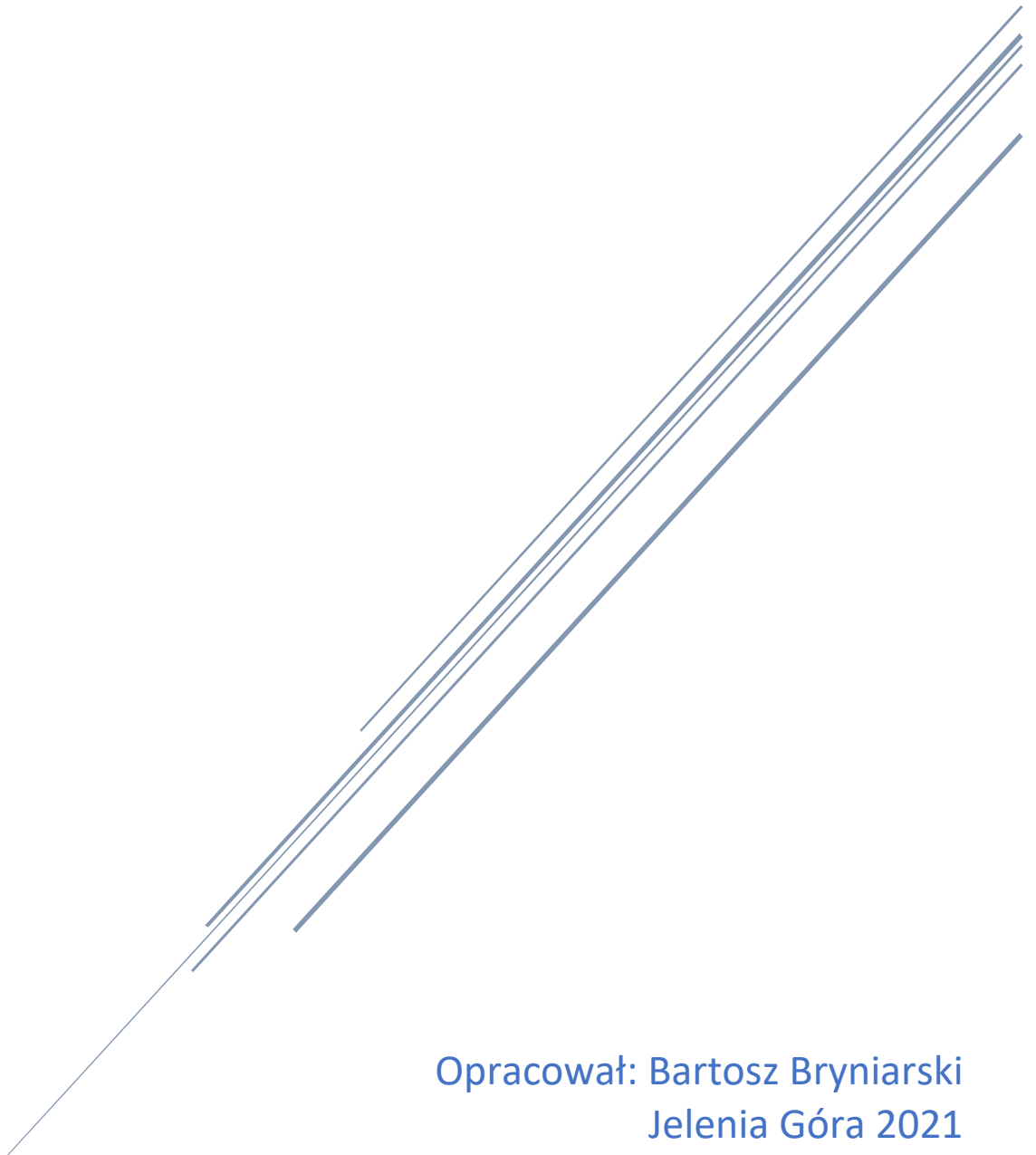


Instalacja i konfiguracja Poczty elektronicznej

Serwerowe Systemy Operacyjne



Opracował: Bartosz Bryniarski
Jelenia Góra 2021

SPIS TREŚCI

1	Opis projektu.....	3
1.1.	System operacyjny	4
1.2.	Protokół komunikacyjny SSH	5
1.3.	System zarządzania bazą danych MySQL.....	5
1.4.	Serwer poczty elektronicznej MTA – Postfix.....	6
1.5.	Serwer POP3 i IMAP – Dovecot.....	7
1.6.	Serwer http Apache	8
1.6.1.	Skryptowy język programowania PHP	8
1.6.2.	SSL dla Apache – Let’s Encrypt.....	9
1.7.	Narzędzie do zarządzania skrzynkami PostfixAdmin	10
1.8.	Internetowy klient pocztowy Roundcube.....	10
1.9.	Ochrona przed brute force – Fail2Ban.....	11
2.	Wymagania sprzętowe i programowe	11
3.	Instalacja i konfiguracja oprogramowania.....	12
3.1.	Instalacja systemu operacyjnego.....	12
3.2.	Konfiguracja adresów DNS i revDNS.....	15
3.3.	Konfiguracja SSH	16
3.4.	Instalacja i konfiguracja Apache.....	16
3.4.1.	Instalacja i konfiguracja Let’s Encrypt (protokół https)	20
3.4.2.	Instalacja i konfiguracja PHP	26
3.5.	Instalacja i konfiguracja MySQL	28
3.5.1.	Instalacja i konfiguracja phpMyAdmin.....	31
3.5.2.	Dodanie tabel do obsługi systemu pocztowego	35
3.6.	Instalacja i konfiguracja Dovecot (POP3 i IMAP).....	38
3.7.	Instalacja i konfiguracja Postfix (SMTP)	50
3.8.	Instalacja i konfiguracja PostfixAdmin	57
3.9.	konfiguracja SpamAssassin’a i Clam Anti-Virus’a	66
3.10.	Instalacja i konfiguracja Maia-Mailguard.....	68
3.11.	Instalacja i konfiguracja Roundcube	74
3.12.	Uruchomienie i sprawdzenie działania usług lokalnie	77
3.12.1.	Uruchomienie i test Postfix i Dovecot.....	77
3.12.2.	Test PostfixAdmin	81
3.12.3.	Test Maia-Mailguard.....	81
3.12.4.	Test Roundcube	82

3.13.	Instalacja i konfiguracja Fail2ban.....	82
4.	Testy usług	85
4.1.	Test ssh.....	85
4.2.	Test Systemu Zarządzania Bazą Danych MySQL	86
4.3.	Test HTTP i HTTPS	88
4.4.	Test SMTP.....	90
4.5.	Test POP3	94
4.6.	Test IMAP	95
4.7.	Test Fail2Ban	98
5.	Podsumowanie.....	100
6.	Bibliografia	101

1 OPIS PROJEKTU

Projekt przedstawia instalację oraz konfigurację systemu poczty elektronicznej. System poczty elektronicznej składa się z kilku usług. Pierwsza i zarazem główna usługa służy do przesyłania listów elektronicznych z komputera użytkownika na serwer i z serwera na serwer docelowy – usługę tą realizuje protokół komunikacyjny SMTP (Simple Mail Transfer Protocol). Po dostarczeniu listu na serwer docelowy niezbędna jest kolejna usługa, która umożliwia pobieranie wiadomości z serwera przez użytkownika – usługę tą realizuje protokół internetowy POP3 (Post Office Protocol). Protokół ten ma wiele ograniczeń, między innymi nie można zarządzać wiadomościami na serwerze. Przez co powstała konieczność stworzenia nowego protokołu, który umożliwia zarządzania wiadomościami na serwerze – ten protokół to IMAP (Internet Message Access Protocol). Do poprawnego działania powyższych usług niezbędna będzie także instalacja systemu zarządzania bazą danych MySQL. Dodatkowo niezależnie od usług SMTP oraz POP3/IMAP dzięki którym będzie można skonfigurować klienta pocztowego MUA do poprawnej obsługi poczty zainstalowane i skonfigurowane zostanie aplikacja internetowa do obsługi poczty – RoundCube, oraz niezbędny do jej działania serwer www Apache oraz usługa ssl dla protokołu http. Ostatnim narzędziem jakie zostanie skonfigurowane to narzędzie do zabezpieczenia systemu pocztowego przez atakami typu brute force – oprogramowanie Fail2ban.

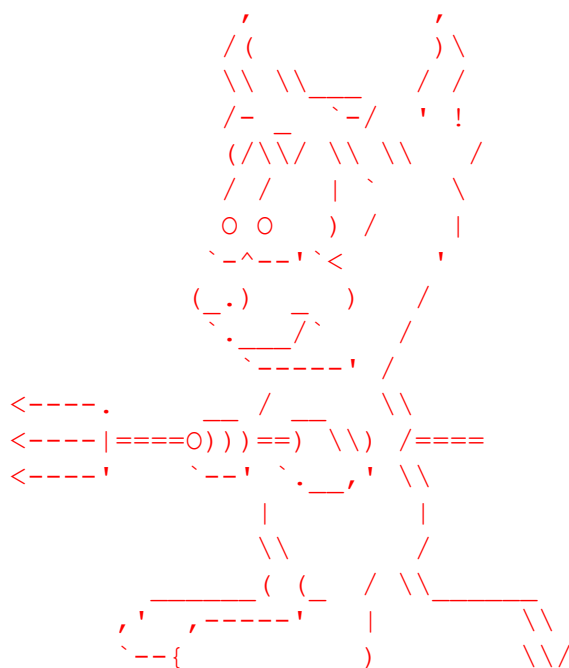
1.1. SYSTEM OPERACYJNY

Do poprawnego działania systemu pocztowego wybrałem system operacyjny FreeBSD w wersji 13. FreeBSD¹ jest systemem z rodziny Unix, oparty na BSD – gałęzi Uniksa stworzonej przez Computer Systems Research Group na Uniwersytecie Kalifornijskim w Berkeley. Pierwsza wersja tego systemu została wydana 30 listopada 1993 roku. Do dziś jest rozwijany.²

Z systemu tego korzystam od wersji 4.0 – początkowo służył mi jako brama internetowa w sieci osiedlowej – ma bardzo fajną zaporę sieciową IPFW oraz system kontroli pasma dumynet. W systemie tym bardzo łatwo instaluje się oprogramowanie z paczek przez polecenie pkg, a także można kompilować oprogramowanie z własnymi ustawieniami za pomocą kolekcji portów.

Maskotką FreeBSD jest daemon widocznym w asciart poniżej. Oficjalnym hasłem jest: *The power to serve.*

System FreeBSD dostępny jest na licencji BSD³ (Berkeley Software Distribution Licenses) – licencja zgodna z zasadami wolnego oprogramowania – powstała początkowo na Uniwersytecie Kalifornijskim w Berkeley – skupia się na prawach użytkownika – jest bardzo liberalna, zezwala nie tylko na modyfikowanie kodu źródłowego i jego rozprowadzanie w takiej postaci, ale także na rozprowadzanie produktu bez postaci źródłowej czy włączanie kodu do zamkniętego oprogramowania, pod warunkiem podania informacji o autorach i licencji.



Rys 1.1.1. AsciiArt deamon - maskotka systemu FreeBSD.

¹ Strona domowa: The FreeBSD Project <https://www.freebsd.org/> [dostęp 01.06.2021]

² FreeBSD – Wikipedia <https://pl.wikipedia.org/wiki/FreeBSD> [dostęp 01.06.2021]

³ Licencje BSD – Wikipedia https://pl.wikipedia.org/wiki/Licencje_BSD [dostęp 01.06.2021]

1.2. PROTOKÓŁ KOMUNIKACYJNY SSH

SSH⁴ (Secure Shell – bezpieczna powłoka) to standard protokołów komunikacyjnych używanych w sieciach komputerowych, w architekturze klient-serwer. SSH jest następcą protokołu Telnet⁵, służącego do terminalowego łączenia się ze zdalnymi maszynami. SSH różni się od Telnetu tym, że cała komunikacja klient-serwer jest szyfrowana, czego nie było w przypadku protokołu Telnet. W szerszym znaczeniu SSH to wspólna nazwa dla całej rodziny protokołów, nie tylko terminalowych, lecz także służących do przesyłania plików (SCP – Secure Copy, SFTP – Secure File Transfer Protocol), zdalnej kontroli zasobów, tunelowania, i wielu innych zastosowań.

Protokół SSH korzysta z portu 22 (TCP).

W projekcie wykorzystam otwartą implementację protokołu SSH – OpenSSH⁶ – rozwijaną przez programistów systemu OpenBSD⁷, który to wywodzi się z tej samej rodziny systemów do FreeBSD. OpenSSH dostępny jest na licencji BDS.

Najbardziej znana implementacja klienta to PuTTY (działająca w systemach Windows, Unix/Linux)

1.3. SYSTEM ZARZĄDZANIA BAZĄ DANYCH MYSQL

MySQL⁸ to wolnodostępny, otwartoźródłowy system zarządzania relacyjnymi bazami danych. MySQL rozwijany jest przez firmę Oracle – był pisany raczej z myślą o szybkości niż kompatybilności ze standardem SQL – przez dłuższy czas nie obsługiwał nawet transakcji. MySQL obsługuje większą część obecnego standardu ANSI/ISO (tj. SQL:2003), wprowadzono również swoje rozszerzenia i nowe elementy języka. Od wersji 5 dodawano następujące elementy: procedury składowane, wyzwalacze, widoki, kursory, partycjonowanie tabel, harmonogram zadań, przez co zbliżyło najnowsze wersje MySQL do PostgreSQL pod względem funkcjonalności. Serwer MySQL dostępny jest na wszystkich popularnych platformach systemowych i różnych architekturach procesorów. MySQL oferuje różne typy mechanizmów bazodanowych. MySQL dostępny jest na licencji GPL⁹ (GNU General Public License) – licencji wolnego i otwartego oprogramowania.

System bazodanowy MySQL korzysta z portu 3306 (TCP).

⁴ Secure Shell – Wikipedia https://pl.wikipedia.org/wiki/Secure_Shell [dostęp 01.06.2021]

⁵ Telnet – Wikipedia <https://pl.wikipedia.org/wiki/Telnet> [dostęp 01.06.2021]

⁶ Strona domowa: OpenSSH <https://www.openssh.com/> [dostęp 01.06.2021]

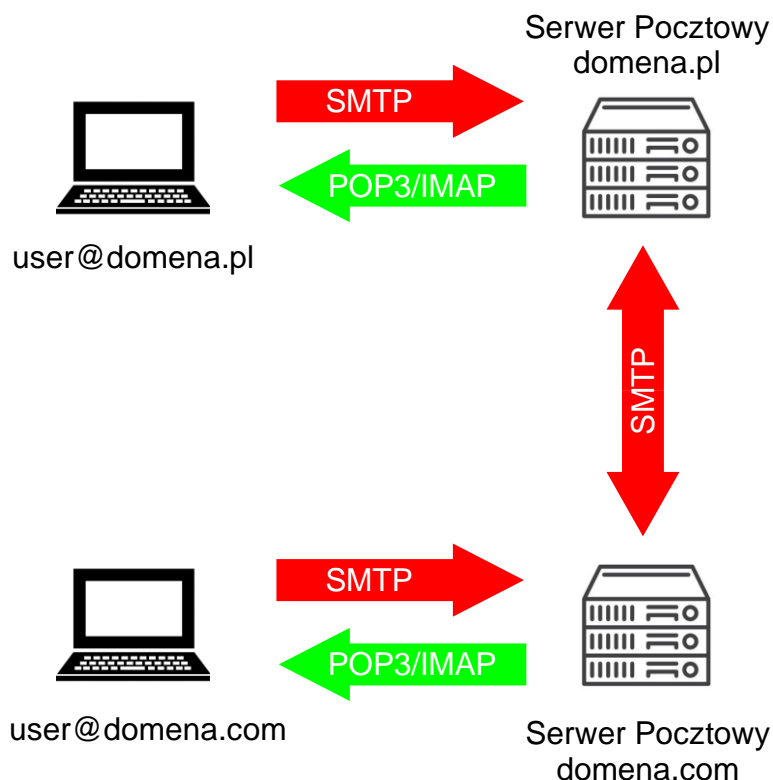
⁷ Strona domowa: OpenBSD <https://www.openbsd.org/> [dostęp 01.06.2021]

⁸ MySQL <https://www.mysql.com/>

⁹ GNU General Public License – Wikipedia https://pl.wikipedia.org/wiki/GNU_General_Public_License [dostęp 01.06.2021]

1.4. SERWER POCZTY ELEKTRONICZNEJ MTA – POSTFIX

Serwer poczty elektronicznej MTA¹⁰ (Mail Transfer Agent) jest to program poczty elektronicznej przesyłający wiadomości internetowe pomiędzy adresami poczty elektronicznej, wykorzystujący architekturę oprogramowania typu klient-serwer. MTA obsługuje protokół komunikacyjny SMTP¹¹ (Simple Mail Transfer Protocol – Prosty Protokół Przesyłania Poczty).



Rys 1.4.1: Schemat dostarczania poczty elektronicznej.

Na rysunku 2 przedstawiono schemat przesyłania poczty elektronicznej. Korespondencja tworzona w programie pocztowym na komputerze oznaczonym jako `user@domena.pl` przesyłana jest na serwer pocztowy `domena.pl` poprzez protokół SMTP. Następnie poczta ta jest na serwerze kolejkowana i w pierwszej kolejności odszukiwany jest serwer docelowy – jeśli jest to ten sam na którym się ona znajduje trafia do odpowiedniej skrzynki pocztowej. Natomiast jeśli serwerem docelowym jest inny serwer w tym przypadku serwer pocztowy `domena.com`, to serwer pierwszy wysyła na ten serwer pocztę elektroniczną przy pomocy protokołu SMTP. Serwer pocztowy `domena.com` kolejkuje tą pocztę i następnie umieszcza ją w odpowiedniej skrzynce. Na tym kończy się przesyłanie poczty z klienta MUA przez MTA do serwera docelowego. Dana wiadomość oczekuje na poprawienie jej protokołem POP3/IMAP przez adresata wiadomości.

¹⁰ Serwer poczty elektronicznej – Wikipedia https://pl.wikipedia.org/wiki/Serwer_poczty_elektronicznej [dostęp 01.06.2021]

¹¹ Simple Mail Transfer Protocol – Wikipedia https://pl.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol [dostęp 01.06.2021]

Protokół SMTP działa na portach 587 (TCP) oraz 25 (TCP) i wersja SSL na porcie 465 (TCP).

W projekcie jako oprogramowanie MTA obsługujące protokół SMTP wybrałem program Postfix¹² – jest to przeznaczonym dla systemów uniksopodobnych serwerem poczty elektronicznej, odpowiedzialnym za przekazywanie i dostarczanie poczty elektronicznej. Postfix obsługuje protokoły komunikacyjne: SMTP, LMTP¹³ (Local Mail Transfer Protocol), IPv6¹⁴ (Internet Protocol version 6), TLS¹⁵ (Transport Layer Security – rozwinięcie protokołu SSL), SASL¹⁶ (Simple Authentication and Security Layer – metoda dodawania warstwy uwierzytelniania do protokołów opartych na połączeniach). Postfix obsługuje skrzynki pocztowe w formacie Maildir oraz mbox, a także domeny wirtualne, posiada szereg mechanizmów używanych do wykrywania i usuwania spamu, obsługuje różne bazy danych przechowujące informacje systemu pocztowego (np. aliasy, nazwy kont, konta wirtualne). Postfix dostępny jest na licencji IBM Public License¹⁷.

1.5. SERWER POP3 I IMAP – DOVECOT

POP3 jest to protokół internetowy pozwalający na odbieranie poczty elektronicznej ze zdalnego serwera pocztowego do lokalnego komputera. Po połączeniu klienta pocztowego do serwera poprzez protokół POP3 pobierane są do klienta wiadomości elektroniczne znajdujące się na serwerze. Protokół POP3 pozwala tylko na pobieranie i kasowanie poczty elektronicznej na serwerze.

Z związku z tymi ograniczeniami zaimplementowano rozszerzenie protokołu POP3 i tak powstał protokół IMAP¹⁸ (Internet Message Access Protocol), dzięki któremu istnieje możliwość zarządzania pocztą elektroniczną bezpośrednio na serwerze.

Protokół POP3 działa na porcie 110 (TCP), wersja szyfrowana SSL 995 (TCP), natomiast protokół IMAP działa na porcie 143 (TCP), wersja szyfrowana SSL 993 (TCP).

W projekcie jako serwer POP3 oraz IMAP wybrałem oprogramowanie Dovecot¹⁹ – napisany ze szczególnym zwróceniem uwagi na bezpieczeństwo i niewygórowane wymagania. Jest przeznaczony dla systemów uniksopodobnych i współpracuje z Postfixem.

¹² Strona domowa: The Postfix Home Page <http://www.postfix.org/> [dostęp 01.06.2021]

¹³ Local Mail Transfer Protocol – Wikipedia https://en.wikipedia.org/wiki/Local_Mail_Transfer_Protocol [dostęp 01.06.2021]

¹⁴ IPv6 – Wikipedia <https://pl.wikipedia.org/wiki/IPv6> [dostęp 01.06.2021]

¹⁵ Transport Layer Security – Wikipedia https://pl.wikipedia.org/wiki/Transport_Layer_Security [dostęp 01.06.2021]

¹⁶ Simple Authentication and Security Layer – Wikipedia https://pl.wikipedia.org/wiki/Simple_Authentication_and_Security_Layer [dostęp 01.06.2021]

¹⁷ IBM Public License – Wikipedia https://en.wikipedia.org/wiki/IBM_Public_License [dostęp 01.06.2021]

¹⁸ Internet Message Access Protocol – Wikipedia https://pl.wikipedia.org/wiki/Internet_Message_Access_Protocol [dostęp 01.06.2021]

¹⁹ Strona domowa: Dovecot <https://www.dovecot.org/> [dostęp 01.06.2021]

Jak podaje wikipedia²⁰ Dovecot obsługuje:

- protokoły IMAP, POP3, IPv6, SSL i TLS,
- skrzynki Maildir, mbox, oraz domeny wirtualne,
- równoczesny dostęp do skrzynek przez inne programy,
- mechanizmy uwierzytelniające: PLAIN, LOGIN, CRAM-MD5, DIGEST-MD5, APOP, NTLM, GSS-SPNEGO, GSSAPI, RPA, OPT, SKEY,
- wiele baz danych przechowujących dane uwierzytelniające, np.: PAM, pliki passwd systemu, LDAP, bazy SQL (MySQL, PostgreSQL, SQLite) i inne,
- mechanizm wtyczek rozszerzających funkcjonalność (np. Quota, listy ACL).

