready defined by app rabbit
patrowl-rabbitmq | 2021-05-10 14:08:06.231 [info] <0.273.0> Running boot step pre_flight defined by app rabbit
patrowl-rabbitmq | 2021-05-10 14:08:06.231 [info] <0.273.0> Running boot step notify_cluster defined by app rabbit
patrowl-rabbitmq | 2021-05-10 14:08:06.231 [info] <0.273.0> Running boot step networking defined by app rabbit
patrowl-rabbitmq | 2021-05-10 14:08:06.231 [info] <0.273.0> Running boot step definition_import_worker_pool defined by app rabbit
patrowl-rabbitmq | 2021-05-10 14:08:06.232 [info] <0.347.0> Starting worker pool 'definition_import_pool' with 1 processes in it
patrowl-rabbitmq | 2021-05-10 14:08:06.232 [info] <0.273.0> Running boot step cluster_name defined by app rabbit
patrowl-rabbitmq | 2021-05-10 14:08:06.233 [info] <0.273.0> Initialising internal cluster ID to 'rabbitmq-cluster-id-NqF5fr6ArfBHOo3WlOrY_g'
patrowl-rabbitmq | 2021-05-10 14:08:06.234 [info] <0.273.0> Running boot step direct_client defined by app rabbit
patrowl-rabbitmq | 2021-05-10 14:08:06.234 [info] <0.718.0> Resetting node maintenance status
patrowl-rabbitmq | 2021-05-10 14:08:06.235 [info] <0.44.0> Application rabbit started on node rabbit@e86669c920ed
patrowl-rabbitmq | 2021-05-10 14:08:06.235 [info] <0.44.0> Application cowlib started on node rabbit@e86669c920ed
patrowl-rabbitmq | 2021-05-10 14:08:06.235 [info] <0.44.0> Application cowboy started on node rabbit@e86669c920ed

```

```

patrowl-rabbitmq | 2021-05-10 14:08:06.237 [info] <0.44.0> Application rabbitmq_management_agent started on node rabbit@e86669c920ed
patrowl-rabbitmq | 2021-05-10 14:08:06.265 [info] <0.44.0> Application prometheus started on node rabbit@e86669c920ed
patrowl-rabbitmq | 2021-05-10 14:08:06.265 [info] <0.44.0> Application rabbitmq_web_dispatch started on node rabbit@e86669c920ed
patrowl-rabbitmq | 2021-05-10 14:08:06.271 [info] <0.744.0> Prometheus metrics: HTTP (non-TLS) listener started on port 15692
patrowl-rabbitmq | 2021-05-10 14:08:06.272 [info] <0.718.0> Ready to start client connection listeners
patrowl-rabbitmq | 2021-05-10 14:08:06.272 [info] <0.44.0> Application rabbitmq_prometheus started on node rabbit@e86669c920ed
patrowl-rabbitmq | 2021-05-10 14:08:06.276 [info] <0.788.0> started TCP listener on [::]:5672
patrowl-rabbitmq | 2021-05-10 14:08:06.690 [info] <0.718.0> Server startup complete; 3 plugins started.
patrowl-rabbitmq | * rabbitmq_prometheus
patrowl-rabbitmq | * rabbitmq_web_dispatch
patrowl-rabbitmq | * rabbitmq_management_agent
patrowl-rabbitmq | completed with 3 plugins.
patrowl-rabbitmq | 2021-05-10 14:08:06.691 [info] <0.718.0> Resetting node maintenance status
patrowl-rabbitmq | 2021-05-10 14:08:06.983 [info] <0.793.0> Closing all channels from connection '172.18.0.7:45734 -> 172.18.0.3:5672' because it has been closed
patrowl-django | [+] PatrowlManager version
patrowl-django | 1.6.15 // Community Edition
patrowl-django | [+] Collect static files
patrowl-django |
patrowl-django | 254 static files copied to '/opt/patrowl-manager/staticfiles'.
patrowl-django | [+] Update DB schema (if already created)
patrowl-django | -- Migrate django_celery_beat
patrowl-django | Operations to perform:
patrowl-django | Apply all migrations: django_celery_beat
patrowl-django | Running migrations:
patrowl-django | Applying django_celery_beat.0001_initial... OK
patrowl-django | Applying django_celery_beat.0002_auto_20161118_0346... OK
patrowl-django | Applying django_celery_beat.0003_auto_20161209_0049... OK
patrowl-django | Applying django_celery_beat.0004_auto_20170221_0000... OK
patrowl-django | Applying django_celery_beat.0005_add_solarschedule_events_choices... OK
patrowl-django | Applying django_celery_beat.0006_auto_20180322_0932... OK
patrowl-django | Applying django_celery_beat.0007_auto_20180521_0826... OK
patrowl-django | Applying django_celery_beat.0008_auto_20180914_1922... OK
patrowl-django | Applying django_celery_beat.0006_auto_20180210_1226... OK
patrowl-django | Applying django_celery_beat.0006_periodictask_priority... OK
patrowl-django | Applying django_celery_beat.0009_periodictask_headers... OK
patrowl-django | Applying django_celery_beat.0010_auto_20190429_0326... OK
patrowl-django | Applying django_celery_beat.0011_auto_20190508_0153... OK
patrowl-django | Applying django_celery_beat.0012_periodictask_expire_seconds... OK
patrowl-django | -- Installed tables:

```

```

patrowl-django | ['django_celery_beat_clockedschedule', 'django_celery_beat_crontabsched-
ule', 'django_celery_beat_intervalschedule', 'django_celery_beat_periodictask', 'django_cel-
ery_beat_periodictasks', 'django_celery_beat_solarschedule', 'django_migrations']
patrowl-django | [+] Make database migrations
patrowl-django | - scans
patrowl-django | No changes detected in app 'scans'
patrowl-django | - findings
patrowl-django | No changes detected in app 'findings'
patrowl-django | - events
patrowl-django | No changes detected in app 'events'
patrowl-django | - ... and all the rest
patrowl-django | No changes detected
patrowl-django | [+] Apply database migrations
patrowl-django | Operations to perform:
patrowl-django | Apply all migrations: admin, assets, auth, authtoken, contenttypes,
django_celery_beat, django_celery_results, engines, events, findings, organizations, rules, scans,
sessions, settings, users
patrowl-django | Running migrations:
patrowl-django | Applying contenttypes.0001_initial... OK
patrowl-django | Applying auth.0001_initial... OK
patrowl-django | Applying admin.0001_initial... OK
patrowl-django | Applying admin.0002_logentry_remove_auto_add... OK
patrowl-django | Applying admin.0003_logentry_add_action_flag_choices... OK
patrowl-django | Applying users.0001_initial... OK
patrowl-django | Applying users.0002_auto_20200616_1704... OK
patrowl-django | Applying assets.0001_initial... OK
patrowl-django | Applying assets.0002_auto_20200616_1735... OK
patrowl-django | Applying assets.0003_asset_owner... OK
patrowl-django | Applying assets.0004_auto_20200617_0958... OK
patrowl-django | Applying assets.0005_auto_20200617_1011... OK
patrowl-django | Applying assets.0006_assetgroup_teams... OK
patrowl-django | Applying assets.0007_auto_20200709_0007... OK
patrowl-django | Applying assets.0008_asset_exposure... OK
patrowl-django | Applying assets.0009_auto_20200921_1151... OK
patrowl-django | Applying assets.0010_auto_20210402_1439... OK
patrowl-django | Applying contenttypes.0002_remove_content_type_name... OK
patrowl-django | Applying auth.0002_alter_permission_name_max_length... OK
patrowl-django | Applying auth.0003_alter_user_email_max_length... OK
patrowl-django | Applying auth.0004_alter_user_username_opts... OK
patrowl-django | Applying auth.0005_alter_user_last_login_null... OK
patrowl-django | Applying auth.0006_require_contenttypes_0002... OK
patrowl-django | Applying auth.0007_alter_validators_add_error_messages... OK
patrowl-django | Applying auth.0008_alter_user_username_max_length... OK
patrowl-django | Applying auth.0009_alter_user_last_name_max_length... OK
patrowl-django | Applying auth.0010_alter_group_name_max_length... OK
patrowl-django | Applying auth.0011_update_proxy_permissions... OK
patrowl-django | Applying authtoken.0001_initial... OK
patrowl-django | Applying authtoken.0002_auto_20160226_1747... OK
patrowl-django | Applying authtoken.0003_tokenproxy... OK

```



```

patrowl-django | Applying django_celery_results.0001_initial... OK
patrowl-django | Applying django_celery_results.0002_add_task_name_args_kwargs... OK
patrowl-django | Applying django_celery_results.0003_auto_20181106_1101... OK
patrowl-django | Applying django_celery_results.0004_auto_20190516_0412... OK
patrowl-django | Applying engines.0001_initial... OK
patrowl-django | Applying users.0003_auto_20200624_0037... OK
patrowl-django | Applying users.0004_remove_profile_role... OK
patrowl-django | Applying scans.0001_initial... OK
patrowl-django | Applying findings.0001_initial... OK
patrowl-django | Applying events.0001_initial... OK
patrowl-django | Applying events.0002_alert... OK
patrowl-django | Applying events.0003_alert_metadata... OK
patrowl-django | Applying events.0004_auto_20200602_1813... OK
patrowl-django | Applying events.0005_auto_20200616_1631... OK
patrowl-django | Applying events.0006_auto_20200624_0923... OK
patrowl-django | Applying events.0007_auditlog... OK
patrowl-django | Applying events.0008_auditlog_owner_username... OK
patrowl-django | Applying events.0009_auditlog_type... OK
patrowl-django | Applying events.0010_auditlog_metadata... OK
patrowl-django | Applying events.0011_auto_20200723_1528... OK
patrowl-django | Applying findings.0002_auto_20200306_0822... OK
patrowl-django | Applying findings.0003_auto_20200602_2323... OK
patrowl-django | Applying findings.0004_auto_20200709_0024... OK
patrowl-django | Applying findings.0005_auto_20200709_0910... OK
patrowl-django | Applying findings.0006_auto_20200720_1829... OK
patrowl-django | Applying findings.0007_auto_20210113_1644... OK
patrowl-django | Applying organizations.0001_initial... OK
patrowl-django | Applying organizations.0002_model_update... OK
patrowl-django | Applying organizations.0003_field_fix_and_editable... OK
patrowl-django | Applying rules.0001_initial... OK
patrowl-django | Applying rules.0002_auto_20200720_1829... OK
patrowl-django | Applying rules.0003_auto_20210113_1644... OK
patrowl-django | Applying scans.0002_scandefinition_teams... OK
patrowl-django | Applying scans.0003_scanjob... OK
patrowl-django | Applying scans.0004_auto_20201202_1448... OK
patrowl-django | Applying scans.0005_auto_20201202_1909... OK
patrowl-django | Applying scans.0006_scandefinition_taggroups_list... OK
patrowl-django | Applying sessions.0001_initial... OK
patrowl-django | Applying settings.0001_initial... OK
patrowl-django | Applying users.0005_profile_is_delegated... OK
patrowl-django | [+] Create the default admin user (if needed)
patrowl-django | [+] Create default team if needed
patrowl-django | [+] Populate the db with default data
patrowl-django | Installed 35 object(s) from 1 fixture(s)
patrowl-django | Installed 29 object(s) from 1 fixture(s)
patrowl-django | Installed 8 object(s) from 1 fixture(s)
patrowl-django | Traceback (most recent call last):
patrowl-django | File "/opt/patrowl-manager/env3/lib/python3.7/site-pack-
ages/django/db/models/fields/__init__.py", line 1375, in to_python

```

```

patrowl-django | parsed = parse_datetime(value)
patrowl-django | File "/opt/patrowl-manager/env3/lib/python3.7/site-pack-
ages/django/utils/dateparse.py", line 121, in parse_datetime
patrowl-django | return datetime.datetime(**kw)
patrowl-django | ValueError: month must be in 1..12
patrowl-django |
patrowl-django | During handling of the above exception, another exception occurred:
patrowl-django |
patrowl-django | Traceback (most recent call last):
patrowl-django | File "/opt/patrowl-manager/env3/lib/python3.7/site-pack-
ages/django/core/serializers/python.py", line 143, in Deserializer
patrowl-django | data[field.name] = field.to_python(field_value)
patrowl-django | File "/opt/patrowl-manager/env3/lib/python3.7/site-pack-
ages/django/db/models/fields/__init__.py", line 1382, in to_python
patrowl-django | params={'value': value},
patrowl-django | django.core.exceptions.ValidationError: ["'2021-28-12T11:30:12.503Z' value
has the correct format (YYYY-MM-DD HH:MM[:ss[.uuuuuu]][TZ]) but it is an invalid date/time."]
patrowl-django |
patrowl-django | During handling of the above exception, another exception occurred:
patrowl-django |
patrowl-django | Traceback (most recent call last):
patrowl-django | File "manage.py", line 22, in <module>
patrowl-django | execute_from_command_line(sys.argv)
patrowl-django | File "/opt/patrowl-manager/env3/lib/python3.7/site-pack-
ages/django/core/management/__init__.py", line 381, in execute_from_command_line
patrowl-django | utility.execute()
patrowl-django | File "/opt/patrowl-manager/env3/lib/python3.7/site-pack-
ages/django/core/management/__init__.py", line 375, in execute
patrowl-django | self.fetch_command(subcommand).run_from_argv(self.argv)
patrowl-django | File "/opt/patrowl-manager/env3/lib/python3.7/site-pack-
ages/django/core/management/base.py", line 323, in run_from_argv
patrowl-django | self.execute(*args, **cmd_options)
patrowl-django | File "/opt/patrowl-manager/env3/lib/python3.7/site-pack-
ages/django/core/management/base.py", line 364, in execute
patrowl-django | output = self.handle(*args, **options)
patrowl-django | File "/opt/patrowl-manager/env3/lib/python3.7/site-pack-
ages/django/core/management/commands/loaddata.py", line 72, in handle
patrowl-django | self.loaddata(fixture_labels)
patrowl-django | File "/opt/patrowl-manager/env3/lib/python3.7/site-pack-
ages/django/core/management/commands/loaddata.py", line 114, in loaddata
patrowl-django | self.load_label(fixture_label)
patrowl-django | File "/opt/patrowl-manager/env3/lib/python3.7/site-pack-
ages/django/core/management/commands/loaddata.py", line 172, in load_label
patrowl-django | for obj in objects:
patrowl-django | File "/opt/patrowl-manager/env3/lib/python3.7/site-pack-
ages/django/core/serializers/json.py", line 69, in Deserializer
patrowl-django | yield from PythonDeserializer(objects, **options)
patrowl-django | File "/opt/patrowl-manager/env3/lib/python3.7/site-pack-
ages/django/core/serializers/python.py", line 145, in Deserializer

```

```

patrowl-django | raise base.DeserializationError.WithData(e, d['model'], d.get('pk'),
field_value)
patrowl-django | django.core.serializers.base.DeserializationError: Problem installing fixture
'/opt/patrowl-manager/var/data/engines.EnginePolicy.json': [""2021-28-12T11:30:12.503Z" value
has the correct format (YYYY-MM-DD HH:MM[:ss[.uuuuuu]][TZ]) but it is an invalid date/time."]:
(engines.enginepolicy:pk=75) field_value was '2021-28-12T11:30:12.503Z'
patrowl-django | [+] Configure the engines nmap, sslscan and owl_dns
patrowl-django | [+] Start Supervisor (Celery workers)
patrowl-django | [+] Starting server
patrowl-django | [2021-05-10 14:08:44 +0000] [125] [INFO] Starting gunicorn 20.0.4
patrowl-django | [2021-05-10 14:08:44 +0000] [125] [INFO] Listening at: http://0.0.0.0:8003
(125)
patrowl-django | [2021-05-10 14:08:44 +0000] [125] [INFO] Using worker: sync
patrowl-django | [2021-05-10 14:08:44 +0000] [128] [INFO] Booting worker with pid: 128
patrowl-rabbitmq | 2021-05-10 14:08:50.414 [info] <0.852.0> Closing all channels from connec-
tion '172.18.0.7:45778 -> 172.18.0.3:5672' because it has been closed
patrowl-rabbitmq | 2021-05-10 14:08:50.414 [info] <0.810.0> supervisor: {<0.810.0>,rabbit_chan-
nel_sup_sup}, errorContext: shutdown_error, reason: shutdown, offender: [{nb_chil-
dren,1},{id,channel_sup},{mfargs,{rabbit_channel_sup,start_link,[]}},{restart_type,tempo-
rary},{shutdown,infinity},{child_type,supervisor}}]
patrowl-rabbitmq | 2021-05-10 14:08:50.415 [error] <0.810.0> Supervisor {<0.810.0>,rab-
bit_channel_sup_sup} had child channel_sup started with rabbit_channel_sup:start_link() at unde-
fined exit with reason shutdown in context shutdown_error
patrowl-rabbitmq | 2021-05-10 14:08:50.418 [info] <0.859.0> Closing all channels from connec-
tion '172.18.0.7:45780 -> 172.18.0.3:5672' because it has been closed
patrowl-rabbitmq | 2021-05-10 14:08:50.418 [info] <0.822.0> supervisor: {<0.822.0>,rabbit_chan-
nel_sup_sup}, errorContext: shutdown_error, reason: shutdown, offender: [{nb_chil-
dren,1},{id,channel_sup},{mfargs,{rabbit_channel_sup,start_link,[]}},{restart_type,tempo-
rary},{shutdown,infinity},{child_type,supervisor}}]
patrowl-rabbitmq | 2021-05-10 14:08:50.419 [error] <0.822.0> Supervisor {<0.822.0>,rab-
bit_channel_sup_sup} had child channel_sup started with rabbit_channel_sup:start_link() at unde-
fined exit with reason shutdown in context shutdown_error
patrowl-rabbitmq | 2021-05-10 14:08:50.816 [info] <0.866.0> Closing all channels from connec-
tion '172.18.0.7:45776 -> 172.18.0.3:5672' because it has been closed

```

### Liite 3. PatrOwlManager ja PatrOwlEngines erilliset asennukset



PatrOwlManager  
install.txt