Dovecot dostępny jest na licencji LGPL²¹ (GNU Lesser General Public License)

1.6. SERWER HTTP APACHE

Protokół HTTP²² (Hypertext Transfer Protocol) to protokół przesyłania dokumentów hipertekstowych – jest protokołem sieci WWW²³ (World Wide Web), działa w oparciu o architekturę klient-serwer. Obecną definicję protokołu HTTP stanowi dokument RFC2616²⁴. Za pomocą protokołu HTTP klienta przesyła do serwera żądania udostępnienia dokumentów www. Natomiast serwer w odpowiedzi przesyła do klienta żądane dokumenty.

Protokół HTTP standardowo korzysta z portu 80 (TCP).

W projekcie użyty zostanie oprogramowanie Apache – jest to otwarty serwer HTTP dostępny dla wielu systemów operacyjnych: UNIX, BSD, Linux, a także MS Windows. Apache jest jednym z częściej stosowanych serwerów HTTP w Internecie. Wg serwisu Netcraft²⁵ w maju 2020 udział Apache w rynku serwerów HTTP wynosił 25,45%, wyprzedza go serwer nginx (36,00%).

1.6.1. SKRYPTOWY JĘZYK PROGRAMOWANIA PHP

PHP²⁶ jest to interpretowany, skryptowy język programowania zaprojektowany do generowania stron internetowych i budowania aplikacji internetowych w czasie rzeczywistym, jest najczęściej stosowany do tworzenia skryptów po stronie serwera WWW. Aktualna najnowsza wersja oprogramowania to 8.0.6 – wersja 8 została wydana 26.11.2020,

²⁰ Dovecot – Wikipedia <https://pl.wikipedia.org/wiki/Dovecot> [dostęp 01.06.2021]

²¹ GNU Lesser General Public License – Wikipedia

https://pl.wikipedia.org/wiki/GNU_Lesser_General_Public_License [dostęp 01.06.2021]

²² Hypertext Transfer Protocol – Wikipedia https://pl.wikipedia.org/wiki/Hypertext_Transfer_Protocol [dostęp 01.06.2021]

²³ World Wide Web – Wikipedia https://pl.wikipedia.org/wiki/World_Wide_Web [dostęp 01.06.2021]

²⁴ Hypertext Transfer Protocol – HTTP/1.1 <https://www.w3.org/Protocols/rfc2616/rfc2616.html> [dostęp 01.06.2021]

²⁵ May 2020 Web Server Survey | Netcraft News <https://news.netcraft.com/archives/2020/05/26/may-2020-web-server-survey.html> [dostęp 01.06.2021]

²⁶ PHP: Hypertext Preprocessor <https://www.php.net/> [dostęp 01.06.2021]

w związku z czym nie nadaje się aktualnie na wersję produkcyjną (nie wszystkie aplikacje internetowe są z nią kompatybilne). W projekcie wykorzystam wersję 7.4.20.

PHP to oprogramowanie z licencją open source (oprogramowanie otwarte). To gwarantuje, że produkt pozostanie bezpłatny. Czasem mówi się o licencji GPL, czyli GNU General Public License. Ostatnio całość programu rozpowszechniana jest na podstawie takiej wolnej licencji, wzorowanej na licencji BSD, zaś Zend²⁷ jest publikowany na podstawie licencji Q Public license²⁸.

1.6.2. SSL DLA APACHE – LET’S ENCRYPT

HTTPS to szyfrowana wersja protokołu HTTP. W przeciwieństwie do komunikacji niezasyfrowanego tekstu w HTTP klient-serwer, HTTPS szyfrował dane przy pomocy protokołu SSL, natomiast obecnie używany jest do tego celu protokół TLS. Zapobiega to przechwytywaniu, podsłuchiwananiu oraz zmienianiu przesyłanych danych.

Dane przesyłane za pomocą HTTPS chroni protokół TLS (Transport Layer Security), który ma trzy główne warstwy zabezpieczeń:

Szyfrowanie – szyfruje przesyłane dane, co zapobiega ich odczytywaniu przez intruzów. Uniemożliwia to przechwytywanie rozmów prowadzonych przez użytkownika, śledzenie jego działań na różnych stronach i wykradanie jego informacji, gdy przegląda on witrynę.

Integralność danych – pozwala na wykrywanie wszystkich celowych lub innych zmian i uszkodzeń danych podczas przesyłania.

Uwierzytelnianie – potwierdza, że użytkownik komunikuje się z właściwą witryną. Chroni ono przed atakami typu „man in the middle”²⁹ i wzbudza zaufanie użytkowników, co przekłada się na korzyści biznesowe.

Protokół HTTPS działa na porcie 443 (TCP).

Let’s Encrypt³⁰ to urząd certyfikacji dostępny jako publiczny produkt od 12 kwietnia 2016 roku. Projekt dostarcza użytkownikom darmowe certyfikaty szyfrowania X.509 Transport Layer Security (TLS) w ramach zautomatyzowanego procesu stworzonego aby wyeliminować wady ręcznego tworzenia, walidacji, podpisywania oraz instalacji certyfikatów dla bezpiecznych stron internetowych. Let’s Encrypt dostarcza zestaw narzędzi do zarządzania certyfikatami oraz automatycznej integracji z serwerami HTTP. Certyfikaty udostępniane przez urząd posiadają datę ważności na 3 miesiące, przed końcem czasu ważności należy odnowić certyfikat na kolejne 3 miesiące – poprzez uruchomienie dedykowanego narzędzia.

²⁷ Zend Technologies – Wikipedia https://pl.wikipedia.org/wiki/Zend_Technologies [dostęp 01.06.2021]

²⁸ Q Public license – Wikipedia https://en.wikipedia.org/wiki/Q_Public_License [dostęp 01.06.2021]

²⁹ Atak man in the middle – Wikipedia https://pl.wikipedia.org/wiki/Atak_man_in_the_middle [dostęp 01.06.2021]

³⁰ Let’s Encrypt <https://letsencrypt.org/> [dostęp 01.06.2021]

1.7. NARZĘDZIE DO ZARZĄDZANIA SKRZYNKAMI POSTFIXADMIN

PostfixAdmin³¹ to aplikacja (oprogramowanie) internetowa do konfigurowania i zarządzania serwerem pocztowym opartym na oprogramowaniu Postfix.

Główne funkcje:

- zarządzanie skrzynkami pocztowymi, wirtualnymi domenami i aliasami,
- tworzenie wiadomości o urlopie/poza biurem,
- domeny aliasowe (przekazywanie jednej domeny do drugiej z weryfikacją adresatów),
- użytkownicy mogą zarządzać własną skrzynką pocztową (zmienić alias, hasło i wiadomość urlopową),
- obsługa przydziału dla pojedynczych skrzynek pocztowych i całkowitego przydziału domeny,
- wyświetla używany limit.

Oprogramowanie PostfixAdmin jest na licencji GPL.

1.8. INTERNETOWY KLIENT POCZTOWY ROUNDKUBE

Roundcube to aplikacja internetowa, wielojęzyczny klient IMAP z interfejsem użytkownika podobnym do aplikacji. Zapewnia pełną funkcjonalność, jaka oczekiwana jest od klienta poczty elektronicznej, w tym obsługę MIME³² (Multipurpose Internet Mail Extensions), książkę adresową, manipulację folderami, wyszukiwanie wiadomości i sprawdzanie pisowni.

Główne funkcje aplikacji:

- zarządzanie wiadomościami metodą „przeciągnij i upuść”,
- pełna obsługa wiadomości MIME i HTML³³,
- wiele tożsamości nadawcy,
- w pełni funkcjonalna książka adresowa z grupami i złączami LDAP,
- integracja z książką adresową Find-as-you-type,
- lista wiadomości w wątkach,
- obsługa IDNA³⁴ i SMTPUTF8³⁵,
- sprawdzanie pisowni,
- responsywna skóra (obsługa wielu urządzeń),
- współdzielone/globalne foldery IMAP,

³¹ Postfix Admin - Web based administration interface <https://postfixadmin.sourceforge.io/> [dostęp 01.06.2021]

³² Typ MIME – Wikipedia https://pl.wikipedia.org/wiki/Typ_MIME [dostęp 01.06.2021]

³³ HTML – Wikipedia <https://pl.wikipedia.org/wiki/HTML> [dostęp 01.06.2021]

³⁴ Internationalized Domain Name – Wikipedia https://pl.wikipedia.org/wiki/Internationalized_Domain_Name [dostęp 01.06.2021]

³⁵ Simple Mail Transfer Protocol – Wikipedia https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol#SMTPUTF8 [dostęp 01.06.2021]

- obsługa list kontroli dostępu (ACL³⁶),
- wbudowana pamięć podręczna zapewniająca szybki dostęp do skrzynki pocztowej,
- nieograniczona liczba użytkowników i wiadomości,
- funkcje importu/eksportu,
- plug-in API dla elastycznych rozszerzeń,
- ochrona przed atakami XSS³⁷,
- obsługa szyfrowania PGP³⁸.

1.9. OCHRONA PRZED BRUTE FORCE – FAIL2BAN

Fail2Ban³⁹ to platforma oprogramowania zapobiegająca włamaniom, która chroni serwery komputerowe przed atakami typu brute-force. Napisany jest w języku programowania Python, może działać w systemach POSIX, które mają interfejs do systemu kontroli pakietów lub zainstalowanego lokalnie firewalla, ipfw w systemie FreeBSD czy iptables w Linuxie.

Fail2Ban skanuje logi systemowe i zgodnie z ustawieniami po spełnieniu określonych warunków blokuje dostęp do danej usługi lub nawet całego serwera dla określonego adresu IP na zadany w ustawieniach czas.

2. WYMAGANIA SPRZĘTOWE I PROGRAMOWE

Przy doborze parametrów sprzętu do przedstawionego systemu pocztowego należy zwrócić uwagę na następujące elementy:

1. Pamięć RAM – to tak zwana pamięć o swobodnym dostępie. Przeznaczona jest do przechowywania danych i przeprowadzania aktualnie wykonywanych operacji. W związku z czym do im więcej pamięci będzie dostępnej w systemie tym szybciej będzie działać oprogramowanie, szczególnie system bazodanowy MySQL, który w pamięci przechowywać będzie tabele.
2. Procesor – ilość rdzeni procesora i szybkość taktowania nie ma aż tak dużego znaczenia, gdyż system pocztowy nie potrzebuje wykonywać skomplikowanych obliczeń. Należy zapewnić minimalną ilość rdzeni i taktowanie procesora aby system operacyjny działał stabilnie.
3. Dysk twardy – służy głównie do przechowywania danych, w systemie pocztowym na nim przechowywana będzie cała korespondencja trafiająca do skrzynek użytkowników. Szybkość dysku nie ma w tym miejscu zbyt dużego znaczenia, gdyż dane są na dysku nie poddawane się tak częstym modyfikacją. W zupełności wystarczy dysk talerzowy HDD. Pojemność dysku zależna od przewidywanej pojemności skrzynek pocztowych. Należy natomiast rozważyć instalację dysku SSD na którym będzie zainstalowany system, tak aby oprogramowanie działało wydajniej.

³⁶ Access-control list – Wikipedia https://pl.wikipedia.org/wiki/Access-control_list [dostęp 01.06.2021]

³⁷ Cross-site scripting – Wikipedia https://pl.wikipedia.org/wiki/Cross-site_scripting [dostęp 01.06.2021]

³⁸ Pretty Good Privacy – Wikipedia https://pl.wikipedia.org/wiki/Pretty_Good_Privacy [dostęp 01.06.2021]

³⁹ Strona domowa: Fail2Ban https://www.fail2ban.org/wiki/index.php/Main_Page [dostęp 01.06.2021]

4. Karta sieciowa – powinna być dostosowana do istniejącej infrastruktury sieciowej.
5. Porty USB – w przypadku wykonywania kopii zapasowych przydadzą się do archiwizacji kopii na nośnikach zewnętrznych (pendrive, dysk twardy) podłączanych poprzez USB.
6. Karta graficzna/monitor – po zainstalowaniu systemu może zostać odłączona od systemu – zarządzanie systemem odbywać się będzie za pomocą usługi SSH.

W projekcie wykorzystam system FreeBSD bez instalacji graficznego GUI, przez co sam system do swojego funkcjonowania nie będzie potrzebował nawet monitora. Komunikacja zdalna z systemem oparta zostanie o protokół ssh oraz wydawanie poleceń w trybie tekstowym. Oprogramowanie systemu pocztowego – Postfix i Dovecot jest stworzone na systemy Unixopodobne, przez co system Windows nie wchodzi w grę.

3. INSTALACJA I KONFIGURACJA OPROGRAMOWANIA

Ze względu na złożoność systemu pocztowego w projekcie wykorzystany zostanie serwer dedykowany zlokalizowany w OVH – francuskie przedsiębiorstwo hostingowe.

Maszyna na której będzie zainstalowany system posiada następujące parametry:

- procesor Atom N2800 – 4 rdzenie, taktowanie 1066MHz
- pamięć RAM 4GB DDR
- dysk HDD 2TB
- karta sieciowa 100Mb/s

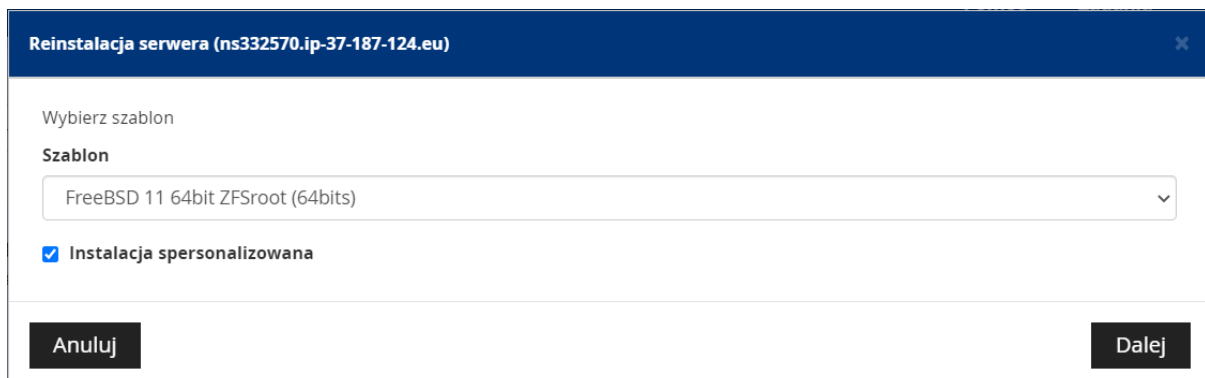
Maszyna posiada adres ipv4: 37.187.124.66.

W DNSie dodany jest rekord A dla domeny proket.brylka.net wskazujący na adres maszyny.

Ustawiony jest także revDNS.

3.1. INSTALACJA SYSTEMU OPERACYJNEGO

OVH udostępnia do instalacji na serwerach dedykowanych 64bitowy system FreeBSD w wersji 11.



The screenshot shows a web interface for server reinstallation. At the top, a dark blue header contains the text "Reinstalacja serwera (ns332570.ip-37-187-124.eu)" and a close button. Below the header, the text "Wybierz szablon" is displayed. Underneath, there is a section titled "Szablon" with a dropdown menu currently showing "FreeBSD 11 64bit ZFSroot (64bits)". Below the dropdown, there is a checked checkbox labeled "Instalacja spersonalizowana". At the bottom of the form, there are two buttons: "Anuluj" on the left and "Dalej" on the right.

Rys 3.1.1: Wybór systemu operacyjnego.

W maszyna na której instalowany jej system pocztowy zainstalowany jest jeden dysk talerzowy HDD, w związku z czym należy go odpowiednio podzielić na partycje, tak aby przepełnienie np. poczty nie spowodowało błędów w funkcjonowaniu systemu operacyjnego. Podczas konfiguracji maszyny należy określić ilość miejsca dla systemu pocztowego. W katalogu /var będzie przechowywana między innymi poczta użytkowników systemu.

Dla lepszego działania systemu operacyjnego należało by rozważyć instalację dysku SSD tylko dla systemu operacyjnego, natomiast pocztę przechowywać na drugim dysku (wystarczy HDD).

Kolejność	Typ	System plików	Punkt montowania	Rozmiar	Dodaj partycję	
1	primary	zfs	/	Pozostała przestrzeń	Edytuj	Usuń
2	primary	zfs	/var	600000 MB	Edytuj	Usuń
3	primary	swap	swap	8192 MB	Edytuj	Usuń
4	logical	zfs	/home	600000 MB	Edytuj	Usuń
5	logical	zfs	/tmp	200000 MB	Edytuj	Usuń

Partycja swap jest obowiązkowa, nie można jej usunąć.

Rys 3.1.2: Podział dysku na partycje (dedykowana partycja /var dla przechowywania poczty).

Po uruchomieniu maszyny przez OVH dostajemy e-maila z danymi do logowania.

```
37.187.124.66 - PuTTY
login as: root
Keyboard-interactive authentication prompts from server:
| Password for root@brylka:
| End of keyboard-interactive prompts from server
Last login: Sun May 16 10:01:08 2021 from cache-prod-b.bastions.ovh.eu
FreeBSD 11.4-RELEASE-p9

server      : 463532
ip          : 37.187.124.66
hostname    : brylka

root@brylka:~ # freebsd-version
11.4-RELEASE-p9
root@brylka:~ # uname -mrs
FreeBSD 11.4-RELEASE-p9 amd64
root@brylka:~ # pas
passwd paste
root@brylka:~ # passwd
Changing local password for root
New Password:
Retype New Password:
root@brylka:~ # █
```

Rys 3.1.3: Pierwsze logowanie do systemu, sprawdzenie wersji i zmiana hasła.

W pierwszej kolejności należy zaktualizować system do wersji 13.

Po wykonaniu kilku podstawowych komend opisanych na stronie <https://www.cyberciti.biz/open-source/freebsd-13-released-how-to-update-upgrade-freebsd-12-to-13/> oraz dodaniu do jądra obsługi IPFW oraz dummynet opisanej w podręczniku <https://docs.freebsd.org/en/books/handbook/kernelconfig/> i dłuższym lub krótszym czasie na kompilację źródeł (tu przydaje się większa liczba rdzeni w procesorze) naszym oczom ukazuje się trzynasta wersja systemu FreeBSD.

```
37.187.124.66 - PuTTY
--ffreestanding -fwrapv -fstack-protector -Wall -Wredundant-decls -Wnested-externs -Wstrict-prototypes -Wmissing-prototypes -Wpointer-arith -Wcast-qual -Wundef -Wno-pointer-sign -D printf = freebsd kprintf -Wmissing-include-dirs -fdiagnostics-show-option -Wno-unknown-pragmas -Wno-error-tautological-compare -Wno-error-empty-body -Wno-error-parentheses-equality -Wno-error-unused-function -Wno-error-pointer-sign -Wno-error-shift-negative-value -Wno-address-of-packed-member -Wno-format-zero-length -mno-aes -mno-avx -std=iso9899:1999 -Werror -mno-mmx -msse -msse4 -msha /usr/src/sys/crypto/aesni/intel_sha256.c
--- intel_shal.o ---
ctfconvert -L VERSION -g intel_shal.o
--- intel_sha256.o ---
ctfconvert -L VERSION -g intel_sha256.o
--- x86emu.o ---
ctfconvert -L VERSION -g x86emu.o
--- sym_hipd.o ---
ctfconvert -L VERSION -g sym_hipd.o
--- vers.o ---
MAKE="make" sh /usr/src/sys/conf/newvers.sh BRYLKAKERNEL
--- vers.o ---
cc -target x86_64-unknown-freebsd13.0 --sysroot=/usr/obj/usr/src/amd64.amd64/tmp -B/usr/obj/usr/src/amd64.amd64/tmp/usr/bin -c -O2 -pipe -fno-strict-aliasing -g -nostdinc -I. -I/usr/src/sys -I/usr/src/sys/contrib/ck/include -I/usr/src/sys/contrib/libfdt -D_KERNEL -DHAVE_KERNEL_OPTION_HEADERS -include opt_global.h -fno-common -fno-omit-frame-pointer -mno-omit-leaf-frame-pointer -fdebug-prefix-map=/machine=/usr/src/sys/amd64/include -fdebug-prefix-map=/usr/src/sys/x86/include -mmodel=kernel -mno-red-zone -mno-mmx -mno-sse -msoft-float -fno-asynchronous-unwind-tables -ffreestanding -fwrapv -fstack-protector -Wall -Wredundant-decls -Wnested-externs -Wstrict-prototypes -Wmissing-prototypes -Wpointer-arith -Wcast-qual -Wundef -Wno-pointer-sign -D printf = freebsd kprintf -Wmissing-include-dirs -fdiagnostics-show-option -Wno-unknown-pragmas -Wno-error-tautological-compare -Wno-error-empty-body -Wno-error-parentheses-equality -Wno-error-unused-function -Wno-error-pointer-sign -Wno-error-shift-negative-value -Wno-address-of-packed-member -Wno-format-zero-length -mno-aes -mno-avx -std=iso9899:1999 -Werror vers.o
ctfconvert -L VERSION -g vers.o
--- kernel.full ---
linking kernel.full
ctfmerge -L VERSION -g -o kernel.full ...
      text      data      bss      dec      hex      filename
22955694 1822271 4462720 29240685 0x1be2d6d kernel.full
--- kernel.debug ---
objcopy --only-keep-debug kernel.full kernel.debug
--- kernel ---
objcopy --strip-debug --add-gnu-debuglink=kernel.debug kernel.full kernel
-----
>>> Kernel build for BRYLKAKERNEL completed on Sun May 16 13:50:04 CEST 2021
-----
>>> Kernel(s) BRYLKAKERNEL built in 5025 seconds, ncpu: 4, make -j4
-----
root@brylka:/usr/src # █
|brylka| (0$ csh) 1-9 csh 2$ csh [05/16/21 2:02 PM]
```

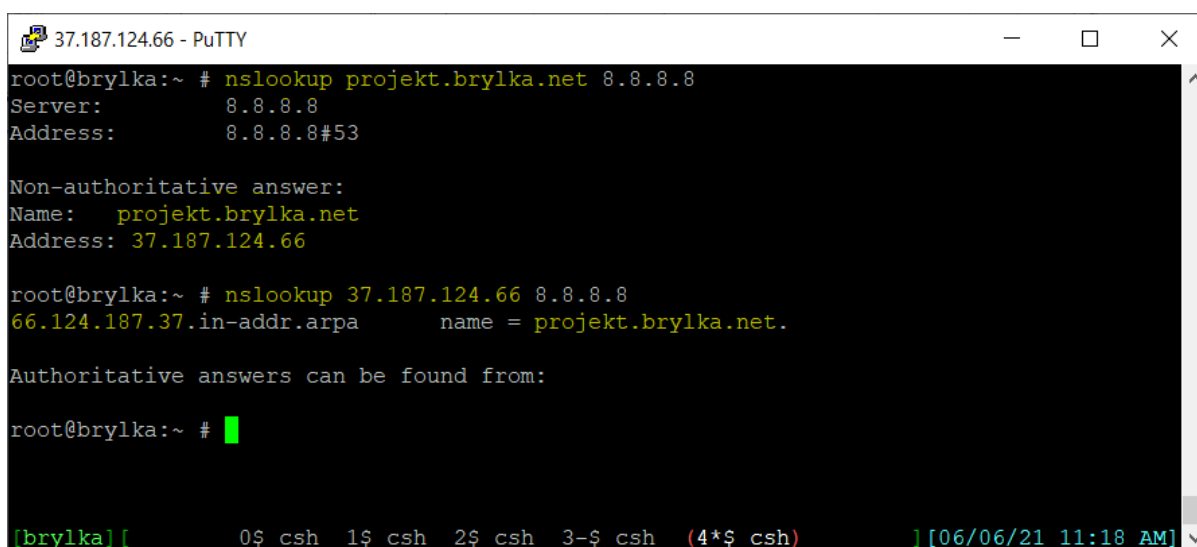
Rys 3.1.4: Na zrzucie widzimy czas budowania kernela 5025s ≈ 84 minuty – przy 4 rdzeniach

>>> Installing kernel BRYLKAKERNEL completed on Sun May 16 14:03:44 CEST 2021

Po aktualizacji system gotowy jest do instalacji i konfiguracji niezbędnego do obsługi systemu pocztowego oprogramowania.

3.2. KONFIGURACJA ADRESÓW DNS I REVDNS

W DNS w ustawieniach w OVH zostały dodane odpowiednie wpisy dla domeny projekt.brylka.net oraz revDNS dla adresu IP 37.187.124.66.



```
37.187.124.66 - PuTTY
root@brylka:~ # nslookup projekt.brylka.net 8.8.8.8
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   projekt.brylka.net
Address: 37.187.124.66

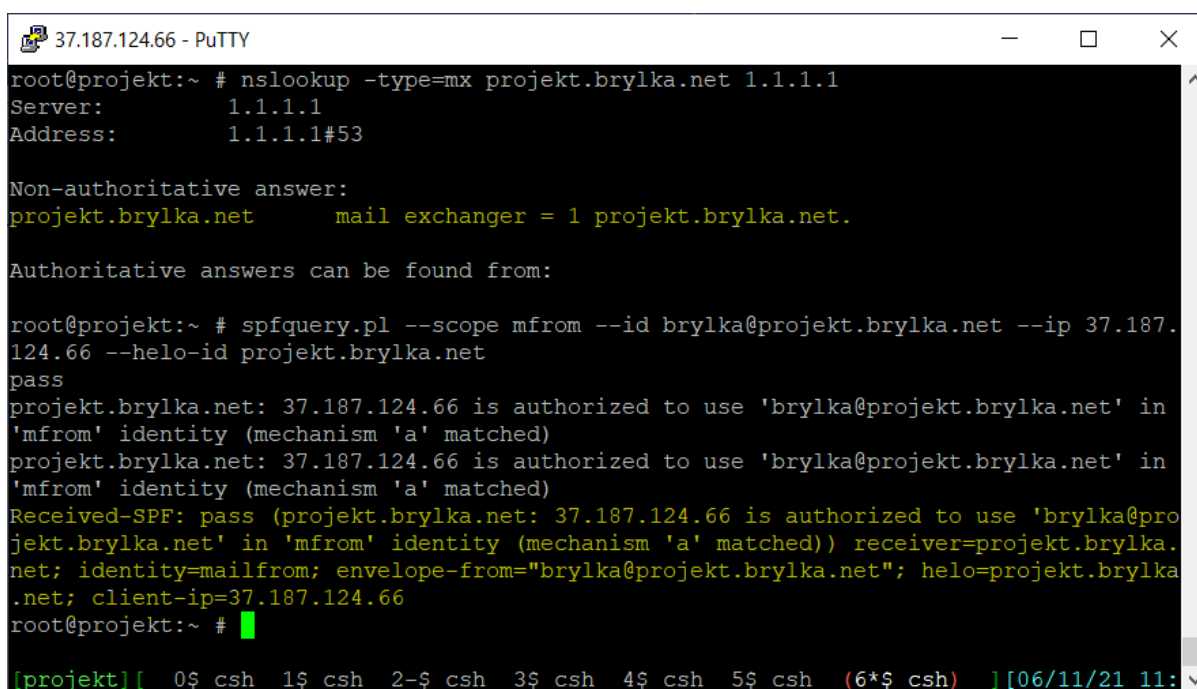
root@brylka:~ # nslookup 37.187.124.66 8.8.8.8
66.124.187.37.in-addr.arpa      name = projekt.brylka.net.

Authoritative answers can be found from:

root@brylka:~ # █

[brylka] [ 0$ csh 1$ csh 2$ csh 3-$ csh (4*$ csh) ] [06/06/21 11:18 AM]
```

Rys 3.2.1: Odpytanie DNS google o nazwę projekt.nrylka.net oraz adres IP 37.187.124.66.



```
37.187.124.66 - PuTTY
root@projekt:~ # nslookup -type=mx projekt.brylka.net 1.1.1.1
Server:      1.1.1.1
Address:     1.1.1.1#53

Non-authoritative answer:
projekt.brylka.net      mail exchanger = 1 projekt.brylka.net.

Authoritative answers can be found from:

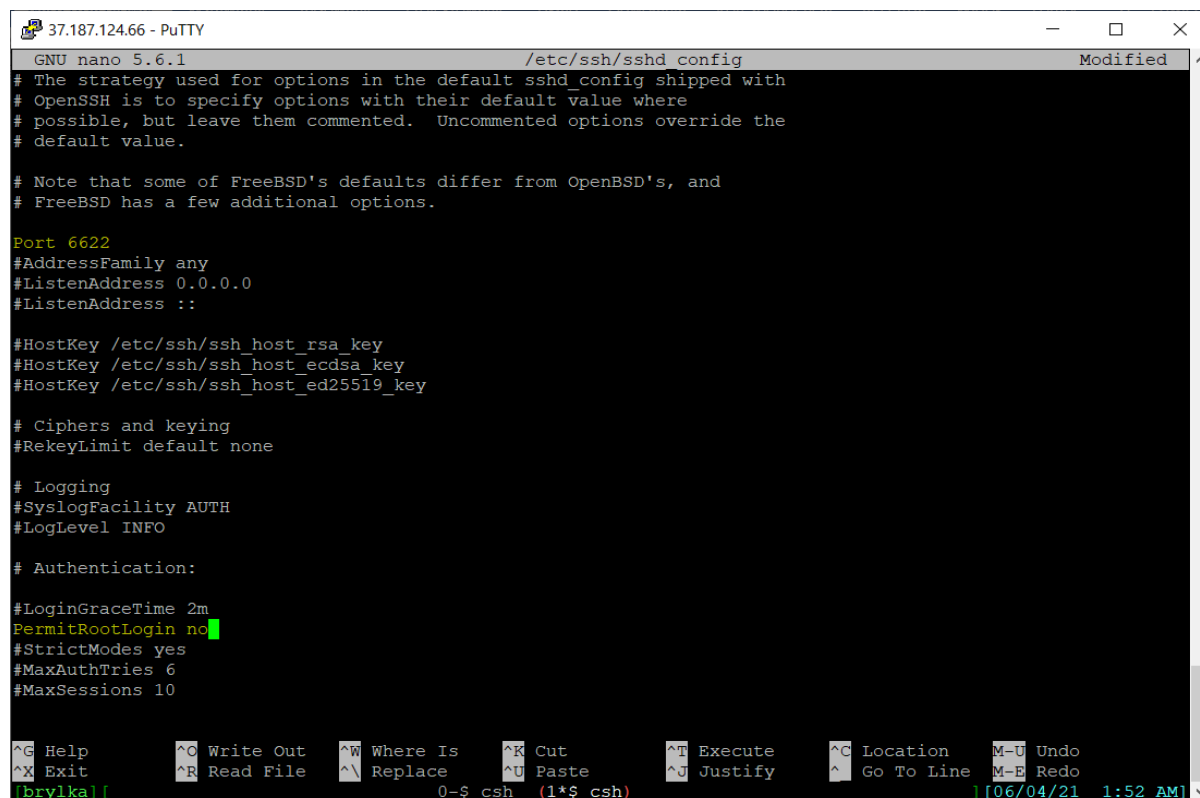
root@projekt:~ # spfquery.pl --scope mfrom --id brylka@projekt.brylka.net --ip 37.187.124.66 --helo-id projekt.brylka.net
pass
projekt.brylka.net: 37.187.124.66 is authorized to use 'brylka@projekt.brylka.net' in 'mfrom' identity (mechanism 'a' matched)
projekt.brylka.net: 37.187.124.66 is authorized to use 'brylka@projekt.brylka.net' in 'mfrom' identity (mechanism 'a' matched)
Received-SPF: pass (projekt.brylka.net: 37.187.124.66 is authorized to use 'brylka@projekt.brylka.net' in 'mfrom' identity (mechanism 'a' matched)) receiver=projekt.brylka.net; identity=mailfrom; envelope-from="brylka@projekt.brylka.net"; helo=projekt.brylka.net; client-ip=37.187.124.66
root@projekt:~ # █

[projekt] [ 0$ csh 1$ csh 2-$ csh 3$ csh 4$ csh 5$ csh (6*$ csh) ] [06/11/21 11:18 AM]
```

Rys 3.2.2: Rekordy MX i SPF dla domeny projekt.brylka.net.

3.3. KONFIGURACJA SSH

Standardowo w systemie dostarczonym przez OVH dostępna jest usługa SSH, mało tego możliwość logowania otrzymał także użytkownik root – administrator systemu, należy to wyłączyć. Także dobrym rozwiązaniem zabezpieczającym przed próbami włamania jest przeniesienie usługi SSH na inny port, najlepiej wysoki aby nie był skanowany przez potencjalnych intruzów.



```
GNU nano 5.6.1 /etc/ssh/sshd config Modified
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

# Note that some of FreeBSD's defaults differ from OpenBSD's, and
# FreeBSD has a few additional options.

Port 6622
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify   ^_ Go To Line  M-E Redo
[brylka] 0-$ csh (1*$ csh) [06/04/21 1:52 AM]
```

Rys 3.3.1: W demonie sshd zmieniony został port na 6622, zabroniono logowanie na konto root.

Przed przeladowaniem usługi sshd należy pamiętać o dodaniu użytkownika do systemu w grupie wheel, tak aby po zalogowaniu się przez ssh mógł wykonać polecenie su.

3.4. INSTALACJA I KONFIGURACJA APACHE

Apache zostanie zainstalowany jako jedna z pierwszych usług. Pozwoli to na uruchamianie podczas instalacji innych usług „nakładek” www dla tych usług, np. phpMyAdmin dla MySQL, czy PostfixAdmin do zarządzania Postfixem.

Instalację rozpoczynamy poleceniem:

```
pkg install apache24
```

Instalator informuje nas o pomyślnym zainstalowaniu apache, i konieczności dodania w pliku /etc/rc.conf wpisu apache24_enable="yes". Możemy wyedytować ten plik lub użyć polecenia:

```
sysrc apache24_enable="YES"
```

```
37.187.124.66 - PuTTY
root@brylka:~ # pkg install apache24
Updating FreeBSD_latest repository catalogue...
FreeBSD_latest repository is up to date.
All repositories are up to date.
The following 5 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:
  apache24: 2.4.48
  apr: 1.7.0.1.6.1_1
  db5: 5.3.28_7
  gdbm: 1.19
  libxml2: 2.9.10_4

Number of packages to be installed: 5

The process will require 84 MiB more space.
19 MiB to be downloaded.

Proceed with this action? [y/N]: y

[brylka] [ 0$ csh (1*$ csh) 2-$ csh ] [06/04/21 11:01 PM]
```

Rys 3.4.1: Informacja o instalowanych pakietach razem z serwerem apache.

```
37.187.124.66 - PuTTY
Message from apache24-2.4.48:

--
To run apache www server from startup, add apache24_enable="yes"
in your /etc/rc.conf. Extra options can be found in startup script.

Your hostname must be resolvable using at least 1 mechanism in
/etc/nsswitch.conf typically DNS or /etc/hosts or apache might
have issues starting depending on the modules you are using.

- apache24 default build changed from static MPM to modular MPM
- more modules are now enabled per default in the port
- icons and error pages moved from WWWDIR to DATADIR

If build with modular MPM and no MPM is activated in
httpd.conf, then mpm_prefork will be activated as default
MPM in etc/apache24/modules.d to keep compatibility with
existing php/perl/python modules!

Please compare the existing httpd.conf with httpd.conf.sample
and merge missing modules/instructions into httpd.conf!
root@brylka:~ #
root@brylka:~ # sysrc apache24_enable="YES"
apache24_enable: -> YES
root@brylka:~ #
[brylka] [ 0$ csh (1*$ csh) 2-$ csh ] [06/04/21 11:06 PM]
```

Rys 3.4.2: Informacje poinstalacyjne. Dodanie wpisu do pliku `/etc/rc.conf` informującym o aktywnym serwerze apache w systemie.

Przy starcie serwera apache wyświetla błędy związane ze zmienną ServerName.

```
service apache24 start
```

Performing sanity check on apache24 configuration:

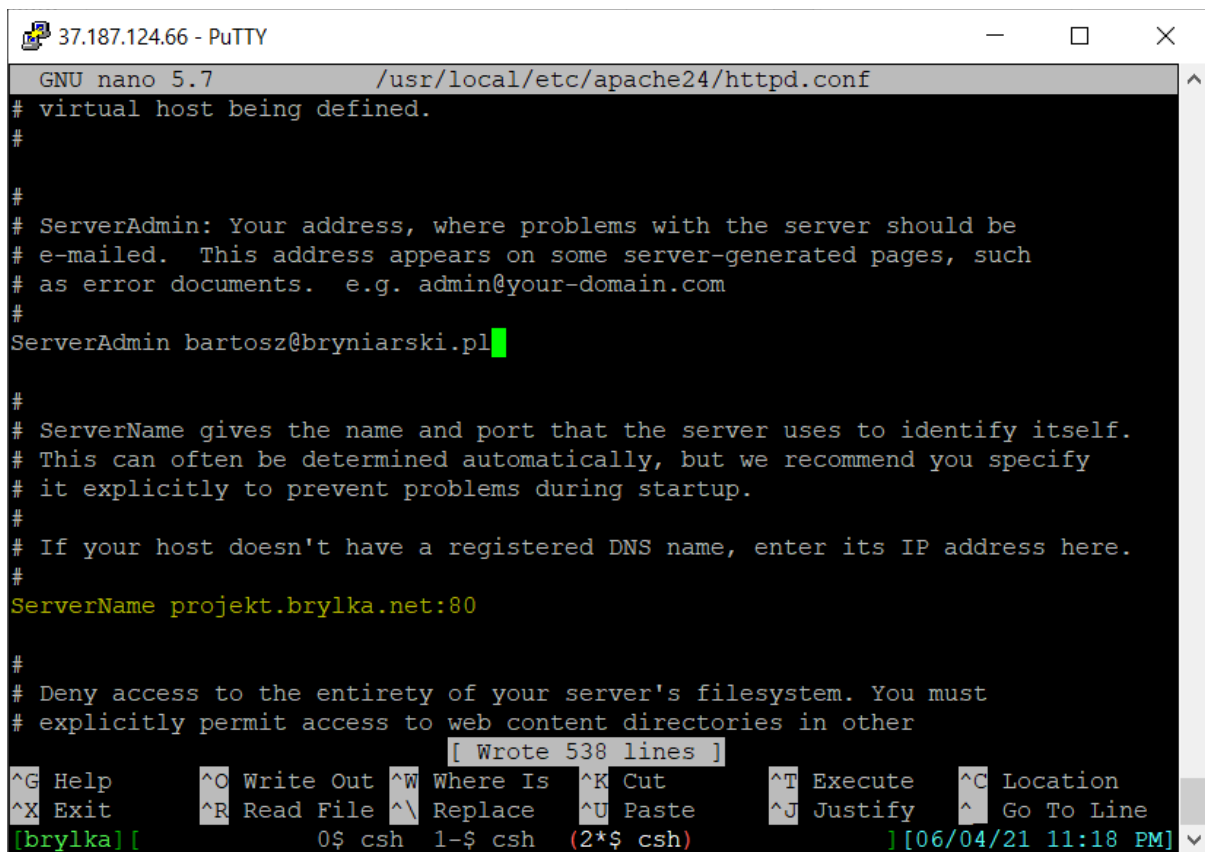
```
AH00557: httpd: apr_sockaddr_info_get() failed for brylka
```

```
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1. Set the 'ServerName' directive globally to suppress this message
```

```
Syntax OK
```

Starting apache24.

Należy wyedytować plik `/usr/local/etc/apache24/httpd.conf` i wprowadzić odpowiednie dane.



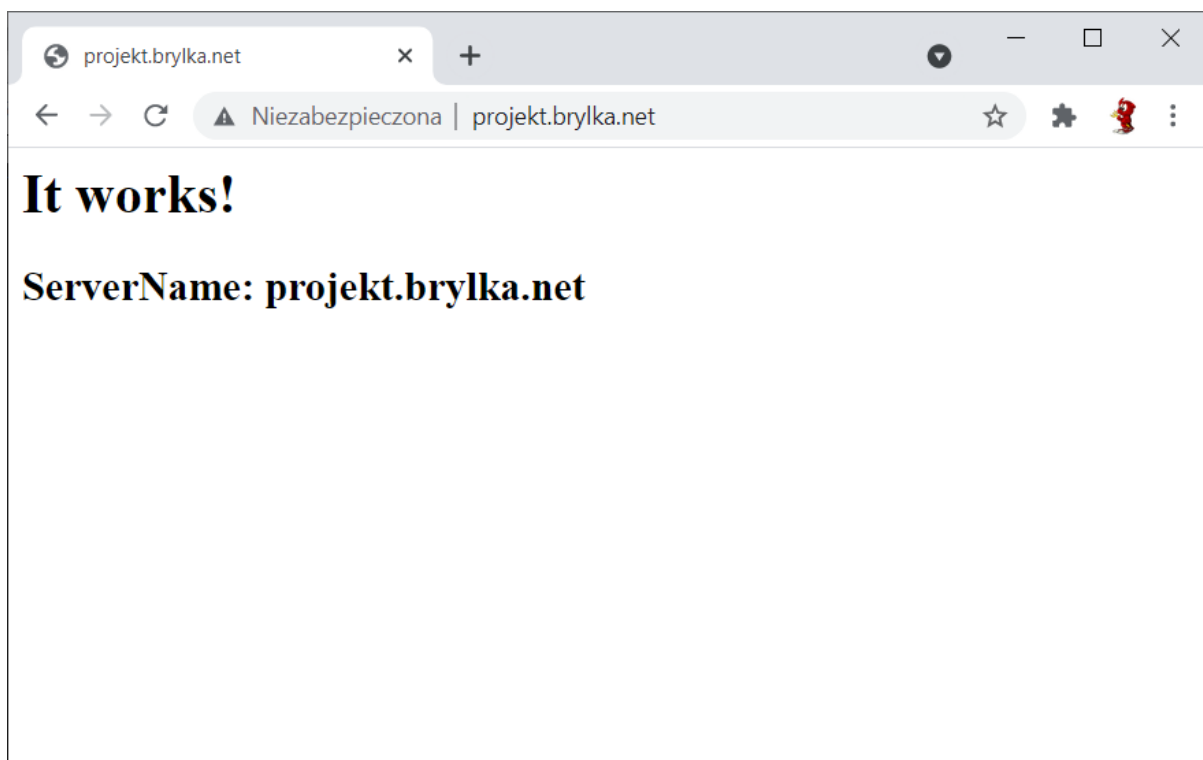
```
37.187.124.66 - PuTTY
GNU nano 5.7 /usr/local/etc/apache24/httpd.conf
# virtual host being defined.
#
#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed. This address appears on some server-generated pages, such
# as error documents. e.g. admin@your-domain.com
#
ServerAdmin bartosz@bryniarski.pl
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
ServerName projekt.brylka.net:80
#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# directories.
#
# [ Wrote 538 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut      ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace  ^U Paste    ^J Justify  ^_ Go To Line
[brylka] [ 0$ csh 1-$ csh (2*$ csh) ] [06/04/21 11:18 PM]
```

Rys 3.4.3: Dodanie wpisu ServerName w pliku konfiguracyjnym apache.

```
37.187.124.66 - PuTTY
root@brylka:~ # service apache24 start
Performing sanity check on apache24 configuration:
AH00557: httpd: apr_sockaddr_info_get() failed for brylka
AH00558: httpd: Could not reliably determine the server's fully qualified domain
name, using 127.0.0.1. Set the 'ServerName' directive globally to suppress this
message
Syntax OK
Starting apache24.
AH00557: httpd: apr_sockaddr_info_get() failed for brylka
AH00558: httpd: Could not reliably determine the server's fully qualified domain
name, using 127.0.0.1. Set the 'ServerName' directive globally to suppress this
message
root@brylka:~ # service apache24 restart
Performing sanity check on apache24 configuration:
Syntax OK
Stopping apache24.
Waiting for PIDS: 16662.
Performing sanity check on apache24 configuration:
Syntax OK
Starting apache24.
root@brylka:~ # █

[brylka] [ 0$ csh (1*$ csh) 2-$ csh ] [06/04/21 11:19 PM]
```

Rys 3.4.4: Przeładowanie apache z ustawioną wartością ServerName nie wyświetla już błędów.