```

z@z:~$ git clone https://github.com/Patrowl/PatrowlManager.git
Cloning into 'PatrowlManager'...
remote: Enumerating objects: 4309, done.
remote: Counting objects: 100% (127/127), done.
remote: Compressing objects: 100% (84/84), done.
remote: Total 4309 (delta 64), reused 67 (delta 40), pack-reused 4182
Receiving objects: 100% (4309/4309), 2.16 MiB | 2.90 MiB/s, done.
Resolving deltas: 100% (3158/3158), done.
z@z:~$ cd PatrowlManager
z@z:~/PatrowlManager$ docker-compose build --force-rm
rabbitmq uses an image, skipping
db uses an image, skipping
nginx uses an image, skipping
Building web
Sending build context to Docker daemon 7.237MB
Step 1/14 : FROM python:3.7-slim
3.7-slim: Pulling from library/python
f7ec5a41d630: Pull complete
6f318b7b4c32: Pull complete
af3fa3eb7bae: Pull complete
4e08e182f49d: Pull complete
16277d8ed69c: Pull complete
Digest: sha256:857dfa69e667f8c5762fbc6d89b0f17072b0c1c2dfd3643c122c0ea98f41cede
Status: Downloaded newer image for python:3.7-slim
---> e7d86653f62f
Step 2/14 : MAINTAINER Patrowl.io "getsupport@patrowl.io"
---> Running in 7b14ce2bba4f
Removing intermediate container 7b14ce2bba4f
---> c529612bb288
Step 3/14 : LABEL Name="PatrowlManager" Version="1.6.16"
---> Running in 607c67346620
Removing intermediate container 607c67346620
---> d87a8c291810
Step 4/14 : ENV PYTHONUNBUFFERED 1
---> Running in b57de671acd7
Removing intermediate container b57de671acd7
---> 59dfab37627b
Step 5/14 : RUN mkdir -p /opt/patrowl-manager/
---> Running in 468ab01e4de5
Removing intermediate container 468ab01e4de5
---> 48c07e45a6a7

```

Step 6/14 : WORKDIR /opt/patrowl-manager/

---> Running in fb8a08c9e031

Removing intermediate container fb8a08c9e031

---> 4ce8dd9c8cd0

Step 7/14 : RUN apt-get update -yq && apt-get install -yq --no-install-recommends apt-utils

python3 python3-pip libmagic-dev python3-dev gcc && apt-get purge -y --auto-remove -o

APT::AutoRemove::RecommendsImportant=false && rm -rf /var/lib/apt/lists/\* /tmp/\*

/var/tmp/\*

---> Running in cdce2a9760b7

Get:1 http://security.debian.org/debian-security buster/updates InRelease [65.4 kB]

Get:2 http://deb.debian.org/debian buster InRelease [121 kB]

Get:3 http://deb.debian.org/debian buster-updates InRelease [51.9 kB]

Get:4 http://security.debian.org/debian-security buster/updates/main amd64 Packages [286 kB]

Get:5 http://deb.debian.org/debian buster/main amd64 Packages [7907 kB]

Get:6 http://deb.debian.org/debian buster-updates/main amd64 Packages [10.9 kB]

Fetchd 8442 kB in 3s (3265 kB/s)

Reading package lists...

Reading package lists...

Building dependency tree...

Reading state information...

The following additional packages will be installed:

apt binutils binutils-common binutils-x86-64-linux-gnu cpp cpp-8 dh-python

gcc-8 libapt-inst2.0 libasan5 libatomic1 libbinutils libc-dev-bin libc6-dev

libcc1-0 libexpat1-dev libgcc-8-dev libgomp1 libisl19 libitm1 liblsan0

libmagic-mgc libmagic1 libmpc3 libmpdec2 libmpfr6 libmpx2 libpython3-dev

libpython3-stdlib libpython3.7 libpython3.7-dev libpython3.7-minimal

libpython3.7-stdlib libquadmath0 libtsan0 libubsan1 linux-libc-dev

mime-support python-pip-whl python3-distutils python3-lib2to3

python3-minimal python3.7 python3.7-dev python3.7-minimal

Suggested packages:

apt-doc aptitude | synaptic | wajig dpkg-dev gnupg | gnupg2 | gnupg1

powermgmt-base binutils-doc cpp-doc gcc-8-locales libdpkg-perl gcc-multilib

make manpages-dev autoconf automake libtool flex bison gdb gcc-doc

gcc-8-multilib gcc-8-doc libgcc1-dbg libgomp1-dbg libitm1-dbg libatomic1-dbg

libasan5-dbg liblsan0-dbg libtsan0-dbg libubsan1-dbg libmpx2-dbg

libquadmath0-dbg glibc-doc file python3-doc python3-tk python3-venv

python3.7-venv python3.7-doc binfmt-support

Recommended packages:

manpages manpages-dev bzip2 file xz-utils build-essential python3-setuptools

python3-wheel

The following NEW packages will be installed:

apt-utils binutils binutils-common binutils-x86-64-linux-gnu cpp cpp-8

dh-python gcc gcc-8 libapt-inst2.0 libasan5 libatomic1 libbinutils

libc-dev-bin libc6-dev libcc1-0 libexpat1-dev libgcc-8-dev libgomp1 libisl19

libitm1 liblsan0 libmagic-dev libmagic-mgc libmagic1 libmpc3 libmpdec2

libmpfr6 libmpx2 libpython3-dev libpython3-stdlib libpython3.7

libpython3.7-dev libpython3.7-minimal libpython3.7-stdlib libquadmath0

libtsan0 libubsan1 linux-libc-dev mime-support python-pip-whl python3

python3-dev python3-distutils python3-lib2to3 python3-minimal python3-pip

python3.7 python3.7-dev python3.7-minimal

The following packages will be upgraded:

apt

1 upgraded, 50 newly installed, 0 to remove and 1 not upgraded.

Need to get 92.0 MB of archives.

After this operation, 256 MB of additional disk space will be used.

Get:1 <http://deb.debian.org/debian> buster-updates/main amd64 apt amd64 1.8.2.3 [1418 kB]

Get:2 <http://deb.debian.org/debian> buster/main amd64 libpython3.7-minimal amd64 3.7.3-2+deb10u3 [589 kB]

Get:3 <http://deb.debian.org/debian> buster/main amd64 python3.7-minimal amd64 3.7.3-2+deb10u3 [1737 kB]

Get:4 <http://deb.debian.org/debian> buster/main amd64 python3-minimal amd64 3.7.3-1 [36.6 kB]

Get:5 <http://deb.debian.org/debian> buster/main amd64 mime-support all 3.62 [37.2 kB]

Get:6 <http://deb.debian.org/debian> buster/main amd64 libmpdec2 amd64 2.4.2-2 [87.2 kB]

Get:7 <http://deb.debian.org/debian> buster/main amd64 libpython3.7-stdlib amd64 3.7.3-2+deb10u3 [1734 kB]

Get:8 <http://deb.debian.org/debian> buster/main amd64 python3.7 amd64 3.7.3-2+deb10u3 [330 kB]

Get:9 <http://deb.debian.org/debian> buster/main amd64 libpython3-stdlib amd64 3.7.3-1 [20.0 kB]

Get:10 <http://deb.debian.org/debian> buster/main amd64 python3 amd64 3.7.3-1 [61.5 kB]

Get:11 <http://deb.debian.org/debian> buster-updates/main amd64 libapt-inst2.0 amd64 1.8.2.3 [204 kB]

Get:12 <http://deb.debian.org/debian> buster-updates/main amd64 apt-utils amd64 1.8.2.3 [421 kB]

Get:13 <http://deb.debian.org/debian> buster/main amd64 binutils-common amd64 2.31.1-16 [2073 kB]

Get:14 <http://deb.debian.org/debian> buster/main amd64 libbinutils amd64 2.31.1-16 [478 kB]

Get:15 <http://deb.debian.org/debian> buster/main amd64 binutils-x86-64-linux-gnu amd64 2.31.1-16 [1823 kB]

Get:16 <http://deb.debian.org/debian> buster/main amd64 binutils amd64 2.31.1-16 [56.8 kB]

Get:17 <http://deb.debian.org/debian> buster/main amd64 libisl19 amd64 0.20-2 [587 kB]

Get:18 <http://deb.debian.org/debian> buster/main amd64 libmpfr6 amd64 4.0.2-1 [775 kB]

Get:19 <http://deb.debian.org/debian> buster/main amd64 libmpc3 amd64 1.1.0-1 [41.3 kB]

Get:20 <http://deb.debian.org/debian> buster/main amd64 cpp-8 amd64 8.3.0-6 [8914 kB]

Get:21 <http://deb.debian.org/debian> buster/main amd64 cpp amd64 4:8.3.0-1 [19.4 kB]

Get:22 <http://deb.debian.org/debian> buster/main amd64 python3-lib2to3 all 3.7.3-1 [76.7 kB]

Get:23 <http://deb.debian.org/debian> buster/main amd64 python3-distutils all 3.7.3-1 [142 kB]

Get:24 <http://deb.debian.org/debian> buster/main amd64 dh-python all 3.20190308 [99.3 kB]

Get:25 <http://deb.debian.org/debian> buster/main amd64 libcc1-0 amd64 8.3.0-6 [46.6 kB]

Get:26 <http://deb.debian.org/debian> buster/main amd64 libgomp1 amd64 8.3.0-6 [75.8 kB]

Get:27 <http://deb.debian.org/debian> buster/main amd64 libitm1 amd64 8.3.0-6 [27.7 kB]

Get:28 <http://deb.debian.org/debian> buster/main amd64 libatomic1 amd64 8.3.0-6 [9032 B]

Get:29 <http://deb.debian.org/debian> buster/main amd64 libasan5 amd64 8.3.0-6 [362 kB]

Get:30 <http://deb.debian.org/debian> buster/main amd64 liblsan0 amd64 8.3.0-6 [131 kB]

Get:31 <http://deb.debian.org/debian> buster/main amd64 libtsan0 amd64 8.3.0-6 [283 kB]

Get:32 <http://deb.debian.org/debian> buster/main amd64 libubsan1 amd64 8.3.0-6 [120 kB]

Get:33 <http://deb.debian.org/debian> buster/main amd64 libmpx2 amd64 8.3.0-6 [11.4 kB]

Get:34 <http://deb.debian.org/debian> buster/main amd64 libquadmath0 amd64 8.3.0-6 [133 kB]

Get:35 <http://deb.debian.org/debian> buster/main amd64 libgcc-8-dev amd64 8.3.0-6 [2298 kB]

Get:36 http://deb.debian.org/debian buster/main amd64 gcc-8 amd64 8.3.0-6 [9452 kB]  
Get:37 http://deb.debian.org/debian buster/main amd64 gcc amd64 4:8.3.0-1 [5196 B]  
Get:38 http://deb.debian.org/debian buster/main amd64 libc-dev-bin amd64 2.28-10 [275 kB]  
Get:39 http://deb.debian.org/debian buster/main amd64 linux-libc-dev amd64 4.19.181-1 [1441 kB]  
Get:40 http://deb.debian.org/debian buster/main amd64 libc6-dev amd64 2.28-10 [2691 kB]  
Get:41 http://deb.debian.org/debian buster/main amd64 libexpat1-dev amd64 2.2.6-2+deb10u1 [153 kB]  
Get:42 http://deb.debian.org/debian buster/main amd64 libmagic-mgc amd64 1:5.35-4+deb10u2 [242 kB]  
Get:43 http://deb.debian.org/debian buster/main amd64 libmagic1 amd64 1:5.35-4+deb10u2 [118 kB]  
Get:44 http://deb.debian.org/debian buster/main amd64 libmagic-dev amd64 1:5.35-4+deb10u2 [130 kB]  
Get:45 http://deb.debian.org/debian buster/main amd64 libpython3.7 amd64 3.7.3-2+deb10u3 [1498 kB]  
Get:46 http://deb.debian.org/debian buster/main amd64 libpython3.7-dev amd64 3.7.3-2+deb10u3 [48.4 MB]  
Get:47 http://deb.debian.org/debian buster/main amd64 libpython3-dev amd64 3.7.3-1 [20.1 kB]  
Get:48 http://deb.debian.org/debian buster/main amd64 python-pip-whl all 18.1-5 [1591 kB]  
Get:49 http://deb.debian.org/debian buster/main amd64 python3.7-dev amd64 3.7.3-2+deb10u3 [510 kB]  
Get:50 http://deb.debian.org/debian buster/main amd64 python3-dev amd64 3.7.3-1 [1264 B]  
Get:51 http://deb.debian.org/debian buster/main amd64 python3-pip all 18.1-5 [171 kB]  
debconf: delaying package configuration, since apt-utils is not installed  
Fetched 92.0 MB in 9s (10.4 MB/s)  
(Reading database ... 6840 files and directories currently installed.)  
Preparing to unpack .../archives/apt\_1.8.2.3\_amd64.deb ...  
Unpacking apt (1.8.2.3) over (1.8.2.2) ...  
Setting up apt (1.8.2.3) ...  
Selecting previously unselected package libpython3.7-minimal:amd64.  
(Reading database ... 6840 files and directories currently installed.)  
Preparing to unpack .../libpython3.7-minimal\_3.7.3-2+deb10u3\_amd64.deb ...  
Unpacking libpython3.7-minimal:amd64 (3.7.3-2+deb10u3) ...  
Selecting previously unselected package python3.7-minimal.  
Preparing to unpack .../python3.7-minimal\_3.7.3-2+deb10u3\_amd64.deb ...  
Unpacking python3.7-minimal (3.7.3-2+deb10u3) ...  
Setting up libpython3.7-minimal:amd64 (3.7.3-2+deb10u3) ...  
Setting up python3.7-minimal (3.7.3-2+deb10u3) ...  
Selecting previously unselected package python3-minimal.  
(Reading database ... 7081 files and directories currently installed.)  
Preparing to unpack .../0-python3-minimal\_3.7.3-1\_amd64.deb ...  
Unpacking python3-minimal (3.7.3-1) ...  
Selecting previously unselected package mime-support.  
Preparing to unpack .../1-mime-support\_3.62\_all.deb ...  
Unpacking mime-support (3.62) ...  
Selecting previously unselected package libmpdec2:amd64.  
Preparing to unpack .../2-libmpdec2\_2.4.2-2\_amd64.deb ...  
Unpacking libmpdec2:amd64 (2.4.2-2) ...

Selecting previously unselected package libpython3.7-stdlib:amd64.  
Preparing to unpack .../3-libpython3.7-stdlib\_3.7.3-2+deb10u3\_amd64.deb ...  
Unpacking libpython3.7-stdlib:amd64 (3.7.3-2+deb10u3) ...  
Selecting previously unselected package python3.7.  
Preparing to unpack .../4-python3.7\_3.7.3-2+deb10u3\_amd64.deb ...  
Unpacking python3.7 (3.7.3-2+deb10u3) ...  
Selecting previously unselected package libpython3-stdlib:amd64.  
Preparing to unpack .../5-libpython3-stdlib\_3.7.3-1\_amd64.deb ...  
Unpacking libpython3-stdlib:amd64 (3.7.3-1) ...  
Setting up python3-minimal (3.7.3-1) ...  
Selecting previously unselected package python3.  
(Reading database ... 7518 files and directories currently installed.)  
Preparing to unpack .../00-python3\_3.7.3-1\_amd64.deb ...  
Unpacking python3 (3.7.3-1) ...  
Selecting previously unselected package libapt-inst2.0:amd64.  
Preparing to unpack .../01-libapt-inst2.0\_1.8.2.3\_amd64.deb ...  
Unpacking libapt-inst2.0:amd64 (1.8.2.3) ...  
Selecting previously unselected package apt-utils.  
Preparing to unpack .../02-apt-utils\_1.8.2.3\_amd64.deb ...  
Unpacking apt-utils (1.8.2.3) ...  
Selecting previously unselected package binutils-common:amd64.  
Preparing to unpack .../03-binutils-common\_2.31.1-16\_amd64.deb ...  
Unpacking binutils-common:amd64 (2.31.1-16) ...  
Selecting previously unselected package libbinutils:amd64.  
Preparing to unpack .../04-libbinutils\_2.31.1-16\_amd64.deb ...  
Unpacking libbinutils:amd64 (2.31.1-16) ...  
Selecting previously unselected package binutils-x86-64-linux-gnu.  
Preparing to unpack .../05-binutils-x86-64-linux-gnu\_2.31.1-16\_amd64.deb ...  
Unpacking binutils-x86-64-linux-gnu (2.31.1-16) ...  
Selecting previously unselected package binutils.  
Preparing to unpack .../06-binutils\_2.31.1-16\_amd64.deb ...  
Unpacking binutils (2.31.1-16) ...  
Selecting previously unselected package libisl19:amd64.  
Preparing to unpack .../07-libisl19\_0.20-2\_amd64.deb ...  
Unpacking libisl19:amd64 (0.20-2) ...  
Selecting previously unselected package libmpfr6:amd64.  
Preparing to unpack .../08-libmpfr6\_4.0.2-1\_amd64.deb ...  
Unpacking libmpfr6:amd64 (4.0.2-1) ...  
Selecting previously unselected package libmpc3:amd64.  
Preparing to unpack .../09-libmpc3\_1.1.0-1\_amd64.deb ...  
Unpacking libmpc3:amd64 (1.1.0-1) ...  
Selecting previously unselected package cpp-8.  
Preparing to unpack .../10-cpp-8\_8.3.0-6\_amd64.deb ...  
Unpacking cpp-8 (8.3.0-6) ...  
Selecting previously unselected package cpp.  
Preparing to unpack .../11-cpp\_4%3a8.3.0-1\_amd64.deb ...  
Unpacking cpp (4:8.3.0-1) ...  
Selecting previously unselected package python3-lib2to3.  
Preparing to unpack .../12-python3-lib2to3\_3.7.3-1\_all.deb ...



Unpacking python3-lib2to3 (3.7.3-1) ...  
Selecting previously unselected package python3-distutils.  
Preparing to unpack .../13-python3-distutils\_3.7.3-1\_all.deb ...  
Unpacking python3-distutils (3.7.3-1) ...  
Selecting previously unselected package dh-python.  
Preparing to unpack .../14-dh-python\_3.20190308\_all.deb ...  
Unpacking dh-python (3.20190308) ...  
Selecting previously unselected package libcc1-0:amd64.  
Preparing to unpack .../15-libcc1-0\_8.3.0-6\_amd64.deb ...  
Unpacking libcc1-0:amd64 (8.3.0-6) ...  
Selecting previously unselected package libgomp1:amd64.  
Preparing to unpack .../16-libgomp1\_8.3.0-6\_amd64.deb ...  
Unpacking libgomp1:amd64 (8.3.0-6) ...  
Selecting previously unselected package libitm1:amd64.  
Preparing to unpack .../17-libitm1\_8.3.0-6\_amd64.deb ...  
Unpacking libitm1:amd64 (8.3.0-6) ...  
Selecting previously unselected package libatomic1:amd64.  
Preparing to unpack .../18-libatomic1\_8.3.0-6\_amd64.deb ...  
Unpacking libatomic1:amd64 (8.3.0-6) ...  
Selecting previously unselected package libasan5:amd64.  
Preparing to unpack .../19-libasan5\_8.3.0-6\_amd64.deb ...  
Unpacking libasan5:amd64 (8.3.0-6) ...  
Selecting previously unselected package liblsan0:amd64.  
Preparing to unpack .../20-liblsan0\_8.3.0-6\_amd64.deb ...  
Unpacking liblsan0:amd64 (8.3.0-6) ...  
Selecting previously unselected package libtsan0:amd64.  
Preparing to unpack .../21-libtsan0\_8.3.0-6\_amd64.deb ...  
Unpacking libtsan0:amd64 (8.3.0-6) ...  
Selecting previously unselected package libubsan1:amd64.  
Preparing to unpack .../22-libubsan1\_8.3.0-6\_amd64.deb ...  
Unpacking libubsan1:amd64 (8.3.0-6) ...  
Selecting previously unselected package libmpx2:amd64.  
Preparing to unpack .../23-libmpx2\_8.3.0-6\_amd64.deb ...  
Unpacking libmpx2:amd64 (8.3.0-6) ...  
Selecting previously unselected package libquadmath0:amd64.  
Preparing to unpack .../24-libquadmath0\_8.3.0-6\_amd64.deb ...  
Unpacking libquadmath0:amd64 (8.3.0-6) ...  
Selecting previously unselected package libgcc-8-dev:amd64.  
Preparing to unpack .../25-libgcc-8-dev\_8.3.0-6\_amd64.deb ...  
Unpacking libgcc-8-dev:amd64 (8.3.0-6) ...  
Selecting previously unselected package gcc-8.  
Preparing to unpack .../26-gcc-8\_8.3.0-6\_amd64.deb ...  
Unpacking gcc-8 (8.3.0-6) ...  
Selecting previously unselected package gcc.  
Preparing to unpack .../27-gcc\_4%3a8.3.0-1\_amd64.deb ...  
Unpacking gcc (4:8.3.0-1) ...  
Selecting previously unselected package libc-dev-bin.  
Preparing to unpack .../28-libc-dev-bin\_2.28-10\_amd64.deb ...  
Unpacking libc-dev-bin (2.28-10) ...

Selecting previously unselected package linux-libc-dev:amd64.  
Preparing to unpack .../29-linux-libc-dev\_4.19.181-1\_amd64.deb ...  
Unpacking linux-libc-dev:amd64 (4.19.181-1) ...  
Selecting previously unselected package libc6-dev:amd64.  
Preparing to unpack .../30-libc6-dev\_2.28-10\_amd64.deb ...  
Unpacking libc6-dev:amd64 (2.28-10) ...  
Selecting previously unselected package libexpat1-dev:amd64.  
Preparing to unpack .../31-libexpat1-dev\_2.2.6-2+deb10u1\_amd64.deb ...  
Unpacking libexpat1-dev:amd64 (2.2.6-2+deb10u1) ...  
Selecting previously unselected package libmagic-mgc.  
Preparing to unpack .../32-libmagic-mgc\_1%3a5.35-4+deb10u2\_amd64.deb ...  
Unpacking libmagic-mgc (1:5.35-4+deb10u2) ...  
Selecting previously unselected package libmagic1:amd64.  
Preparing to unpack .../33-libmagic1\_1%3a5.35-4+deb10u2\_amd64.deb ...  
Unpacking libmagic1:amd64 (1:5.35-4+deb10u2) ...  
Selecting previously unselected package libmagic-dev:amd64.  
Preparing to unpack .../34-libmagic-dev\_1%3a5.35-4+deb10u2\_amd64.deb ...  
Unpacking libmagic-dev:amd64 (1:5.35-4+deb10u2) ...  
Selecting previously unselected package libpython3.7:amd64.  
Preparing to unpack .../35-libpython3.7\_3.7.3-2+deb10u3\_amd64.deb ...  
Unpacking libpython3.7:amd64 (3.7.3-2+deb10u3) ...  
Selecting previously unselected package libpython3.7-dev:amd64.  
Preparing to unpack .../36-libpython3.7-dev\_3.7.3-2+deb10u3\_amd64.deb ...  
Unpacking libpython3.7-dev:amd64 (3.7.3-2+deb10u3) ...  
Selecting previously unselected package libpython3-dev:amd64.  
Preparing to unpack .../37-libpython3-dev\_3.7.3-1\_amd64.deb ...  
Unpacking libpython3-dev:amd64 (3.7.3-1) ...  
Selecting previously unselected package python-pip-whl.  
Preparing to unpack .../38-python-pip-whl\_18.1-5\_all.deb ...  
Unpacking python-pip-whl (18.1-5) ...  
Selecting previously unselected package python3.7-dev.  
Preparing to unpack .../39-python3.7-dev\_3.7.3-2+deb10u3\_amd64.deb ...  
Unpacking python3.7-dev (3.7.3-2+deb10u3) ...  
Selecting previously unselected package python3-dev.  
Preparing to unpack .../40-python3-dev\_3.7.3-1\_amd64.deb ...  
Unpacking python3-dev (3.7.3-1) ...  
Selecting previously unselected package python3-pip.  
Preparing to unpack .../41-python3-pip\_18.1-5\_all.deb ...  
Unpacking python3-pip (18.1-5) ...  
Setting up mime-support (3.62) ...  
Setting up libmagic-mgc (1:5.35-4+deb10u2) ...  
Setting up binutils-common:amd64 (2.31.1-16) ...  
Setting up libmagic1:amd64 (1:5.35-4+deb10u2) ...  
Setting up linux-libc-dev:amd64 (4.19.181-1) ...  
Setting up libmagic-dev:amd64 (1:5.35-4+deb10u2) ...  
Setting up libgomp1:amd64 (8.3.0-6) ...  
Setting up libapt-inst2.0:amd64 (1.8.2.3) ...  
Setting up libasan5:amd64 (8.3.0-6) ...  
Setting up libmpfr6:amd64 (4.0.2-1) ...

```

Setting up libquadmath0:amd64 (8.3.0-6) ...
Setting up libmpc3:amd64 (1.1.0-1) ...
Setting up libatomic1:amd64 (8.3.0-6) ...
Setting up libmpx2:amd64 (8.3.0-6) ...
Setting up libubsan1:amd64 (8.3.0-6) ...
Setting up libisl19:amd64 (0.20-2) ...
Setting up python-pip-whl (18.1-5) ...
Setting up libmpdec2:amd64 (2.4.2-2) ...
Setting up libbinutils:amd64 (2.31.1-16) ...
Setting up cpp-8 (8.3.0-6) ...
Setting up libc-dev-bin (2.28-10) ...
Setting up libcc1-0:amd64 (8.3.0-6) ...
Setting up liblsan0:amd64 (8.3.0-6) ...
Setting up libitm1:amd64 (8.3.0-6) ...
Setting up binutils-x86-64-linux-gnu (2.31.1-16) ...
Setting up libtsan0:amd64 (8.3.0-6) ...
Setting up libpython3.7-stdlib:amd64 (3.7.3-2+deb10u3) ...
Setting up apt-utils (1.8.2.3) ...
Setting up libpython3.7:amd64 (3.7.3-2+deb10u3) ...
Setting up binutils (2.31.1-16) ...
Setting up libgcc-8-dev:amd64 (8.3.0-6) ...
Setting up cpp (4:8.3.0-1) ...
Setting up libc6-dev:amd64 (2.28-10) ...
Setting up libpython3-stdlib:amd64 (3.7.3-1) ...
Setting up python3.7 (3.7.3-2+deb10u3) ...
Setting up gcc-8 (8.3.0-6) ...
Setting up python3 (3.7.3-1) ...
running python rtupdate hooks for python3.7...
running python post-rtupdate hooks for python3.7...
Setting up gcc (4:8.3.0-1) ...
Setting up libexpat1-dev:amd64 (2.2.6-2+deb10u1) ...
Setting up python3-lib2to3 (3.7.3-1) ...
Setting up python3-distutils (3.7.3-1) ...
Setting up dh-python (3.20190308) ...
Setting up libpython3.7-dev:amd64 (3.7.3-2+deb10u3) ...
Setting up python3.7-dev (3.7.3-2+deb10u3) ...
Setting up python3-pip (18.1-5) ...
Setting up libpython3-dev:amd64 (3.7.3-1) ...
Setting up python3-dev (3.7.3-1) ...
Processing triggers for libc-bin (2.28-10) ...
Reading package lists...
Building dependency tree...
Reading state information...
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
Removing intermediate container cdce2a9760b7
---> bba2c0b224a2
Step 8/14 : ADD ./requirements.txt /root/
---> 2171e3a8e5c2

```