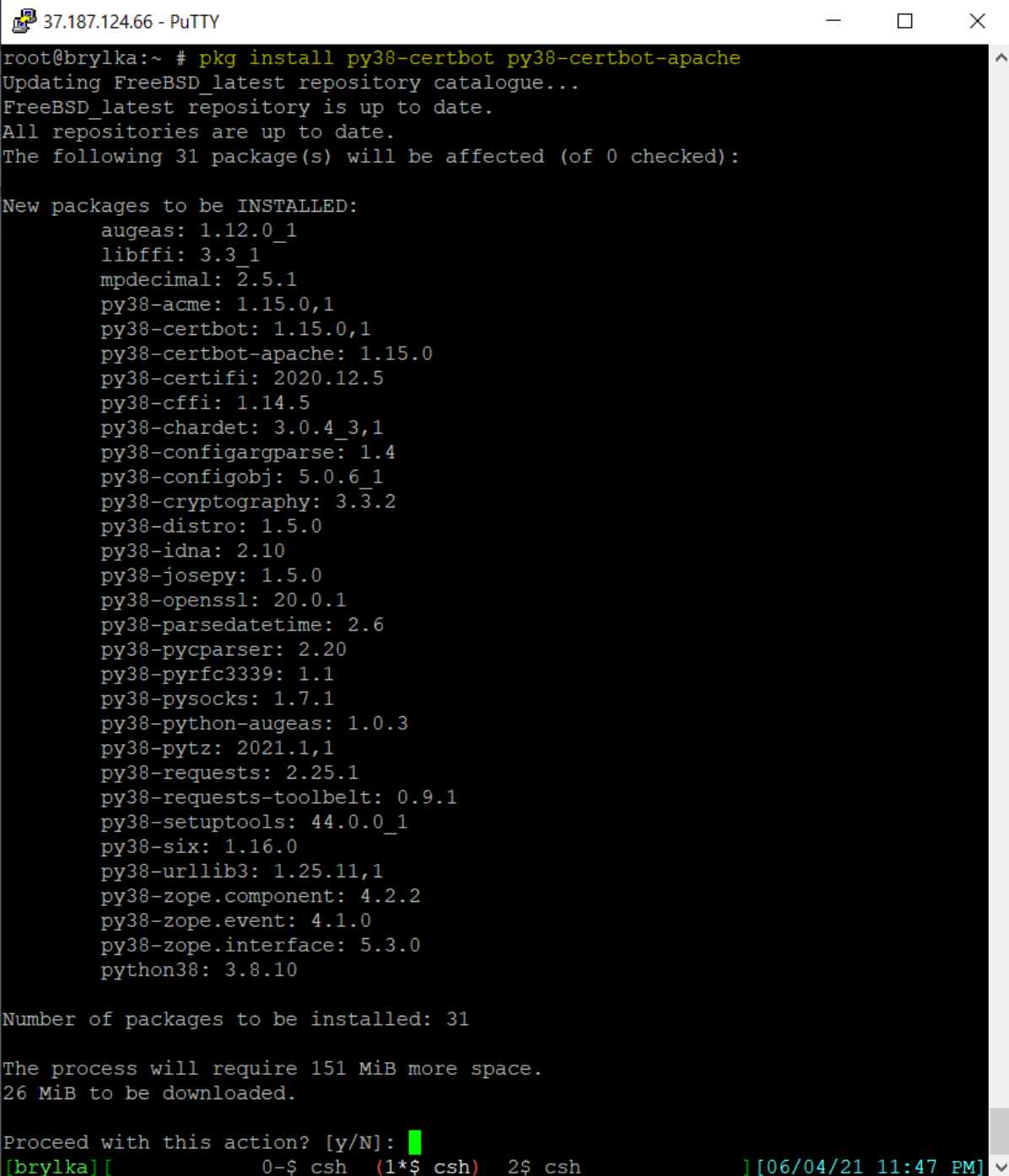
Rys 3.4.5: Sprawdzenie działania apache'a w przeglądarce na dowolnym komputerze podłączonym do Internetu.

3.4.1. INSTALACJA I KONFIGURACJA LET'S ENCRYPT (PROTOKÓŁ HTTPS)

Instalujemy klienta Let's Encrypt:

```
pkg install py38-certbot py38-certbot-apache
```

Ponieważ w systemie nie był dotychczas instalowany python, zostanie on zainstalowany razem z innymi niezbędnymi pakietami.



```
37.187.124.66 - PuTTY
root@brylka:~ # pkg install py38-certbot py38-certbot-apache
Updating FreeBSD_latest repository catalogue...
FreeBSD_latest repository is up to date.
All repositories are up to date.
The following 31 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:
  augeas: 1.12.0_1
  libffi: 3.3_1
  mpdecimal: 2.5.1
  py38-acme: 1.15.0,1
  py38-certbot: 1.15.0,1
  py38-certbot-apache: 1.15.0
  py38-certifi: 2020.12.5
  py38-cffi: 1.14.5
  py38-chardet: 3.0.4_3,1
  py38-configargparse: 1.4
  py38-configobj: 5.0.6_1
  py38-cryptography: 3.3.2
  py38-distro: 1.5.0
  py38-idna: 2.10
  py38-josepy: 1.5.0
  py38-openssl: 20.0.1
  py38-parsedatetime: 2.6
  py38-pycparser: 2.20
  py38-pyrfc3339: 1.1
  py38-pysocks: 1.7.1
  py38-python-augeas: 1.0.3
  py38-pytz: 2021.1,1
  py38-requests: 2.25.1
  py38-requests-toolbelt: 0.9.1
  py38-setuptools: 44.0.0_1
  py38-six: 1.16.0
  py38-urllib3: 1.25.11,1
  py38-zope.component: 4.2.2
  py38-zope.event: 4.1.0
  py38-zope.interface: 5.3.0
  python38: 3.8.10

Number of packages to be installed: 31

The process will require 151 MiB more space.
26 MiB to be downloaded.

Proceed with this action? [y/N]: █
[brylka] [ 0-$ csh (1*$ csh) 2$ csh ] [06/04/21 11:47 PM]
```

Rys 3.4.1.1: Rozpoczęty proces instalacji klienta Let's Encrypt.

```
37.187.124.66 - PuTTY
Message from py38-certbot-1.15.0,1:

--
This port installs the "standalone" client only, which does not use and
is not the certbot-auto bootstrap/wrapper script.

The simplest form of usage to obtain certificates is:

# sudo certbot certonly --standalone -d <domain>, [domain2, ... domainN]>

NOTE:

The client requires the ability to bind on TCP port 80 or 443 (depending
on the --preferred-challenges option used). If a server is running on that
port, it will need to be temporarily stopped so that the standalone server
can listen on that port to complete the challenge authentication process.

For more information on the 'standalone' mode, see:

https://certbot.eff.org/docs/using.html#standalone

The certbot plugins to support apache and nginx certificate installation
will be made available in the following ports:

* Apache plugin: security/py-certbot-apache
* Nginx plugin: security/py-certbot-nginx

In order to automatically renew the certificates, add this line to
/etc/periodic.conf:

weekly_certbot_enable="YES"

More config details in the certbot periodic script:

/usr/local/etc/periodic/weekly/500.certbot-3.8
root@brylka:~ # █
[brylka] [ 0-$ csh (1*$ csh) 2$ csh ] [06/04/21 11:50 PM]
```

Rys 3.4.1.2: Informacje poinstalacyjne klienta Let's Encrypt informujące o kolejnych krokach konfiguracji klienta.

```
37.187.124.66 - PuTTY
#LoadModule slotmem_plain_module libexec/apache24/mod_slotmem_plain.so
LoadModule ssl_module /usr/local/libexec/apache24/mod_ssl.so
#LoadModule dialup_module libexec/apache24/mod_dialup.so
#LoadModule http2_module libexec/apache24/mod_http2.so
#LoadModule proxy_http2_module libexec/apache24/mod_proxy_http2.so
#LoadModule md_module libexec/apache24/mod_md.so
#LoadModule lbmethod_byrequests_module libexec/apache24/mod_lbmethod_byrequests.so
#LoadModule lbmethod_bytraffic_module libexec/apache24/mod_lbmethod_bytraffic.so
#LoadModule lbmethod_bybusyness_module libexec/apache24/mod_lbmethod_bybusyness.so
#LoadModule lbmethod_heartbeat_module libexec/apache24/mod_lbmethod_heartbeat.so
LoadModule unixd_module libexec/apache24/mod_unixd.so
#LoadModule heartbeat_module libexec/apache24/mod_heartbeat.so
#LoadModule heartmonitor_module libexec/apache24/mod_heartmonitor.so
#LoadModule dav_module libexec/apache24/mod_dav.so
LoadModule status_module libexec/apache24/mod_status.so
LoadModule autoindex_module libexec/apache24/mod_autoindex.so
#LoadModule asis_module libexec/apache24/mod_asis.so

root@brylka:~ # service apache24 restart
Performing sanity check on apache24 configuration:
Syntax OK
Stopping apache24.
Waiting for PIDS: 17038.
Performing sanity check on apache24 configuration:
Syntax OK
Starting apache24.
root@brylka:~ # █
[brylka] [ 0$ csh 1$ csh 2-$ csh (3*$ csh) 4$ csh ] [06/05/21 12:03 AM]
```

Rys 3.4.1.3: W konfiguracji apache należy dodać ładowanie modułu mod_ssl.

Przed uruchomieniem certbota należy dodać virtualnego hosta do konfiguracji apache:

```
37.187.124.66 - PuTTY
# Almost any Apache directive may go into a VirtualHost container.
# The first VirtualHost section is used for all requests that do not
# match a ServerName or ServerAlias in any <VirtualHost> block.
#

<VirtualHost *:80>
    ServerAdmin bartosz@bryniarski.pl
    DocumentRoot "/usr/local/www/apache24/data/"
    ServerName projekt.brylka.net
    ServerAlias www.projekt.brylka.net
    ErrorLog "/var/log/projekt.brylka.net-error_log"
    CustomLog "/var/log/projekt.brylka.net-access_log" common
</VirtualHost>

root@brylka:/usr/local/etc/apache24 # service apache24 restart
Performing sanity check on apache24 configuration:
Syntax OK
Stopping apache24.
Waiting for PIDS: 17457.
Performing sanity check on apache24 configuration:
Syntax OK
Starting apache24.
root@brylka:/usr/local/etc/apache24 # █
[brylka] [ 0$ csh 1$ csh 2-$ csh (3*$ csh) 4$ csh ] [06/05/21 12:14 AM]
```

Rys 3.4.1.4: Dodanie vhosta projekt.brylka.net.

```
37.187.124.66 - PuTTY
root@brylka:~ # certbot --apache
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache

Which names would you like to activate HTTPS for?
-----
1: projekt.brylka.net
2: www.projekt.brylka.net
-----
Select the appropriate numbers separated by commas and/or spaces, or leave input
blank to select all options shown (Enter 'c' to cancel):
Requesting a certificate for projekt.brylka.net and www.projekt.brylka.net
Performing the following challenges:
http-01 challenge for projekt.brylka.net
http-01 challenge for www.projekt.brylka.net
Waiting for verification...
Cleaning up challenges
Created an SSL vhost at /usr/local/etc/apache24/extra/httpd-vhosts-le-ssl.conf
Deploying Certificate to VirtualHost /usr/local/etc/apache24/extra/httpd-vhosts-le-ssl.conf
Enabling site /usr/local/etc/apache24/extra/httpd-vhosts-le-ssl.conf by adding Include
to root configuration
Deploying Certificate to VirtualHost /usr/local/etc/apache24/extra/httpd-vhosts-le-ssl.conf
Redirecting vhost in /usr/local/etc/apache24/extra/httpd-vhosts.conf to ssl vhost in
/usr/local/etc/apache24/extra/httpd-vhosts-le-ssl.conf

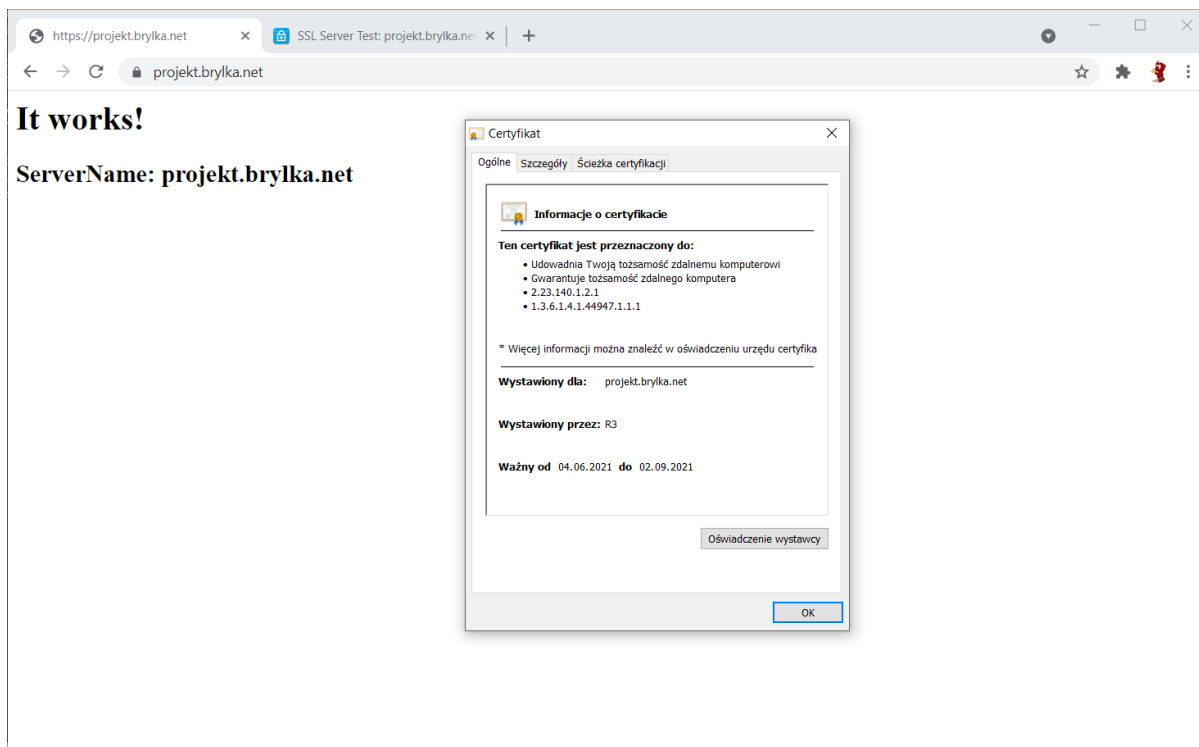
-----
Congratulations! You have successfully enabled https://projekt.brylka.net and
https://www.projekt.brylka.net
-----
Subscribe to the EFF mailing list (email: bartosz@bryniarski.pl).

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /usr/local/etc/letsencrypt/live/projekt.brylka.net/fullchain.pem
  Your key file has been saved at:
  /usr/local/etc/letsencrypt/live/projekt.brylka.net/privkey.pem
  Your certificate will expire on 2021-09-02. To obtain a new or
  tweaked version of this certificate in the future, simply run
  certbot again with the "certonly" option. To non-interactively
  renew *all* of your certificates, run "certbot renew"
- If you like Certbot, please consider supporting our work by:

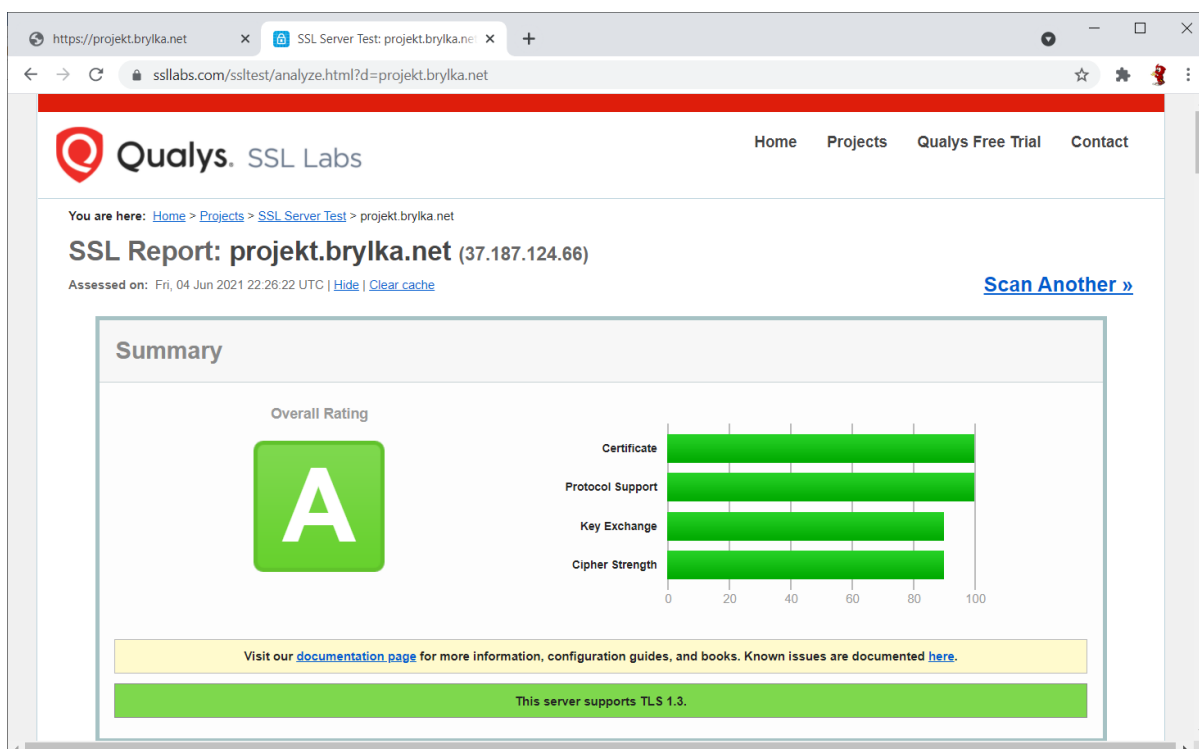
  Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
  Donating to EFF: https://eff.org/donate-le

root@brylka:~ # █
[brylka] 0$ csh 1$ csh (2*$ csh) 3-$ csh 4$ csh [06/05/21 12:20 AM] v
```

Rys 3.4.1.5: Instalacja certyfikatu ssl dla domen podpiętych do serwera.



Rys 3.4.1.6: Strona pobrana przy pomocy protokołu https oraz informacje o certyfikacie.



Rys 3.4.1.7: Analiza przy pomocy ssllabs.com wskazuje dobre zabezpieczenie adresu projekt.brylka.net.

Od teraz na serwerze wykorzystywany jest tylko protokół https – wpisanie w przeglądarkę protokołu http przekieruje na protokół https – spowodowane jest to dopisaniem przez certbota odpowiednich liniiek w plikach konfiguracyjnych.

```
37.187.124.66 - PuTTY
GNU nano 5.7 /usr/local/etc/apache24/extra/httpd-vhosts.conf
# Almost any Apache directive may go into a VirtualHost container.
# The first VirtualHost section is used for all requests that do not
# match a ServerName or ServerAlias in any <VirtualHost> block.
#
<VirtualHost *:80>
    ServerAdmin bartosz@bryniarski.pl
    DocumentRoot "/usr/local/www/apache24/data/"
    ServerName projekt.brylka.net
    ServerAlias www.projekt.brylka.net
    ErrorLog "/var/log/projekt.brylka.net-error_log"
    CustomLog "/var/log/projekt.brylka.net-access_log" common
RewriteEngine on
RewriteCond %{SERVER_NAME} =projekt.brylka.net [OR]
RewriteCond %{SERVER_NAME} =www.projekt.brylka.net
RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [END,NE,R=permanent]
</VirtualHost>
[ Read 14 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
[brylka] 0$ csh 1$ csh 2-$ csh (3*$ csh) 4$ csh [06/05/21 12:39 AM]
```

Rys 3.4.1.8: Dodane regułek Rewrite do vhosta.

```
37.187.124.66 - PuTTY
GNU nano 5.7 /usr/local/etc/apache24/extra/httpd-vhosts-le-ssl.conf
IfModule mod_ssl.c>
<VirtualHost *:443>
    ServerAdmin bartosz@bryniarski.pl
    DocumentRoot "/usr/local/www/apache24/data/"
    ServerName projekt.brylka.net
    ServerAlias www.projekt.brylka.net
    ErrorLog "/var/log/projekt.brylka.net-error_log"
    CustomLog "/var/log/projekt.brylka.net-access_log" common
Include /usr/local/etc/letsencrypt/options-ssl-apache.conf
SSLCertificateFile /usr/local/etc/letsencrypt/live/projekt.brylka.net/fullchain.pem
SSLCertificateKeyFile /usr/local/etc/letsencrypt/live/projekt.brylka.net/privkey.pem
</VirtualHost>
</IfModule>
[ Read 14 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
[brylka] 0$ csh 1$ csh 2-$ csh (3*$ csh) 4$ csh [06/05/21 12:40 AM]
```

Rys 3.4.1.9: Położenie kluczy Let's Encrypt w konfiguracji vhosta.

Ostatnim etapem konfiguracji klienta Let's Encrypt to ustawienie automatycznego odnawiania certyfikatu. Zgodnie z informacjami poinstalacyjnymi dopisanie `weekly_certbot_enable: -> "YES"` do pliku konfiguracyjnego systemu powinno spowodować automatyczne odnawianie certyfikatów. W poprzednich wersjach klienta Let's Encrypt

używałem narzędzia crontab do odnawiania certyfikatów. Sprawdzę za trzy miesiące czy ten nowy sposób działa.

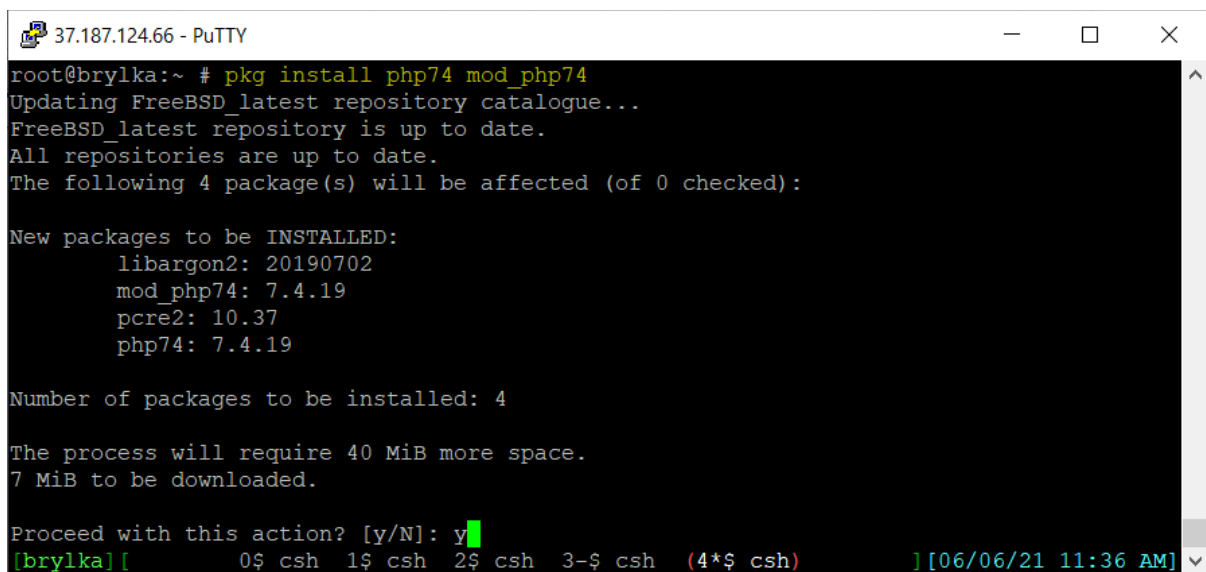
3.4.2. INSTALACJA I KONFIGURACJA PHP

Instalacja PHP sprowadza się do wykonania polecenia:

```
pkg install php74 mod_php74
```

mod_php74 to moduł php do Apache i tak zostanie skonfigurowany php. Natomiast istnieje także możliwość integracji php z Apachem za pomocą FastCGI Procesor Manager (FPM)⁴⁰⁴¹.

Inne pakiety php niezbędne do działania aplikacji instalowanych w dalszym etapie będą instalowane razem z daną aplikacją.



```
37.187.124.66 - PuTTY
root@brylka:~ # pkg install php74 mod_php74
Updating FreeBSD_latest repository catalogue...
FreeBSD_latest repository is up to date.
All repositories are up to date.
The following 4 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:
  libargon2: 20190702
  mod_php74: 7.4.19
  pcre2: 10.37
  php74: 7.4.19

Number of packages to be installed: 4

The process will require 40 MiB more space.
7 MiB to be downloaded.

Proceed with this action? [y/N]: y
[brylka] [ 0$ csh 1$ csh 2$ csh 3-$ csh (4*$ csh) ] [06/06/21 11:36 AM]
```

Rys 3.4.2.1: Rozpoczęcie instalacji PHP.

⁴⁰ PHP: FastCGI Process Manager (FPM) – Manual <https://www.php.net/manual/en/install.fpm.php> [dostęp 01.06.2021]

⁴¹ Optymalizacja PHP-FPM - Hosting WWW – OVH <https://www.ovh.pl/hosting/optimisation-php-fpm.xml> [dostęp 01.06.2021]

```
37.187.124.66 - PuTTY
[4/4] Extracting mod_php74-7.4.19: 100%
[activating module `php7' in /usr/local/etc/apache24/httpd.conf]
=====
Message from mod_php74-7.4.19:
--
*****
Make sure index.php is part of your DirectoryIndex.

You should add the following to your Apache configuration file:

<FilesMatch "\.php$" >
    SetHandler application/x-httpd-php
</FilesMatch >
<FilesMatch "\.phps$" >
    SetHandler application/x-httpd-php-source
</FilesMatch >

*****

If you are building PHP-based ports in poudriere(8) or Synth with ZTS enabled,
add WITH_MPM=event to /etc/make.conf to prevent build failures.

*****
root@brylka:~ #
[brylka] [ 0$ csh 1$ csh 2$ csh 3-$ csh (4*$ csh) ] [06/06/21 11:47 AM]
```

Rys 3.4.2.2: Informacje poinstalacyjne mod_php.

Po instalacji pakietów należy dopisać odpowiednie linijki do pliku konfiguracyjnego Apache, tak aby wiedział, że pliki *.php ma wykonywać PHP.

```
37.187.124.66 - PuTTY
Include etc/apache24/Includes/*.conf

<IfModule mod_ssl.c>
Listen 443
</IfModule>
Include /usr/local/etc/apache24/extra/httpd-vhosts-le-ssl.conf

<FilesMatch "\.php$" >
    SetHandler application/x-httpd-php
</FilesMatch >
<FilesMatch "\.phps$" >
    SetHandler application/x-httpd-php-source
</FilesMatch >

root@brylka:/usr/local/etc/apache24 # service apache24 restart
Performing sanity check on apache24 configuration:
Syntax OK
Stopping apache24.
Waiting for PIDS: 33899.
Performing sanity check on apache24 configuration:
Syntax OK
Starting apache24.
root@brylka:/usr/local/etc/apache24 #
[brylka] [ 0$ csh 1$ csh 2$ csh (3*$ csh) 4$ csh 5-$ csh ] [06/06/21 11:55 AM]
```

Rys 3.4.2.3: Dopisanie informacji o plikach *.php w konfiguracji Apache.

PHP Version 7.4.19	
System	FreeBSD brylka 13.0-RELEASE FreeBSD 13.0-RELEASE #0: Sun May 16 13:48:35 CEST 2021; root@brylka:/usr/obj/usr/src/amd64.amd64/sys/BRYLKAKERNEL amd64
Build Date	May 30 2021 09:03:27
Configure Command	'./configure' '--with-layout=GNU' '--with-config-file-scan-dir=/usr/local/etc/php' '--disable-all' '--enable-password-argon2=/usr/local' '--program-prefix=' '--enable-mysqld' '--disable-cli' '--disable-apxs2=/usr/local/sbin/apxs' '--enable-dtrace' '--prefix=/usr/local' '--localstatedir=/var' '--mandir=/usr/local/share/info' '--build=amd64-portbld-freebsd13.0' 'build_alias=amd64-portbld-freebsd13.0' 'PKG_CONFIG=pkgconf' 'CFLAGS=-O2 -pipe -fstack-protector-strong -fno-strict-aliasing' 'CXXFLAGS=-O2 -pipe -fstack-protector-strong -fno-strict-aliasing'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php
Additional .ini files parsed	(none)
PHP API	20190902
PHP Extension	20190902

Rys 3.4.2.4: Obsługa php na serwerze zainstalowana.

3.5. INSTALACJA I KONFIGURACJA MYSQL

Aby zainstalować MySQL w wersji 5.7 wykonujemy polecenie:

```
pkg install mysql57-server mysql57-client
```

Zostanie wyświetlona informacja z pakietami jakie zostaną zainstalowane razem z serwerem i klientem MySQL.

```

37.187.124.66 - PuTTY
root@brylka:~ # pkg install mysql57-server mysql57-client
Updating FreeBSD_latest repository catalogue...
FreeBSD_latest repository is up to date.
All repositories are up to date.
The following 9 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:
  cyrus-sasl: 2.1.27_1
  groff: 1.22.4_3
  libedit: 3.1.20210216,1
  libpaper: 1.1.24.4
  mysql57-client: 5.7.34
  mysql57-server: 5.7.34
  protobuf: 3.14.0,1
  psutils: 1.17_5
  uchardet: 0.0.7

Number of packages to be installed: 9
The process will require 246 MiB more space.
23 MiB to be downloaded.

Proceed with this action? [y/N]: █

[brylka] [0-$ csh (1*$ csh) ] [06/04/21 9:43 AM]

```

Rys 3.5.1.: Informacje o nowych pakietach instalowanych razem z serw. i klientem MySQL.

```
37.187.124.66 - PuTTY
If you want to use GSSAPI mechanism, install
ports/security/cyrus-sasl2-gssapi.
If you want to use SRP mechanism, install
ports/security/cyrus-sasl2-srp.
If you want to use LDAP auxprop plugin, install
ports/security/cyrus-sasl2-ldapdb.
=====
Message from mysql57-client-5.7.34:
--
This is the mysql CLIENT without the server.
for complete server and client, please install databases/mysql57-server
=====
Message from mysql57-server-5.7.34:
--
Initial password for first time use of MySQL is saved in $HOME/.mysql_secret
ie. when you want to use "mysql -u root -p" first you should see password
in /root/.mysql_secret

MySQL57 has a default /usr/local/etc/mysql/my.cnf,
remember to replace it with your own
or set `mysql_optfile="$YOUR_CNF_FILE` in rc.conf.
root@brylka:~ # █
[brylka] 0$ csh (1*$ csh) 2-$ csh [06/04/21 9:48 AM]
```

Rys 3.5.2: Po instalacji otrzymujemy informacje o hasle administratora oraz pliku konfiguracyjnym.

Jeszcze do niedawna po instalacji poprzednich wersji serwera MySQL haslo administratora bylo nienadawane, bylo puste, w związku z czym można było popełnić poważny bład zabezpieczenia serwera, pozostawiając haslo puste – przez co każdy użytkownik Internetu mógł się połączyć z serwerem podając tylko użytkownika root i otrzymując uprawnienia administratora systemu bazodanowego MySQL.

Dopisujemy do pliku konfiguracyjnego systemu /etc/rc.conf informacje o uruchamianiu MySQL.

```
sysrc mysql_enable="yes"
```

Następnie uruchamiany serwer.

```
service mysql-server start
```

Serwer został uruchomiony.

```
37.187.124.66 - PuTTY
If you want to use LDAP auxprop plugin, install
ports/security/cyrus-sasl2-ldapdb.
=====
Message from mysql57-client-5.7.34:
--
This is the mysql CLIENT without the server.
for complete server and client, please install databases/mysql57-server
=====
Message from mysql57-server-5.7.34:
--
Initial password for first time use of MySQL is saved in $HOME/.mysql_secret
ie. when you want to use "mysql -u root -p" first you should see password
in /root/.mysql_secret

MySQL57 has a default /usr/local/etc/mysql/my.cnf,
remember to replace it with your own
or set `mysql_optfile="$YOUR_CNFILE` in rc.conf.
root@brylka:~ # sysrc mysql_enable="yes"
mysql_enable: -> yes
root@brylka:~ # service mysql-server start
Starting mysql.
root@brylka:~ # █
[brylka] 0$ csh (1*$ csh) 2-$ csh [06/04/21 9:58 AM]
```

Rys 3.5.3: Dopisanie informacji do rc.conf oraz uruchomienie serwera MySQL.

Zaleca się zabezpieczenie MySQL przed użyciem jej do użytku produkcyjnego. Należy użyć polecenia:

```
mysql_secure_installation
```

Po wykonaniu polecenia skrypt zada nam kilka pytań (odpowiadamy Y – tak) oraz zmienimy hasło administratora.

```
# mysql_secure_installation
```

```
Securing the MySQL server deployment.
```

```
Connecting to MySQL server using password in '/root/.mysql_secret'
```

```
VALIDATE PASSWORD PLUGIN can be used to test passwords
and improve security. It checks the strength of the password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD plugin?
```

```
Press y|Y for Yes, any other key for No: y
```

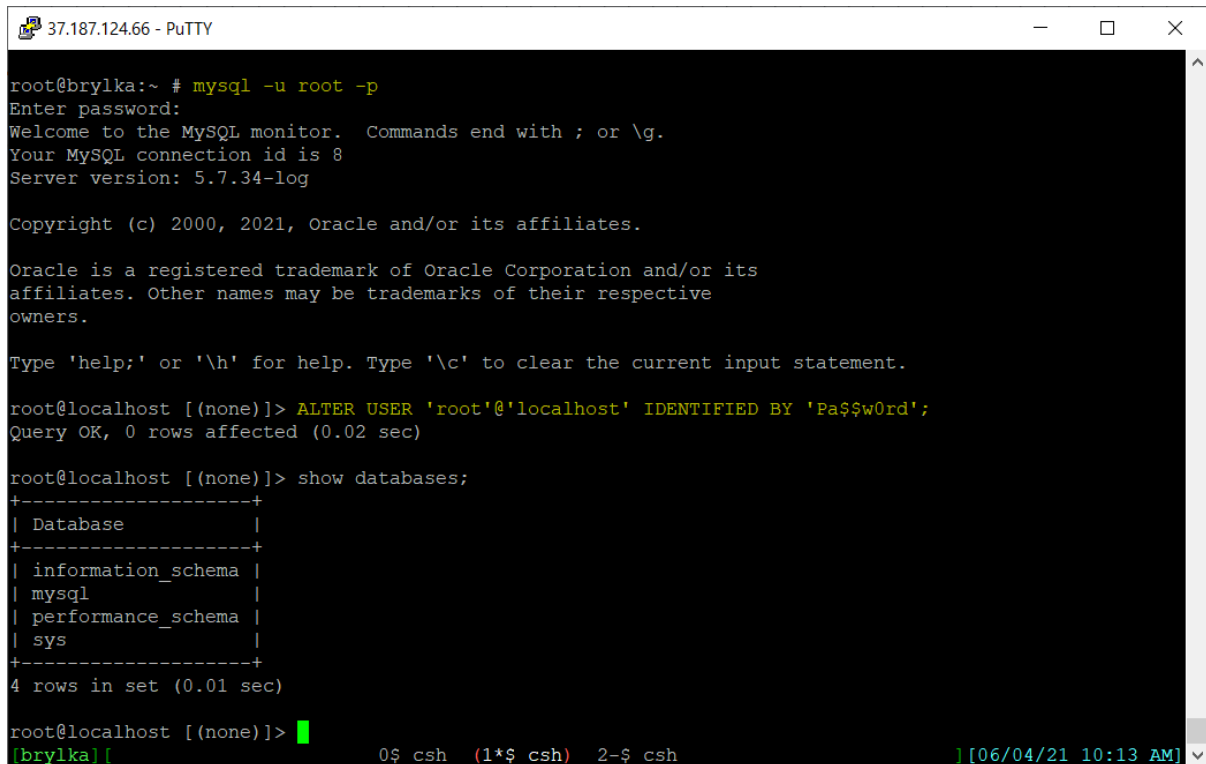
```
There are three levels of password validation policy:
```

```
LOW      Length >= 8
MEDIUM  Length >= 8, numeric, mixed case, and special characters
STRONG Length >= 8, numeric, mixed case, special characters and dictionary
file
```

```
Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 1
Change the password for root ? : y
Do you wish to continue with the password provided? : y
Remove anonymous users? : y
Disallow root login remotely? : y
Remove test database and access to it? : y
```

```
Reload privilege tables now? : y
All done!
```

Po połączeniu z MySQL przed wykonaniem jakiegokolwiek komendy należy ponownie zmienić hasło.



```
37.187.124.66 - PuTTY
root@brylka:~ # mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 5.7.34-log

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.

root@localhost [(none)]> ALTER USER 'root'@'localhost' IDENTIFIED BY 'Pa$$w0rd';
Query OK, 0 rows affected (0.02 sec)

root@localhost [(none)]> show databases;
+-----+
| Database          |
+-----+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+-----+
4 rows in set (0.01 sec)

root@localhost [(none)]> █
[brylka] 0$ csh (1*$ csh) 2-$ csh [06/04/21 10:13 AM]
```

Rys 3.5.4: Zalogowanie się jako administrator do MySQL, zmiana hasła (hasło na rysunku nie jest poprawnym ustawionym hasłem w systemie).

System zarządzania bazą danych (SZBD) MySQL w wersji 5.7 został zainstalowany i skonfigurowany - ustawione hasło administratora oraz wyłączenie możliwości logowania się na root'a z innej lokalizacji niż localhost.

3.5.1. INSTALACJA I KONFIGURACJA PHPMYADMIN

Instalację phpMyAdmin rozpoczynamy od odnalezienia odpowiedniego dla wersji php pakietu, następnie wykonujemy polecenie:

```
pkg install phpMyAdmin5-php74
```

Wraz z phpMyAdmin zainstalowane zostaną inne niezbędne do działania pakiety.


```
37.187.124.66 - PuTTY
root@brylka:/usr/local/etc/apache24 # pkg search phpmyadmin
phpMyAdmin-php73-4.9.7      Set of PHP-scripts to manage MySQL over the web
phpMyAdmin-php74-4.9.7      Set of PHP-scripts to manage MySQL over the web
phpMyAdmin-php80-4.9.7      Set of PHP-scripts to manage MySQL over the web
phpMyAdmin5-php73-5.1.0     Set of PHP-scripts to manage MySQL over the web
phpMyAdmin5-php74-5.1.0     Set of PHP-scripts to manage MySQL over the web
phpMyAdmin5-php80-5.1.0     Set of PHP-scripts to manage MySQL over the web
root@brylka:/usr/local/etc/apache24 # pkg install phpMyAdmin5-php74
Updating FreeBSD_latest repository catalogue...
FreeBSD_latest repository is up to date.
All repositories are up to date.
The following 25 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:
  fontconfig: 2.13.93,1
  freetype2: 2.10.4
  giflib: 5.2.1
  jbigkit: 2.1_1
  jpeg-turbo: 2.0.6
  libgd: 2.3.1,1
  libzip: 1.7.3
  oniguruma: 6.9.7.1
  php74-bz2: 7.4.19
  php74-ctype: 7.4.19
  php74-filter: 7.4.19
  php74-gd: 7.4.19
  php74-json: 7.4.19
  php74-mbstring: 7.4.19
  php74-mysqli: 7.4.19
  php74-openssl: 7.4.19
  php74-session: 7.4.19
  php74-xml: 7.4.19
  php74-xmlwriter: 7.4.19
  php74-zip: 7.4.19
  php74-zlib: 7.4.19
  phpMyAdmin5-php74: 5.1.0
  png: 1.6.37_1
  tiff: 4.3.0
  webp: 1.2.0

Number of packages to be installed: 25

The process will require 76 MiB more space.
13 MiB to be downloaded.

Proceed with this action? [y/N]: █
[brylka] [ 0$ csh 1$ csh 2$ csh (3*$ csh) 4$ csh 5-$ csh ] [06/06/21 12:03 PM]
```

Ryz 3.5.1.1: Rozpoczęcie instalacji phpMyAdmin.

Po instalacji phpMyAdmin należy do pliku konfiguracyjnego Apache dopisać odpowiednie linijki.

```
37.187.124.66 - PuTTY
--
phpMyAdmin5-php74-5.1.0 has been installed into:

    /usr/local/www/phpMyAdmin

Please edit config.inc.php to suit your needs.

To make phpMyAdmin available through your web site, I suggest
that you add something like the following to httpd.conf:

For Apache versions earlier than 2.4:

Alias /phpmyadmin/ "/usr/local/www/phpMyAdmin/"

<Directory "/usr/local/www/phpMyAdmin/">
    Options none
    AllowOverride Limit

    Order Deny,Allow
    Deny from all
    Allow from 127.0.0.1 .example.com
</Directory>

For Apache version 2.4.x or above:

Alias /phpmyadmin/ "/usr/local/www/phpMyAdmin/"

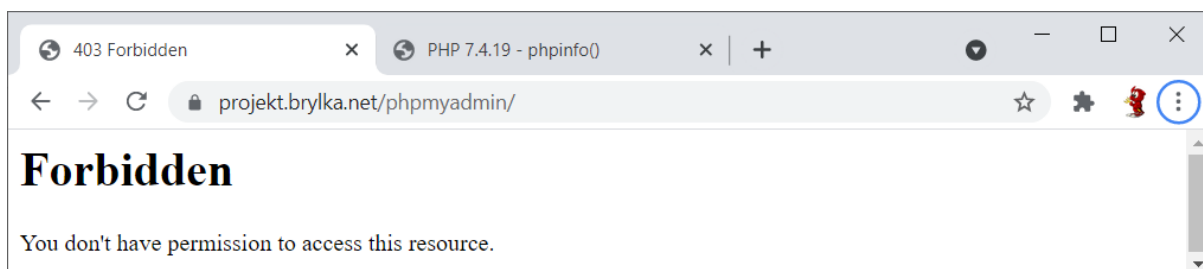
<Directory "/usr/local/www/phpMyAdmin/">
    Options None
    AllowOverride Limit

    Require local
    Require host .example.com
</Directory>

SECURITY NOTE: phpMyAdmin is an administrative tool that has had several
remote vulnerabilities discovered in the past, some allowing remote
attackers to execute arbitrary code with the web server's user credential.
All known problems have been fixed, but the FreeBSD Security Team strongly
advises that any instance be protected with an additional protection layer,
e.g. a different access control mechanism implemented by the web server
as shown in the example. Do consider enabling phpMyAdmin only when it
is in use.
root@brylka:/usr/local/etc/apache24 # █
[brylka][ 0$ csh 1$ csh 2$ csh (3*$ csh) 4$ csh 5-$ csh ] [06/06/21 12:07 PM]
```

Rys 3.5.1.2: Informacje poinstalacyjne phpMyAdmin.

W pliku konfiguracyjnym należy w odpowiednią linię wpisać swoją (klienta) nazwę domenową. Ustawienie to ma za zadanie ograniczyć dostęp do aplikacji dla potencjalnych włamywaczy.



Rys 3.5.1.3: Brak dostępu dla hostów innych niż wpisane w ustawieniu Apache.

```
37.187.124.66 - PuTTY
Alias /phpmyadmin/ "/usr/local/www/phpMyAdmin/"

<Directory "/usr/local/www/phpMyAdmin/">
    Options None
    AllowOverride Limit
    Require local
    Require host home.brylka.net
</Directory>

root@brylka:~ # service apache2 restart
Performing sanity check on apache24 configuration:
Syntax OK
Stopping apache24.
Waiting for PIDS: 34452.
Performing sanity check on apache24 configuration:
Syntax OK
Starting apache24.
root@brylka:~ #
[brylka] 0$ csh 1$ csh 2$ csh 3$ csh (4*$ csh) 5-$ csh ] [06/06/21 12:20 PM]
```

Rys 5.3.1.4: Dopisanie odpowiednich linijek do konfiguracji Apache i restart.