```

Step 9/14 : RUN python --version      && pip3 install virtualenv && virtualenv env3      &&
/opt/patrowl-manager/env3/bin/pip3 install --no-cache-dir -r /root/requirements.txt
--> Running in 39a892ccbfe4
Python 3.7.10
Collecting virtualenv
  Downloading virtualenv-20.4.6-py2.py3-none-any.whl (7.2 MB)
Collecting filelock<4,>=3.0.0
  Downloading filelock-3.0.12-py3-none-any.whl (7.6 kB)
Collecting six<2,>=1.9.0
  Downloading six-1.16.0-py2.py3-none-any.whl (11 kB)
Collecting appdirs<2,>=1.4.3
  Downloading appdirs-1.4.4-py2.py3-none-any.whl (9.6 kB)
Collecting importlib-metadata>=0.12
  Downloading importlib_metadata-4.0.1-py3-none-any.whl (16 kB)
Collecting distlib<1,>=0.3.1
  Downloading distlib-0.3.1-py2.py3-none-any.whl (335 kB)
Collecting zipp>=0.5
  Downloading zipp-3.4.1-py3-none-any.whl (5.2 kB)
Collecting typing-extensions>=3.6.4
  Downloading typing_extensions-3.10.0.0-py3-none-any.whl (26 kB)
Installing collected packages: zipp, typing-extensions, six, importlib-metadata, filelock, distlib, ap-
pdirs, virtualenv
Successfully installed appdirs-1.4.4 distlib-0.3.1 filelock-3.0.12 importlib-metadata-4.0.1 six-1.16.0
typing-extensions-3.10.0.0 virtualenv-20.4.6 zipp-3.4.1
WARNING: Running pip as root will break packages and permissions. You should install packages
reliably by using venv: https://pip.pypa.io/warnings/venv
created virtual environment CPython3.7.10.final.0-64 in 952ms
  creator CPython3Posix(dest=/opt/patrowl-manager/env3, clear=False, no_vcs_ignore=False,
global=False)
  seeder FromAppData(download=False, pip=bundle, setuptools=bundle, wheel=bundle, via=copy,
app_data_dir=/root/.local/share/virtualenv)
  added seed packages: pip==21.1.1, setuptools==56.0.0, wheel==0.36.2
  activators BashActivator,CShellActivator,FishActivator,PowerShellActivator,PythonActivator,Xon-
shActivator
Collecting amqp==2.5.1
  Downloading amqp-2.5.1-py2.py3-none-any.whl (49 kB)
Collecting Babel==2.4.0
  Downloading Babel-2.4.0-py2.py3-none-any.whl (6.8 MB)
Collecting backports-abc==0.5
  Downloading backports_abc-0.5-py2.py3-none-any.whl (5.2 kB)
Collecting billiard==3.6.1.0
  Downloading billiard-3.6.1.0-py3-none-any.whl (89 kB)
Collecting celery==4.4.0rc3
  Downloading celery-4.4.0rc3-py2.py3-none-any.whl (417 kB)
Collecting certifi==2017.4.17
  Downloading certifi-2017.4.17-py2.py3-none-any.whl (375 kB)
Collecting chardet==3.0.4
  Downloading chardet-3.0.4-py2.py3-none-any.whl (133 kB)
Collecting coreapi==2.3.3

```

Downloading coreapi-2.3.3-py2.py3-none-any.whl (25 kB)  
Collecting coreschema==0.0.4  
  Downloading coreschema-0.0.4.tar.gz (10 kB)  
Collecting Django==2.2.19  
  Downloading Django-2.2.19-py3-none-any.whl (7.5 MB)  
Collecting django-celery-beat==2.0.0  
  Downloading django\_celery\_beat-2.0.0-py2.py3-none-any.whl (37 kB)  
Collecting django-celery-results==1.1.2  
  Downloading django\_celery\_results-1.1.2-py2.py3-none-any.whl (18 kB)  
Collecting django-cursor-pagination==0.1.4  
  Downloading django\_cursor\_pagination-0.1.4-py3-none-any.whl (5.6 kB)  
Collecting django-datetime-widget==0.9.3  
  Downloading django-datetime-widget-0.9.3.tar.gz (37 kB)  
Collecting django-debug-toolbar==2.0  
  Downloading django\_debug\_toolbar-2.0-py3-none-any.whl (198 kB)  
Collecting django-extensions==2.1.9  
  Downloading django\_extensions-2.1.9-py2.py3-none-any.whl (223 kB)  
Collecting django-rest-swagger==2.2.0  
  Downloading django\_rest\_swagger-2.2.0-py2.py3-none-any.whl (495 kB)  
Collecting django-timezone-field==4.0  
  Downloading django\_timezone\_field-4.0-py3-none-any.whl (7.6 kB)  
Collecting djangorestframework>=3.11.2  
  Downloading djangorestframework-3.12.4-py3-none-any.whl (957 kB)  
Collecting flower==0.9.2  
  Downloading flower-0.9.2.tar.gz (1.3 MB)  
Collecting future==0.16.0  
  Downloading future-0.16.0.tar.gz (824 kB)  
Collecting futures==3.1.1  
  Downloading futures-3.1.1-py3-none-any.whl (2.8 kB)  
Collecting gunicorn==20.0.4  
  Downloading gunicorn-20.0.4-py2.py3-none-any.whl (77 kB)  
Collecting idna==2.5  
  Downloading idna-2.5-py2.py3-none-any.whl (55 kB)  
Collecting importlib-metadata==0.23  
  Downloading importlib\_metadata-0.23-py2.py3-none-any.whl (28 kB)  
Collecting itypes==1.1.0  
  Downloading itypes-1.1.0.tar.gz (2.2 kB)  
Collecting Jinja2==2.11.3  
  Downloading Jinja2-2.11.3-py2.py3-none-any.whl (125 kB)  
Collecting jsonfield==2.0.2  
  Downloading jsonfield-2.0.2-py2.py3-none-any.whl (13 kB)  
Collecting kombu==4.6.4  
  Downloading kombu-4.6.4-py2.py3-none-any.whl (182 kB)  
Collecting libmagic==1.0  
  Downloading libmagic-1.0.tar.gz (3.7 kB)  
Collecting MarkupSafe==1.1.0  
  Downloading MarkupSafe-1.1.0-cp37-cp37m-manylinux1\_x86\_64.whl (27 kB)  
Collecting meld3==1.0.2  
  Downloading meld3-1.0.2-py2.py3-none-any.whl (24 kB)

Collecting more-itertools==7.2.0  
 Downloading more\_itertools-7.2.0-py3-none-any.whl (57 kB)  
Collecting netaddr==0.7.19  
 Downloading netaddr-0.7.19-py2.py3-none-any.whl (1.6 MB)  
Collecting openapi-codec==1.3.2  
 Downloading openapi-codec-1.3.2.tar.gz (6.3 kB)  
Collecting psycpg2-binary==2.7.5  
 Downloading psycpg2\_binary-2.7.5-cp37-cp37m-manylinux1\_x86\_64.whl (2.7 MB)  
Collecting python-crontab==2.3.6  
 Downloading python-crontab-2.3.6.tar.gz (44 kB)  
Collecting python-dateutil==2.8.0  
 Downloading python\_dateutil-2.8.0-py2.py3-none-any.whl (226 kB)  
Collecting python-magic==0.4.15  
 Downloading python\_magic-0.4.15-py2.py3-none-any.whl (5.5 kB)  
Collecting python-memcached==1.59  
 Downloading python\_memcached-1.59-py2.py3-none-any.whl (16 kB)  
Collecting pytz==2019.2  
 Downloading pytz-2019.2-py2.py3-none-any.whl (508 kB)  
Collecting requests==2.22.0  
 Downloading requests-2.22.0-py2.py3-none-any.whl (57 kB)  
Collecting simplejson==3.16.0  
 Downloading simplejson-3.16.0.tar.gz (81 kB)  
Collecting singledispatch==3.4.0.3  
 Downloading singledispatch-3.4.0.3-py2.py3-none-any.whl (12 kB)  
Collecting six==1.10.0  
 Downloading six-1.10.0-py2.py3-none-any.whl (10 kB)  
Collecting sqlparse==0.3.0  
 Downloading sqlparse-0.3.0-py2.py3-none-any.whl (39 kB)  
Collecting supervisor==4.2.1  
 Downloading supervisor-4.2.1-py2.py3-none-any.whl (738 kB)  
Collecting thehive4py==1.4.3  
 Downloading thehive4py-1.4.3-py2.py3-none-any.whl (11 kB)  
Collecting tornado==5.1  
 Downloading tornado-5.1.tar.gz (516 kB)  
Collecting tzlocal==1.5.1  
 Downloading tzlocal-1.5.1.tar.gz (16 kB)  
Collecting uritemplate==3.0.0  
 Downloading uritemplate-3.0.0-py2.py3-none-any.whl (10 kB)  
Collecting urllib3==1.25.9  
 Downloading urllib3-1.25.9-py2.py3-none-any.whl (126 kB)  
Collecting vine==1.3.0  
 Downloading vine-1.3.0-py2.py3-none-any.whl (14 kB)  
Collecting Werkzeug==0.15.3  
 Downloading Werkzeug-0.15.3-py2.py3-none-any.whl (327 kB)  
Collecting zipp==0.6.0  
 Downloading zipp-0.6.0-py2.py3-none-any.whl (4.1 kB)  
Collecting django-filter==2.4.0  
 Downloading django\_filter-2.4.0-py3-none-any.whl (73 kB)  
Collecting django-cors-headers==3.2.0

Downloading django\_cors\_headers-3.2.0-py3-none-any.whl (14 kB)  
 Collecting django-rest-framework-simplejwt==4.4.0  
 Downloading django-rest-framework-simplejwt-4.4.0-py3-none-any.whl (29 kB)  
 Collecting django-health-check==3.12.1  
 Downloading django\_health\_check-3.12.1-py2.py3-none-any.whl (25 kB)  
 Collecting psutil==5.7.0  
 Downloading psutil-5.7.0.tar.gz (449 kB)  
 Collecting django-organizations==1.1.2  
 Downloading django\_organizations-1.1.2-py2.py3-none-any.whl (56 kB)  
 Collecting django-annoying==0.10.6  
 Downloading django\_annoying-0.10.6-py2.py3-none-any.whl (9.5 kB)  
 Collecting django-reset-migrations  
 Downloading django\_reset\_migrations-0.4.0-py3-none-any.whl (8.0 kB)  
 Collecting django-dbconn-retry  
 Downloading django\_dbconn\_retry-0.1.5-py3-none-any.whl (8.6 kB)  
 Requirement already satisfied: setuptools>=3.0 in ./env3/lib/python3.7/site-packages (from gunicorn==20.0.4->r /root/requirements.txt (line 24)) (56.0.0)  
 Collecting pyjwt  
 Downloading PyJWT-2.1.0-py3-none-any.whl (16 kB)  
 Building wheels for collected packages: coreschema, django-datetime-widget, flower, future, itypes, libmagic, openapi-codec, python-crontab, simplejson, tornado, tzlocal, psutil  
 Building wheel for coreschema (setup.py): started  
 Building wheel for coreschema (setup.py): finished with status 'done'  
 Created wheel for coreschema: filename=coreschema-0.0.4-py3-none-any.whl size=15031 sha256=1a4656d3b6b31b5e336896f1b448cff59e1e7eb50615d3690c0f49dd485a1dd2  
 Stored in directory: /tmp/pip-ephem-wheel-cache-1eu04sct/wheels/29/28/77/73539fe0ce161da7a571cd8278a9296adbda257406bb6f100d  
 Building wheel for django-datetime-widget (setup.py): started  
 Building wheel for django-datetime-widget (setup.py): finished with status 'done'  
 Created wheel for django-datetime-widget: filename=django\_datetime\_widget-0.9.3-py3-none-any.whl size=55480 sha256=c7da5257097fa2d108c30a5cbd548bb851a66653fc9c8a61a0c24a04351338b2  
 Stored in directory: /tmp/pip-ephem-wheel-cache-1eu04sct/wheels/c2/1a/ea/1bc6eb473fe391682592bf5eb0b178098f020ef06e5bead42a  
 Building wheel for flower (setup.py): started  
 Building wheel for flower (setup.py): finished with status 'done'  
 Created wheel for flower: filename=flower-0.9.2-py2.py3-none-any.whl size=455328 sha256=47c9b77342d74720c38b42b5e572d27603c6e9dc5485bdbbcb737fca841cc82a  
 Stored in directory: /tmp/pip-ephem-wheel-cache-1eu04sct/wheels/f4/9b/c6/38f40eb6b98ab9819317b03c892a94423dec8d056e8dc83eba  
 Building wheel for future (setup.py): started  
 Building wheel for future (setup.py): finished with status 'done'  
 Created wheel for future: filename=future-0.16.0-py3-none-any.whl size=487798 sha256=f85f5514be4e19e4cebb62b57de3f3f32fc154efe76d8bd885f4b4360895f1e0  
 Stored in directory: /tmp/pip-ephem-wheel-cache-1eu04sct/wheels/7c/09/6f/dfd31fb2ebe951aefbee461a0dfce1bdc2e4b2c1016e85d233  
 Building wheel for itypes (setup.py): started  
 Building wheel for itypes (setup.py): finished with status 'done'

Created wheel for itypes: filename=itypes-1.1.0-py3-none-any.whl size=2311  
sha256=b1fabf1cb2dd3097142c6cd47a3f70856b18fd2ae954a47486b9e2696d41cc05  
Stored in directory: /tmp/pip-ephem-wheel-cache-  
1eu04sct/wheels/a5/92/71/4ee11d4146fae4155e5585d0d7261463943c36380c87395899  
Building wheel for libmagic (setup.py): started  
Building wheel for libmagic (setup.py): finished with status 'done'  
Created wheel for libmagic: filename=libmagic-1.0-py3-none-any.whl size=4287  
sha256=af0510df4a446595ce836fd608a58784219d7ce0884e4072ebd8e5ee3f5c7d1b  
Stored in directory: /tmp/pip-ephem-wheel-cache-  
1eu04sct/wheels/1f/09/8f/b428f254d5cdbc8b9b158355f5bc10119dc4914e0b22852aaa  
Building wheel for openapi-codec (setup.py): started  
Building wheel for openapi-codec (setup.py): finished with status 'done'  
Created wheel for openapi-codec: filename=openapi\_codec-1.3.2-py3-none-any.whl size=7307  
sha256=f8b1f1d65a1de6e1468c7445ad133d61da77e75ed55adb825e20a39f33f1333a  
Stored in directory: /tmp/pip-ephem-wheel-cache-  
1eu04sct/wheels/90/4f/a2/0cef56e55966463564e594a0fcd8ff1a858917fe7c1585cc6d  
Building wheel for python-crontab (setup.py): started  
Building wheel for python-crontab (setup.py): finished with status 'done'  
Created wheel for python-crontab: filename=python\_crontab-2.3.6-py3-none-any.whl  
size=24893 sha256=2ce5b83afbb693becaeeca960d739817cfd7dfd6f0140828c0280c176208170  
Stored in directory: /tmp/pip-ephem-wheel-cache-1eu04sct/wheels/21/06/e4/c12ad-  
ffcb4876a05e4ace2bf90a390323007708964fe9101a2  
Building wheel for simplejson (setup.py): started  
Building wheel for simplejson (setup.py): finished with status 'done'  
Created wheel for simplejson: filename=simplejson-3.16.0-cp37-cp37m-linux\_x86\_64.whl  
size=74378 sha256=09d307265582bf19e2c302fc9398ffc5a3ab017ee46520b440c16aad99eb96f8  
Stored in directory: /tmp/pip-ephem-wheel-cache-  
1eu04sct/wheels/00/6f/29/109ee3b85a9f9861d4294b05e4597363d5ad3c9dfaccc78787  
Building wheel for tornado (setup.py): started  
Building wheel for tornado (setup.py): finished with status 'done'  
Created wheel for tornado: filename=tornado-5.1-cp37-cp37m-linux\_x86\_64.whl size=451545  
sha256=a8343439d4cd0a85c5b554cbb6a5a20fd655c3dfa0c16fa351bcd3301e3ddf05  
Stored in directory: /tmp/pip-ephem-wheel-cache-  
1eu04sct/wheels/8e/53/de/6a6860ebf6d2958e20a9a8337f25b0369f1666002ade0ce284  
Building wheel for tzlocal (setup.py): started  
Building wheel for tzlocal (setup.py): finished with status 'done'  
Created wheel for tzlocal: filename=tzlocal-1.5.1-py3-none-any.whl size=17541  
sha256=1910bb8484dc3f9735b526a6fe36f3b34fd9ae5a7633b474b60ec93987bffa1  
Stored in directory: /tmp/pip-ephem-wheel-cache-  
1eu04sct/wheels/6a/76/b4/f97e26f8f60b5b2b1287415f1202e2b34a97775cead74072be  
Building wheel for psutil (setup.py): started  
Building wheel for psutil (setup.py): finished with status 'done'  
Created wheel for psutil: filename=psutil-5.7.0-cp37-cp37m-linux\_x86\_64.whl size=217145  
sha256=3485cd10087fecba2df013c643f61a332d691253f793e582de453bc785a5a7f5  
Stored in directory: /tmp/pip-ephem-wheel-cache-  
1eu04sct/wheels/b6/e7/50/ae9cc966163d74430f13f208171dee22f11efa4a4a826661c  
Successfully built coreshema django-datetime-widget flower future itypes libmagic openapi-co-  
dec python-crontab simplejson tornado tzlocal psutil



Installing collected packages: more-iterertools, MarkupSafe, zipp, vine, urllib3, Jinja2, idna, chardet, certifi, uritemplate, sqlparse, six, requests, pytz, itypes, importlib-metadata, coreschema, amqp, python-dateutil, kombu, Django, coreapi, billiard, tornado, simplejson, python-magic, python-crontab, pyjwt, openapi-codec, future, djangoestframework, django-timezone-field, celery, Babel, Werkzeug, tzlocal, thehive4py, supervisor, singledispatch, python-memcached, psycpg2-binary, psutil, netaddr, meld3, libmagic, jsonfield, gunicorn, futures, flower, djangoestframework-simplejwt, django-rest-swagger, django-reset-migrations, django-organizations, django-health-check, django-filter, django-extensions, django-debug-toolbar, django-dbconn-retry, django-datetime-widget, django-cursor-pagination, django-cors-headers, django-celery-results, django-celery-beat, django-annoying, backports-abc

Successfully installed Babel-2.4.0 Django-2.2.19 Jinja2-2.11.3 MarkupSafe-1.1.0 Werkzeug-0.15.3 amqp-2.5.1 backports-abc-0.5 billiard-3.6.1.0 celery-4.4.0rc3 certifi-2017.4.17 chardet-3.0.4 coreapi-2.3.3 coreschema-0.0.4 django-annoying-0.10.6 django-celery-beat-2.0.0 django-celery-results-1.1.2 django-cors-headers-3.2.0 django-cursor-pagination-0.1.4 django-datetime-widget-0.9.3 django-dbconn-retry-0.1.5 django-debug-toolbar-2.0 django-extensions-2.1.9 django-filter-2.4.0 django-health-check-3.12.1 django-organizations-1.1.2 django-reset-migrations-0.4.0 django-rest-swagger-2.2.0 django-timezone-field-4.0 djangoestframework-3.12.4 djangoestframework-simplejwt-4.4.0 flower-0.9.2 future-0.16.0 futures-3.1.1 gunicorn-20.0.4 idna-2.5 importlib-metadata-0.23 itypes-1.1.0 jsonfield-2.0.2 kombu-4.6.4 libmagic-1.0 meld3-1.0.2 more-iterertools-7.2.0 netaddr-0.7.19 openapi-codec-1.3.2 psutil-5.7.0 psycpg2-binary-2.7.5 pyjwt-2.1.0 python-crontab-2.3.6 python-dateutil-2.8.0 python-magic-0.4.15 python-memcached-1.59 pytz-2019.2 requests-2.22.0 simplejson-3.16.0 singledispatch-3.4.0.3 six-1.10.0 sqlparse-0.3.0 supervisor-4.2.1 thehive4py-1.4.3 tornado-5.1 tzlocal-1.5.1 uritemplate-3.0.0 urllib3-1.25.9 vine-1.3.0 zipp-0.6.0

Removing intermediate container 39a892ccbfe4  
 ---> 0ad6a7352501  
 Step 10/14 : COPY ./opt/patrowl-manager/  
 ---> 64dda699f024  
 Step 11/14 : COPY app/settings.py.sample /opt/patrowl-manager/app/settings.py  
 ---> a2b1bef58cbf  
 Step 12/14 : EXPOSE 8003  
 ---> Running in 29a51622b73a  
 Removing intermediate container 29a51622b73a  
 ---> 92f1d60de765  
 Step 13/14 : ENTRYPOINT ["/opt/patrowl-manager/docker-entrypoint.sh"]  
 ---> Running in e5a8159b0eb0  
 Removing intermediate container e5a8159b0eb0  
 ---> 1806579d58e6  
 Step 14/14 : CMD ["run"]  
 ---> Running in 08d98da335bd  
 Removing intermediate container 08d98da335bd  
 ---> b971506463fc  
 Successfully built b971506463fc  
 Successfully tagged patrowl/patrowl-manager-community-edition:latest



```

z@z:~$ git clone https://github.com/Patrowl/PatrowlEngines.git
Cloning into 'PatrowlEngines'...
remote: Enumerating objects: 4460, done.
remote: Counting objects: 100% (316/316), done.
remote: Compressing objects: 100% (231/231), done.
remote: Total 4460 (delta 193), reused 138 (delta 79), pack-reused 4144
Receiving objects: 100% (4460/4460), 1.43 MiB | 2.47 MiB/s, done.
Resolving deltas: 100% (3223/3223), done.
z@z:~$ cd PatrowlEngines
z@z:~/PatrowlEngines$ sudo bash scripts/build-docker-engines.sh
Building engine 'patrowl-apivoid' docker image... [-]
sha256:fb1c4432923d06b3ae6898f8922f64255b5241356f6e8748a88c3e885f137c4f
Done.
Building engine 'patrowl-arachni' docker image... [\]
sha256:925f8a3fe72c8322d4079817db977692c82e75acdd8d491bd50055a9d1950de3
Done.
Building engine 'patrowl-censys' docker image... [-] Sending build context to Docker daemon
73.73kB
Step 1/17 : FROM alpine:latest
---> 6dbb9cc54074
Step 2/17 : MAINTAINER Patrowl.io "getsupport@patrowl.io"
---> Using cache
---> 97bd234bc387
Step 3/17 : LABEL Name="Censys\ ((Patrowl engine\))" Version="1.0.0"
---> Running in a66838527d2a
Removing intermediate container a66838527d2a
---> 97cba3d1d99c
Step 4/17 : RUN mkdir -p /opt/patrowl-engines/censys
---> Running in 32e4228f74a7
Removing intermediate container 32e4228f74a7
---> f4cbdb4b2293
Step 5/17 : RUN mkdir -p /opt/patrowl-engines/censys/results
---> Running in 38f639558a69
Removing intermediate container 38f639558a69
---> 40c48bac3bd0
Step 6/17 : WORKDIR /opt/patrowl-engines/censys
---> Running in 910a2e1b7b07
Removing intermediate container 910a2e1b7b07
---> 48bc66466ed7
Step 7/17 : COPY __init__.py .
---> 9c23a280372f
Step 8/17 : COPY engine-censys.py .
---> d6df3e2a515f
Step 9/17 : COPY censys.json.sample censys.json
---> 060387e9ed64
Step 10/17 : COPY requirements.txt .
---> ba5d741a1574
Step 11/17 : COPY README.md .
---> 3f5deae12167

```

```

Step 12/17 : RUN mkdir -p results
---> Running in 13b489c53ead
Removing intermediate container 13b489c53ead
---> 24a4b4ee457a
Step 13/17 : RUN apk add --update linux-headers build-base libffi-dev openssl-dev py-
thon python-dev py3-pip && rm -rf /var/cache/apk/*
---> Running in dd11db410e80
fetch https://dl-cdn.alpinelinux.org/alpine/v3.13/main/x86_64/APKINDEX.tar.gz
fetch https://dl-cdn.alpinelinux.org/alpine/v3.13/community/x86_64/APKINDEX.tar.gz
ERROR: unable to select packages:
python (no such package):
  required by: world[python]
python-dev (no such package):
  required by: world[python-dev]
The command '/bin/sh -c apk add --update linux-headers build-base libffi-dev openssl-dev
python python-dev py3-pip && rm -rf /var/cache/apk/*' returned a non-zero code: 2
Done.
Building engine 'patrowl-certstream' docker image... [\]
sha256:be4f3ae88cafd95ab16073874a88e2152aa84243bf5ac633e17f571422d4d928
Done.
Building engine 'patrowl-cortex' docker image... [/]
sha256:1120f49853622fd8243c633a54b04f7dfc1b97556a95a10f7a93690f1532498e
Done.
Building engine 'patrowl-cybelangel' docker image... [-]
sha256:bb9cf1ef3cf90de97b9b15b786a61084df164c66374bc16aa08bb9f26b72cea8
Done.
Building engine 'patrowl-droopescan' docker image... [\]
sha256:03ead005d4c80c19d8ec35742c24949c6130fd637b0c10a788297e3c101eee54
Done.
Building engine 'patrowl-eyewitness' docker image... [\]
sha256:419ba7f927de54cff638cd3718b63d5d34224900f6a45824c0aba448a515bb7f
Done.
Building engine 'patrowl-nessus' docker image... [-]
sha256:2ef537e68ee34c1d6e41f710176138e78b72d656688337f53c0bb104fe0446c2
Done.
Building engine 'patrowl-nmap' docker image... [-]
sha256:44b138296b4d9cf17e9a25a25f1fd6c5567ad35d638229af2676970d46a75e78
Done.
Building engine 'patrowl-opnvas' docker image... [[]]
sha256:a5d581debf8ec23d5116bceb499d10da834bed904226cc08eba2c164b86ea096
Done.
Building engine 'patrowl-owl_code' docker image... [-] Sending build context to Docker daemon
30.21kB
Step 1/22 : FROM alpine:latest
---> 6dbb9cc54074
Step 2/22 : MAINTAINER Patrowl.io "getsupport@patrowl.io"
---> Using cache
---> 97bd234bc387
Step 3/22 : LABEL Name="Patrowl\ Code\ Security\ review\ \ (Patrowl engine\)" Version="1.4.18"

```

```
---> Running in 29ec2cbf329a
Removing intermediate container 29ec2cbf329a
---> d4d033e7f79b
Step 4/22 : RUN apk add --update --no-cache wget unzip openjdk8-jre git subversion py-
thon3 python3-dev py3-pip nodejs nodejs-npm && rm -rf /var/cache/apk/* && rm -rf /tmp/*
---> Running in 7197ffebabda
fetch https://dl-cdn.alpinelinux.org/alpine/v3.13/main/x86_64/APKINDEX.tar.gz
fetch https://dl-cdn.alpinelinux.org/alpine/v3.13/community/x86_64/APKINDEX.tar.gz
(1/98) Installing ca-certificates (20191127-r5)
(2/98) Installing brotli-libs (1.0.9-r3)
(3/98) Installing nghttp2-libs (1.42.0-r1)
(4/98) Installing libcurl (7.76.1-r0)
(5/98) Installing expat (2.2.10-r1)
(6/98) Installing pcre2 (10.36-r0)
(7/98) Installing git (2.30.2-r0)
(8/98) Installing c-ares (1.17.1-r1)
(9/98) Installing libgcc (10.2.1_pre1-r3)
(10/98) Installing libstdc++ (10.2.1_pre1-r3)
(11/98) Installing nodejs (14.16.1-r1)
(12/98) Installing npm (14.16.1-r1)
(13/98) Installing libbz2 (1.0.8-r1)
(14/98) Installing libpng (1.6.37-r1)
(15/98) Installing freetype (2.10.4-r1)
(16/98) Installing libuuid (2.36.1-r1)
(17/98) Installing fontconfig (2.13.1-r3)
(18/98) Installing encodings (1.0.5-r0)
(19/98) Installing libfontenc (1.1.4-r0)
(20/98) Installing mkfontscale (1.2.1-r1)
(21/98) Installing ttf-dejavu (2.37-r1)
(22/98) Installing libxau (1.0.9-r0)
(23/98) Installing libbsd (0.10.0-r0)
(24/98) Installing libxdmcp (1.1.3-r0)
(25/98) Installing libxcb (1.14-r1)
(26/98) Installing libx11 (1.7.0-r0)
(27/98) Installing libxcomposite (0.4.5-r0)
(28/98) Installing libxext (1.3.4-r0)
(29/98) Installing libxi (1.7.10-r0)
(30/98) Installing libxrender (0.9.10-r3)
(31/98) Installing libxtst (1.2.3-r3)
(32/98) Installing alsa-lib (1.2.4-r2)
(33/98) Installing giflib (5.2.1-r0)
(34/98) Installing libjpeg-turbo (2.1.0-r0)
(35/98) Installing openjdk8-jre-lib (8.275.01-r0)
(36/98) Installing java-common (0.2-r0)
(37/98) Installing libffi (3.3-r2)
(38/98) Installing p11-kit (0.23.22-r0)
(39/98) Installing libtasn1 (4.16.0-r1)
(40/98) Installing p11-kit-trust (0.23.22-r0)
(41/98) Installing java-cacerts (1.0-r1)
```

(42/98) Installing nspr (4.29-r0)  
(43/98) Installing sqlite-libs (3.34.1-r0)  
(44/98) Installing nss (3.63-r1)  
(45/98) Installing krb5-conf (1.0-r2)  
(46/98) Installing libcom\_err (1.45.7-r0)  
(47/98) Installing keyutils-libs (1.6.3-r0)  
(48/98) Installing libverto (0.3.1-r1)  
(49/98) Installing krb5-libs (1.18.3-r1)  
(50/98) Installing lcms2 (2.11-r0)  
(51/98) Installing pcsc-lite-libs (1.9.0-r0)  
(52/98) Installing libksctp (1.0.18-r1)  
(53/98) Installing openjdk8-jre-base (8.275.01-r0)  
(54/98) Installing openjdk8-jre (8.275.01-r0)  
(55/98) Installing gdbm (1.19-r0)  
(56/98) Installing xz-libs (5.2.5-r0)  
(57/98) Installing ncurses-terminfo-base (6.2\_p20210109-r0)  
(58/98) Installing ncurses-libs (6.2\_p20210109-r0)  
(59/98) Installing readline (8.1.0-r0)  
(60/98) Installing python3 (3.8.10-r0)  
(61/98) Installing py3-appdirs (1.4.4-r1)  
(62/98) Installing py3-ordered-set (4.0.2-r0)  
(63/98) Installing py3-parsing (2.4.7-r1)  
(64/98) Installing py3-six (1.15.0-r0)  
(65/98) Installing py3-packaging (20.9-r0)  
(66/98) Installing py3-setuptools (51.3.3-r0)  
(67/98) Installing py3-chardet (4.0.0-r0)  
(68/98) Installing py3-idna (3.1-r0)  
(69/98) Installing py3-urllib3 (1.26.2-r1)  
(70/98) Installing py3-requests (2.25.1-r1)  
(71/98) Installing py3-msgpack (1.0.2-r0)  
(72/98) Installing py3-lockfile (0.12.2-r3)  
(73/98) Installing py3-cachecontrol (0.12.6-r0)  
(74/98) Installing py3-colorama (0.4.4-r0)  
(75/98) Installing py3-contextlib2 (0.6.0-r0)  
(76/98) Installing py3-distlib (0.3.1-r1)  
(77/98) Installing py3-distro (1.5.0-r1)  
(78/98) Installing py3-webencodings (0.5.1-r3)  
(79/98) Installing py3-html5lib (1.1-r0)  
(80/98) Installing py3-pytoml (0.1.21-r0)  
(81/98) Installing py3-pep517 (0.9.1-r0)  
(82/98) Installing py3-progress (1.5-r0)  
(83/98) Installing py3-retrying (1.3.3-r0)  
(84/98) Installing py3-toml (0.10.2-r0)  
(85/98) Installing py3-pip (20.3.4-r0)  
(86/98) Installing pkgconf (1.7.3-r0)  
(87/98) Installing python3-dev (3.8.10-r0)  
(88/98) Installing apr (1.7.0-r0)  
(89/98) Installing apr-util (1.6.1-r7)  
(90/98) Installing lz4-libs (1.9.2-r0)

```

(91/98) Installing libsasl (2.1.27-r10)
(92/98) Installing serf (1.3.9-r5)
(93/98) Installing subversion-libs (1.14.1-r0)
(94/98) Installing subversion (1.14.1-r0)
Executing subversion-1.14.1-r0.pre-install
(95/98) Installing unzip (6.0-r8)
(96/98) Installing libunistring (0.9.10-r0)
(97/98) Installing libidn2 (2.3.0-r0)
(98/98) Installing wget (1.21.1-r1)
Executing busybox-1.32.1-r6.trigger
Executing ca-certificates-20191127-r5.trigger
Executing fontconfig-2.13.1-r3.trigger
Executing mkfontscale-1.2.1-r1.trigger
Executing java-common-0.2-r0.trigger
OK: 294 MiB in 112 packages
Removing intermediate container 7197ffebabda
---> fe578814b9fe
Step 5/22 : RUN mkdir -p /opt/patrowl-engines/owl_code
---> Running in 495ac7887b5d
Removing intermediate container 495ac7887b5d
---> 82c1fe2b607f
Step 6/22 : RUN mkdir -p /opt/patrowl-engines/owl_code/results
---> Running in c16ee1dc8165
Removing intermediate container c16ee1dc8165
---> 9ae23fa10d73
Step 7/22 : RUN mkdir -p /opt/patrowl-engines/owl_code/libs
---> Running in c3f6e7ca72f6
Removing intermediate container c3f6e7ca72f6
---> 6b34442afefc
Step 8/22 : RUN mkdir -p /opt/patrowl-engines/owl_code/utils
---> Running in c9f1e160d33f
Removing intermediate container c9f1e160d33f
---> 104ec70c87a5
Step 9/22 : WORKDIR /tmp/
---> Running in 89d470e2da78
Removing intermediate container 89d470e2da78
---> 3b1be3f5d9a4
Step 10/22 : RUN npm install -g retire
---> Running in 7f39ea63e8f0
/usr/bin/retire -> /usr/lib/node_modules/retire/bin/retire
+ retire@2.2.5
added 43 packages from 37 contributors in 3.548s
Removing intermediate container 7f39ea63e8f0
---> 2780abf4e009
Step 11/22 : ENV version_url=https://jeremylong.github.io/DependencyCheck/current.txt
---> Running in 83878a60fff8
Removing intermediate container 83878a60fff8
---> 238909a976c0
Step 12/22 : ENV download_url=https://dl.bintray.com/jeremy-long/owasp

```

```

---> Running in 95103bd01593
Removing intermediate container 95103bd01593
---> b7f7c18ca654
Step 13/22 : RUN wget -qO- -O /tmp/current.txt ${version_url}          && version=$(cat
/tmp/current.txt)          && file="dependency-check-6.0.3-release.zip"
&& wget "$download_url/$file"          && unzip ${file}
&& rm ${file}          && mv dependency-check /opt/patrowl-en-
gines/owl_code/libs          && cd /opt/patrowl-engines/owl_code/libs          &&
chmod +x dependency-check/bin/dependency-check.sh          && dependency-
check/bin/dependency-check.sh --updateonly

```