Po uruchomieniu phpMyAdmin w przeglądarce oprogramowanie poinformowało o braku jeszcze jednego rozszerzenia php: php74-iconv

```
37.187.124.66 - PuTTY
The following 1 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:
    php74-iconv: 7.4.19

Number of packages to be installed: 1

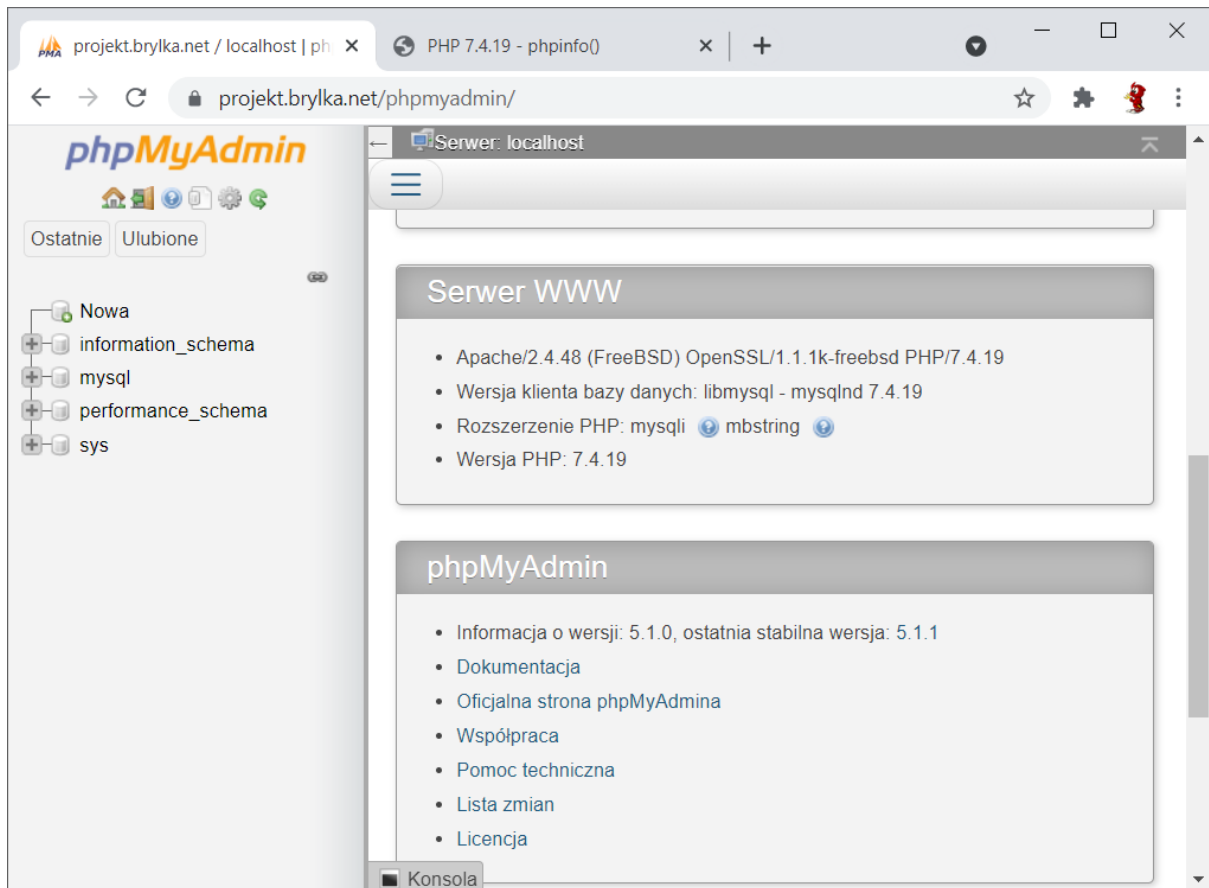
17 KiB to be downloaded.

Proceed with this action? [y/N]: y
[1/1] Fetching php74-iconv-7.4.19.txz: 100% 17 KiB 17.8kB/s 00:01
Checking integrity... done (0 conflicting)
[1/1] Installing php74-iconv-7.4.19...
[1/1] Extracting php74-iconv-7.4.19: 100%
=====
Message from php74-iconv-7.4.19:

--
This file has been added to automatically load the installed extension:
/usr/local/etc/php/ext-20-iconv.ini
root@brylka:~ #
[brylka] 0$ csh 1$ csh 2$ csh 3$ csh (4*$ csh) 5-$ csh ] [06/06/21 12:27 PM]
```

Rys 5.3.1.5: Instalacja rozszerzenia php74-iconv.

Po doinstalowaniu tego pakietu, phpMyAdmin pozwolił na zalogowanie się do systemu bazodanowego MySQL zainstalowanego na serwerze.



Rys 5.3.1.6: Zalogowanie się do phpMyAdmin na konto administratora.

3.5.2. DODANIE TABEL DO OBSŁUGI SYSTEMU POCZTOWEGO

Dodajemy użytkownika i bazę danych maia, a następnie importujemy zawartość pliku `/usr/local/share/doc/maia/maia-mysql.sql`. Niestety podczas wykonywania kwerend z pliku wystąpił błąd, w związku z czym resztę pliku dodałem ręcznie z poziomu phpMyAdmin.

```
37.187.124.66 - PuTTY

root@brylka:~ # mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 45
Server version: 5.7.34-log Source distribution

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.

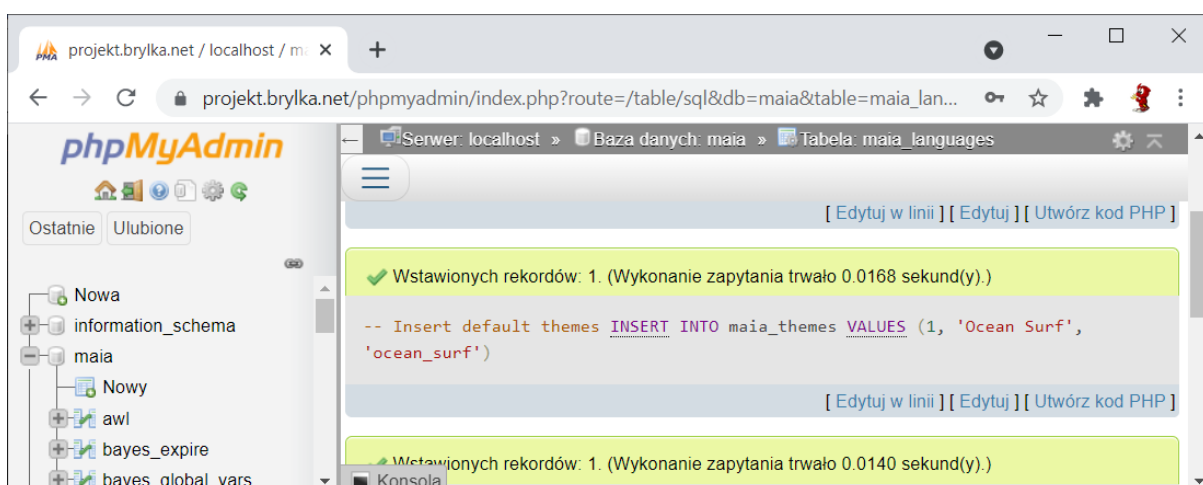
root@localhost [(none)]> CREATE DATABASE maia;
Query OK, 1 row affected (0.08 sec)

root@localhost [(none)]> GRANT ALL PRIVILEGES ON maia.* TO vscan@localhost IDENTIFIED BY '██████████';
Query OK, 0 rows affected, 1 warning (0.05 sec)

root@localhost [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.05 sec)

root@localhost [(none)]> QUIT;
Bye
root@brylka:~ # mysql -u vscan -p < /usr/local/share/doc/maia/maia-mysql.sql
Enter password:
ERROR 1046 (3D000) at line 79: No database selected
root@brylka:~ # mysql -u vscan -p maia < /usr/local/share/doc/maia/maia-mysql.sql
1
Enter password:
ERROR 1366 (HY000) at line 716: Incorrect string value: '\xC2\x9Atina' for column
n 'language_name' at row 1
root@brylka:~ # █
[brylka] [ 0$ csh 1$ csh 2$ csh 3$ csh (4*$ csh) 5-$ csh 6$ csh ] [06/07/2
```

Rys 3.5.2.1: Dodanie użytkownika i bazy danych maia do MySQL, import pliku sql.



Rys 3.5.2.2: Ręczny import reszty kwerend z pliku maia-mysql.sql

Dodajemy użytkownika i bazę danych postfix, będzie ona potrzebna do konfiguracji postfixa, tu będą przechowywane wszystkie informacje o skrynkach pocztowych.

```
37.187.124.66 - PuTTY
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.

root@localhost [(none)]> CREATE DATABASE postfix;
Query OK, 1 row affected (0.02 sec)

root@localhost [(none)]> CREATE USER 'postfix'@'localhost' IDENTIFIED BY '██████████';
Query OK, 0 rows affected (0.03 sec)

root@localhost [(none)]> GRANT ALL PRIVILEGES ON `postfix`.* TO 'postfix'@'localhost';
Query OK, 0 rows affected (0.02 sec)

root@localhost [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.02 sec)

root@localhost [(none)]> QUIT;
Bye
root@brylka:~ # █
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/21 8:36
```

Rys 3.5.2.3: Dodanie użytkownika i bazę danych postfix.

Dodajemy użytkownika i bazę danych rouncube w której będą przechowywane dane aplikacji.

```
37.187.124.66 - PuTTY
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 557
Server version: 5.7.34-log Source distribution

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.

root@localhost [mysql]> CREATE DATABASE rouncube;
Query OK, 1 row affected (0.08 sec)

root@localhost [mysql]> GRANT ALL PRIVILEGES ON rouncube.* TO rouncube@localho
st IDENTIFIED BY '██████████';
Query OK, 0 rows affected, 1 warning (0.15 sec)

root@localhost [mysql]> QUIT;
Bye
root@brylka:~ # █
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh (4*$ csh) 5$ csh 6-$ csh ] [06/10/2
```

Rys 3.5.2.4: Dodanie użytkownika i bazę danych rouncube.

3.6. INSTALACJA I KONFIGURACJA DOVECOT (POP3 I IMAP)

Przed instalacją serwera SMTP zainstalowany zostanie serwer POP3 i IMAP tak aby wcześniej zorganizować obsługę skrzynek pocztowych.

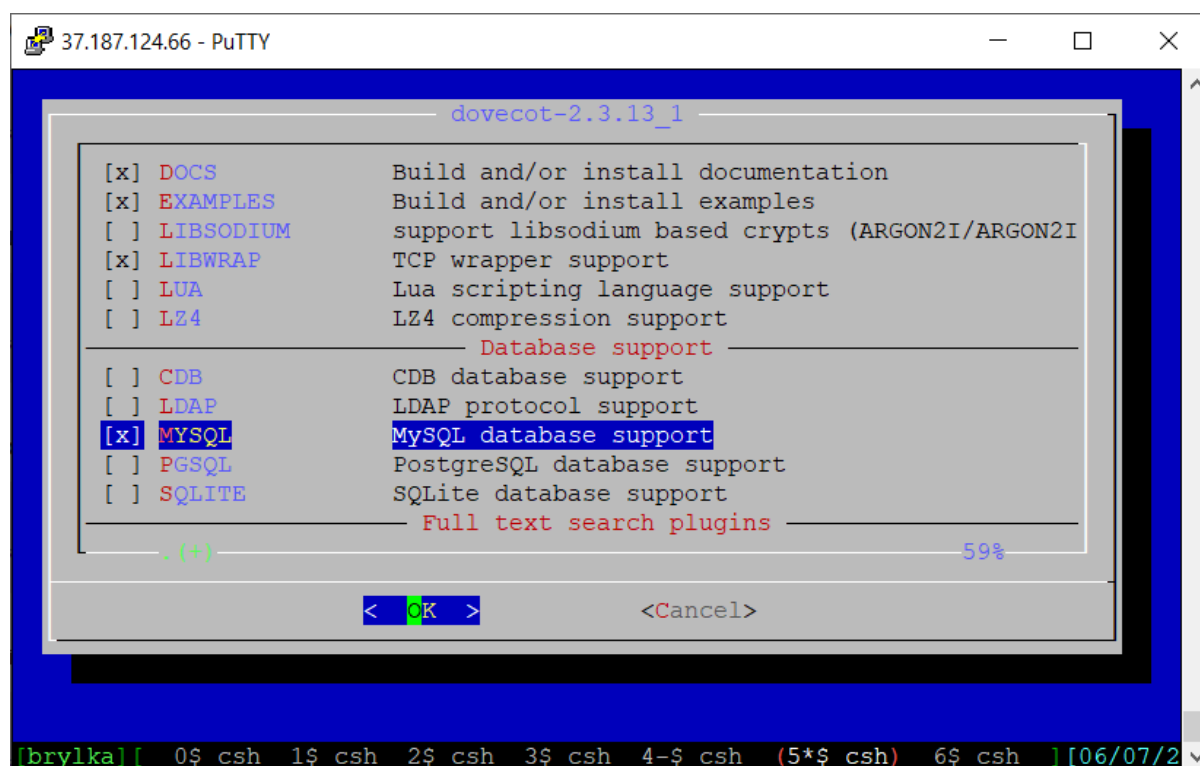
Dovecota musimy skompilować dodając opcje „MYSQL”

```
make config -C /usr/ports/mail/dovecot
```

Następnie wykonujemy polecenie:

```
portmaster -dG mail/dovecot  
portmaster -dG mail/dovecot-pigeonhole
```

które zainstaluje nam Dovecot’a oraz pakiet co obsługi języka Sieve (RFC 5228⁴²) i protokołu ManageSieve (RFC 5804⁴³). Projekt Pigeonhole zapewnia obsługę Sieve jako wtyczkę dla lokalnego agenta dostawy Dovecot (LDA), a także dla jego usługi LMTP. Wtyczka implementuje interpreter Sieve, który filtruje przychodzące wiadomości za pomocą skryptu określonego w języku Sieve. Wiadomości mogą być dostarczane do określonych folderów, przekazywane dalej, odrzucane, odrzucane, itp.



Rys 3.6.1: Konfiguracja Dovecot z obsługą MySQL.

⁴² rfc5228 <https://datatracker.ietf.org/doc/html/rfc5228> [dostęp 01.06.2021]

⁴³ rfc5804 <https://datatracker.ietf.org/doc/html/rfc5804> [dostęp 01.06.2021]

```
37.187.124.66 - PuTTY
===>>> pkg-message for dovecot-2.3.13_1
On install:
You must create the configuration files yourself. Copy them over
to /usr/local/etc/dovecot and edit them as desired:

    cp -R /usr/local/etc/dovecot/example-config/* \
        /usr/local/etc/dovecot

The default configuration includes IMAP and POP3 services, will
authenticate users against the system's passwd file, and will use
the default /var/mail/$USER mbox files.

Next, enable dovecot in /etc/rc.conf:

    dovecot_enable="YES"

To avoid a risk of mailbox corruption, do not set the
security.bsd.see_other_uids or .see_other_gids sysctls to 0
if Dovecot is storing mail for multiple concurrent users (PR 218392).

Similarly, setting sysctls security.bsd.hardlink_check_uid or
:
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4-$ csh (5*$ csh) 6$ csh ][06/07/2
```

Rys 3.6.2: Informacje poinstalacyjne Dovecota.

Dodajemy dovecota do uruchamianych programów podczas startu systemu. Następnie kopiujemy przykładowe pliki konfiguracyjne.

```
37.187.124.66 - PuTTY
root@brylka:/usr/local/etc/dovecot # sysrc dovecot_enable=YES
dovecot_enable: -> YES
root@brylka:/usr/local/etc/dovecot # cp -a /usr/local/etc/dovecot/example-config/* /u
sr/local/etc/dovecot
root@brylka:/usr/local/etc/dovecot # ls -la
total 62
drwxr-xr-x  4 root  wheel   11 Jun  6 21:32 .
drwxr-xr-x 19 root  wheel   41 Jun  6 21:22 ..
-rw-r--r--  1 root  wheel  116 May 27 19:57 README
drwxr-xr-x  2 root  wheel   26 Jun  6 21:22 conf.d
-rw-r--r--  1 root  wheel 1507 May 27 19:57 dovecot-dict-auth.conf.ext
-rw-r--r--  1 root  wheel  852 May 27 19:57 dovecot-dict-sql.conf.ext
-rw-r--r--  1 root  wheel  5733 May 27 19:57 dovecot-ldap.conf.ext
-rw-r--r--  1 root  wheel  2095 May 27 19:57 dovecot-oauth2.conf.ext
-rw-r--r--  1 root  wheel  5834 May 27 19:57 dovecot-sql.conf.ext
-rw-r--r--  1 root  wheel  4421 May 27 19:57 dovecot.conf
drwxr-xr-x  3 root  wheel    9 Jun  6 21:22 example-config
root@brylka:/usr/local/etc/dovecot #
```

Rys 3.6.3: Dodanie Dovecota do startu systemu, skopiowanie plików konfiguracyjnych.

W pliku `/usr/local/etc/dovecot/conf.d/10-auth.conf` dodajemy następujące ustawienia:

```
disable_plaintext_auth = no
auth_mechanisms = plain login
!include auth-sql.conf.ext
```


W pliku `/usr/local/etc/dovecot/conf.d/10-mail.conf` dodajemy następujące ustawienia:

```
# miejsce przechowywania skrzynek
mail_location = maildir:/usr/local/virtual/%d/%n

# organizacja folderów w skrzynce
namespace inbox {
    type = private
    separator = /

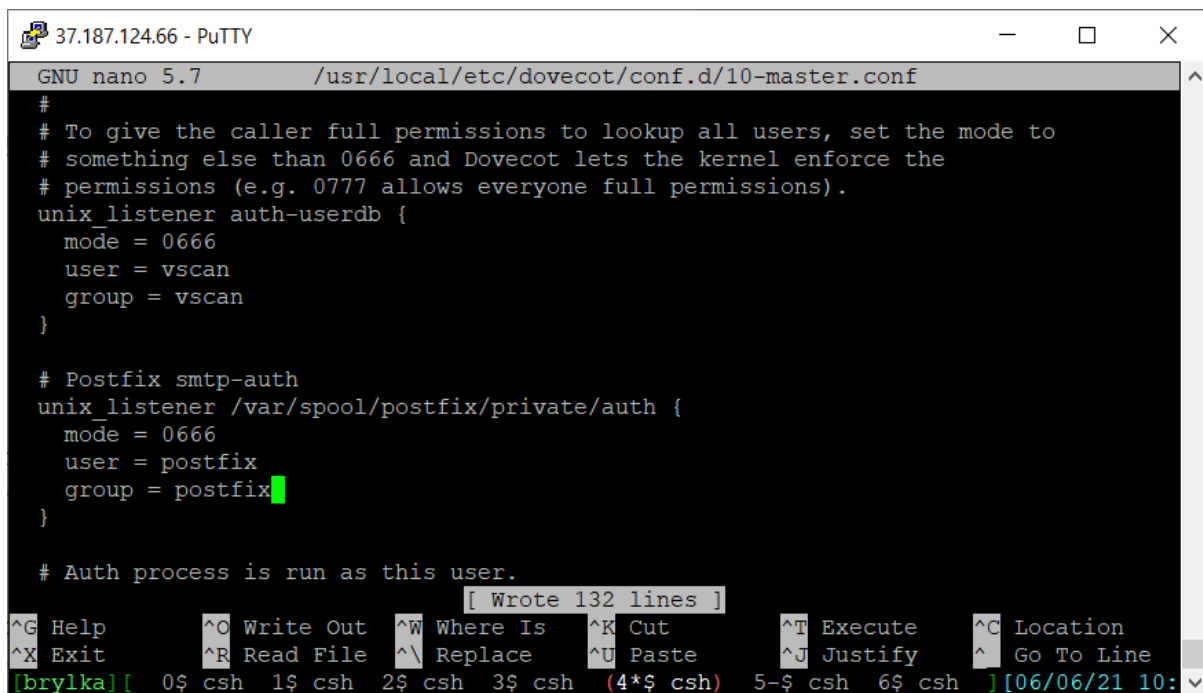
    mailbox Sent {
        auto = subscribe
        special_use = \Sent
    }
    mailbox Drafts {
        auto = subscribe
        special_use = \Drafts
    }
    mailbox Trash {
        auto = subscribe
        special_use = \Trash
    }
    mailbox Junk {
        auto = subscribe
        special_use = \Junk
    }
}

# ustawienie uid i gid na vscan (instalacja za chwilę)
first_valid_uid = 110
last_valid_uid = 110
first_valid_gid = 110
last_valid_gid = 110
# dodanie dodatkowych wtyczek
mail_plugins = mail_log notify
```

W pliku `/usr/local/etc/dovecot/conf.d/10-master.conf` dodajemy następujące ustawienia:

```
unix_listener auth-userdb {
    mode = 0666
    user = vscan
    group = vscan
}

# Postfix smtp-auth
unix_listener /var/spool/postfix/private/auth {
    mode = 0666
    user = postfix
    group = postfix
}
```



```
GNU nano 5.7 /usr/local/etc/dovecot/conf.d/10-master.conf
#
# To give the caller full permissions to lookup all users, set the mode to
# something else than 0666 and Dovecot lets the kernel enforce the
# permissions (e.g. 0777 allows everyone full permissions).
unix_listener auth-userdb {
    mode = 0666
    user = vscan
    group = vscan
}

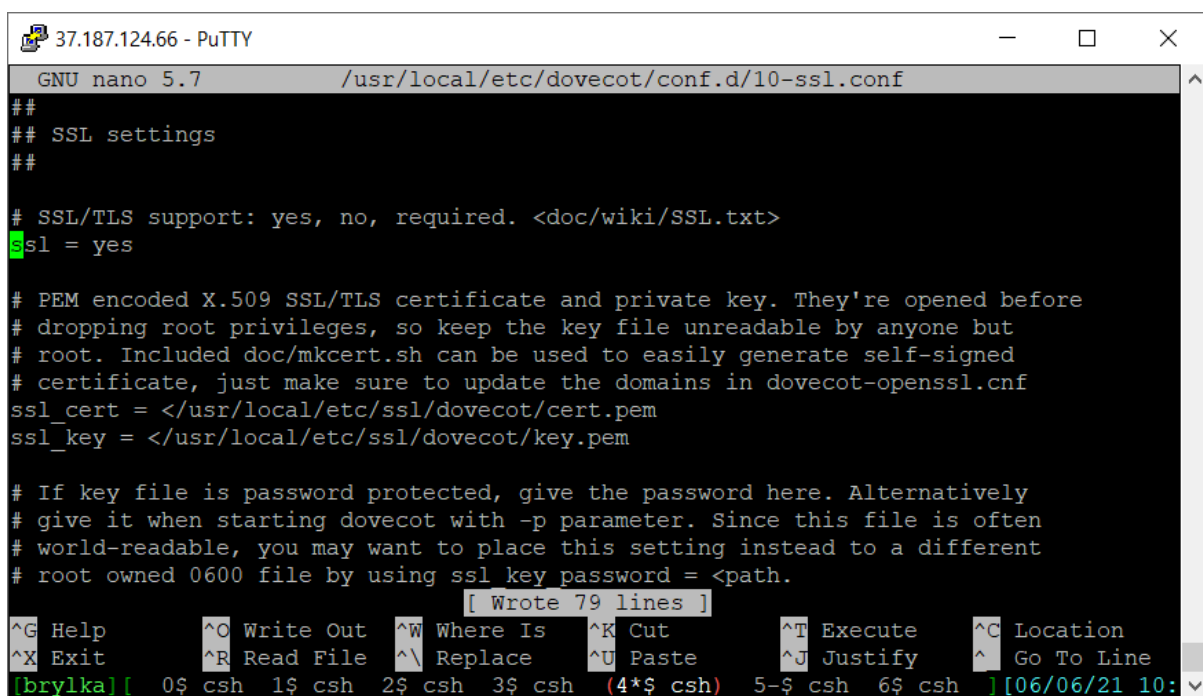
# Postfix smtp-auth
unix_listener /var/spool/postfix/private/auth {
    mode = 0666
    user = postfix
    group = postfix
}

# Auth process is run as this user.
[ Wrote 132 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh (4*$ csh) 5-$ csh 6$ csh ] [06/06/21 10:
```

Rys 3.6.4: Dodanie ustawień do pliku 10-master.conf

W pliku /usr/local/etc/dovecot/conf.d/10-ssl.conf dodajemy następujące ustawienia:

```
ssl = yes
ssl_cert = </usr/local/etc/ssl/dovecot/cert.pem
ssl_key = </usr/local/etc/ssl/dovecot/key.pem
ssl_ca = </usr/local/etc/ssl/dovecot/cert.pem
ssl_verify_client_cert = yes
ssl_dh = </usr/local/etc/ssl/dovecot/dh.pem
ssl_min_protocol = TLSv1.2
```



```
GNU nano 5.7 /usr/local/etc/dovecot/conf.d/10-ssl.conf
##
## SSL settings
##
# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
ssl = yes

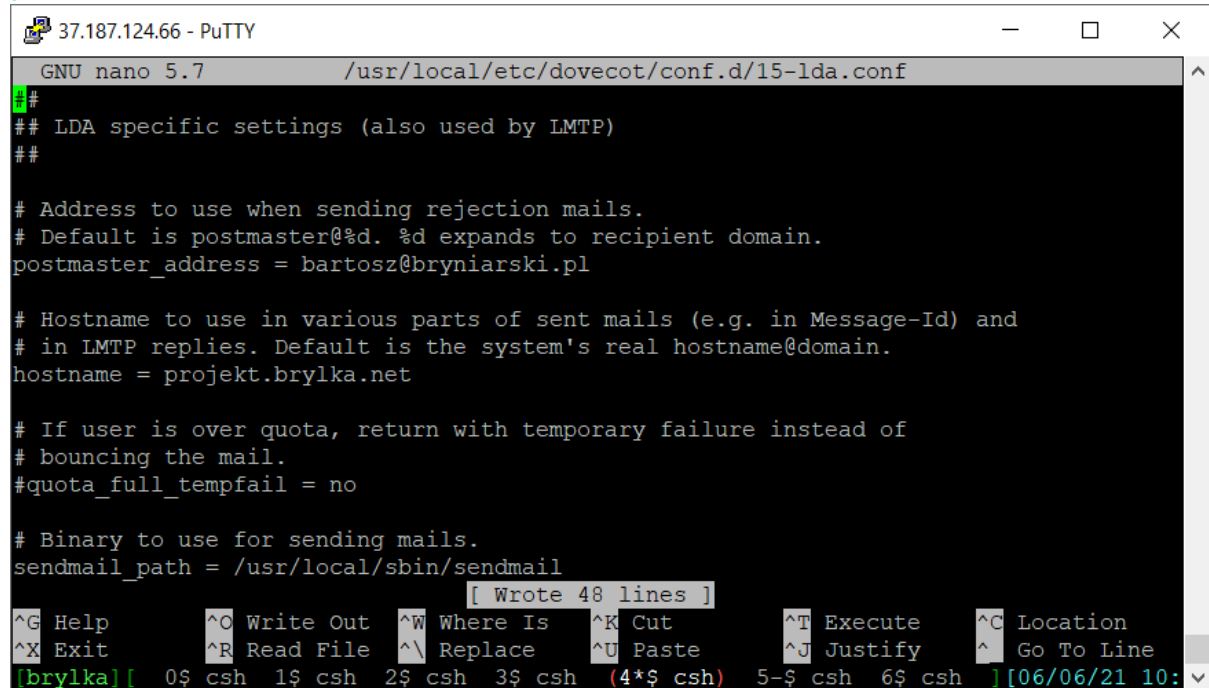
# PEM encoded X.509 SSL/TLS certificate and private key. They're opened before
# dropping root privileges, so keep the key file unreadable by anyone but
# root. Included doc/mkcert.sh can be used to easily generate self-signed
# certificate, just make sure to update the domains in dovecot-openssl.cnf
ssl_cert = </usr/local/etc/ssl/dovecot/cert.pem
ssl_key = </usr/local/etc/ssl/dovecot/key.pem

# If key file is password protected, give the password here. Alternatively
# give it when starting dovecot with -p parameter. Since this file is often
# world-readable, you may want to place this setting instead to a different
# root owned 0600 file by using ssl key password = <path>
[ Wrote 79 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh (4*$ csh) 5-$ csh 6$ csh ] [06/06/21 10:
```

Rys 3.6.5: Dodanie ustawień do pliku 10-ssl.conf.

W pliku /usr/local/etc/dovecot/conf.d/15-lda.conf dodajemy następujące ustawienia:

```
postmaster_address = bartosz@bryniarski.pl
hostname = projekt.brylka.net
sendmail_path = /usr/local/sbin/sendmail
lda_mailbox_autocreate = yes
protocol lda {
    mail_plugins = $mail_plugins sieve
}
```



The screenshot shows a terminal window titled "37.187.124.66 - PuTTY" with a nano editor open to the file "/usr/local/etc/dovecot/conf.d/15-lda.conf". The editor displays the following configuration:

```
##
## LDA specific settings (also used by LMTP)
##

# Address to use when sending rejection mails.
# Default is postmaster@d. %d expands to recipient domain.
postmaster_address = bartosz@bryniarski.pl

# Hostname to use in various parts of sent mails (e.g. in Message-Id) and
# in LMTP replies. Default is the system's real hostname@domain.
hostname = projekt.brylka.net

# If user is over quota, return with temporary failure instead of
# bouncing the mail.
#quota_full_tempfail = no

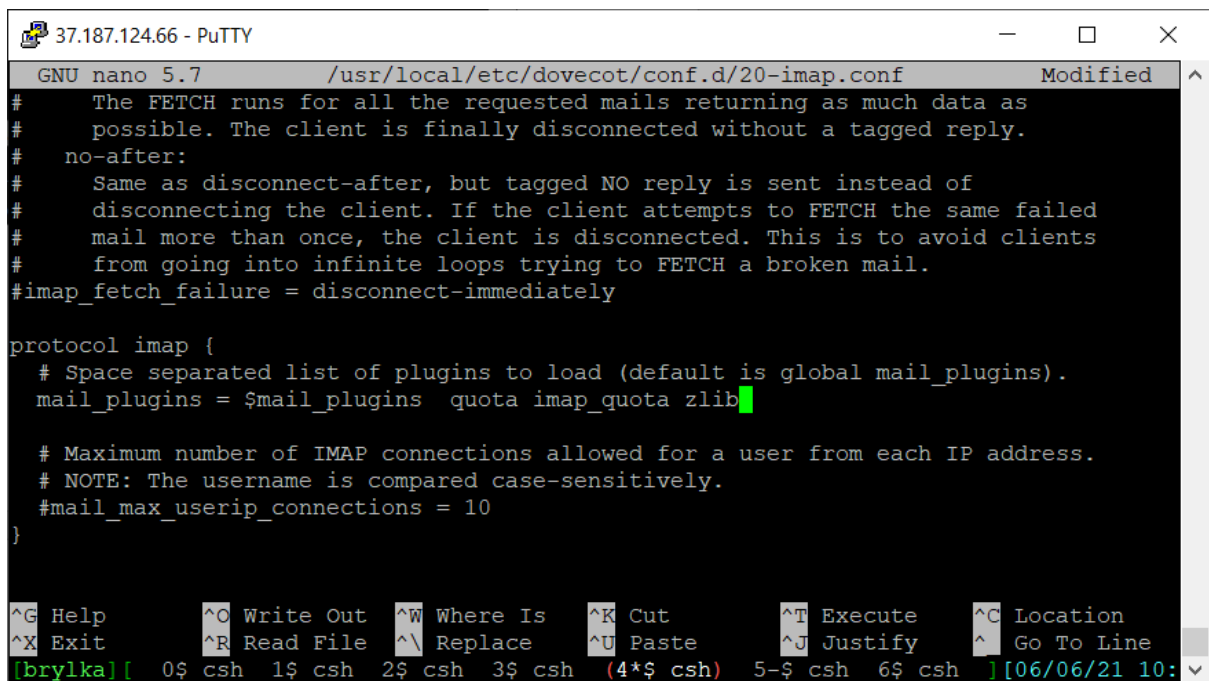
# Binary to use for sending mails.
sendmail_path = /usr/local/sbin/sendmail
```

The terminal also shows a status bar at the bottom with the prompt "[brylka]" and a menu of keyboard shortcuts: ^G Help, ^O Write Out, ^W Where Is, ^K Cut, ^T Execute, ^C Location, ^X Exit, ^R Read File, ^\ Replace, ^U Paste, ^J Justify, ^ Go To Line. The date and time are shown as "[06/06/21 10:". A notification "[Wrote 48 lines]" is visible in the center of the terminal.

Rys 3.6.6: Dodanie ustawień do pliku 15-lda.conf.

W pliku /usr/local/etc/dovecot/conf.d/20-imap.conf dodajemy następujące ustawienia:

```
protocol imap {
    # Space separated list of plugins to load (default is global mail_plugins).
    mail_plugins = $mail_plugins quota imap_quota zlib
}
```



```
GNU nano 5.7 /usr/local/etc/dovecot/conf.d/20-imap.conf Modified
# The FETCH runs for all the requested mails returning as much data as
# possible. The client is finally disconnected without a tagged reply.
# no-after:
# Same as disconnect-after, but tagged NO reply is sent instead of
# disconnecting the client. If the client attempts to FETCH the same failed
# mail more than once, the client is disconnected. This is to avoid clients
# from going into infinite loops trying to FETCH a broken mail.
#imap_fetch_failure = disconnect-immediately

protocol imap {
  # Space separated list of plugins to load (default is global mail_plugins).
  mail_plugins = $mail_plugins quota imap_quota zlib
}

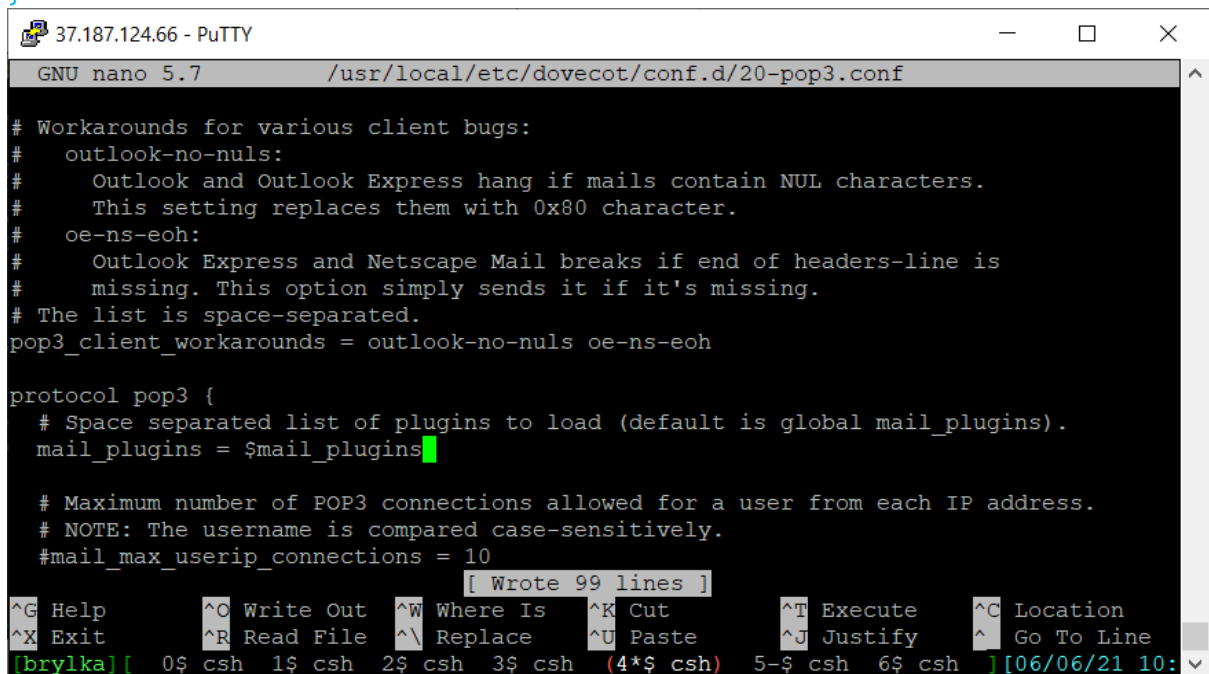
# Maximum number of IMAP connections allowed for a user from each IP address.
# NOTE: The username is compared case-sensitively.
#mail_max_userip_connections = 10
}

^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
[brylka] 0$ csh 1$ csh 2$ csh 3$ csh (4*$ csh) 5-$ csh 6$ csh ] [06/06/21 10:
```

Rys 3.6.7: Dodanie ustawień do pliku 20-imap.conf.

W pliku /usr/local/etc/dovecot/conf.d/20-pop3.conf dodajemy następujące ustawienia:

```
pop3_client_workarounds = outlook-no-nuls oe-ns-eoh
protocol pop3 {
  mail_plugins = $mail_plugins
}
```



```
GNU nano 5.7 /usr/local/etc/dovecot/conf.d/20-pop3.conf

# Workarounds for various client bugs:
# outlook-no-nuls:
# Outlook and Outlook Express hang if mails contain NUL characters.
# This setting replaces them with 0x80 character.
# oe-ns-eoh:
# Outlook Express and Netscape Mail breaks if end of headers-line is
# missing. This option simply sends it if it's missing.
# The list is space-separated.
pop3_client_workarounds = outlook-no-nuls oe-ns-eoh

protocol pop3 {
  # Space separated list of plugins to load (default is global mail_plugins).
  mail_plugins = $mail_plugins
}

# Maximum number of POP3 connections allowed for a user from each IP address.
# NOTE: The username is compared case-sensitively.
#mail_max_userip_connections = 10
}

[ Wrote 99 lines ]
^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
[brylka] 0$ csh 1$ csh 2$ csh 3$ csh (4*$ csh) 5-$ csh 6$ csh ] [06/06/21 10:
```

Rys 3.6.8: Dodanie ustawień do pliku 20-pop3.conf.

W pliku /usr/local/etc/dovecot/conf.d/90-plugin.conf dodajemy następujące ustawienia:

```
plugin {
  expire = Trash
  mail_log_events = delete undelete expunge copy mailbox_delete mailbox_rename
```

```

mail_log_fields = uid box msgid size
}

plugin {
  sieve = /var/mail/vhosts/%d/%n/.dovecot.sieve
  sieve_dir = /var/mail/vhosts/home/%d/%n/sieve
  sieve_global_path = /var/mail/vhosts/default.sieve
  mail_home = /var/mail/vhosts/%d/%n
}

```

The screenshot shows a terminal window titled "37.187.124.66 - PuTTY" with a nano editor window open at "/usr/local/etc/dovecot/conf.d/90-plugin.conf". The editor shows the configuration for the 90-plugin.conf file, including comments and two plugin blocks. The first plugin block sets 'expire = Trash' and 'mail_log_events = delete undelete expunge copy mailbox_delete mailbox_rename'. The second plugin block sets 'sieve = /var/mail/vhosts/%d/%n/.dovecot.sieve', 'sieve_dir = /var/mail/vhosts/home/%d/%n/sieve', 'sieve_global_path = /var/mail/vhosts/default.sieve', and 'mail_home = /var/mail/vhosts/%d/%n'. A status bar at the bottom indicates "[Wrote 20 lines]" and a prompt "[brylka] [0\$ csh 1\$ csh 2\$ csh 3\$ csh (4*\$ csh) 5-\$ csh 6\$ csh] [06/06/21 10:..." is visible.

Rys 3.6.9: Dodanie ustawień do pliku 90-plugin.conf.

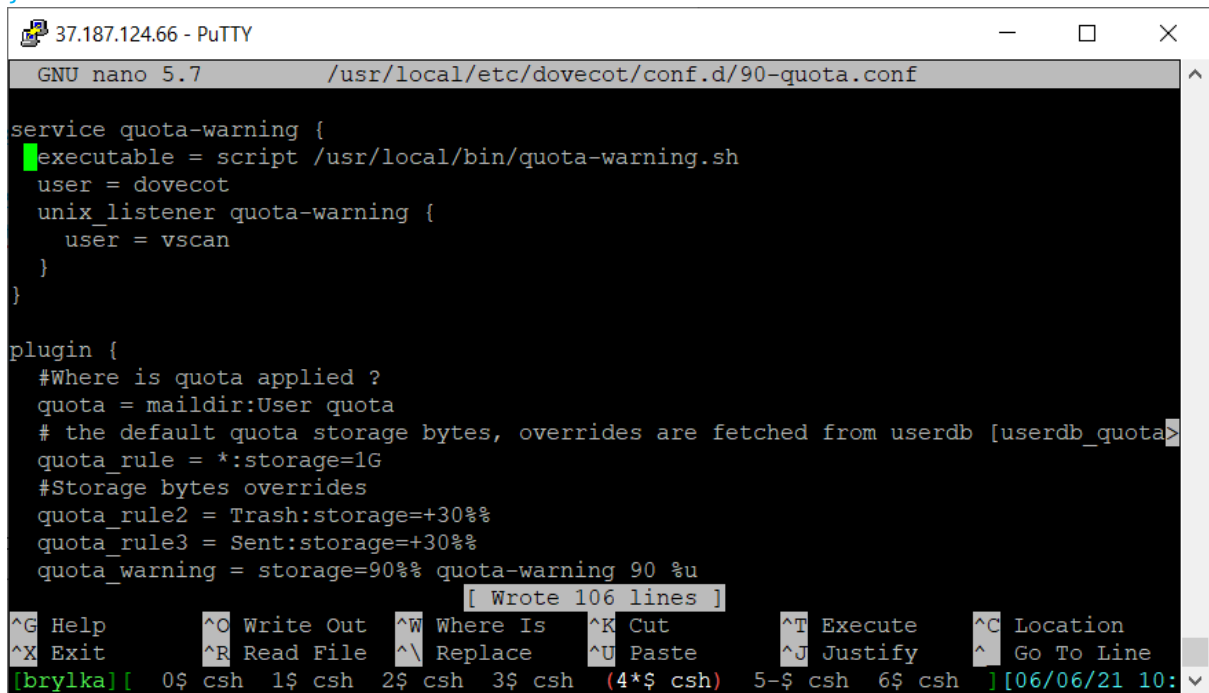
W pliku /usr/local/etc/dovecot/conf.d/90-quota.conf dodajemy następujące ustawienia:

```

service quota-warning {
  executable = script /usr/local/bin/quota-warning.sh
  user = dovecot
  unix_listener quota-warning {
    user = vscan
  }
}
...
(Add to end of file...)
plugin {
  #Where is quota applied ?
  quota = maildir:User quota
  # the default quota storage bytes, overrides are fetched from userdb
[userdb_quota_ruleX]
  quota_rule = *:storage=1G
  #Storage bytes overrides
  quota_rule2 = Trash:storage=+30%%
  quota_rule3 = Sent:storage=+30%%
  quota_warning = storage=90%% quota-warning 90 %u
  quota_warning2 = storage=75%% quota-warning 75 %u
  #What message to send to IMAP clients (and SMTP senders) when quota is exceeded?

```

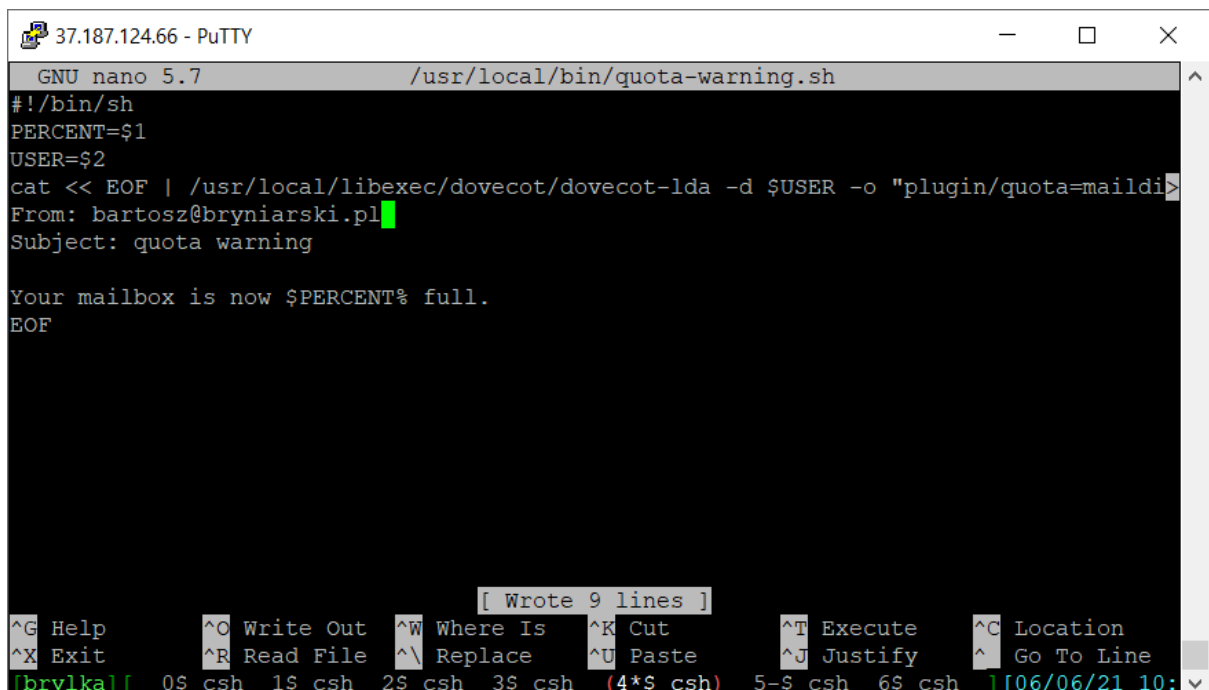
```
    quota_exceeded_message = Storage quota for this account has been exceeded,  
    please try again later.  
}
```



```
37.187.124.66 - PuTTY  
GNU nano 5.7 /usr/local/etc/dovecot/conf.d/90-quota.conf  
service quota-warning {  
  executable = script /usr/local/bin/quota-warning.sh  
  user = dovecot  
  unix_listener quota-warning {  
    user = vscan  
  }  
}  
  
plugin {  
  #Where is quota applied ?  
  quota = maildir:User quota  
  # the default quota storage bytes, overrides are fetched from userdb [userdb_quota  
  quota_rule = *:storage=1G  
  #Storage bytes overrides  
  quota_rule2 = Trash:storage=+30%%  
  quota_rule3 = Sent:storage=+30%%  
  quota_warning = storage=90%% quota-warning 90 %u  
  [ Wrote 106 lines ]  
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location  
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh (4*$ csh) 5-$ csh 6$ csh ] [06/06/21 10: >
```

Rys 3.6.10: Dodanie ustawień do pliku 90-quota.conf.