```

---> Running in 078251a6c0b8
--2021-05-12 12:11:52-- https://dl.bintray.com/jeremy-long/owasp/dependency-check-6.0.3-re-
lease.zip
Resolving dl.bintray.com (dl.bintray.com)... 3.66.199.110, 18.193.131.58
Connecting to dl.bintray.com (dl.bintray.com)|3.66.199.110|:443... connected.
HTTP request sent, awaiting response... 403 Forbidden
2021-05-12 12:11:52 ERROR 403: Forbidden.

```

```

The command '/bin/sh -c wget -qO- -O /tmp/current.txt ${version_url}          && ver-
sion=$(cat /tmp/current.txt)          && file="dependency-check-6.0.3-re-
lease.zip"          && wget "$download_url/$file"          && unzip
${file}          && rm ${file}          && mv
dependency-check /opt/patrowl-engines/owl_code/libs          && cd /opt/patrowl-en-
gines/owl_code/libs          && chmod +x dependency-check/bin/dependency-
check.sh          && dependency-check/bin/dependency-check.sh --updateonly' returned a
non-zero code: 8

```

Done.

Building engine 'patrowl-owl\_dns' docker image... [\]

sha256:20eb8fc883e0009ff2668a780a3fea1d5f259308a1961acb6f4f48442d6857d1

Done.

Building engine 'patrowl-owl\_leaks' docker image... [/]

sha256:bbe0b71098f507f114403ed447645dda7c8817921a17ee8652b3aaa136f904d2

Done.

Building engine 'patrowl-owl\_request' docker image... [/]

sha256:b204825325238379c55e89e06d867c714ddfd5a0a0cceda2a282d6449acc584e

Done.

Building engine 'patrowl-pastebin\_monitor' docker image... [\]

sha256:d679fe3f23215cd6fb9729ad3ff8e356c6e326edc9f8fa1bc7c1dccf33856d9d

Done.

Building engine 'patrowl-ssllabs' docker image... [\]

sha256:2a7f1adee719fc96509c5576d268a4ac4cf48c158c8ec3bb9d2498b75f27b9c4

Done.

Building engine 'patrowl-sslscan' docker image... [[]]

sha256:9c756d830882ab585d1b521144c3ea39859da83b0b0360856b5c236a9b270eb7

Done.

Building engine 'patrowl-urlvoid' docker image... [-]

sha256:5db409934c4c987c0d25670214e511087752e57a4b6afcbddcf33abafb4e713

Done.

Building engine 'patrowl-virustotal' docker image... [\]

sha256:b5fcede9211347f58078523ff23f6e6f184cd34c779e3b3b76e9214fd0f80870

Done.

Building engine 'patrowl-wpscan' docker image... [/]

sha256:dbaa4825dc2597c7c92373d90207819b7fa2bf7b8ddb301636636d450bfa2428

Done.



## Liite 4. GRR Rapid Response asennus



GRR Install.txt

```

z@z:~$ sudo apt-get install mysql-server -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
 libaio1 libcgi-fast-perl libcgi-pm-perl libevent-core-2.1-7 libevent-pthreads-2.1-7 libfcgi-bin libfcgi-
perl libfcgi0ldbl libhtml-template-perl
 libmecab2 libprotobuf-lite23 mecab-ipadic mecab-ipadic-utf8 mecab-utils mysql-client-8.0 mysql-
client-core-8.0 mysql-common mysql-server-8.0
 mysql-server-core-8.0
Suggested packages:
 libipc-sharedcache-perl mailx tinyca
The following NEW packages will be installed:
 libaio1 libcgi-fast-perl libcgi-pm-perl libevent-core-2.1-7 libevent-pthreads-2.1-7 libfcgi-bin libfcgi-
perl libfcgi0ldbl libhtml-template-perl
 libmecab2 libprotobuf-lite23 mecab-ipadic mecab-ipadic-utf8 mecab-utils mysql-client-8.0 mysql-
client-core-8.0 mysql-common mysql-server
 mysql-server-8.0 mysql-server-core-8.0
0 upgraded, 20 newly installed, 0 to remove and 3 not upgraded.
Need to get 28,8 MB of archives.
After this operation, 239 MB of additional disk space will be used.
Get:1 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 mysql-common all 5.8+1.0.5ub-
untu2 [7 496 B]
Get:2 http://fi.archive.ubuntu.com/ubuntu hirsute-updates/main amd64 mysql-client-core-8.0
amd64 8.0.25-0ubuntu0.21.04.1 [3 927 kB]
Get:3 http://fi.archive.ubuntu.com/ubuntu hirsute-updates/main amd64 mysql-client-8.0 amd64
8.0.25-0ubuntu0.21.04.1 [22,0 kB]
Get:4 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 libaio1 amd64 0.3.112-9ubuntu1
[6 972 B]
Get:5 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 libevent-core-2.1-7 amd64
2.1.12-stable-1 [89,4 kB]
Get:6 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 libevent-pthreads-2.1-7 amd64
2.1.12-stable-1 [7 364 B]
Get:7 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 libmecab2 amd64 0.996-14build3
[217 kB]
Get:8 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 libprotobuf-lite23 amd64 3.12.4-
1ubuntu2 [190 kB]
Get:9 http://fi.archive.ubuntu.com/ubuntu hirsute-updates/main amd64 mysql-server-core-8.0
amd64 8.0.25-0ubuntu0.21.04.1 [15,9 MB]
Get:10 http://fi.archive.ubuntu.com/ubuntu hirsute-updates/main amd64 mysql-server-8.0
amd64 8.0.25-0ubuntu0.21.04.1 [1 381 kB]

```

```

Get:11 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 libcgi-pm-perl all 4.51-1 [186 kB]
Get:12 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 libfcgi0ldbl amd64 2.4.2-2 [26,1
kB]
Get:13 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 libfcgi-perl amd64 0.79+ds-2
[21,6 kB]
Get:14 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 libcgi-fast-perl all 1:2.15-1 [10,5
kB]
Get:15 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 libfcgi-bin amd64 2.4.2-2 [10,7
kB]
Get:16 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 libhtml-template-perl all 2.97-
1.1 [59,1 kB]
Get:17 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 mecab-utils amd64 0.996-
14build3 [4 916 B]
Get:18 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 mecab-ipadic all 2.7.0-
20070801+main-3 [6 718 kB]
Get:19 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 mecab-ipadic-utf8 all 2.7.0-
20070801+main-3 [4 384 B]
Get:20 http://fi.archive.ubuntu.com/ubuntu hirsute-updates/main amd64 mysql-server all 8.0.25-
0ubuntu0.21.04.1 [9 536 B]
Fetched 28,8 MB in 4s (7 928 kB/s)
Preconfiguring packages ...
Selecting previously unselected package mysql-common.
(Reading database ... 127257 files and directories currently installed.)
Preparing to unpack .../0-mysql-common_5.8+1.0.5ubuntu2_all.deb ...
Unpacking mysql-common (5.8+1.0.5ubuntu2) ...
Selecting previously unselected package mysql-client-core-8.0.
Preparing to unpack .../1-mysql-client-core-8.0_8.0.25-0ubuntu0.21.04.1_amd64.deb ...
Unpacking mysql-client-core-8.0 (8.0.25-0ubuntu0.21.04.1) ...
Selecting previously unselected package mysql-client-8.0.
Preparing to unpack .../2-mysql-client-8.0_8.0.25-0ubuntu0.21.04.1_amd64.deb ...
Unpacking mysql-client-8.0 (8.0.25-0ubuntu0.21.04.1) ...
Selecting previously unselected package libaio1:amd64.
Preparing to unpack .../3-libaio1_0.3.112-9ubuntu1_amd64.deb ...
Unpacking libaio1:amd64 (0.3.112-9ubuntu1) ...
Selecting previously unselected package libevent-core-2.1-7:amd64.
Preparing to unpack .../4-libevent-core-2.1-7_2.1.12-stable-1_amd64.deb ...
Unpacking libevent-core-2.1-7:amd64 (2.1.12-stable-1) ...
Selecting previously unselected package libevent-pthreads-2.1-7:amd64.
Preparing to unpack .../5-libevent-pthreads-2.1-7_2.1.12-stable-1_amd64.deb ...
Unpacking libevent-pthreads-2.1-7:amd64 (2.1.12-stable-1) ...
Selecting previously unselected package libmecab2:amd64.
Preparing to unpack .../6-libmecab2_0.996-14build3_amd64.deb ...
Unpacking libmecab2:amd64 (0.996-14build3) ...
Selecting previously unselected package libprotobuf-lite23:amd64.
Preparing to unpack .../7-libprotobuf-lite23_3.12.4-1ubuntu2_amd64.deb ...
Unpacking libprotobuf-lite23:amd64 (3.12.4-1ubuntu2) ...
Selecting previously unselected package mysql-server-core-8.0.
Preparing to unpack .../8-mysql-server-core-8.0_8.0.25-0ubuntu0.21.04.1_amd64.deb ...
Unpacking mysql-server-core-8.0 (8.0.25-0ubuntu0.21.04.1) ...

```

```

Setting up mysql-common (5.8+1.0.5ubuntu2) ...
update-alternatives: using /etc/mysql/my.cnf.fallback to provide /etc/mysql/my.cnf (my.cnf) in
auto mode
Selecting previously unselected package mysql-server-8.0.
(Reading database ... 127485 files and directories currently installed.)
Preparing to unpack .../00-mysql-server-8.0_8.0.25-0ubuntu0.21.04.1_amd64.deb ...
Unpacking mysql-server-8.0 (8.0.25-0ubuntu0.21.04.1) ...
Selecting previously unselected package libcgi-pm-perl.
Preparing to unpack .../01-libcgi-pm-perl_4.51-1_all.deb ...
Unpacking libcgi-pm-perl (4.51-1) ...
Selecting previously unselected package libfcgi0ldbl:amd64.
Preparing to unpack .../02-libfcgi0ldbl_2.4.2-2_amd64.deb ...
Unpacking libfcgi0ldbl:amd64 (2.4.2-2) ...
Selecting previously unselected package libfcgi-perl:amd64.
Preparing to unpack .../03-libfcgi-perl_0.79+ds-2_amd64.deb ...
Unpacking libfcgi-perl:amd64 (0.79+ds-2) ...
Selecting previously unselected package libcgi-fast-perl.
Preparing to unpack .../04-libcgi-fast-perl_1%3a2.15-1_all.deb ...
Unpacking libcgi-fast-perl (1:2.15-1) ...
Selecting previously unselected package libfcgi-bin.
Preparing to unpack .../05-libfcgi-bin_2.4.2-2_amd64.deb ...
Unpacking libfcgi-bin (2.4.2-2) ...
Selecting previously unselected package libhtml-template-perl.
Preparing to unpack .../06-libhtml-template-perl_2.97-1.1_all.deb ...
Unpacking libhtml-template-perl (2.97-1.1) ...
Selecting previously unselected package mecab-utils.
Preparing to unpack .../07-mecab-utils_0.996-14build3_amd64.deb ...
Unpacking mecab-utils (0.996-14build3) ...
Selecting previously unselected package mecab-ipadic.
Preparing to unpack .../08-mecab-ipadic_2.7.0-20070801+main-3_all.deb ...
Unpacking mecab-ipadic (2.7.0-20070801+main-3) ...
Selecting previously unselected package mecab-ipadic-utf8.
Preparing to unpack .../09-mecab-ipadic-utf8_2.7.0-20070801+main-3_all.deb ...
Unpacking mecab-ipadic-utf8 (2.7.0-20070801+main-3) ...
Selecting previously unselected package mysql-server.
Preparing to unpack .../10-mysql-server_8.0.25-0ubuntu0.21.04.1_all.deb ...
Unpacking mysql-server (8.0.25-0ubuntu0.21.04.1) ...
Setting up libmecab2:amd64 (0.996-14build3) ...
Setting up mysql-client-core-8.0 (8.0.25-0ubuntu0.21.04.1) ...
Setting up libfcgi0ldbl:amd64 (2.4.2-2) ...
Setting up libcgi-pm-perl (4.51-1) ...
Setting up libfcgi-bin (2.4.2-2) ...
Setting up libhtml-template-perl (2.97-1.1) ...
Setting up libprotobuf-lite23:amd64 (3.12.4-1ubuntu2) ...
Setting up mecab-utils (0.996-14build3) ...
Setting up libevent-core-2.1-7:amd64 (2.1.12-stable-1) ...
Setting up mysql-client-8.0 (8.0.25-0ubuntu0.21.04.1) ...
Setting up libfcgi-perl:amd64 (0.79+ds-2) ...
Setting up libaio1:amd64 (0.3.112-9ubuntu1) ...

```

```

Setting up libevent-threads-2.1-7:amd64 (2.1.12-stable-1) ...
Setting up mecab-ipadic (2.7.0-20070801+main-3) ...
Compiling IPA dictionary for Mecab. This takes long time...
reading /usr/share/mecab/dic/ipadic/unk.def ... 40
emitting double-array: 100% |#####|
/usr/share/mecab/dic/ipadic/model.def is not found. skipped.
reading /usr/share/mecab/dic/ipadic/Noun.name.csv ... 34202
reading /usr/share/mecab/dic/ipadic/Noun.org.csv ... 16668
reading /usr/share/mecab/dic/ipadic/Symbol.csv ... 208
reading /usr/share/mecab/dic/ipadic/Noun.others.csv ... 151
reading /usr/share/mecab/dic/ipadic/Prefix.csv ... 221
reading /usr/share/mecab/dic/ipadic/Noun.adverbial.csv ... 795
reading /usr/share/mecab/dic/ipadic/Adnominal.csv ... 135
reading /usr/share/mecab/dic/ipadic/Noun.place.csv ... 72999
reading /usr/share/mecab/dic/ipadic/Interjection.csv ... 252
reading /usr/share/mecab/dic/ipadic/Filler.csv ... 19
reading /usr/share/mecab/dic/ipadic/Noun.number.csv ... 42
reading /usr/share/mecab/dic/ipadic/Noun.demonst.csv ... 120
reading /usr/share/mecab/dic/ipadic/Noun.csv ... 60477
reading /usr/share/mecab/dic/ipadic/Postp-col.csv ... 91
reading /usr/share/mecab/dic/ipadic/Conjunction.csv ... 171
reading /usr/share/mecab/dic/ipadic/Noun.nai.csv ... 42
reading /usr/share/mecab/dic/ipadic/Adj.csv ... 27210
reading /usr/share/mecab/dic/ipadic/Auxil.csv ... 199
reading /usr/share/mecab/dic/ipadic/Noun.adjv.csv ... 3328
reading /usr/share/mecab/dic/ipadic/Adverb.csv ... 3032
reading /usr/share/mecab/dic/ipadic/Noun.proper.csv ... 27328
reading /usr/share/mecab/dic/ipadic/Others.csv ... 2
reading /usr/share/mecab/dic/ipadic/Suffix.csv ... 1393
reading /usr/share/mecab/dic/ipadic/Verb.csv ... 130750
reading /usr/share/mecab/dic/ipadic/Noun.verbal.csv ... 12146
reading /usr/share/mecab/dic/ipadic/Postp.csv ... 146
emitting double-array: 100% |#####|
reading /usr/share/mecab/dic/ipadic/matrix.def ... 1316x1316
emitting matrix : 100% |#####|

done!
update-alternatives: using /var/lib/mecab/dic/ipadic to provide /var/lib/mecab/dic/debian
(mecab-dictionary) in auto mode
Setting up libcgi-fast-perl (1:2.15-1) ...
Setting up mysql-server-core-8.0 (8.0.25-0ubuntu0.21.04.1) ...
Setting up mecab-ipadic-utf8 (2.7.0-20070801+main-3) ...
Compiling IPA dictionary for Mecab. This takes long time...
reading /usr/share/mecab/dic/ipadic/unk.def ... 40
emitting double-array: 100% |#####|
/usr/share/mecab/dic/ipadic/model.def is not found. skipped.
reading /usr/share/mecab/dic/ipadic/Noun.name.csv ... 34202
reading /usr/share/mecab/dic/ipadic/Noun.org.csv ... 16668
reading /usr/share/mecab/dic/ipadic/Symbol.csv ... 208

```

```

reading /usr/share/mecab/dic/ipadic/Noun.others.csv ... 151
reading /usr/share/mecab/dic/ipadic/Prefix.csv ... 221
reading /usr/share/mecab/dic/ipadic/Noun.adverbial.csv ... 795
reading /usr/share/mecab/dic/ipadic/Adnominal.csv ... 135
reading /usr/share/mecab/dic/ipadic/Noun.place.csv ... 72999
reading /usr/share/mecab/dic/ipadic/Interjection.csv ... 252
reading /usr/share/mecab/dic/ipadic/Filler.csv ... 19
reading /usr/share/mecab/dic/ipadic/Noun.number.csv ... 42
reading /usr/share/mecab/dic/ipadic/Noun.demonst.csv ... 120
reading /usr/share/mecab/dic/ipadic/Noun.csv ... 60477
reading /usr/share/mecab/dic/ipadic/Postp-col.csv ... 91
reading /usr/share/mecab/dic/ipadic/Conjunction.csv ... 171
reading /usr/share/mecab/dic/ipadic/Noun.nai.csv ... 42
reading /usr/share/mecab/dic/ipadic/Adj.csv ... 27210
reading /usr/share/mecab/dic/ipadic/Auxil.csv ... 199
reading /usr/share/mecab/dic/ipadic/Noun.adjv.csv ... 3328
reading /usr/share/mecab/dic/ipadic/Adverb.csv ... 3032
reading /usr/share/mecab/dic/ipadic/Noun.proper.csv ... 27328
reading /usr/share/mecab/dic/ipadic/Others.csv ... 2
reading /usr/share/mecab/dic/ipadic/Suffix.csv ... 1393
reading /usr/share/mecab/dic/ipadic/Verb.csv ... 130750
reading /usr/share/mecab/dic/ipadic/Noun.verbal.csv ... 12146
reading /usr/share/mecab/dic/ipadic/Postp.csv ... 146
emitting double-array: 100% |#####|
reading /usr/share/mecab/dic/ipadic/matrix.def ... 1316x1316
emitting matrix : 100% |#####|

```

done!

update-alternatives: using /var/lib/mecab/dic/ipadic-utf8 to provide /var/lib/mecab/dic/debian (mecab-dictionary) in auto mode

Setting up mysql-server-8.0 (8.0.25-0ubuntu0.21.04.1) ...

update-alternatives: using /etc/mysql/mysql.cnf to provide /etc/mysql/my.cnf (my.cnf) in auto mode

Renaming removed key\_buffer and myisam-recover options (if present)

mysqld will log errors to /var/log/mysql/error.log

mysqld is running as pid 2444

Created symlink /etc/systemd/system/multi-user.target.wants/mysql.service → /lib/systemd/system/mysql.service.

Setting up mysql-server (8.0.25-0ubuntu0.21.04.1) ...

Processing triggers for man-db (2.9.4-2) ...

Processing triggers for libc-bin (2.33-0ubuntu5) ...

z@z:~\$ mysql -u root -p

Enter password:

ERROR 1698 (28000): Access denied for user 'root'@'localhost'

z@z:~\$ sudo mysql -u root -p

Enter password:

Welcome to the MySQL monitor. Commands end with ; or \g.

Your MySQL connection id is 9

Server version: 8.0.25-0ubuntu0.21.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

```
mysql> SET GLOBAL max_allowed_packet=41943040;
Query OK, 0 rows affected (0,00 sec)
```

```
mysql> CREATE USER 'grr'@'localhost' IDENTIFIED BY 'z';
Query OK, 0 rows affected (0,06 sec)
```

```
mysql> CREATE DATABASE grr;
Query OK, 1 row affected (0,01 sec)
```

```
mysql> GRANT ALL ON grr.* TO 'grr'@'localhost';
Query OK, 0 rows affected (0,19 sec)
```

```
mysql> exit
```

Bye

```
z@z:~$ wget https://storage.googleapis.com/releases.grr-response.com/grr-server_3.4.2-4_amd64.deb
```

```
--2021-05-14 16:41:19-- https://storage.googleapis.com/releases.grr-response.com/grr-server_3.4.2-4_amd64.deb
```

```
Resolving storage.googleapis.com (storage.googleapis.com)... 142.250.74.112, 172.217.20.48, 172.217.21.176, ...
```

```
Connecting to storage.googleapis.com (storage.googleapis.com)|142.250.74.112|:443... connected.
```

```
HTTP request sent, awaiting response... 200 OK
```

```
Length: 121033876 (115M) [application/vnd.debian.binary-package]
```

```
Saving to: 'grr-server_3.4.2-4_amd64.deb'
```

```
grr-server_3.4.2-4_amd64.deb
```

```
100%[=====]
] 115,43M 9,00MB/s in 12s
```

```
2021-05-14 16:41:31 (9,91 MB/s) - 'grr-server_3.4.2-4_amd64.deb' saved [121033876/121033876]
```

```
z@z:~$ sudo apt install -y ./grr-server_3.4.2-4_amd64.deb
```

```
Reading package lists... Done
```

```
Building dependency tree... Done
```

```
Reading state information... Done
```

```
Note, selecting 'grr-server' instead of './grr-server_3.4.2-4_amd64.deb'
```

```
The following additional packages will be installed:
```

```
autoconf automake autopoint autotools-dev binutils binutils-common binutils-x86-64-linux-gnu
build-essential debhelper debugedit dh-autoreconf dh-make
```

dh-strip-nondeterminism dpkg-dev dwz fakeroot g++ g++-10 gcc gcc-10 gettext intltool-debian javascript-common libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libarchive-cpio-perl libarchive-zip-perl libasan6 libatomic1 libbinutils libc-dev-bin libc-devtools libc6-dev libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libdebhelper-perl libexpat1-dev libfakeroot libfile-stripnondeterminism-perl libgcc-10-dev libitm1 libjs-jquery libjs-sphinxdoc libjs-underscore liblsan0 libltdl-dev liblua5.2-0 libmail-sendmail-perl libmysqlclient21 libnsl-dev libpython3-dev libpython3.9-dev libquadmath0 librpm9 librpmbuild9 librpmio9 librpmio9 librpmio9 libsigsegv2 libstdc++-10-dev libsub-override-perl libsys-hostname-long-perl libtirpc-dev libtool libtsan0 libubsan1 linux-libc-dev lto-disabled-list m4 make manpages-dev po-debconf python3-dev python3-distutils python3-lib2to3 python3-mysqldb python3.9-dev rpcsvc-proto rpm rpm-common rpm2cpio zlib1g-dev

Suggested packages:

autoconf-archive gnu-standards autoconf-doc binutils-doc debian-keyring g++-multilib g++-10-multilib gcc-10-doc gcc-multilib flex bison gcc-doc gcc-10-multilib gcc-10-locales gettext-doc libasprintf-dev libgettextpo-dev apache2 | lighttpd | httpd glibc-doc libtool-doc libstdc++-10-doc gfortran | fortran95-compiler gcj-jdk m4-doc make-doc libmail-box-perl python3-mysqldb-dbg alien elfutils rpmlint rpm2html rpm-i18n

The following NEW packages will be installed:

autoconf automake autopoint autotools-dev binutils binutils-common binutils-x86-64-linux-gnu build-essential debhelper debugedit dh-autoreconf dh-make dh-strip-nondeterminism dpkg-dev dwz fakeroot g++ g++-10 gcc gcc-10 gettext grr-server intltool-debian javascript-common libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libarchive-cpio-perl libarchive-zip-perl libasan6 libatomic1 libbinutils libc-dev-bin libc-devtools libc6-dev libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libdebhelper-perl libexpat1-dev libfakeroot libfile-stripnondeterminism-perl libgcc-10-dev libitm1 libjs-jquery libjs-sphinxdoc libjs-underscore liblsan0 libltdl-dev liblua5.2-0 libmail-sendmail-perl libmysqlclient21 libnsl-dev libpython3-dev libpython3.9-dev libquadmath0 librpm9 librpmbuild9 librpmio9 librpmio9 libsigsegv2 libstdc++-10-dev libsub-override-perl libsys-hostname-long-perl libtirpc-dev libtool libtsan0 libubsan1 linux-libc-dev lto-disabled-list m4 make manpages-dev po-debconf python3-dev python3-distutils python3-lib2to3 python3-mysqldb python3.9-dev rpcsvc-proto rpm rpm-common rpm2cpio zlib1g-dev

0 upgraded, 85 newly installed, 0 to remove and 3 not upgraded.

Need to get 59,4 MB/180 MB of archives.

After this operation, 562 MB of additional disk space will be used.

Get:1 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libsigsegv2 amd64 2.13-1ubuntu1 [14,2 kB]

Get:2 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 m4 amd64 1.4.18-5 [200 kB]

Get:3 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 autoconf all 2.69-14 [293 kB]

Get:4 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 autotools-dev all 20180224.1+nmu1 [39,4 kB]

Get:5 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 automake all 1:1.16.3-2ubuntu1 [552 kB]

Get:6 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 autopoint all 0.21-3ubuntu2 [422 kB]  
Get:7 [/home/z/grr-server\\_3.4.2-4\\_amd64.deb](#) grr-server amd64 3.4.2-4 [121 MB]  
Get:8 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 binutils-common amd64 2.36.1-6ubuntu1 [217 kB]  
Get:9 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libbinutils amd64 2.36.1-6ubuntu1 [584 kB]  
Get:10 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libctf-nobfd0 amd64 2.36.1-6ubuntu1 [97,8 kB]  
Get:11 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libctf0 amd64 2.36.1-6ubuntu1 [95,0 kB]  
Get:12 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 binutils-x86-64-linux-gnu amd64 2.36.1-6ubuntu1 [1 830 kB]  
Get:13 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 binutils amd64 2.36.1-6ubuntu1 [3 388 B]  
Get:14 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libc-dev-bin amd64 2.33-0ubuntu5 [19,3 kB]  
Get:15 <http://fi.archive.ubuntu.com/ubuntu> hirsute-updates/main amd64 linux-libc-dev amd64 5.11.0-17.18 [1 202 kB]  
Get:16 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libcrypt-dev amd64 1:4.4.17-1ubuntu3 [104 kB]  
Get:17 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 rpcsvc-proto amd64 1.4.2-0ubuntu4 [62,8 kB]  
Get:18 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libtirpc-dev amd64 1.3.1-1build1 [183 kB]  
Get:19 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libnsl-dev amd64 1.3.0-0ubuntu3 [66,4 kB]  
Get:20 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libc6-dev amd64 2.33-0ubuntu5 [2 143 kB]  
Get:21 <http://fi.archive.ubuntu.com/ubuntu> hirsute-updates/main amd64 libcc1-0 amd64 11.1.0-1ubuntu1~21.04 [48,8 kB]  
Get:22 <http://fi.archive.ubuntu.com/ubuntu> hirsute-updates/main amd64 libitm1 amd64 11.1.0-1ubuntu1~21.04 [26,4 kB]  
Get:23 <http://fi.archive.ubuntu.com/ubuntu> hirsute-updates/main amd64 libatomic1 amd64 11.1.0-1ubuntu1~21.04 [9 236 B]  
Get:24 <http://fi.archive.ubuntu.com/ubuntu> hirsute-updates/main amd64 libasan6 amd64 11.1.0-1ubuntu1~21.04 [2 139 kB]  
Get:25 <http://fi.archive.ubuntu.com/ubuntu> hirsute-updates/main amd64 liblsan0 amd64 11.1.0-1ubuntu1~21.04 [893 kB]  
Get:26 <http://fi.archive.ubuntu.com/ubuntu> hirsute-updates/main amd64 libtsan0 amd64 11.1.0-1ubuntu1~21.04 [2 090 kB]  
Get:27 <http://fi.archive.ubuntu.com/ubuntu> hirsute-updates/main amd64 libubsan1 amd64 11.1.0-1ubuntu1~21.04 [844 kB]  
Get:28 <http://fi.archive.ubuntu.com/ubuntu> hirsute-updates/main amd64 libquadmath0 amd64 11.1.0-1ubuntu1~21.04 [146 kB]  
Get:29 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libgcc-10-dev amd64 10.3.0-1ubuntu1 [2 337 kB]  
Get:30 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 gcc-10 amd64 10.3.0-1ubuntu1 [17,5 MB]



Get:31 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 gcc amd64 4:10.3.0-1ubuntu1 [5 212 B]  
Get:32 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libstdc++-10-dev amd64 10.3.0-1ubuntu1 [1 754 kB]  
Get:33 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 g++-10 amd64 10.3.0-1ubuntu1 [9 803 kB]  
Get:34 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 g++ amd64 4:10.3.0-1ubuntu1 [1 608 B]  
Get:35 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 make amd64 4.3-4ubuntu1 [167 kB]  
Get:36 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 lto-disabled-list all 7 [11,9 kB]  
Get:37 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 dpkg-dev all 1.20.9ubuntu1 [937 kB]  
Get:38 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 build-essential amd64 12.8ubuntu3 [4 640 B]  
Get:39 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libdebhelper-perl all 13.3.4ubuntu1 [61,1 kB]  
Get:40 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libtool all 2.4.6-15 [161 kB]  
Get:41 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 dh-autoreconf all 20 [16,1 kB]  
Get:42 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libarchive-zip-perl all 1.68-1 [90,2 kB]  
Get:43 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libsub-override-perl all 0.09-2 [9 532 B]  
Get:44 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libfile-stripnondeterminism-perl all 1.11.0-1 [17,0 kB]  
Get:45 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 dh-strip-nondeterminism all 1.11.0-1 [5 236 B]  
Get:46 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 debugedit amd64 1:0.1-0ubuntu2 [39,7 kB]  
Get:47 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 dwz amd64 0.14-1 [98,1 kB]  
Get:48 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 gettext amd64 0.21-3ubuntu2 [825 kB]  
Get:49 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 intltool-debian all 0.35.0+20060710.5 [24,9 kB]  
Get:50 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 po-debconf all 1.0.21+nmu1 [233 kB]  
Get:51 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 debhelper all 13.3.4ubuntu1 [920 kB]  
Get:52 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 dh-make all 2.202003 [31,8 kB]  
Get:53 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libfakeroot amd64 1.25.3-1.1ubuntu2 [28,1 kB]  
Get:54 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 fakeroot amd64 1.25.3-1.1ubuntu2 [62,9 kB]  
Get:55 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 javascript-common all 11+nmu1 [5 936 B]  
Get:56 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libalgorithm-diff-perl all 1.201-1 [41,8 kB]  
Get:57 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libalgorithm-diff-xs-perl amd64 0.04-6build1 [11,4 kB]

Get:58 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libalgorithm-merge-perl all 0.08-3 [12,0 kB]

Get:59 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libarchive-cpio-perl all 0.10-1.1 [9 928 B]

Get:60 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libc-devtools amd64 2.33-0ubuntu5 [27,2 kB]

Get:61 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libexpat1-dev amd64 2.2.10-2 [118 kB]

Get:62 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libjs-jquery all 3.5.1+dfsg+~3.5.5-7 [314 kB]

Get:63 <http://fi.archive.ubuntu.com/ubuntu> hirsute-updates/main amd64 libjs-underscore all 1.9.1~dfsg-1ubuntu0.21.04.1 [99,3 kB]

Get:64 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libjs-sphinxdoc all 3.5.4-1 [130 kB]

Get:65 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libltdl-dev amd64 2.4.6-15 [162 kB]

Get:66 <http://fi.archive.ubuntu.com/ubuntu> hirsute/universe amd64 liblua5.2-0 amd64 5.2.4-1.1build3 [106 kB]

Get:67 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libsys-hostname-long-perl all 1.5-2 [11,5 kB]

Get:68 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libmail-sendmail-perl all 0.80-1.1 [22,7 kB]

Get:69 <http://fi.archive.ubuntu.com/ubuntu> hirsute-updates/main amd64 libmysqlclient21 amd64 8.0.25-0ubuntu0.21.04.1 [1 064 kB]

Get:70 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 zlib1g-dev amd64 1:1.2.11.dfsg-2ubuntu6 [156 kB]

Get:71 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libpython3.9-dev amd64 3.9.4-1 [4 036 kB]

Get:72 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 libpython3-dev amd64 3.9.4-1 [7 216 B]

Get:73 <http://fi.archive.ubuntu.com/ubuntu> hirsute/universe amd64 librpio9 amd64 4.16.1.2+dfsg1-0.6ubuntu2 [80,3 kB]

Get:74 <http://fi.archive.ubuntu.com/ubuntu> hirsute/universe amd64 librpm9 amd64 4.16.1.2+dfsg1-0.6ubuntu2 [178 kB]

Get:75 <http://fi.archive.ubuntu.com/ubuntu> hirsute/universe amd64 librpmbuild9 amd64 4.16.1.2+dfsg1-0.6ubuntu2 [72,9 kB]

Get:76 <http://fi.archive.ubuntu.com/ubuntu> hirsute/universe amd64 librpm9 amd64 4.16.1.2+dfsg1-0.6ubuntu2 [8 312 B]

Get:77 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 manpages-dev all 5.10-1 [2 309 kB]

Get:78 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 python3.9-dev amd64 3.9.4-1 [515 kB]

Get:79 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 python3-lib2to3 all 3.9.4-0ubuntu1 [76,1 kB]

Get:80 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 python3-distutils all 3.9.4-0ubuntu1 [140 kB]

Get:81 <http://fi.archive.ubuntu.com/ubuntu> hirsute/main amd64 python3-dev amd64 3.9.4-1 [24,9 kB]

```
Get:82 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 python3-mysqldb amd64 1.4.4-2build3 [44,8 kB]
Get:83 http://fi.archive.ubuntu.com/ubuntu hirsute/universe amd64 rpm-common amd64 4.16.1.2+dfsg1-0.6ubuntu2 [30,4 kB]
Get:84 http://fi.archive.ubuntu.com/ubuntu hirsute/universe amd64 rpm2cpio amd64 4.16.1.2+dfsg1-0.6ubuntu2 [8 584 B]
Get:85 http://fi.archive.ubuntu.com/ubuntu hirsute/universe amd64 rpm amd64 4.16.1.2+dfsg1-0.6ubuntu2 [145 kB]
Fetched 59,4 MB in 9s (6 921 kB/s)
Extracting templates from packages: 100%
Selecting previously unselected package libsigsegv2:amd64.
(Reading database ... 127656 files and directories currently installed.)
Preparing to unpack .../00-libsigsegv2_2.13-1ubuntu1_amd64.deb ...
Unpacking libsigsegv2:amd64 (2.13-1ubuntu1) ...
Selecting previously unselected package m4.
Preparing to unpack .../01-m4_1.4.18-5_amd64.deb ...
Unpacking m4 (1.4.18-5) ...
Selecting previously unselected package autoconf.
Preparing to unpack .../02-autoconf_2.69-14_all.deb ...
Unpacking autoconf (2.69-14) ...
Selecting previously unselected package autotools-dev.
Preparing to unpack .../03-autotools-dev_20180224.1+nmu1_all.deb ...
Unpacking autotools-dev (20180224.1+nmu1) ...
Selecting previously unselected package automake.
Preparing to unpack .../04-automake_1%3a1.16.3-2ubuntu1_all.deb ...
Unpacking automake (1:1.16.3-2ubuntu1) ...
Selecting previously unselected package autopoint.
Preparing to unpack .../05-autopoint_0.21-3ubuntu2_all.deb ...
Unpacking autopoint (0.21-3ubuntu2) ...
Selecting previously unselected package binutils-common:amd64.
Preparing to unpack .../06-binutils-common_2.36.1-6ubuntu1_amd64.deb ...
Unpacking binutils-common:amd64 (2.36.1-6ubuntu1) ...
Selecting previously unselected package libbinutils:amd64.
Preparing to unpack .../07-libbinutils_2.36.1-6ubuntu1_amd64.deb ...
Unpacking libbinutils:amd64 (2.36.1-6ubuntu1) ...
Selecting previously unselected package libctf-nobfd0:amd64.
Preparing to unpack .../08-libctf-nobfd0_2.36.1-6ubuntu1_amd64.deb ...
Unpacking libctf-nobfd0:amd64 (2.36.1-6ubuntu1) ...
Selecting previously unselected package libctf0:amd64.
Preparing to unpack .../09-libctf0_2.36.1-6ubuntu1_amd64.deb ...
Unpacking libctf0:amd64 (2.36.1-6ubuntu1) ...
Selecting previously unselected package binutils-x86-64-linux-gnu.
Preparing to unpack .../10-binutils-x86-64-linux-gnu_2.36.1-6ubuntu1_amd64.deb ...
Unpacking binutils-x86-64-linux-gnu (2.36.1-6ubuntu1) ...
Selecting previously unselected package binutils.
Preparing to unpack .../11-binutils_2.36.1-6ubuntu1_amd64.deb ...
Unpacking binutils (2.36.1-6ubuntu1) ...
Selecting previously unselected package libc-dev-bin.
Preparing to unpack .../12-libc-dev-bin_2.33-0ubuntu5_amd64.deb ...
```

Unpacking libc-dev-bin (2.33-0ubuntu5) ...  
Selecting previously unselected package linux-libc-dev:amd64.  
Preparing to unpack .../13-linux-libc-dev\_5.11.0-17.18\_amd64.deb ...  
Unpacking linux-libc-dev:amd64 (5.11.0-17.18) ...  
Selecting previously unselected package libcrypt-dev:amd64.  
Preparing to unpack .../14-libcrypt-dev\_1%3a4.4.17-1ubuntu3\_amd64.deb ...  
Unpacking libcrypt-dev:amd64 (1:4.4.17-1ubuntu3) ...  
Selecting previously unselected package rpcsvc-proto.  
Preparing to unpack .../15-rpcsvc-proto\_1.4.2-0ubuntu4\_amd64.deb ...  
Unpacking rpcsvc-proto (1.4.2-0ubuntu4) ...  
Selecting previously unselected package libtirpc-dev:amd64.  
Preparing to unpack .../16-libtirpc-dev\_1.3.1-1build1\_amd64.deb ...  
Unpacking libtirpc-dev:amd64 (1.3.1-1build1) ...  
Selecting previously unselected package libnsl-dev:amd64.  
Preparing to unpack .../17-libnsl-dev\_1.3.0-0ubuntu3\_amd64.deb ...  
Unpacking libnsl-dev:amd64 (1.3.0-0ubuntu3) ...  
Selecting previously unselected package libc6-dev:amd64.  
Preparing to unpack .../18-libc6-dev\_2.33-0ubuntu5\_amd64.deb ...  
Unpacking libc6-dev:amd64 (2.33-0ubuntu5) ...  
Selecting previously unselected package libcc1-0:amd64.  
Preparing to unpack .../19-libcc1-0\_11.1.0-1ubuntu1~21.04\_amd64.deb ...  
Unpacking libcc1-0:amd64 (11.1.0-1ubuntu1~21.04) ...  
Selecting previously unselected package libitm1:amd64.  
Preparing to unpack .../20-libitm1\_11.1.0-1ubuntu1~21.04\_amd64.deb ...  
Unpacking libitm1:amd64 (11.1.0-1ubuntu1~21.04) ...  
Selecting previously unselected package libatomic1:amd64.  
Preparing to unpack .../21-libatomic1\_11.1.0-1ubuntu1~21.04\_amd64.deb ...  
Unpacking libatomic1:amd64 (11.1.0-1ubuntu1~21.04) ...  
Selecting previously unselected package libasan6:amd64.  
Preparing to unpack .../22-libasan6\_11.1.0-1ubuntu1~21.04\_amd64.deb ...  
Unpacking libasan6:amd64 (11.1.0-1ubuntu1~21.04) ...  
Selecting previously unselected package liblsan0:amd64.  
Preparing to unpack .../23-liblsan0\_11.1.0-1ubuntu1~21.04\_amd64.deb ...  
Unpacking liblsan0:amd64 (11.1.0-1ubuntu1~21.04) ...  
Selecting previously unselected package libtsan0:amd64.  
Preparing to unpack .../24-libtsan0\_11.1.0-1ubuntu1~21.04\_amd64.deb ...  
Unpacking libtsan0:amd64 (11.1.0-1ubuntu1~21.04) ...  
Selecting previously unselected package libubsan1:amd64.  
Preparing to unpack .../25-libubsan1\_11.1.0-1ubuntu1~21.04\_amd64.deb ...  
Unpacking libubsan1:amd64 (11.1.0-1ubuntu1~21.04) ...  
Selecting previously unselected package libquadmath0:amd64.  
Preparing to unpack .../26-libquadmath0\_11.1.0-1ubuntu1~21.04\_amd64.deb ...  
Unpacking libquadmath0:amd64 (11.1.0-1ubuntu1~21.04) ...  
Selecting previously unselected package libgcc-10-dev:amd64.  
Preparing to unpack .../27-libgcc-10-dev\_10.3.0-1ubuntu1\_amd64.deb ...  
Unpacking libgcc-10-dev:amd64 (10.3.0-1ubuntu1) ...  
Selecting previously unselected package gcc-10.  
Preparing to unpack .../28-gcc-10\_10.3.0-1ubuntu1\_amd64.deb ...  
Unpacking gcc-10 (10.3.0-1ubuntu1) ...

Selecting previously unselected package gcc.  
Preparing to unpack .../29-gcc\_4%3a10.3.0-1ubuntu1\_amd64.deb ...  
Unpacking gcc (4:10.3.0-1ubuntu1) ...  
Selecting previously unselected package libstdc++-10-dev:amd64.  
Preparing to unpack .../30-libstdc++-10-dev\_10.3.0-1ubuntu1\_amd64.deb ...  
Unpacking libstdc++-10-dev:amd64 (10.3.0-1ubuntu1) ...  
Selecting previously unselected package g++-10.  
Preparing to unpack .../31-g++-10\_10.3.0-1ubuntu1\_amd64.deb ...  
Unpacking g++-10 (10.3.0-1ubuntu1) ...  
Selecting previously unselected package g++.  
Preparing to unpack .../32-g++\_4%3a10.3.0-1ubuntu1\_amd64.deb ...  
Unpacking g++ (4:10.3.0-1ubuntu1) ...  
Selecting previously unselected package make.  
Preparing to unpack .../33-make\_4.3-4ubuntu1\_amd64.deb ...  
Unpacking make (4.3-4ubuntu1) ...  
Selecting previously unselected package lto-disabled-list.  
Preparing to unpack .../34-lto-disabled-list\_7\_all.deb ...  
Unpacking lto-disabled-list (7) ...  
Selecting previously unselected package dpkg-dev.  
Preparing to unpack .../35-dpkg-dev\_1.20.9ubuntu1\_all.deb ...  
Unpacking dpkg-dev (1.20.9ubuntu1) ...  
Selecting previously unselected package build-essential.  
Preparing to unpack .../36-build-essential\_12.8ubuntu3\_amd64.deb ...  
Unpacking build-essential (12.8ubuntu3) ...  
Selecting previously unselected package libdebhelper-perl.  
Preparing to unpack .../37-libdebhelper-perl\_13.3.4ubuntu1\_all.deb ...  
Unpacking libdebhelper-perl (13.3.4ubuntu1) ...  
Selecting previously unselected package libtool.  
Preparing to unpack .../38-libtool\_2.4.6-15\_all.deb ...  
Unpacking libtool (2.4.6-15) ...  
Selecting previously unselected package dh-autoreconf.  
Preparing to unpack .../39-dh-autoreconf\_20\_all.deb ...  
Unpacking dh-autoreconf (20) ...  
Selecting previously unselected package libarchive-zip-perl.  
Preparing to unpack .../40-libarchive-zip-perl\_1.68-1\_all.deb ...  
Unpacking libarchive-zip-perl (1.68-1) ...  
Selecting previously unselected package libsub-override-perl.  
Preparing to unpack .../41-libsub-override-perl\_0.09-2\_all.deb ...  
Unpacking libsub-override-perl (0.09-2) ...  
Selecting previously unselected package libfile-stripnondeterminism-perl.  
Preparing to unpack .../42-libfile-stripnondeterminism-perl\_1.11.0-1\_all.deb ...  
Unpacking libfile-stripnondeterminism-perl (1.11.0-1) ...  
Selecting previously unselected package dh-strip-nondeterminism.  
Preparing to unpack .../43-dh-strip-nondeterminism\_1.11.0-1\_all.deb ...  
Unpacking dh-strip-nondeterminism (1.11.0-1) ...  
Selecting previously unselected package debugedit.  
Preparing to unpack .../44-debugedit\_1%3a0.1-0ubuntu2\_amd64.deb ...  
Unpacking debugedit (1:0.1-0ubuntu2) ...  
Selecting previously unselected package dwz.

Preparing to unpack .../45-dwz\_0.14-1\_amd64.deb ...  
Unpacking dwz (0.14-1) ...  
Selecting previously unselected package gettext.  
Preparing to unpack .../46-gettext\_0.21-3ubuntu2\_amd64.deb ...  
Unpacking gettext (0.21-3ubuntu2) ...  
Selecting previously unselected package intltool-debian.  
Preparing to unpack .../47-intltool-debian\_0.35.0+20060710.5\_all.deb ...  
Unpacking intltool-debian (0.35.0+20060710.5) ...  
Selecting previously unselected package po-debconf.  
Preparing to unpack .../48-po-debconf\_1.0.21+nmu1\_all.deb ...  
Unpacking po-debconf (1.0.21+nmu1) ...  
Selecting previously unselected package debhelper.  
Preparing to unpack .../49-debhelper\_13.3.4ubuntu1\_all.deb ...  
Unpacking debhelper (13.3.4ubuntu1) ...  
Selecting previously unselected package dh-make.  
Preparing to unpack .../50-dh-make\_2.202003\_all.deb ...  
Unpacking dh-make (2.202003) ...  
Selecting previously unselected package libfakeroot:amd64.  
Preparing to unpack .../51-libfakeroot\_1.25.3-1.1ubuntu2\_amd64.deb ...  
Unpacking libfakeroot:amd64 (1.25.3-1.1ubuntu2) ...  
Selecting previously unselected package fakeroot.  
Preparing to unpack .../52-fakeroot\_1.25.3-1.1ubuntu2\_amd64.deb ...  
Unpacking fakeroot (1.25.3-1.1ubuntu2) ...  
Selecting previously unselected package javascript-common.  
Preparing to unpack .../53-javascript-common\_11+nmu1\_all.deb ...  
Unpacking javascript-common (11+nmu1) ...  
Selecting previously unselected package libalgorithm-diff-perl.  
Preparing to unpack .../54-libalgorithm-diff-perl\_1.201-1\_all.deb ...  
Unpacking libalgorithm-diff-perl (1.201-1) ...  
Selecting previously unselected package libalgorithm-diff-xs-perl.  
Preparing to unpack .../55-libalgorithm-diff-xs-perl\_0.04-6build1\_amd64.deb ...  
Unpacking libalgorithm-diff-xs-perl (0.04-6build1) ...  
Selecting previously unselected package libalgorithm-merge-perl.  
Preparing to unpack .../56-libalgorithm-merge-perl\_0.08-3\_all.deb ...  
Unpacking libalgorithm-merge-perl (0.08-3) ...  
Selecting previously unselected package libarchive-cpio-perl.  
Preparing to unpack .../57-libarchive-cpio-perl\_0.10-1.1\_all.deb ...  
Unpacking libarchive-cpio-perl (0.10-1.1) ...  
Selecting previously unselected package libc-devtools.  
Preparing to unpack .../58-libc-devtools\_2.33-0ubuntu5\_amd64.deb ...  
Unpacking libc-devtools (2.33-0ubuntu5) ...  
Selecting previously unselected package libexpat1-dev:amd64.  
Preparing to unpack .../59-libexpat1-dev\_2.2.10-2\_amd64.deb ...  
Unpacking libexpat1-dev:amd64 (2.2.10-2) ...  
Selecting previously unselected package libjs-jquery.  
Preparing to unpack .../60-libjs-jquery\_3.5.1+dfsg+~3.5.5-7\_all.deb ...  
Unpacking libjs-jquery (3.5.1+dfsg+~3.5.5-7) ...  
Selecting previously unselected package libjs-underscore.  
Preparing to unpack .../61-libjs-underscore\_1.9.1~dfsg-1ubuntu0.21.04.1\_all.deb ...

Unpacking libjs-underscore (1.9.1~dfsg-1ubuntu0.21.04.1) ...  
Selecting previously unselected package libjs-sphinxdoc.  
Preparing to unpack .../62-libjs-sphinxdoc\_3.5.4-1\_all.deb ...  
Unpacking libjs-sphinxdoc (3.5.4-1) ...  
Selecting previously unselected package libltdl-dev:amd64.  
Preparing to unpack .../63-libltdl-dev\_2.4.6-15\_amd64.deb ...  
Unpacking libltdl-dev:amd64 (2.4.6-15) ...  
Selecting previously unselected package liblua5.2-0:amd64.  
Preparing to unpack .../64-liblua5.2-0\_5.2.4-1.1build3\_amd64.deb ...  
Unpacking liblua5.2-0:amd64 (5.2.4-1.1build3) ...  
Selecting previously unselected package libsys-hostname-long-perl.  
Preparing to unpack .../65-libsys-hostname-long-perl\_1.5-2\_all.deb ...  
Unpacking libsys-hostname-long-perl (1.5-2) ...  
Selecting previously unselected package libmail-sendmail-perl.  
Preparing to unpack .../66-libmail-sendmail-perl\_0.80-1.1\_all.deb ...  
Unpacking libmail-sendmail-perl (0.80-1.1) ...  
Selecting previously unselected package libmysqlclient21:amd64.  
Preparing to unpack .../67-libmysqlclient21\_8.0.25-0ubuntu0.21.04.1\_amd64.deb ...  
Unpacking libmysqlclient21:amd64 (8.0.25-0ubuntu0.21.04.1) ...  
Selecting previously unselected package zlib1g-dev:amd64.  
Preparing to unpack .../68-zlib1g-dev\_1%3a1.2.11.dfsg-2ubuntu6\_amd64.deb ...  
Unpacking zlib1g-dev:amd64 (1:1.2.11.dfsg-2ubuntu6) ...  
Selecting previously unselected package libpython3.9-dev:amd64.  
Preparing to unpack .../69-libpython3.9-dev\_3.9.4-1\_amd64.deb ...  
Unpacking libpython3.9-dev:amd64 (3.9.4-1) ...  
Selecting previously unselected package libpython3-dev:amd64.  
Preparing to unpack .../70-libpython3-dev\_3.9.4-1\_amd64.deb ...  
Unpacking libpython3-dev:amd64 (3.9.4-1) ...  
Selecting previously unselected package librpmio9.  
Preparing to unpack .../71-librpmio9\_4.16.1.2+dfsg1-0.6ubuntu2\_amd64.deb ...  
Unpacking librpmio9 (4.16.1.2+dfsg1-0.6ubuntu2) ...  
Selecting previously unselected package librpm9.  
Preparing to unpack .../72-librpm9\_4.16.1.2+dfsg1-0.6ubuntu2\_amd64.deb ...  
Unpacking librpm9 (4.16.1.2+dfsg1-0.6ubuntu2) ...  
Selecting previously unselected package librpmbuild9.  
Preparing to unpack .../73-librpmbuild9\_4.16.1.2+dfsg1-0.6ubuntu2\_amd64.deb ...  
Unpacking librpmbuild9 (4.16.1.2+dfsg1-0.6ubuntu2) ...  
Selecting previously unselected package librpm9.  
Preparing to unpack .../74-librpm9\_4.16.1.2+dfsg1-0.6ubuntu2\_amd64.deb ...  
Unpacking librpm9 (4.16.1.2+dfsg1-0.6ubuntu2) ...  
Selecting previously unselected package manpages-dev.  
Preparing to unpack .../75-manpages-dev\_5.10-1\_all.deb ...  
Unpacking manpages-dev (5.10-1) ...  
Selecting previously unselected package python3.9-dev.  
Preparing to unpack .../76-python3.9-dev\_3.9.4-1\_amd64.deb ...  
Unpacking python3.9-dev (3.9.4-1) ...  
Selecting previously unselected package python3-lib2to3.  
Preparing to unpack .../77-python3-lib2to3\_3.9.4-0ubuntu1\_all.deb ...  
Unpacking python3-lib2to3 (3.9.4-0ubuntu1) ...

Selecting previously unselected package python3-distutils.  
 Preparing to unpack .../78-python3-distutils\_3.9.4-0ubuntu1\_all.deb ...  
 Unpacking python3-distutils (3.9.4-0ubuntu1) ...  
 Selecting previously unselected package python3-dev.  
 Preparing to unpack .../79-python3-dev\_3.9.4-1\_amd64.deb ...  
 Unpacking python3-dev (3.9.4-1) ...  
 Selecting previously unselected package python3-mysqldb.  
 Preparing to unpack .../80-python3-mysqldb\_1.4.4-2build3\_amd64.deb ...  
 Unpacking python3-mysqldb (1.4.4-2build3) ...  
 Selecting previously unselected package rpm-common.  
 Preparing to unpack .../81-rpm-common\_4.16.1.2+dfsg1-0.6ubuntu2\_amd64.deb ...  
 Unpacking rpm-common (4.16.1.2+dfsg1-0.6ubuntu2) ...  
 Selecting previously unselected package rpm2cpio.  
 Preparing to unpack .../82-rpm2cpio\_4.16.1.2+dfsg1-0.6ubuntu2\_amd64.deb ...  
 Unpacking rpm2cpio (4.16.1.2+dfsg1-0.6ubuntu2) ...  
 Selecting previously unselected package rpm.  
 Preparing to unpack .../83-rpm\_4.16.1.2+dfsg1-0.6ubuntu2\_amd64.deb ...  
 Unpacking rpm (4.16.1.2+dfsg1-0.6ubuntu2) ...  
 Selecting previously unselected package grr-server.  
 Preparing to unpack .../84-grr-server\_3.4.2-4\_amd64.deb ...  
 Unpacking grr-server (3.4.2-4) ...  
 Setting up javascript-common (11+nmu1) ...  
 Setting up manpages-dev (5.10-1) ...  
 Setting up libmysqlclient21:amd64 (8.0.25-0ubuntu0.21.04.1) ...  
 Setting up lto-disabled-list (7) ...  
 Setting up gettext (0.21-3ubuntu2) ...  
 Setting up libalgorithm-diff-perl (1.201-1) ...  
 Setting up libarchive-zip-perl (1.68-1) ...  
 Setting up libdebhelper-perl (13.3.4ubuntu1) ...  
 Setting up binutils-common:amd64 (2.36.1-6ubuntu1) ...  
 Setting up linux-libc-dev:amd64 (5.11.0-17.18) ...  
 Setting up libctf-nobfd0:amd64 (2.36.1-6ubuntu1) ...  
 Setting up libfakeroot:amd64 (1.25.3-1.1ubuntu2) ...  
 Setting up libasan6:amd64 (11.1.0-1ubuntu1~21.04) ...  
 Setting up intltool-debian (0.35.0+20060710.5) ...  
 Setting up fakeroot (1.25.3-1.1ubuntu2) ...  
 update-alternatives: using /usr/bin/fakeroot-sysv to provide /usr/bin/fakeroot (fakeroot) in auto mode  
 Setting up python3-mysqldb (1.4.4-2build3) ...  
 Setting up autotools-dev (20180224.1+nmu1) ...  
 Setting up libtirpc-dev:amd64 (1.3.1-1build1) ...  
 Setting up rpcsvc-proto (1.4.2-0ubuntu4) ...  
 Setting up make (4.3-4ubuntu1) ...  
 Setting up libsigsegv2:amd64 (2.13-1ubuntu1) ...  
 Setting up libquadmath0:amd64 (11.1.0-1ubuntu1~21.04) ...  
 Setting up libatomic1:amd64 (11.1.0-1ubuntu1~21.04) ...  
 Setting up autopoint (0.21-3ubuntu2) ...  
 Setting up libubsan1:amd64 (11.1.0-1ubuntu1~21.04) ...  
 Setting up dwz (0.14-1) ...



Setting up liblua5.2-0:amd64 (5.2.4-1.1build3) ...  
 Setting up libnsl-dev:amd64 (1.3.0-0ubuntu3) ...  
 Setting up libcrypt-dev:amd64 (1:4.4.17-1ubuntu3) ...  
 Setting up libarchive-cpio-perl (0.10-1.1) ...  
 Setting up debugedit (1:0.1-0ubuntu2) ...  
 Setting up libsub-override-perl (0.09-2) ...  
 Setting up libjs-jquery (3.5.1+dfsg+~3.5.5-7) ...  
 Setting up libbinutils:amd64 (2.36.1-6ubuntu1) ...  
 Setting up libc-dev-bin (2.33-0ubuntu5) ...  
 Setting up python3-lib2to3 (3.9.4-0ubuntu1) ...  
 Setting up libsys-hostname-long-perl (1.5-2) ...  
 Setting up libalgorithm-diff-xs-perl (0.04-6build1) ...  
 Setting up libcc1-0:amd64 (11.1.0-1ubuntu1~21.04) ...  
 Setting up liblsan0:amd64 (11.1.0-1ubuntu1~21.04) ...  
 Setting up libitm1:amd64 (11.1.0-1ubuntu1~21.04) ...  
 Setting up librpmio9 (4.16.1.2+dfsg1-0.6ubuntu2) ...  
 Setting up libc-devtools (2.33-0ubuntu5) ...  
 Setting up libjs-underscore (1.9.1~dfsg-1ubuntu0.21.04.1) ...  
 Setting up libalgorithm-merge-perl (0.08-3) ...  
 Setting up libtsan0:amd64 (11.1.0-1ubuntu1~21.04) ...  
 Setting up libctf0:amd64 (2.36.1-6ubuntu1) ...  
 Setting up python3-distutils (3.9.4-0ubuntu1) ...  
 Setting up libfile-stripnondeterminism-perl (1.11.0-1) ...  
 Setting up librpm9 (4.16.1.2+dfsg1-0.6ubuntu2) ...  
 Setting up po-debconf (1.0.21+nmu1) ...  
 Setting up libgcc-10-dev:amd64 (10.3.0-1ubuntu1) ...  
 Setting up m4 (1.4.18-5) ...  
 Setting up rpm-common (4.16.1.2+dfsg1-0.6ubuntu2) ...  
 Setting up libmail-sendmail-perl (0.80-1.1) ...  
 Setting up librpmbuild9 (4.16.1.2+dfsg1-0.6ubuntu2) ...  
 Setting up libjs-sphinxdoc (3.5.4-1) ...  
 Setting up autoconf (2.69-14) ...  
 Setting up dh-strip-nondeterminism (1.11.0-1) ...  
 Setting up librpm9 (4.16.1.2+dfsg1-0.6ubuntu2) ...  
 Setting up libc6-dev:amd64 (2.33-0ubuntu5) ...  
 Setting up binutils-x86-64-linux-gnu (2.36.1-6ubuntu1) ...  
 Setting up automake (1:1.16.3-2ubuntu1) ...  
 update-alternatives: using /usr/bin/automake-1.16 to provide /usr/bin/automake (automake) in auto mode  
 Setting up libstdc++-10-dev:amd64 (10.3.0-1ubuntu1) ...  
 Setting up rpm2cpio (4.16.1.2+dfsg1-0.6ubuntu2) ...  
 Setting up rpm (4.16.1.2+dfsg1-0.6ubuntu2) ...  
 Setting up binutils (2.36.1-6ubuntu1) ...  
 Setting up dpkg-dev (1.20.9ubuntu1) ...  
 Setting up libltdl-dev:amd64 (2.4.6-15) ...  
 Setting up libexpat1-dev:amd64 (2.2.10-2) ...  
 Setting up gcc-10 (10.3.0-1ubuntu1) ...  
 Setting up zlib1g-dev:amd64 (1:1.2.11.dfsg-2ubuntu6) ...  
 Setting up g++-10 (10.3.0-1ubuntu1) ...

```

Setting up libtool (2.4.6-15) ...
Setting up libpython3.9-dev:amd64 (3.9.4-1) ...
Setting up gcc (4:10.3.0-1ubuntu1) ...
Setting up dh-autoreconf (20) ...
Setting up g++ (4:10.3.0-1ubuntu1) ...
update-alternatives: using /usr/bin/g++ to provide /usr/bin/c++ (c++) in auto mode
Setting up python3.9-dev (3.9.4-1) ...
Setting up build-essential (12.8ubuntu3) ...
Setting up libpython3-dev:amd64 (3.9.4-1) ...
Setting up debhelper (13.3.4ubuntu1) ...
Setting up dh-make (2.202003) ...
Setting up python3-dev (3.9.4-1) ...
Setting up grr-server (3.4.2-4) ...
cp: cannot stat '/usr/bin/python3.6': No such file or directory
cp: cannot stat '/usr/bin/python3.6': No such file or directory
WARNING: Some error occured while updating /usr/share/grr-server/bin/python3
Created symlink /etc/systemd/system/multi-user.target.wants/grr-server.service → /lib/syste
m/systemd/system/grr-server.service.
fleetspeak-server.service is a disabled or a static unit, not starting it.
Adding system user `fleetspeak' (UID 128) ...
Adding new user `fleetspeak' (UID 128) with group `nogroup' ...
Creating home directory `/home/fleetspeak' ...
#####
Running grr_config_updater initialize
To avoid this prompting, set DEBIAN_FRONTEND=noninteractive
#####
Could not find platform independent libraries <prefix>
Could not find platform dependent libraries <exec_prefix>
Consider setting $PYTHONHOME to <prefix>[:<exec_prefix>]
Fatal Python error: Py_Initialize: Unable to get the locale encoding
ModuleNotFoundError: No module named 'encodings'

Current thread 0x00007f32dc4d4740 (most recent call first):
/usr/bin/grr_config_updater: line 34: 4806 Aborted          (core dumped)
"${GRR_PREFIX}/bin/${NAME}" "${GRR_EXTRA_ARGS[@]}" "${@}"
dpkg: error processing package grr-server (--configure):
 installed grr-server package post-installation script subprocess returned error exit status 134
Processing triggers for libc-bin (2.33-0ubuntu5) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for install-info (6.7.0.dfsg.2-6) ...
Errors were encountered while processing:
 grr-server
N: Download is performed unsandboxed as root as file '/home/z/grr-server_3.4.2-4_amd64.deb'
couldn't be accessed by user '_apt'. - pkgAcquire::Run (13: Permission denied)
E: Sub-process /usr/bin/dpkg returned an error code (1)

```

## Liite 5. TheHive asennus



TheHive install.txt

```

z@z:~$ sudo apt-get install -y openjdk-8-jre-headless
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ca-certificates-java java-common
Suggested packages:
  default-jre fonts-dejavu-extra fonts-ipafont-gothic fonts-ipafont-mincho fonts-wqy-microhei
fonts-wqy-zenhei
The following NEW packages will be installed:
  ca-certificates-java java-common openjdk-8-jre-headless
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 28,2 MB of archives.
After this operation, 104 MB of additional disk space will be used.
Get:1 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 java-common all 0.72 [6 816 B]
Get:2 http://fi.archive.ubuntu.com/ubuntu hirsute-updates/universe amd64 openjdk-8-jre-head-
less amd64 8u292-b10-0ubuntu1 [28,2 MB]
Get:3 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 ca-certificates-java all 20190909
[12,1 kB]
Fetched 28,2 MB in 4s (7 437 kB/s)
Selecting previously unselected package java-common.
(Reading database ... 165502 files and directories currently installed.)
Preparing to unpack .../java-common_0.72_all.deb ...
Unpacking java-common (0.72) ...
Selecting previously unselected package openjdk-8-jre-headless:amd64.
Preparing to unpack .../openjdk-8-jre-headless_8u292-b10-0ubuntu1_amd64.deb ...
Unpacking openjdk-8-jre-headless:amd64 (8u292-b10-0ubuntu1) ...
Selecting previously unselected package ca-certificates-java.
Preparing to unpack .../ca-certificates-java_20190909_all.deb ...
Unpacking ca-certificates-java (20190909) ...
Setting up java-common (0.72) ...
Setting up openjdk-8-jre-headless:amd64 (8u292-b10-0ubuntu1) ...
update-alternatives: using /usr/lib/jvm/java-8-openjdk-amd64/jre/bin/java to provide
/usr/bin/java (java) in auto mode
update-alternatives: using /usr/lib/jvm/java-8-openjdk-amd64/jre/bin/jjs to provide /usr/bin/jjs
(jjs) in auto mode
update-alternatives: using /usr/lib/jvm/java-8-openjdk-amd64/jre/bin/keytool to provide
/usr/bin/keytool (keytool) in auto mode
update-alternatives: using /usr/lib/jvm/java-8-openjdk-amd64/jre/bin/pack200 to provide
/usr/bin/pack200 (pack200) in auto mode

```

update-alternatives: using /usr/lib/jvm/java-8-openjdk-amd64/jre/bin/rmid to provide /usr/bin/rmid (rmid) in auto mode

update-alternatives: using /usr/lib/jvm/java-8-openjdk-amd64/jre/bin/rmiregistry to provide /usr/bin/rmiregistry (rmiregistry) in auto mode

update-alternatives: using /usr/lib/jvm/java-8-openjdk-amd64/jre/bin/unpack200 to provide /usr/bin/unpack200 (unpack200) in auto mode

update-alternatives: using /usr/lib/jvm/java-8-openjdk-amd64/jre/bin/orbd to provide /usr/bin/orbd (orbd) in auto mode

update-alternatives: using /usr/lib/jvm/java-8-openjdk-amd64/jre/bin/servertool to provide /usr/bin/servertool (servertool) in auto mode

update-alternatives: using /usr/lib/jvm/java-8-openjdk-amd64/jre/bin/tnameserv to provide /usr/bin/tnameserv (tnameserv) in auto mode

update-alternatives: using /usr/lib/jvm/java-8-openjdk-amd64/jre/lib/jexec to provide /usr/bin/jexec (jexec) in auto mode

WARNING: tempfile is deprecated; consider using mktemp instead.

Setting up ca-certificates-java (20190909) ...

head: cannot open '/etc/ssl/certs/java/cacerts' for reading: No such file or directory

Adding debian:Microsec\_e-Szigno\_Root\_CA\_2009.pem

Adding debian:Microsoft\_ECC\_Root\_Certificate\_Authority\_2017.pem

Adding debian:COMODO\_ECC\_Certification\_Authority.pem

Adding debian:EC-ACC.pem

Adding debian:D-TRUST\_Root\_Class\_3\_CA\_2\_EV\_2009.pem

Adding debian:GlobalSign\_Root\_CA.pem

Adding debian:emSign\_Root\_CA\_-\_C1.pem

Adding debian:QuoVadis\_Root\_CA\_1\_G3.pem

Adding debian:GlobalSign\_Root\_CA\_-\_R3.pem

Adding debian:Entrust\_Root\_Certification\_Authority\_-\_G2.pem

Adding debian:Go\_Daddy\_Root\_Certificate\_Authority\_-\_G2.pem

Adding debian:Go\_Daddy\_Class\_2\_CA.pem

Adding debian:Atos\_TrustedRoot\_2011.pem

Adding debian:T-TeleSec\_GlobalRoot\_Class\_3.pem

Adding debian:TUBITAK\_Kamu\_SM\_SSL\_Kok\_Sertifikasi\_-\_Surum\_1.pem

Adding debian:Trustwave\_Global\_Certification\_Authority.pem

Adding debian:Chambers\_of\_Commerce\_Root\_-\_2008.pem

Adding debian:Hongkong\_Post\_Root\_CA\_1.pem

Adding debian:Starfield\_Root\_Certificate\_Authority\_-\_G2.pem

Adding debian:GlobalSign\_Root\_CA\_-\_R6.pem

Adding debian:ISRG\_Root\_X1.pem

Adding debian:DigiCert\_Assured\_ID\_Root\_G3.pem

Adding debian:GTS\_Root\_R4.pem

Adding debian:Cybertrust\_Global\_Root.pem

Adding debian:Actalis\_Authentication\_Root\_CA.pem

Adding debian:SecureTrust\_CA.pem

Adding debian:AC\_RAIZ\_FNMT-RCM.pem

Adding debian:SwissSign\_Silver\_CA\_-\_G2.pem

Adding debian:Certum\_Trusted\_Network\_CA\_2.pem

Adding debian:Amazon\_Root\_CA\_4.pem

Adding debian:QuoVadis\_Root\_CA\_2\_G3.pem

Adding debian:DigiCert\_Assured\_ID\_Root\_CA.pem

Adding debian:ssl-cert-snakeoil.pem  
Adding debian:Entrust.net\_Premium\_2048\_Secure\_Server\_CA.pem  
Adding debian:COMODO\_Certification\_Authority.pem  
Adding debian:Certigna.pem  
Adding debian:CA\_Disig\_Root\_R2.pem  
Adding debian:Network\_Solutions\_Certificate\_Authority.pem  
Adding debian:AffirmTrust\_Premium\_ECC.pem  
Adding debian:DigiCert\_Global\_Root\_G2.pem  
Adding debian:Starfield\_Services\_Root\_Certificate\_Authority\_-\_G2.pem  
Adding debian:DigiCert\_Assured\_ID\_Root\_G2.pem  
Adding debian:SSL.com\_EV\_Root\_Certification\_Authority\_ECC.pem  
Adding debian:ACCVRAIZ1.pem  
Adding debian:DST\_Root\_CA\_X3.pem  
Adding debian:Buypass\_Class\_2\_Root\_CA.pem  
Adding debian:QuoVadis\_Root\_CA\_2.pem  
Adding debian:SecureSign\_RootCA11.pem  
Adding debian:TrustCor\_ECA-1.pem  
Adding debian:AffirmTrust\_Commercial.pem  
Adding debian:USERTrust\_ECC\_Certification\_Authority.pem  
Adding debian:Microsoft\_RSA\_Root\_Certificate\_Authority\_2017.pem  
Adding debian:USERTrust\_RSA\_Certification\_Authority.pem  
Adding debian:Staat\_der\_Nederlanden\_Root\_CA\_-\_G3.pem  
Adding debian:SZAFIR\_ROOT\_CA2.pem  
Adding debian:Hellenic\_Academic\_and\_Research\_Institutions\_RootCA\_2015.pem  
Adding debian:Amazon\_Root\_CA\_1.pem  
Adding debian:Staat\_der\_Nederlanden\_EV\_Root\_CA.pem  
Adding debian:D-TRUST\_Root\_Class\_3\_CA\_2\_2009.pem  
Adding debian:OISTE\_WISeKey\_Global\_Root\_GC\_CA.pem  
Adding debian:TrustCor\_RootCert\_CA-2.pem  
Adding debian:SwissSign\_Gold\_CA\_-\_G2.pem  
Adding debian:Hellenic\_Academic\_and\_Research\_Institutions\_ECC\_RootCA\_2015.pem  
Adding debian:Amazon\_Root\_CA\_3.pem  
Adding debian:XRamp\_Global\_CA\_Root.pem  
Adding debian:Hellenic\_Academic\_and\_Research\_Institutions\_RootCA\_2011.pem  
Adding debian:Security\_Communication\_RootCA2.pem  
Adding debian:Certum\_Trusted\_Network\_CA.pem  
Adding debian:GTS\_Root\_R2.pem  
Adding debian:certSIGN\_Root\_CA\_G2.pem  
Adding debian:Autoridad\_de\_Certificacion\_Firmaprofesional\_CIF\_A62634068.pem  
Adding debian:UCA\_Global\_G2\_Root.pem  
Adding debian:DigiCert\_High\_Assurance\_EV\_Root\_CA.pem  
Adding debian:GlobalSign\_ECC\_Root\_CA\_-\_R4.pem  
Adding debian:DigiCert\_Global\_Root\_G3.pem  
Adding debian:TWCA\_Global\_Root\_CA.pem  
Adding debian:VeriSign\_Universal\_Root\_Certification\_Authority.pem  
Adding debian:GeoTrust\_Primary\_Certification\_Authority\_-\_G2.pem  
Adding debian:QuoVadis\_Root\_CA.pem  
Adding debian:IdenTrust\_Commercial\_Root\_CA\_1.pem  
Adding debian:E-Tugra\_Certification\_Authority.pem

Adding debian:SSL.com\_Root\_Certification\_Authority\_ECC.pem  
Adding debian:Entrust\_Root\_Certification\_Authority\_-\_EC1.pem  
Adding debian:GTS\_Root\_R1.pem  
Adding debian:IdenTrust\_Public\_Sector\_Root\_CA\_1.pem  
Adding debian:Sonera\_Class\_2\_Root\_CA.pem  
Adding debian:TWCA\_Root\_Certification\_Authority.pem  
Adding debian:e-Szigno\_Root\_CA\_2017.pem  
Adding debian:Secure\_Global\_CA.pem  
Adding debian:Security\_Communication\_Root\_CA.pem  
Adding debian:Starfield\_Class\_2\_CA.pem  
Adding debian:Certigna\_Root\_CA.pem  
Adding debian:DigiCert\_Trusted\_Root\_G4.pem  
Adding debian:GlobalSign\_ECC\_Root\_CA\_-\_R5.pem  
Adding debian:SSL.com\_EV\_Root\_Certification\_Authority\_RSA\_R2.pem  
Adding debian:GlobalSign\_Root\_CA\_-\_R2.pem  
Adding debian:certSIGN\_ROOT\_CA.pem  
Adding debian:Trustwave\_Global\_ECC\_P256\_Certification\_Authority.pem  
Adding debian:COMODO\_RSA\_Certification\_Authority.pem  
Adding debian:SSL.com\_Root\_Certification\_Authority\_RSA.pem  
Adding debian:CFCA\_EV\_ROOT.pem  
Adding debian:Comodo\_AAA\_Services\_root.pem  
Adding debian:OISTE\_WISEKey\_Global\_Root\_GB\_CA.pem  
Adding debian:Baltimore\_CyberTrust\_Root.pem  
Adding debian:Entrust\_Root\_Certification\_Authority\_-\_G4.pem  
Adding debian:GDCA\_TrustAUTH\_R5\_ROOT.pem  
Adding debian:TrustCor\_RootCert\_CA-1.pem  
Adding debian:Entrust\_Root\_Certification\_Authority.pem  
Adding debian:UCA\_Extended\_Validation\_Root.pem  
Adding debian:NAVER\_Global\_Root\_Certification\_Authority.pem  
Adding debian:TeliaSonera\_Root\_CA\_v1.pem  
Adding debian:T-TeleSec\_GlobalRoot\_Class\_2.pem  
Adding debian:Amazon\_Root\_CA\_2.pem  
Adding debian:GTS\_Root\_R3.pem  
Adding debian:QuoVadis\_Root\_CA\_3\_G3.pem  
Adding debian:Trustwave\_Global\_ECC\_P384\_Certification\_Authority.pem  
Adding debian:NetLock\_Arany\_=Class\_Gold=\_Főtanúsítvány.pem  
Adding debian:AffirmTrust\_Premium.pem  
Adding debian:lzenpe.com.pem  
Adding debian:emSign\_Root\_CA\_-\_G1.pem  
Adding debian:AffirmTrust\_Networking.pem  
Adding debian:ePKI\_Root\_Certification\_Authority.pem  
Adding debian:Trustis\_FPS\_Root\_CA.pem  
Adding debian:emSign\_ECC\_Root\_CA\_-\_G3.pem  
Adding debian:Hongkong\_Post\_Root\_CA\_3.pem  
Adding debian:QuoVadis\_Root\_CA\_3.pem  
Adding debian:Global\_Chambersign\_Root\_-\_2008.pem  
Adding debian:Buypass\_Class\_3\_Root\_CA.pem  
Adding debian:emSign\_ECC\_Root\_CA\_-\_C3.pem  
Adding debian:DigiCert\_Global\_Root\_CA.pem

done.

Processing triggers for man-db (2.9.4-2) ...

Processing triggers for ca-certificates (20210119build1) ...

Updating certificates in /etc/ssl/certs...

0 added, 0 removed; done.

Running hooks in /etc/ca-certificates/update.d...

done.

done.

```
z@z:~$ echo JAVA_HOME="/usr/lib/jvm/java-8-openjdk-amd64" >> /etc/environment
```

```
bash: /etc/environment: Permission denied
```

```
z@z:~$ sudo echo JAVA_HOME="/usr/lib/jvm/java-8-openjdk-amd64" >> /etc/environment
```

```
bash: /etc/environment: Permission denied
```

```
z@z:~$ export JAVA_HOME="/usr/lib/jvm/java-8-openjdk-amd64"
```

```
z@z:~$ curl -fsSL https://www.apache.org/dist/cassandra/KEYS | sudo apt-key add -
```

```
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
```

```
Command 'curl' not found, but can be installed with:
```

```
sudo snap install curl # version 7.76.1, or
```

```
sudo apt install curl # version 7.74.0-1ubuntu2
```

```
See 'snap info curl' for additional versions.
```

```
gpg: no valid OpenPGP data found.
```

```
z@z:~$ sudo apt install curl
```

```
Reading package lists... Done
```

```
Building dependency tree... Done
```

```
Reading state information... Done
```

```
The following NEW packages will be installed:
```

```
curl
```

```
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
```

```
Need to get 170 kB of archives.
```

```
After this operation, 430 kB of additional disk space will be used.
```

```
Get:1 http://fi.archive.ubuntu.com/ubuntu hirsute/main amd64 curl amd64 7.74.0-1ubuntu2 [170 kB]
```

```
Fetches 170 kB in 0s (1 024 kB/s)
```

```
Selecting previously unselected package curl.
```

```
(Reading database ... 165757 files and directories currently installed.)
```

```
Preparing to unpack .../curl_7.74.0-1ubuntu2_amd64.deb ...
```

```
Unpacking curl (7.74.0-1ubuntu2) ...
```

```
Setting up curl (7.74.0-1ubuntu2) ...
```

```
Processing triggers for man-db (2.9.4-2) ...
```

```
z@z:~$ curl -fsSL https://www.apache.org/dist/cassandra/KEYS | sudo apt-key add -
```

```
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
```

```
OK
```

```
z@z:~$ echo "deb http://www.apache.org/dist/cassandra/debian 311x main" | sudo tee -a /etc/apt/sources.list.d/cassandra.sources.list
```

```
deb http://www.apache.org/dist/cassandra/debian 311x main
```

```
z@z:~$ sudo apt update
```

```
Hit:1 http://fi.archive.ubuntu.com/ubuntu hirsute InRelease
```

```
Hit:3 http://fi.archive.ubuntu.com/ubuntu hirsute-updates InRelease
```

```
Hit:4 http://fi.archive.ubuntu.com/ubuntu hirsute-backports InRelease
```

```

Hit:5 http://security.ubuntu.com/ubuntu hirsute-security InRelease
Get:2 https://downloads.apache.org/cassandra/debian 311x InRelease [3 903 B]
Get:6 https://downloads.apache.org/cassandra/debian 311x/main amd64 Packages [686 B]
Get:7 https://downloads.apache.org/cassandra/debian 311x/main i386 Packages [686 B]
Fetched 5 275 B in 1s (6 678 B/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
z@z:~$ sudo apt install cassandra
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libpython2-stdlib libpython2.7-minimal libpython2.7-stdlib python-is-python2 python2 python2-
minimal python2.7 python2.7-minimal
Suggested packages:
  cassandra-tools python2-doc python-tk python2.7-doc binutils binfmt-support
The following NEW packages will be installed:
  cassandra libpython2-stdlib libpython2.7-minimal libpython2.7-stdlib python-is-python2 python2
python2-minimal python2.7 python2.7-minimal
0 upgraded, 9 newly installed, 0 to remove and 0 not upgraded.
Need to get 34,4 MB of archives.
After this operation, 56,8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:2 http://fi.archive.ubuntu.com/ubuntu hirsute/universe amd64 libpython2.7-minimal amd64
2.7.18-6 [335 kB]
Get:3 http://fi.archive.ubuntu.com/ubuntu hirsute/universe amd64 python2.7-minimal amd64
2.7.18-6 [1 260 kB]
Get:1 https://downloads.apache.org/cassandra/debian 311x/main amd64 cassandra all 3.11.10
[30,7 MB]
Get:4 http://fi.archive.ubuntu.com/ubuntu hirsute/universe amd64 python2-minimal amd64
2.7.18-2 [13,5 kB]
Get:5 http://fi.archive.ubuntu.com/ubuntu hirsute/universe amd64 libpython2.7-stdlib amd64
2.7.18-6 [1 867 kB]
Get:6 http://fi.archive.ubuntu.com/ubuntu hirsute/universe amd64 python2.7 amd64 2.7.18-6
[248 kB]
Get:7 http://fi.archive.ubuntu.com/ubuntu hirsute/universe amd64 libpython2-stdlib amd64
2.7.18-2 [7 332 B]
Get:8 http://fi.archive.ubuntu.com/ubuntu hirsute/universe amd64 python2 amd64 2.7.18-2
[9 068 B]
Get:9 http://fi.archive.ubuntu.com/ubuntu hirsute/universe amd64 python-is-python2 all 2.7.18-9
[2 976 B]
Fetched 34,4 MB in 6s (6 208 kB/s)
Selecting previously unselected package libpython2.7-minimal:amd64.
(Reading database ... 165764 files and directories currently installed.)
Preparing to unpack .../0-libpython2.7-minimal_2.7.18-6_amd64.deb ...
Unpacking libpython2.7-minimal:amd64 (2.7.18-6) ...
Selecting previously unselected package python2.7-minimal.

```



```

Preparing to unpack .../1-python2.7-minimal_2.7.18-6_amd64.deb ...
Unpacking python2.7-minimal (2.7.18-6) ...
Selecting previously unselected package python2-minimal.
Preparing to unpack .../2-python2-minimal_2.7.18-2_amd64.deb ...
Unpacking python2-minimal (2.7.18-2) ...
Selecting previously unselected package libpython2.7-stdlib:amd64.
Preparing to unpack .../3-libpython2.7-stdlib_2.7.18-6_amd64.deb ...
Unpacking libpython2.7-stdlib:amd64 (2.7.18-6) ...
Selecting previously unselected package python2.7.
Preparing to unpack .../4-python2.7_2.7.18-6_amd64.deb ...
Unpacking python2.7 (2.7.18-6) ...
Selecting previously unselected package libpython2-stdlib:amd64.
Preparing to unpack .../5-libpython2-stdlib_2.7.18-2_amd64.deb ...
Unpacking libpython2-stdlib:amd64 (2.7.18-2) ...
Setting up libpython2.7-minimal:amd64 (2.7.18-6) ...
Setting up python2.7-minimal (2.7.18-6) ...
Linking and byte-compiling packages for runtime python2.7...
Setting up python2-minimal (2.7.18-2) ...
Selecting previously unselected package python2.
(Reading database ... 166499 files and directories currently installed.)
Preparing to unpack .../python2_2.7.18-2_amd64.deb ...
Unpacking python2 (2.7.18-2) ...
Selecting previously unselected package python-is-python2.
Preparing to unpack .../python-is-python2_2.7.18-9_all.deb ...
Unpacking python-is-python2 (2.7.18-9) ...
Selecting previously unselected package cassandra.
Preparing to unpack .../cassandra_3.11.10_all.deb ...
Unpacking cassandra (3.11.10) ...
Setting up libpython2.7-stdlib:amd64 (2.7.18-6) ...
Setting up python2.7 (2.7.18-6) ...
Setting up libpython2-stdlib:amd64 (2.7.18-2) ...
Setting up python2 (2.7.18-2) ...
Setting up python-is-python2 (2.7.18-9) ...
Setting up cassandra (3.11.10) ...
Adding group `cassandra' (GID 134) ...
Done.
vm.max_map_count = 1048575
net.ipv4.tcp_keepalive_time = 300
update-rc.d: warning: start and stop actions are no longer supported; falling back to defaults
Processing triggers for desktop-file-utils (0.26-1ubuntu1) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for mailcap (3.68ubuntu1) ...
z@z:~$ cqlsh localhost 9042
Connected to Test Cluster at localhost:9042.
[cqlsh 5.0.1 | Cassandra 3.11.10 | CQL spec 3.4.4 | Native protocol v4]
Use HELP for help.
cqlsh> UPDATE system.local SET cluster_name = 'thp' where key='local';
cqlsh> exit

```



```
1+0 records out
1024 bytes (1,0 kB, 1,0 KiB) copied, 0,000557336 s, 1,8 MB/s
z@z:~$ sudo nano /etc/thehive/application.conf
z@z:~$ chown -R thehive:thehive /opt/thp_data/files/thehive
chown: changing ownership of '/opt/thp_data/files/thehive': Operation not permitted
z@z:~$ sudo chown -R thehive:thehive /opt/thp_data/files/thehive
z@z:~$ sudo nano /etc/thehive/application.conf
z@z:~$ service thehive start
```

## Liite 6. Shuffle asennus



Shuffle install.txt

```
z@z:~$ git clone https://github.com/frikky/Shuffle
Cloning into 'Shuffle'...
remote: Enumerating objects: 9479, done.
remote: Counting objects: 100% (3961/3961), done.
remote: Compressing objects: 100% (1785/1785), done.
remote: Total 9479 (delta 3001), reused 2986 (delta 2147), pack-reused 5518
Receiving objects: 100% (9479/9479), 51.98 MiB | 4.71 MiB/s, done.
Resolving deltas: 100% (7152/7152), done.
z@z:~$ cd Shuffle
z@z:~/Shuffle$ sudo chown 1000:1000 -R shuffle-database
[sudo] password for z:
chown: cannot access 'shuffle-database': No such file or directory
z@z:~/Shuffle$ docker-compose up -d
Starting shuffle-backend ... done
Starting shuffle-opensearch ... done
Starting shuffle-orborus ... done
Starting shuffle-frontend ... done
z@z:~/Shuffle$ sudo chown 1000:1000 -R shuffle-database
z@z:~/Shuffle$ sudo docker-compose restart
Restarting shuffle-frontend ... done
Restarting shuffle-orborus ... done
Restarting shuffle-opensearch ... done
Restarting shuffle-backend ... done
```

## Liite 7. GRR Rapid Response asennus 2



GRR install 2.txt

```

z@z:~$ sudo apt install -y mysql-server
[sudo] password for z:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
 fonts-liberation2 fonts-opensymbol gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0 gir1.2-gudev-
1.0 gir1.2-udisks-2.0 grilo-plugins-0.3-base
 gstreamer1.0-gtk3 libboost-date-time1.65.1 libboost-filesystem1.65.1 libboost-iostreams1.65.1
libboost-locale1.65.1 libcdr-0.1-1
 libclucene-contribs1v5 libclucene-core1v5 libcmis-0.5-5v5 libcolamd2 libdazzle-1.0-0 libe-book-
0.1-1 libedataserverui-1.2-2 libeat0 libepubgen-0.1-1
 libetonyek-0.1-1 libevent-2.1-6 libexiv2-14 libfreerdp-client2-2 libfreerdp2-2 libgc1c2 libgee-0.8-2
libgexiv2-2 libgom-1.0-0 libgpgmepp6
 libgpod-common libgpod4 liblangtag-common liblangtag1 liblirc-client0 liblua5.3-0 libmediaart-
2.0-0 libmsp-0.1-1 libodfgen-0.1-1 libqqwing2v5
 libraw16 librevenge-0.0-0 libsgutils2-2 libssh-4 libsuitesparseconfig5 libvncclient1 libwinpr2-2
libxapian30 libxmlsec1 libxmlsec1-nss lp-solve
 media-player-info python3-mako python3-markupsafe syslinux syslinux-common syslinux-legacy
usb-creator-common
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
 libaio1 libevent-core-2.1-6 libhtml-template-perl mysql-client-5.7 mysql-client-core-5.7 mysql-
common mysql-server-5.7 mysql-server-core-5.7
Suggested packages:
 libipc-sharedcache-perl mailx tinyca
The following NEW packages will be installed:
 libaio1 libevent-core-2.1-6 libhtml-template-perl mysql-client-5.7 mysql-client-core-5.7 mysql-
common mysql-server mysql-server-5.7
mysql-server-core-5.7
0 upgraded, 9 newly installed, 0 to remove and 67 not upgraded.
Need to get 19,1 MB of archives.
After this operation, 154 MB of additional disk space will be used.
Get:1 http://fi.archive.ubuntu.com/ubuntu bionic/main amd64 mysql-common all 5.8+1.0.4
[7 308 B]
Get:2 http://fi.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libaio1 amd64 0.3.110-
5ubuntu0.1 [6 476 B]
Get:3 http://fi.archive.ubuntu.com/ubuntu bionic-updates/main amd64 mysql-client-core-5.7
amd64 5.7.36-0ubuntu0.18.04.1 [6 638 kB]
Get:4 http://fi.archive.ubuntu.com/ubuntu bionic-updates/main amd64 mysql-client-5.7 amd64
5.7.36-0ubuntu0.18.04.1 [1 942 kB]
Get:5 http://fi.archive.ubuntu.com/ubuntu bionic-updates/main amd64 mysql-server-core-5.7
amd64 5.7.36-0ubuntu0.18.04.1 [7 426 kB]

```

```

Get:6 http://fi.archive.ubuntu.com/ubuntu bionic/main amd64 libevent-core-2.1-6 amd64 2.1.8-
stable-4build1 [85,9 kB]
Get:7 http://fi.archive.ubuntu.com/ubuntu bionic-updates/main amd64 mysql-server-5.7 amd64
5.7.36-0ubuntu0.18.04.1 [2 906 kB]
Get:8 http://fi.archive.ubuntu.com/ubuntu bionic/main amd64 libhtml-template-perl all 2.97-1
[59,0 kB]
Get:9 http://fi.archive.ubuntu.com/ubuntu bionic-updates/main amd64 mysql-server all 5.7.36-
0ubuntu0.18.04.1 [9 944 B]
Fetched 19,1 MB in 28s (673 kB/s)
Preconfiguring packages ...
Selecting previously unselected package mysql-common.
(Reading database ... 114570 files and directories currently installed.)
Preparing to unpack .../0-mysql-common_5.8+1.0.4_all.deb ...
Unpacking mysql-common (5.8+1.0.4) ...
Selecting previously unselected package libaio1:amd64.
Preparing to unpack .../1-libaio1_0.3.110-5ubuntu0.1_amd64.deb ...
Unpacking libaio1:amd64 (0.3.110-5ubuntu0.1) ...
Selecting previously unselected package mysql-client-core-5.7.
Preparing to unpack .../2-mysql-client-core-5.7_5.7.36-0ubuntu0.18.04.1_amd64.deb ...
Unpacking mysql-client-core-5.7 (5.7.36-0ubuntu0.18.04.1) ...
Selecting previously unselected package mysql-client-5.7.
Preparing to unpack .../3-mysql-client-5.7_5.7.36-0ubuntu0.18.04.1_amd64.deb ...
Unpacking mysql-client-5.7 (5.7.36-0ubuntu0.18.04.1) ...
Selecting previously unselected package mysql-server-core-5.7.
Preparing to unpack .../4-mysql-server-core-5.7_5.7.36-0ubuntu0.18.04.1_amd64.deb ...
Unpacking mysql-server-core-5.7 (5.7.36-0ubuntu0.18.04.1) ...
Selecting previously unselected package libevent-core-2.1-6:amd64.
Preparing to unpack .../5-libevent-core-2.1-6_2.1.8-stable-4build1_amd64.deb ...
Unpacking libevent-core-2.1-6:amd64 (2.1.8-stable-4build1) ...
Setting up mysql-common (5.8+1.0.4) ...
update-alternatives: using /etc/mysql/my.cnf.fallback to provide /etc/mysql/my.cnf (my.cnf) in
auto mode
Selecting previously unselected package mysql-server-5.7.
(Reading database ... 114738 files and directories currently installed.)
Preparing to unpack .../mysql-server-5.7_5.7.36-0ubuntu0.18.04.1_amd64.deb ...
Unpacking mysql-server-5.7 (5.7.36-0ubuntu0.18.04.1) ...
Selecting previously unselected package libhtml-template-perl.
Preparing to unpack .../libhtml-template-perl_2.97-1_all.deb ...
Unpacking libhtml-template-perl (2.97-1) ...
Selecting previously unselected package mysql-server.
Preparing to unpack .../mysql-server_5.7.36-0ubuntu0.18.04.1_all.deb ...
Unpacking mysql-server (5.7.36-0ubuntu0.18.04.1) ...
Setting up libevent-core-2.1-6:amd64 (2.1.8-stable-4build1) ...
Setting up libhtml-template-perl (2.97-1) ...
Setting up libaio1:amd64 (0.3.110-5ubuntu0.1) ...
Setting up mysql-client-core-5.7 (5.7.36-0ubuntu0.18.04.1) ...
Setting up mysql-server-core-5.7 (5.7.36-0ubuntu0.18.04.1) ...
Setting up mysql-client-5.7 (5.7.36-0ubuntu0.18.04.1) ...
Setting up mysql-server-5.7 (5.7.36-0ubuntu0.18.04.1) ...

```

update-alternatives: using /etc/mysql/mysql.cnf to provide /etc/mysql/my.cnf (my.cnf) in auto mode

Renaming removed key\_buffer and myisam-recover options (if present)

Created symlink /etc/systemd/system/multi-user.target.wants/mysql.service → /lib/systemd/system/mysql.service.

Setting up mysql-server (5.7.36-0ubuntu0.18.04.1) ...

Processing triggers for libc-bin (2.27-3ubuntu1.4) ...

Processing triggers for systemd (237-3ubuntu10.52) ...

Processing triggers for man-db (2.8.3-2ubuntu0.1) ...

Processing triggers for ureadahead (0.100.0-21) ...

```
z@z:~$ sudo nano /etc/mysql/my.cnf
```

```
z@z:~$ service mysql restart
```

```
z@z:~$ sudo mysql -u root -p
```

Enter password:

Welcome to the MySQL monitor. Commands end with ; or \g.

Your MySQL connection id is 2

Server version: 5.7.36-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

```
mysql> CREATE USER 'grr'@'localhost' IDENTIFIED BY 'z';
```

```
Query OK, 0 rows affected (0,00 sec)
```

```
mysql> CREATE DATABASE grr;
```

```
Query OK, 1 row affected (0,00 sec)
```

```
mysql> GRANT ALL ON grr.* TO 'grr'@'localhost';
```

```
Query OK, 0 rows affected (0,00 sec)
```

```
mysql> CREATE USER 'fleetspeak'@'localhost' IDENTIFIED BY 'z';
```

```
Query OK, 0 rows affected (0,00 sec)
```

```
mysql> CREATE DATABASE fleetspeak;
```

```
Query OK, 1 row affected (0,00 sec)
```

```
mysql> GRANT ALL ON fleetspeak.* TO 'fleetspeak'@'localhost';
```

```
Query OK, 0 rows affected (0,00 sec)
```

```
mysql> exit
```

Bye

```
z@z:~$ wget https://storage.googleapis.com/releases.grr-response.com/grr-server_3.4.5-1_amd64.deb
```

```
--2021-12-02 17:14:51-- https://storage.googleapis.com/releases.grr-response.com/grr-
server_3.4.5-1_amd64.deb
Resolving storage.googleapis.com (storage.googleapis.com)... 216.58.209.176, 216.58.210.144,
216.58.209.208, ...
Connecting to storage.googleapis.com (storage.googleapis.com)|216.58.209.176|:443... con-
nected.
HTTP request sent, awaiting response... 200 OK
Length: 141762472 (135M) [application/vnd.debian.binary-package]
Saving to: 'grr-server_3.4.5-1_amd64.deb'
```

```
grr-server_3.4.5-1_amd64.deb
100%[=====>
] 135,19M  916KB/s  in 5m 37s
```

```
2021-12-02 17:20:29 (411 KB/s) - 'grr-server_3.4.5-1_amd64.deb' saved [141762472/141762472]
```

```
z@z:~$ sudo apt install -y ./grr-server_3.4.5-1_amd64.deb
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'grr-server' instead of './grr-server_3.4.5-1_amd64.deb'
The following packages were automatically installed and are no longer required:
 fonts-liberation2 fonts-opensymbol gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0 gir1.2-gudev-
1.0 gir1.2-udisks-2.0 grilo-plugins-0.3-base
 gstreamer1.0-gtk3 libboost-date-time1.65.1 libboost-filesystem1.65.1 libboost-iostreams1.65.1
 libboost-locale1.65.1 libcdr-0.1-1
 libclucene-contribs1v5 libclucene-core1v5 libcmis-0.5-5v5 libcolamd2 libdazzle-1.0-0 libe-book-
0.1-1 libedataserverui-1.2-2 libeot0 libepubgen-0.1-1
 libetonyek-0.1-1 libevent-2.1-6 libexiv2-14 libfreerdp-client2-2 libfreerdp2-2 libgc1c2 libgee-0.8-2
 libgexiv2-2 libgom-1.0-0 libgpgmepp6
 libgpod-common libgpod4 liblangtag-common liblangtag1 liblirc-client0 liblua5.3-0 libmediaart-
2.0-0 libmsspub-0.1-1 libodfgen-0.1-1 libqqwing2v5
 libraw16 librevenge-0.0-0 libsgutils2-2 libssh-4 libsuitesparseconfig5 libvncclient1 libwinpr2-2
 libxapian30 libxmlsec1 libxmlsec1-nss lp-solve
 media-player-info python3-mako python3-markupsafe syslinux syslinux-common syslinux-legacy
 usb-creator-common
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
 autoconf automake autopoint autotools-dev build-essential debhelper debugedit dh-autoreconf
 dh-make dh-python dh-strip-nondeterminism dpkg-dev
 fakeroot g++ g++-7 gcc gcc-7 libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-
perl libarchive-cpio-perl libasan4 libatomic1
 libc-dev-bin libc6-dev libcilkrts5 libexpat1-dev libfakeroot libfile-stripnondeterminism-perl libgcc-
7-dev libitm1 liblsan0 libltdl-dev liblua5.2-0
 libmail-sendmail-perl libmpx2 libmysqlclient20 libpython3-dev libpython3.6-dev libquadmath0
 librpm8 librpmbuild8 librpmio8 librpsign8 libsigsegv2
 libstdc++-7-dev libsys-hostname-long-perl libtool libtsan0 libubsan0 linux-libc-dev m4 make
 manpages-dev po-debconf python3-dev python3-distutils
 python3-lib2to3 python3-mysqldb python3.6-dev rpm rpm-common rpm2cpio
```



## Suggested packages:

autoconf-archive gnu-standards autoconf-doc dwz rpm-i18n debian-keyring g++-multilib g++-7-multilib gcc-7-doc libstdc++6-7-dbg gcc-multilib flex bison  
gcc-doc gcc-7-multilib gcc-7-locales libgcc1-dbg libgomp1-dbg libitm1-dbg libatomic1-dbg libasan4-dbg liblsan0-dbg libtsan0-dbg libubsan0-dbg  
libcilkrts5-dbg libmpx2-dbg libquadmath0-dbg glibc-doc libtool-doc libstdc++-7-doc gfortran |  
fortran95-compiler gcj-jdk m4-doc make-doc  
libmail-box-perl python-egenix-mxdatetime python3-mysqldb-dbg alien python elfutils rpmlint rpm2html

## The following NEW packages will be installed:

autoconf automake autopoint autotools-dev build-essential debhelper debugedit dh-autoreconf dh-make dh-python dh-strip-nondeterminism dpkg-dev  
fakeroot g++ g++-7 gcc gcc-7 grr-server libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libarchive-cpio-perl libasan4  
libatomic1 libc-dev-bin libc6-dev libcilkrts5 libexpat1-dev libfakeroot libfile-stripnondeterminism-perl libgcc-7-dev libitm1 liblsan0 libltdl-dev  
liblua5.2-0 libmail-sendmail-perl libmpx2 libmysqlclient20 libpython3-dev libpython3.6-dev libquadmath0 librpm8 librpmbuild8 librpmio8 librpsign8  
libsigsegv2 libstdc++-7-dev libsys-hostname-long-perl libtool libtsan0 libubsan0 linux-libc-dev m4 make manpages-dev po-debconf python3-dev  
python3-distutils python3-lib2to3 python3-mysqldb python3.6-dev rpm rpm-common rpm2cpio  
0 upgraded, 64 newly installed, 0 to remove and 67 not upgraded.

Need to get 81,1 MB/223 MB of archives.

After this operation, 544 MB of additional disk space will be used.

Get:1 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 libsigsegv2 amd64 2.12-1 [14,7 kB]  
Get:2 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 m4 amd64 1.4.18-1 [197 kB]  
Get:3 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 autoconf all 2.69-11 [322 kB]  
Get:4 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 autotools-dev all 20180224.1 [39,6 kB]  
Get:5 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 automake all 1:1.15.1-3ubuntu2 [509 kB]  
Get:6 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 autopoint all 0.19.8.1-6ubuntu0.3 [426 kB]  
Get:7 [/home/z/grr-server\\_3.4.5-1\\_amd64.deb](http://home/z/grr-server_3.4.5-1_amd64.deb) grr-server amd64 3.4.5-1 [142 MB]  
Get:8 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 libc-dev-bin amd64 2.27-3ubuntu1.4 [71,8 kB]  
Get:9 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 linux-libc-dev amd64 4.15.0-163.171 [994 kB]  
Get:10 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 libc6-dev amd64 2.27-3ubuntu1.4 [2 585 kB]  
Get:11 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 libitm1 amd64 8.4.0-1ubuntu1~18.04 [27,9 kB]  
Get:12 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 libatomic1 amd64 8.4.0-1ubuntu1~18.04 [9 192 B]  
Get:13 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 libasan4 amd64 7.5.0-3ubuntu1~18.04 [358 kB]  
Get:14 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 liblsan0 amd64 8.4.0-1ubuntu1~18.04 [133 kB]

Get:15 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 libtsan0 amd64 8.4.0-1ubuntu1~18.04 [288 kB]  
Get:16 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 libubsan0 amd64 7.5.0-3ubuntu1~18.04 [126 kB]  
Get:17 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 libcilkrts5 amd64 7.5.0-3ubuntu1~18.04 [42,5 kB]  
Get:18 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 libmpx2 amd64 8.4.0-1ubuntu1~18.04 [11,6 kB]  
Get:19 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 libquadmath0 amd64 8.4.0-1ubuntu1~18.04 [134 kB]  
Get:20 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 libgcc-7-dev amd64 7.5.0-3ubuntu1~18.04 [2 378 kB]  
Get:21 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 gcc-7 amd64 7.5.0-3ubuntu1~18.04 [9 381 kB]  
Get:22 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 gcc amd64 4:7.4.0-1ubuntu2.3 [5 184 B]  
Get:23 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 libstdc++-7-dev amd64 7.5.0-3ubuntu1~18.04 [1 471 kB]  
Get:24 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 g++-7 amd64 7.5.0-3ubuntu1~18.04 [9 697 kB]  
Get:25 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 g++ amd64 4:7.4.0-1ubuntu2.3 [1 568 B]  
Get:26 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 make amd64 4.1-9.1ubuntu1 [154 kB]  
Get:27 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 dpkg-dev all 1.19.0.5ubuntu2.3 [607 kB]  
Get:28 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 build-essential amd64 12.4ubuntu1 [4 758 B]  
Get:29 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 libtool all 2.4.6-2 [194 kB]  
Get:30 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 dh-autoreconf all 17 [15,8 kB]  
Get:31 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 libfile-stripnondeterminism-perl all 0.040-1.1~build1 [13,8 kB]  
Get:32 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 dh-strip-nondeterminism all 0.040-1.1~build1 [5 208 B]  
Get:33 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 po-debconf all 1.0.20 [232 kB]  
Get:34 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 debhelper all 11.1.6ubuntu2 [902 kB]  
Get:35 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 liblua5.2-0 amd64 5.2.4-1.1build1 [108 kB]  
Get:36 <http://fi.archive.ubuntu.com/ubuntu> bionic/universe amd64 librpmio8 amd64 4.14.1+dfsg1-2 [74,6 kB]  
Get:37 <http://fi.archive.ubuntu.com/ubuntu> bionic/universe amd64 debugedit amd64 4.14.1+dfsg1-2 [19,1 kB]  
Get:38 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 dh-make all 2.201701 [31,6 kB]  
Get:39 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 python3-lib2to3 all 3.6.9-1~18.04 [77,4 kB]  
Get:40 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 python3-distutils all 3.6.9-1~18.04 [144 kB]

Get:41 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 dh-python all 3.20180325ubuntu2 [89,2 kB]  
Get:42 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 libfakeroot amd64 1.22-2ubuntu1 [25,9 kB]  
Get:43 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 fakeroot amd64 1.22-2ubuntu1 [62,3 kB]  
Get:44 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 libalgorithm-diff-perl all 1.19.03-1 [47,6 kB]  
Get:45 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 libalgorithm-diff-xs-perl amd64 0.04-5 [11,1 kB]  
Get:46 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 libalgorithm-merge-perl all 0.08-3 [12,0 kB]  
Get:47 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 libarchive-cpio-perl all 0.10-1 [9 644 B]  
Get:48 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 libexpat1-dev amd64 2.2.5-3ubuntu0.2 [122 kB]  
Get:49 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 libltdl-dev amd64 2.4.6-2 [162 kB]  
Get:50 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 libsys-hostname-long-perl all 1.5-1 [11,7 kB]  
Get:51 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 libmail-sendmail-perl all 0.80-1 [22,6 kB]  
Get:52 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 libmysqlclient20 amd64 5.7.36-0ubuntu0.18.04.1 [689 kB]  
Get:53 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 libpython3.6-dev amd64 3.6.9-1~18.04ubuntu1.4 [44,9 MB]  
Get:54 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 libpython3-dev amd64 3.6.7-1~18.04 [7 328 B]  
Get:55 <http://fi.archive.ubuntu.com/ubuntu> bionic/universe amd64 librpm8 amd64 4.14.1+dfsg1-2 [173 kB]  
Get:56 <http://fi.archive.ubuntu.com/ubuntu> bionic/universe amd64 librpm-build8 amd64 4.14.1+dfsg1-2 [70,5 kB]  
Get:57 <http://fi.archive.ubuntu.com/ubuntu> bionic/universe amd64 librpm-sign8 amd64 4.14.1+dfsg1-2 [8 184 B]  
Get:58 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 manpages-dev all 4.15-1 [2 217 kB]  
Get:59 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 python3.6-dev amd64 3.6.9-1~18.04ubuntu1.4 [508 kB]  
Get:60 <http://fi.archive.ubuntu.com/ubuntu> bionic-updates/main amd64 python3-dev amd64 3.6.7-1~18.04 [1 288 B]  
Get:61 <http://fi.archive.ubuntu.com/ubuntu> bionic/main amd64 python3-mysqldb amd64 1.3.10-1build1 [46,0 kB]  
Get:62 <http://fi.archive.ubuntu.com/ubuntu> bionic/universe amd64 rpm-common amd64 4.14.1+dfsg1-2 [28,7 kB]  
Get:63 <http://fi.archive.ubuntu.com/ubuntu> bionic/universe amd64 rpm2cpio amd64 4.14.1+dfsg1-2 [7 988 B]  
Get:64 <http://fi.archive.ubuntu.com/ubuntu> bionic/universe amd64 rpm amd64 4.14.1+dfsg1-2 [119 kB]  
Fetched 81,1 MB in 3min 0s (451 kB/s)

Extracting templates from packages: 100%  
Selecting previously unselected package libsigsegv2:amd64.  
(Reading database ... 114839 files and directories currently installed.)  
Preparing to unpack .../00-libsigsegv2\_2.12-1\_amd64.deb ...  
Unpacking libsigsegv2:amd64 (2.12-1) ...  
Selecting previously unselected package m4.  
Preparing to unpack .../01-m4\_1.4.18-1\_amd64.deb ...  
Unpacking m4 (1.4.18-1) ...  
Selecting previously unselected package autoconf.  
Preparing to unpack .../02-autoconf\_2.69-11\_all.deb ...  
Unpacking autoconf (2.69-11) ...  
Selecting previously unselected package autotools-dev.  
Preparing to unpack .../03-autotools-dev\_20180224.1\_all.deb ...  
Unpacking autotools-dev (20180224.1) ...  
Selecting previously unselected package automake.  
Preparing to unpack .../04-automake\_1%3a1.15.1-3ubuntu2\_all.deb ...  
Unpacking automake (1:1.15.1-3ubuntu2) ...  
Selecting previously unselected package autopoint.  
Preparing to unpack .../05-autopoint\_0.19.8.1-6ubuntu0.3\_all.deb ...  
Unpacking autopoint (0.19.8.1-6ubuntu0.3) ...  
Selecting previously unselected package libc-dev-bin.  
Preparing to unpack .../06-libc-dev-bin\_2.27-3ubuntu1.4\_amd64.deb ...  
Unpacking libc-dev-bin (2.27-3ubuntu1.4) ...  
Selecting previously unselected package linux-libc-dev:amd64.  
Preparing to unpack .../07-linux-libc-dev\_4.15.0-163.171\_amd64.deb ...  
Unpacking linux-libc-dev:amd64 (4.15.0-163.171) ...  
Selecting previously unselected package libc6-dev:amd64.  
Preparing to unpack .../08-libc6-dev\_2.27-3ubuntu1.4\_amd64.deb ...  
Unpacking libc6-dev:amd64 (2.27-3ubuntu1.4) ...  
Selecting previously unselected package libitm1:amd64.  
Preparing to unpack .../09-libitm1\_8.4.0-1ubuntu1~18.04\_amd64.deb ...  
Unpacking libitm1:amd64 (8.4.0-1ubuntu1~18.04) ...  
Selecting previously unselected package libatomic1:amd64.  
Preparing to unpack .../10-libatomic1\_8.4.0-1ubuntu1~18.04\_amd64.deb ...  
Unpacking libatomic1:amd64 (8.4.0-1ubuntu1~18.04) ...  
Selecting previously unselected package libasan4:amd64.  
Preparing to unpack .../11-libasan4\_7.5.0-3ubuntu1~18.04\_amd64.deb ...  
Unpacking libasan4:amd64 (7.5.0-3ubuntu1~18.04) ...  
Selecting previously unselected package liblsan0:amd64.  
Preparing to unpack .../12-liblsan0\_8.4.0-1ubuntu1~18.04\_amd64.deb ...  
Unpacking liblsan0:amd64 (8.4.0-1ubuntu1~18.04) ...  
Selecting previously unselected package libtsan0:amd64.  
Preparing to unpack .../13-libtsan0\_8.4.0-1ubuntu1~18.04\_amd64.deb ...  
Unpacking libtsan0:amd64 (8.4.0-1ubuntu1~18.04) ...  
Selecting previously unselected package libubsan0:amd64.  
Preparing to unpack .../14-libubsan0\_7.5.0-3ubuntu1~18.04\_amd64.deb ...  
Unpacking libubsan0:amd64 (7.5.0-3ubuntu1~18.04) ...  
Selecting previously unselected package libcilkrts5:amd64.  
Preparing to unpack .../15-libcilkrts5\_7.5.0-3ubuntu1~18.04\_amd64.deb ...

Unpacking libcilkrts5:amd64 (7.5.0-3ubuntu1~18.04) ...  
Selecting previously unselected package libmpx2:amd64.  
Preparing to unpack .../16-libmpx2\_8.4.0-1ubuntu1~18.04\_amd64.deb ...  
Unpacking libmpx2:amd64 (8.4.0-1ubuntu1~18.04) ...  
Selecting previously unselected package libquadmath0:amd64.  
Preparing to unpack .../17-libquadmath0\_8.4.0-1ubuntu1~18.04\_amd64.deb ...  
Unpacking libquadmath0:amd64 (8.4.0-1ubuntu1~18.04) ...  
Selecting previously unselected package libgcc-7-dev:amd64.  
Preparing to unpack .../18-libgcc-7-dev\_7.5.0-3ubuntu1~18.04\_amd64.deb ...  
Unpacking libgcc-7-dev:amd64 (7.5.0-3ubuntu1~18.04) ...  
Selecting previously unselected package gcc-7.  
Preparing to unpack .../19-gcc-7\_7.5.0-3ubuntu1~18.04\_amd64.deb ...  
Unpacking gcc-7 (7.5.0-3ubuntu1~18.04) ...  
Selecting previously unselected package gcc.  
Preparing to unpack .../20-gcc\_4%3a7.4.0-1ubuntu2.3\_amd64.deb ...  
Unpacking gcc (4:7.4.0-1ubuntu2.3) ...  
Selecting previously unselected package libstdc++-7-dev:amd64.  
Preparing to unpack .../21-libstdc++-7-dev\_7.5.0-3ubuntu1~18.04\_amd64.deb ...  
Unpacking libstdc++-7-dev:amd64 (7.5.0-3ubuntu1~18.04) ...  
Selecting previously unselected package g++-7.  
Preparing to unpack .../22-g++-7\_7.5.0-3ubuntu1~18.04\_amd64.deb ...  
Unpacking g++-7 (7.5.0-3ubuntu1~18.04) ...  
Selecting previously unselected package g++.  
Preparing to unpack .../23-g++\_4%3a7.4.0-1ubuntu2.3\_amd64.deb ...  
Unpacking g++ (4:7.4.0-1ubuntu2.3) ...  
Selecting previously unselected package make.  
Preparing to unpack .../24-make\_4.1-9.1ubuntu1\_amd64.deb ...  
Unpacking make (4.1-9.1ubuntu1) ...  
Selecting previously unselected package dpkg-dev.  
Preparing to unpack .../25-dpkg-dev\_1.19.0.5ubuntu2.3\_all.deb ...  
Unpacking dpkg-dev (1.19.0.5ubuntu2.3) ...  
Selecting previously unselected package build-essential.  
Preparing to unpack .../26-build-essential\_12.4ubuntu1\_amd64.deb ...  
Unpacking build-essential (12.4ubuntu1) ...  
Selecting previously unselected package libtool.  
Preparing to unpack .../27-libtool\_2.4.6-2\_all.deb ...  
Unpacking libtool (2.4.6-2) ...  
Selecting previously unselected package dh-autoreconf.  
Preparing to unpack .../28-dh-autoreconf\_17\_all.deb ...  
Unpacking dh-autoreconf (17) ...  
Selecting previously unselected package libfile-stripnondeterminism-perl.  
Preparing to unpack .../29-libfile-stripnondeterminism-perl\_0.040-1.1~build1\_all.deb ...  
Unpacking libfile-stripnondeterminism-perl (0.040-1.1~build1) ...  
Selecting previously unselected package dh-strip-nondeterminism.  
Preparing to unpack .../30-dh-strip-nondeterminism\_0.040-1.1~build1\_all.deb ...  
Unpacking dh-strip-nondeterminism (0.040-1.1~build1) ...  
Selecting previously unselected package po-debconf.  
Preparing to unpack .../31-po-debconf\_1.0.20\_all.deb ...  
Unpacking po-debconf (1.0.20) ...

Selecting previously unselected package debhelper.  
Preparing to unpack .../32-debhelper\_11.1.6ubuntu2\_all.deb ...  
Unpacking debhelper (11.1.6ubuntu2) ...  
Selecting previously unselected package liblua5.2-0:amd64.  
Preparing to unpack .../33-liblua5.2-0\_5.2.4-1.1build1\_amd64.deb ...  
Unpacking liblua5.2-0:amd64 (5.2.4-1.1build1) ...  
Selecting previously unselected package librpmio8.  
Preparing to unpack .../34-librpmio8\_4.14.1+dfsg1-2\_amd64.deb ...  
Unpacking librpmio8 (4.14.1+dfsg1-2) ...  
Selecting previously unselected package debugedit.  
Preparing to unpack .../35-debugedit\_4.14.1+dfsg1-2\_amd64.deb ...  
Unpacking debugedit (4.14.1+dfsg1-2) ...  
Selecting previously unselected package dh-make.  
Preparing to unpack .../36-dh-make\_2.201701\_all.deb ...  
Unpacking dh-make (2.201701) ...  
Selecting previously unselected package python3-lib2to3.  
Preparing to unpack .../37-python3-lib2to3\_3.6.9-1~18.04\_all.deb ...  
Unpacking python3-lib2to3 (3.6.9-1~18.04) ...  
Selecting previously unselected package python3-distutils.  
Preparing to unpack .../38-python3-distutils\_3.6.9-1~18.04\_all.deb ...  
Unpacking python3-distutils (3.6.9-1~18.04) ...  
Selecting previously unselected package dh-python.  
Preparing to unpack .../39-dh-python\_3.20180325ubuntu2\_all.deb ...  
Unpacking dh-python (3.20180325ubuntu2) ...  
Selecting previously unselected package libfakeroot:amd64.  
Preparing to unpack .../40-libfakeroot\_1.22-2ubuntu1\_amd64.deb ...  
Unpacking libfakeroot:amd64 (1.22-2ubuntu1) ...  
Selecting previously unselected package fakeroot.  
Preparing to unpack .../41-fakeroot\_1.22-2ubuntu1\_amd64.deb ...  
Unpacking fakeroot (1.22-2ubuntu1) ...  
Selecting previously unselected package libalgorithm-diff-perl.  
Preparing to unpack .../42-libalgorithm-diff-perl\_1.19.03-1\_all.deb ...  
Unpacking libalgorithm-diff-perl (1.19.03-1) ...  
Selecting previously unselected package libalgorithm-diff-xs-perl.  
Preparing to unpack .../43-libalgorithm-diff-xs-perl\_0.04-5\_amd64.deb ...  
Unpacking libalgorithm-diff-xs-perl (0.04-5) ...  
Selecting previously unselected package libalgorithm-merge-perl.  
Preparing to unpack .../44-libalgorithm-merge-perl\_0.08-3\_all.deb ...  
Unpacking libalgorithm-merge-perl (0.08-3) ...  
Selecting previously unselected package libarchive-cpio-perl.  
Preparing to unpack .../45-libarchive-cpio-perl\_0.10-1\_all.deb ...  
Unpacking libarchive-cpio-perl (0.10-1) ...  
Selecting previously unselected package libexpat1-dev:amd64.  
Preparing to unpack .../46-libexpat1-dev\_2.2.5-3ubuntu0.2\_amd64.deb ...  
Unpacking libexpat1-dev:amd64 (2.2.5-3ubuntu0.2) ...  
Selecting previously unselected package libltdl-dev:amd64.  
Preparing to unpack .../47-libltdl-dev\_2.4.6-2\_amd64.deb ...  
Unpacking libltdl-dev:amd64 (2.4.6-2) ...  
Selecting previously unselected package libsys-hostname-long-perl.

Preparing to unpack .../48-libsys-hostname-long-perl\_1.5-1\_all.deb ...  
Unpacking libsys-hostname-long-perl (1.5-1) ...  
Selecting previously unselected package libmail-sendmail-perl.  
Preparing to unpack .../49-libmail-sendmail-perl\_0.80-1\_all.deb ...  
Unpacking libmail-sendmail-perl (0.80-1) ...  
Selecting previously unselected package libmysqlclient20:amd64.  
Preparing to unpack .../50-libmysqlclient20\_5.7.36-0ubuntu0.18.04.1\_amd64.deb ...  
Unpacking libmysqlclient20:amd64 (5.7.36-0ubuntu0.18.04.1) ...  
Selecting previously unselected package libpython3.6-dev:amd64.  
Preparing to unpack .../51-libpython3.6-dev\_3.6.9-1~18.04ubuntu1.4\_amd64.deb ...  
Unpacking libpython3.6-dev:amd64 (3.6.9-1~18.04ubuntu1.4) ...  
Selecting previously unselected package libpython3-dev:amd64.  
Preparing to unpack .../52-libpython3-dev\_3.6.7-1~18.04\_amd64.deb ...  
Unpacking libpython3-dev:amd64 (3.6.7-1~18.04) ...  
Selecting previously unselected package librpm8.  
Preparing to unpack .../53-librpm8\_4.14.1+dfsg1-2\_amd64.deb ...  
Unpacking librpm8 (4.14.1+dfsg1-2) ...  
Selecting previously unselected package librpmbuild8.  
Preparing to unpack .../54-librpmbuild8\_4.14.1+dfsg1-2\_amd64.deb ...  
Unpacking librpmbuild8 (4.14.1+dfsg1-2) ...  
Selecting previously unselected package librpm8-sign8.  
Preparing to unpack .../55-librpm8-sign8\_4.14.1+dfsg1-2\_amd64.deb ...  
Unpacking librpm8-sign8 (4.14.1+dfsg1-2) ...  
Selecting previously unselected package manpages-dev.  
Preparing to unpack .../56-manpages-dev\_4.15-1\_all.deb ...  
Unpacking manpages-dev (4.15-1) ...  
Selecting previously unselected package python3.6-dev.  
Preparing to unpack .../57-python3.6-dev\_3.6.9-1~18.04ubuntu1.4\_amd64.deb ...  
Unpacking python3.6-dev (3.6.9-1~18.04ubuntu1.4) ...  
Selecting previously unselected package python3-dev.  
Preparing to unpack .../58-python3-dev\_3.6.7-1~18.04\_amd64.deb ...  
Unpacking python3-dev (3.6.7-1~18.04) ...  
Selecting previously unselected package python3-mysqldb.  
Preparing to unpack .../59-python3-mysqldb\_1.3.10-1build1\_amd64.deb ...  
Unpacking python3-mysqldb (1.3.10-1build1) ...  
Selecting previously unselected package rpm-common.  
Preparing to unpack .../60-rpm-common\_4.14.1+dfsg1-2\_amd64.deb ...  
Unpacking rpm-common (4.14.1+dfsg1-2) ...  
Selecting previously unselected package rpm2cpio.  
Preparing to unpack .../61-rpm2cpio\_4.14.1+dfsg1-2\_amd64.deb ...  
Unpacking rpm2cpio (4.14.1+dfsg1-2) ...  
Selecting previously unselected package rpm.  
Preparing to unpack .../62-rpm\_4.14.1+dfsg1-2\_amd64.deb ...  
Unpacking rpm (4.14.1+dfsg1-2) ...  
Selecting previously unselected package grr-server.  
Preparing to unpack .../63-grr-server\_3.4.5-1\_amd64.deb ...  
Unpacking grr-server (3.4.5-1) ...  
Setting up libquadmath0:amd64 (8.4.0-1ubuntu1~18.04) ...  
Setting up libatomic1:amd64 (8.4.0-1ubuntu1~18.04) ...

Setting up make (4.1-9.1ubuntu1) ...  
 Setting up libltdl-dev:amd64 (2.4.6-2) ...  
 Setting up po-debconf (1.0.20) ...  
 Setting up libasan4:amd64 (7.5.0-3ubuntu1~18.04) ...  
 Setting up libsigsegv2:amd64 (2.12-1) ...  
 Setting up libcilkrts5:amd64 (7.5.0-3ubuntu1~18.04) ...  
 Setting up libubsan0:amd64 (7.5.0-3ubuntu1~18.04) ...  
 Setting up libtsan0:amd64 (8.4.0-1ubuntu1~18.04) ...  
 Setting up linux-libc-dev:amd64 (4.15.0-163.171) ...  
 Setting up libarchive-cpio-perl (0.10-1) ...  
 Setting up m4 (1.4.18-1) ...  
 Setting up liblsan0:amd64 (8.4.0-1ubuntu1~18.04) ...  
 Setting up libsys-hostname-long-perl (1.5-1) ...  
 Setting up libmpx2:amd64 (8.4.0-1ubuntu1~18.04) ...  
 Setting up dpkg-dev (1.19.0.5ubuntu2.3) ...  
 Setting up libmail-sendmail-perl (0.80-1) ...  
 Setting up autotools-dev (20180224.1) ...  
 Setting up libfakeroot:amd64 (1.22-2ubuntu1) ...  
 Setting up libalgorithm-diff-perl (1.19.03-1) ...  
 Setting up libmysqlclient20:amd64 (5.7.36-0ubuntu0.18.04.1) ...  
 Setting up libc-dev-bin (2.27-3ubuntu1.4) ...  
 Setting up liblua5.2-0:amd64 (5.2.4-1.1build1) ...  
 Setting up python3-lib2to3 (3.6.9-1~18.04) ...  
 Setting up manpages-dev (4.15-1) ...  
 Setting up libc6-dev:amd64 (2.27-3ubuntu1.4) ...  
 Setting up python3-distutils (3.6.9-1~18.04) ...  
 Setting up libitm1:amd64 (8.4.0-1ubuntu1~18.04) ...  
 Setting up autopoint (0.19.8.1-6ubuntu0.3) ...  
 Setting up libfile-stripnondeterminism-perl (0.040-1.1~build1) ...  
 Setting up librpmio8 (4.14.1+dfsg1-2) ...  
 Setting up debugedit (4.14.1+dfsg1-2) ...  
 Setting up python3-mysqldb (1.3.10-1build1) ...  
 Setting up autoconf (2.69-11) ...  
 Setting up fakeroot (1.22-2ubuntu1) ...  
 update-alternatives: using /usr/bin/fakeroot-sysv to provide /usr/bin/fakeroot (fakeroot) in auto mode  
 Setting up libgcc-7-dev:amd64 (7.5.0-3ubuntu1~18.04) ...  
 Setting up libstdc++-7-dev:amd64 (7.5.0-3ubuntu1~18.04) ...  
 Setting up libalgorithm-merge-perl (0.08-3) ...  
 Setting up libalgorithm-diff-xs-perl (0.04-5) ...  
 Setting up automake (1:1.15.1-3ubuntu2) ...  
 update-alternatives: using /usr/bin/automake-1.15 to provide /usr/bin/automake (automake) in auto mode  
 Setting up libexpat1-dev:amd64 (2.2.5-3ubuntu0.2) ...  
 Setting up dh-python (3.20180325ubuntu2) ...  
 Setting up librpm8 (4.14.1+dfsg1-2) ...  
 Setting up gcc-7 (7.5.0-3ubuntu1~18.04) ...  
 Setting up g++-7 (7.5.0-3ubuntu1~18.04) ...  
 Setting up rpm-common (4.14.1+dfsg1-2) ...



```

Setting up librpmsign8 (4.14.1+dfsg1-2) ...
Setting up gcc (4:7.4.0-1ubuntu2.3) ...
Setting up libpython3.6-dev:amd64 (3.6.9-1~18.04ubuntu1.4) ...
Setting up librpmbuild8 (4.14.1+dfsg1-2) ...
Setting up rpm2cpio (4.14.1+dfsg1-2) ...
Setting up g++ (4:7.4.0-1ubuntu2.3) ...
update-alternatives: using /usr/bin/g++ to provide /usr/bin/c++ (c++) in auto mode
Setting up python3.6-dev (3.6.9-1~18.04ubuntu1.4) ...
Setting up libpython3-dev:amd64 (3.6.7-1~18.04) ...
Setting up libtool (2.4.6-2) ...
Setting up build-essential (12.4ubuntu1) ...
Setting up python3-dev (3.6.7-1~18.04) ...
Setting up rpm (4.14.1+dfsg1-2) ...
Setting up dh-autoreconf (17) ...
Setting up dh-strip-nondeterminism (0.040-1.1~build1) ...
Setting up debhelper (11.1.6ubuntu2) ...
Setting up dh-make (2.201701) ...
Setting up grr-server (3.4.5-1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/grr-server.service → /lib/sys-
temd/system/grr-server.service.
Adding system user `fleetspeak' (UID 123) ...
Adding new user `fleetspeak' (UID 123) with group `nogroup' ...
Creating home directory `/home/fleetspeak' ...
#####
Running grr_config_updater initialize
To avoid this prompting, set DEBIAN_FRONTEND=noninteractive
#####
Checking write access on config /etc/grr//server.local.yaml

```

Step 0: Importing Configuration from previous installation.  
No old config file found.

#### Step 1: Setting Basic Configuration Parameters

We are now going to configure the server using a bunch of questions.

Use Fleetspeak (next generation communication framework)? [Yn]: [Y]: y

Please enter your hostname e.g. grr.example.com [z]: z

Fleetspeak public HTTPS port [4443]: 4443

Fleetspeak MySQL Host [localhost]: localhost

Fleetspeak MySQL Port (0 for local socket) [3306]: 3306

Fleetspeak MySQL Database [fleetspeak]: fleetspeak

Fleetspeak MySQL Username [root]: root

Please enter password for database user root:

Unexpected operational error encountered while trying to connect to MySQL. 2 attempts left:  
(1698, "Access denied for user 'root'@'localhost'")

Unexpected operational error encountered while trying to connect to MySQL. 1 attempts left:  
(1698, "Access denied for user 'root'@'localhost'")

Unexpected operational error encountered while trying to connect to MySQL. 0 attempts left:  
(1698, "Access denied for user 'root'@'localhost'")

Successfully connected to MySQL with the given configuration.

**--GRR Datastore--**

For GRR to work each GRR server has to be able to communicate with the datastore. To do this we need to configure a datastore.

GRR will use MySQL as its database backend. Enter connection details:

MySQL Host [localhost]: localhost

MySQL Port (0 for local socket) [0]: 0

MySQL Database [grr]: grr

MySQL Username [root]: root

Please enter password for database user root:

Configure SSL connections for MySQL? [yN]: [N]: N

Successfully connected to MySQL with the provided details.

**--GRR URLs--**

For GRR to work each client has to be able to communicate with the server. To do this we normally need a public dns name or IP address to communicate with. In the standard configuration this will be used to host both the client facing server and the admin user interface.

Please enter your hostname e.g. grr.example.com [z]: z

**--Server URL--**

The Server URL specifies the URL that the clients will connect to communicate with the server. For best results this should be publicly accessible. By default this will be port 8080 with the URL ending in /control.

Frontend URL [http://z:8080/]: http://z:8080/

**--AdminUI URL--:**

The UI URL specifies where the Administrative Web Interface can be found.

AdminUI URL [http://z:8000]: http://z:8000

**--GRR Emails--**

GRR needs to be able to send emails for various logging and alerting functions. The email domain will be appended to GRR usernames when sending emails to users.

**--Monitoring/Email Domain--**

Emails concerning alerts or updates must be sent to this domain.

Email Domain e.g example.com [localhost]: localhost

--Alert Email Address--

Address where monitoring events get sent, e.g. crashed clients, broken server, etc.

Alert Email Address [grr-monitoring@localhost]: grr-monitoring@localhost

--Emergency Email Address--

Address where high priority events such as an emergency ACL bypass are sent.

Emergency Access Email Address [grr-emergency@localhost]: grr-emergency@localhost

Step 2: Key Generation

All keys will have a bit length of 2048.

Generating executable signing key

Generating CA keys

Generating Server keys

Generating secret key for csrf protection.

Writing configuration to /etc/grr//server.local.yaml.

I1202 17:28:03.115618 140144321877824 config\_parser.py:119] Writing back configuration to file /etc/grr//server.local.yaml

Initializing the datastore.

I1202 17:28:03.653266 140144321877824 server\_logging.py:188] Writing log file to /usr/share/grr-server/lib/python3.6/site-packages/grr\_response\_core/var/log//GRRlog.txt

Step 3: Adding GRR Admin User

Please enter password for user 'admin':

Step 4: Repackaging clients with new configuration.

Server debs include client templates. Re-download templates? [yN]: [N]: N

Repack client templates? [Yn]: [Y]: Y

Repacking template: /usr/share/grr-server/grr-response-templates/templates/GRR\_3.4.5.1\_amd64.exe.zip

Using context: ['Target:Windows', 'ClientBuilder Context', 'ClientBuilder Context', 'Arch:amd64', 'Platform:Windows', 'Target:Windows'] and labels: []

Repacked into /usr/share/grr-server/executables/installers/GRR\_3.4.5.1\_amd64.exe

Repacking as debug installer: /usr/share/grr-server/grr-response-templates/templates/GRR\_3.4.5.1\_amd64.exe.zip.

Repacking template: /usr/share/grr-server/grr-response-templates/templates/GRR\_3.4.5.1\_amd64.exe.zip

Using context: ['Target:Windows', 'ClientBuilder Context', 'ClientBuilder Context', 'Arch:amd64', 'Platform:Windows', 'Target:Windows', 'DebugClientBuild Context'] and labels: []

Repacked into /usr/share/grr-server/executables/installers/dbg\_GRR\_3.4.5.1\_amd64.exe

Repacking template: /usr/share/grr-server/grr-response-templates/templates/GRR\_3.4.5.1\_amd64.msi.zip

Using context: ['Target:Windows', 'ClientBuilder Context', 'ClientBuilder Context', 'Arch:amd64', 'Platform:Windows', 'Target:Windows', 'Target:WindowsMsi'] and labels: []

Repacked into /usr/share/grr-server/executables/installers/GRR\_3.4.5.1\_amd64.msi

Repacking as debug installer: /usr/share/grr-server/grr-response-templates/tem-plates/GRR\_3.4.5.1\_amd64.msi.zip.

Repacking template: /usr/share/grr-server/grr-response-templates/tem-plates/GRR\_3.4.5.1\_amd64.msi.zip

Using context: ['Target:Windows', 'ClientBuilder Context', 'ClientBuilder Context', 'Arch:amd64', 'Platform:Windows', 'Target:Windows', 'Target:WindowsMsi', 'DebugClientBuild Context'] and labels: []

Repacked into /usr/share/grr-server/executables/installers/dbg\_GRR\_3.4.5.1\_amd64.msi

Repacking template: /usr/share/grr-server/grr-response-templates/tem-plates/grr\_3.4.5.1\_amd64.rpm.zip

Using context: ['Target:Linux', 'ClientBuilder Context', 'ClientBuilder Context', 'Arch:amd64', 'Platform:Linux', 'Target:Linux', 'Target:LinuxRpm'] and labels: []

Repacked into /usr/share/grr-server/executables/installers/grr\_3.4.5.1\_amd64.rpm

Repacking template: /usr/share/grr-server/grr-response-templates/tem-plates/grr\_3.4.5.1\_amd64.xar.zip

Using context: ['Target:Darwin', 'ClientBuilder Context', 'ClientBuilder Context', 'Arch:amd64', 'Platform:Darwin', 'Target:Darwin'] and labels: []

Repacked into /usr/share/grr-server/executables/installers/grr\_3.4.5.1\_amd64.pkg

Repacking template: /usr/share/grr-server/grr-response-templates/tem-plates/grr\_3.4.5.1\_amd64.deb.zip

Using context: ['Target:Linux', 'ClientBuilder Context', 'ClientBuilder Context', 'Arch:amd64', 'Platform:Linux', 'Target:Linux', 'Target:LinuxDeb'] and labels: []

Repacked into /usr/share/grr-server/executables/installers/grr\_3.4.5.1\_amd64.deb

GRR Initialization complete! You can edit the new configuration in /etc/grr//server.local.yaml.

Restart service for the new configuration to take effect? [Yn]: [Y]: Y

Restarting service: grr-server.

Restarting service: fleetspeak-server.

#####

Install complete.

If upgrading, make sure you read the release notes:

<https://grr-doc.readthedocs.io/en/latest/release-notes.html>

#####

Processing triggers for libc-bin (2.27-3ubuntu1.4) ...

Processing triggers for man-db (2.8.3-2ubuntu0.1) ...

Processing triggers for install-info (6.5.0.dfsg.1-2) ...