Tworzymy plik `/usr/local/bin/quota-warning.sh` odpowiedzialny za informacje o przepełnionej skrzynce.



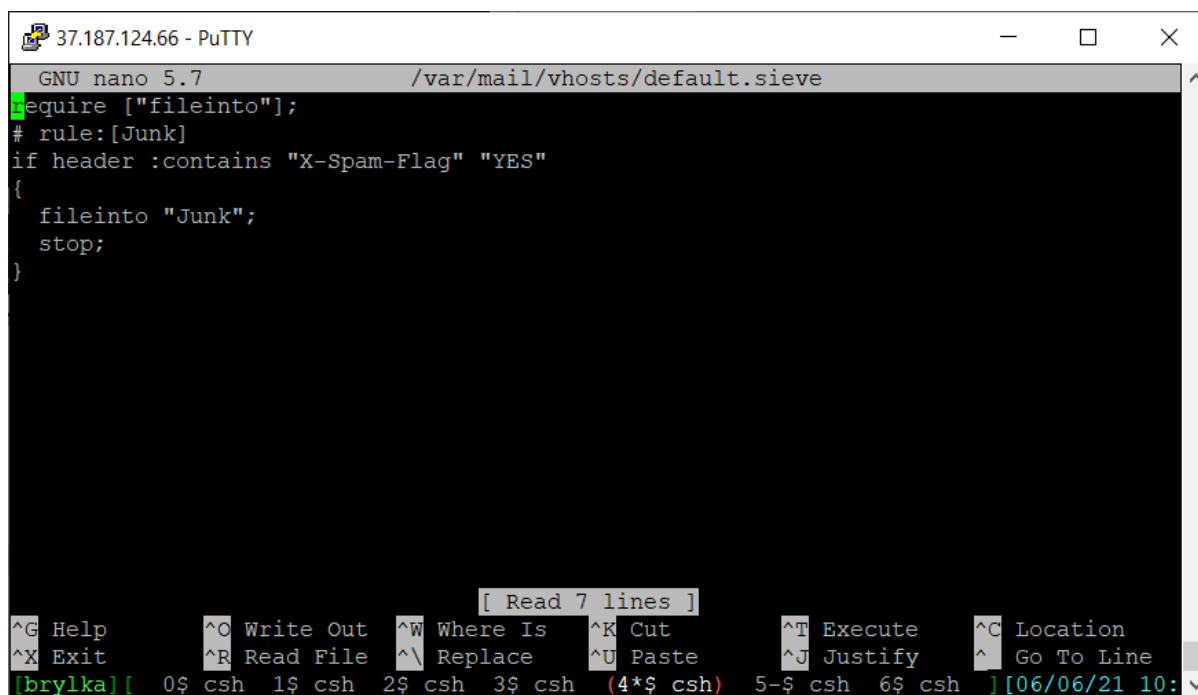
```
37.187.124.66 - PuTTY  
GNU nano 5.7 /usr/local/bin/quota-warning.sh  
#!/bin/sh  
PERCENT=$1  
USER=$2  
cat << EOF | /usr/local/libexec/dovecot/dovecot-lda -d $USER -o "plugin/quota=maildi  
From: bartosz@bryniarski.pl  
Subject: quota warning  
  
Your mailbox is now $PERCENT% full.  
EOF  
[ Wrote 9 lines ]  
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location  
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh (4*$ csh) 5-$ csh 6$ csh ] [06/06/21 10: >
```

Rys 3.6.11: Skrypt wysyłający informacje o przepełnionej skrzynce.

Tworzymy katalog w którym będą przechowywane skrzynki:

```
mkdir -p /var/mail/vhosts
```

Tworzymy plik /var/mail/vhosts/default.sieve:



```
GNU nano 5.7 /var/mail/vhosts/default.sieve
require ["fileinto"];
# rule:[Junk]
if header :contains "X-Spam-Flag" "YES"
{
    fileinto "Junk";
    stop;
}

[ Read 7 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh (4*$ csh) 5-$ csh 6$ csh ] [06/06/21 10: ]
```

Rys 3.6.12: Plik default.sieve.

Wykonujemy komendę sievec z defaultowym plikiem, w którym są regułki odnośnie spamu:

```
sievec /var/mail/vhosts/default.sieve
```

Następnie instalujemy Maia-Mailguard⁴⁴ - internetowy interfejs i system zarządzania oparty na popularnym skanerze poczty amavisd-new i SpamAssassin, daje użytkownikom końcowym kontrolę nad tym, jak ich poczta jest przetwarzana przez skanery antywirusowe i filtry antyspamowe, jednocześnie dając administratorom poczty możliwość konfigurowania ustawień domyślnych i limitów dla całej witryny.

Dodajemy opcje do ustawień maia: APACHE, DOVECOT2, PFA, POSTFIX oraz WEBHOST:

```
make config -C /usr/ports/security/maia
```

Następnie rozpoczynamy instalacje:

```
portmaster -dG --no-confirm security/maia
```

Podczas instalacji pakietu Maia-Mailguard zainstalowane zostały także między innymi Postfix, PostfixAdmin, spamassassin – ich konfiguracja zostanie przedstawiona w dalszej części.

⁴⁴ AboutMaia – Maia Mailguard <http://www.maiamailguard.com/maia/wiki/AboutMaia> [dostęp 01.06.2021]

```
37.187.124.66 - PuTTY
===>>> pkg-message for maia-1.0.4_7
On install:
To use Maia-Mailguard, you need to install at least one virus scanner.
The following virus scanners are available in the FreeBSD ports
collection:

security/clamav      Clam Antivirus
security/f-prot      F-Prot Antivirus
security/drweb       DrWeb antivirus suite

Enable Maia-Mailguard in /etc/rc.conf with the following line:

    maiad_enable="YES"

Configuration templates are available in /usr/local/etc/maia
as maia.conf.dist and maiad.conf.dist.

Please note that Maia Mailguard no longer supports "mysql" but has
moved forward to using "mysqli" instead. So, please check your
/usr/local/www/maia/config.php file and make any appropriate changes.

[brylka][ 0-$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6$ csh ][06/07/2
```

Rys 3.6.13: Informacje poinstalacyjne maia wskazujące na dodanie danych do pliku rc.conf.

Konfiguracją Maia-Mailguard zajmiemy się w dalszej części, w tej chwili należy zmienić hasło dla vscan:

```
passwd vscan
Changing local password for vscan
New Password:
Retype New Password:
```

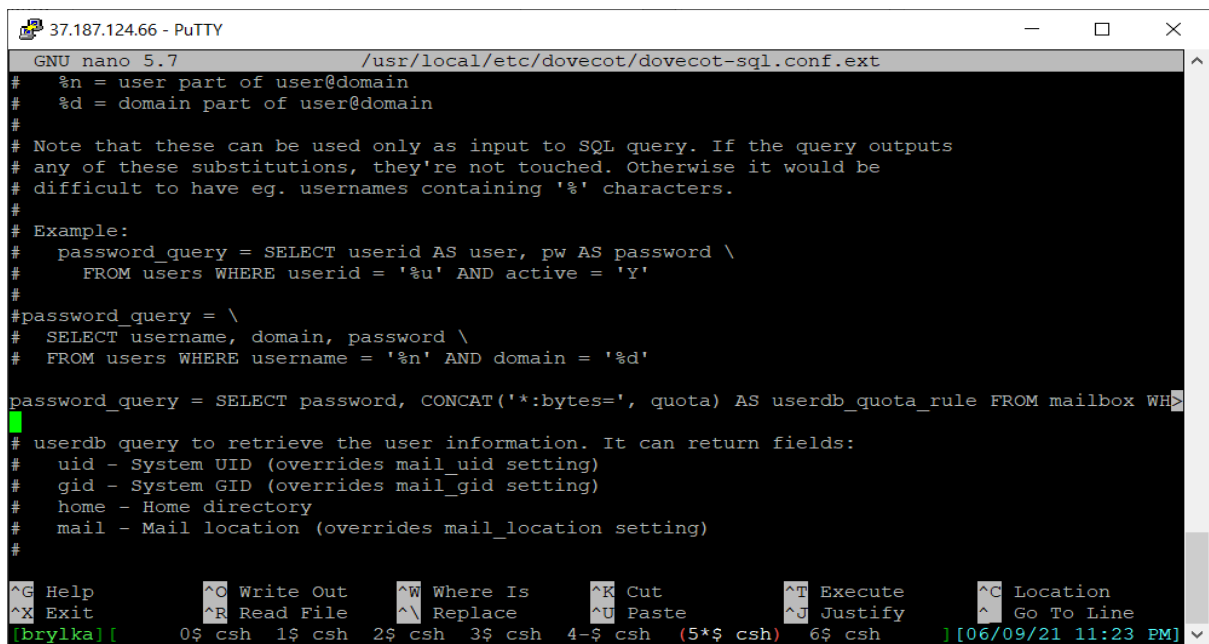
Następnie nadajemy odpowiednie prawa do katalogu /var/mail/vhost

```
37.187.124.66 - PuTTY
maid/ mail/
root@brylka:/usr/local/etc/dovecot # cd /var/mail/
beamium dovecot mysql postfix spamd vscan
cyrus dovenull noderig root vhosts/
root@brylka:/usr/local/etc/dovecot # cd /var/mail/
root@brylka:/var/mail # ls -la
total 903
drwxrwxr-x  3 root      mail      13 Jun  7 03:08 .
drwxr-xr-x 26 root      wheel     26 Jun  7 03:00 ..
-rw-----  1 beamium   beamium   0 May 16 10:00 beamium
-rw-----  1 cyrus     cyrus     0 Jun  4 09:46 cyrus
-rw-----  1 dovecot   dovecot   0 Jun  6 21:22 dovecot
-rw-----  1 dovenull  dovenull  0 Jun  6 21:22 dovenull
-rw-----  1 mysql     mysql     0 Jun  4 09:46 mysql
-rw-----  1 noderig   noderig   0 May 16 10:00 noderig
-rw-----  1 postfix   postfix   0 Jun  7 02:27 postfix
-rw-----  1 root      wheel     3771296 Jun  7 03:08 root
-rw-----  1 spamd     spamd     0 Jun  7 02:46 spamd
drwxr-xr-x  2 root      mail      4 Jun  6 22:54 vhosts
-rw-----  1 vscan     vscan     0 Jun  7 03:00 vscan
root@brylka:/var/mail # chown -R vscan:vscan /var/mail/vhosts
root@brylka:/var/mail # chmod 0755 /var/mail/vhosts
root@brylka:/var/mail #
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh (4*$ csh) 5-$ csh 6$ csh ][06/07/2
```

Rys 3.6.14: Nadanie praw do katalogu /var/mail/vhost

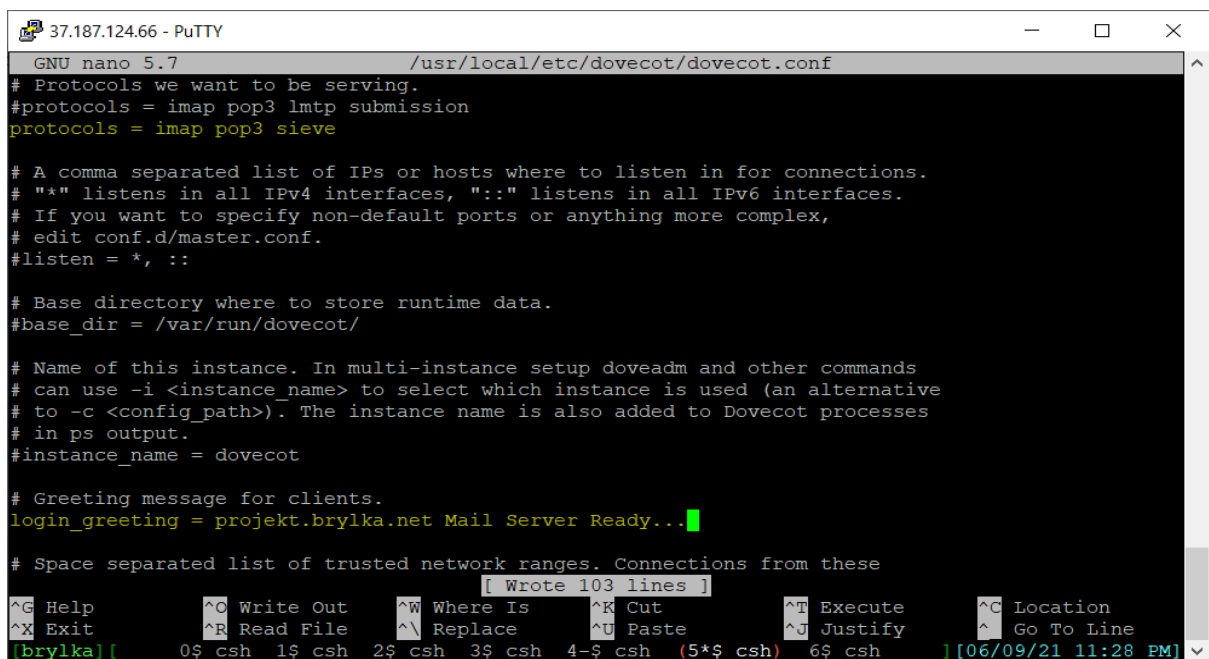
Edytujemy plik `/usr/local/etc/dovecot/dovecot-sql.conf.ext` wpisując następujące ustawienia:

```
driver = mysql
connect = host=localhost dbname=postfix user=postfix password=postfix_sql_password
default_pass_scheme = MD5
password_query = SELECT password, CONCAT('*:bytes=', quota) AS userdb_quota_rule
FROM mailbox WHERE username = '%u' AND active = '1'
user_query = SELECT CONCAT('/usr/local/virtual/', maildir) as home, 110 AS uid,
110 AS gid, CONCAT('*:bytes=', quota) AS quota_rule FROM mailbox WHERE username =
'%u' AND active = '1'
```



The screenshot shows a terminal window titled "37.187.124.66 - PuTTY" with the GNU nano 5.7 editor open to the file `/usr/local/etc/dovecot/dovecot-sql.conf.ext`. The editor displays the configuration file's content, including comments and SQL queries. The cursor is positioned at the end of the `password_query` line. The bottom status bar shows the user `brylka` and the time `[06/09/21 11:23 PM]`.

Rys 3.6.15: Edycja pliku `/usr/local/etc/dovecot/dovecot-sql.conf.ext`

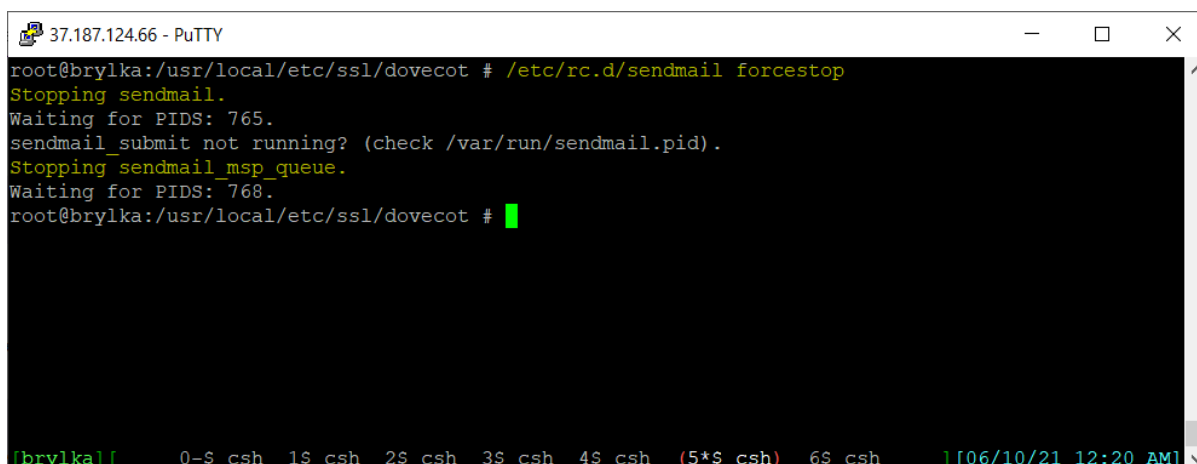


The screenshot shows a terminal window titled "37.187.124.66 - PuTTY" with the GNU nano 5.7 editor open to the file `/usr/local/etc/dovecot/dovecot.conf`. The editor displays the configuration file's content, including protocols, listen address, base directory, instance name, and login greeting. The cursor is positioned at the end of the `login_greeting` line. The bottom status bar shows the user `brylka` and the time `[06/09/21 11:28 PM]`.

Rys 3.6.16: Dodajemy ustawienia do pliku `/usr/local/etc/dovecot/dovecot.conf`

3.7. INSTALACJA I KONFIGURACJA POSTFIX (SMTP)

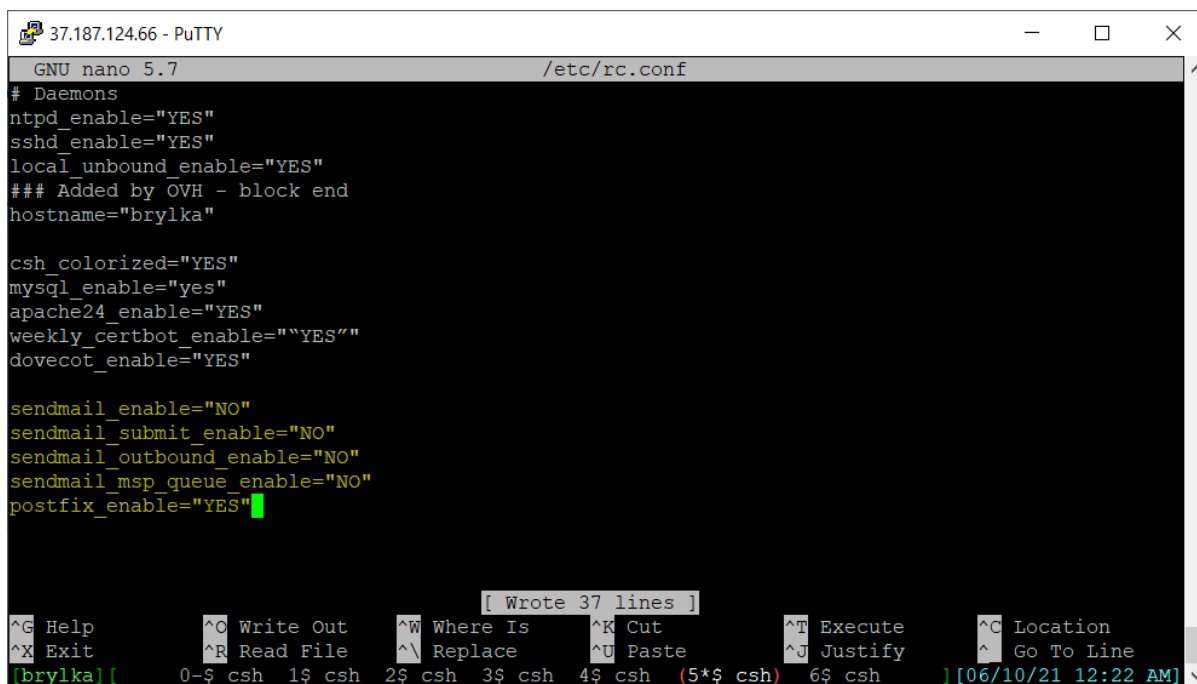
W pierwszej kolejności należy zatrzymać i wyłączyć sendmaila.



```
37.187.124.66 - PuTTY
root@brylka:/usr/local/etc/ssl/dovecot # /etc/rc.d/sendmail forcestop
Stopping sendmail.
Waiting for PIDS: 765.
sendmail_submit not running? (check /var/run/sendmail.pid).
Stopping sendmail_msp_queue.
Waiting for PIDS: 768.
root@brylka:/usr/local/etc/ssl/dovecot #
```

Rys 3.7.1: Zatrzymanie sendmaila.

Do pliku `/etc/rc.conf` dodajemy informacje o nieuruchamianiu sendmaila oraz o uruchamianiu postfixa przy starcie systemu.



```
37.187.124.66 - PuTTY
GNU nano 5.7 /etc/rc.conf
# Daemons
ntpd_enable="YES"
sshd_enable="YES"
local_unbound_enable="YES"
### Added by OVH - block end
hostname="brylka"

csh_colorized="YES"
mysql_enable="yes"
apache24_enable="YES"
weekly_certbot_enable="YES"
dovecot_enable="YES"

sendmail_enable="NO"
sendmail_submit_enable="NO"
sendmail_outbound_enable="NO"
sendmail_msp_queue_enable="NO"
postfix_enable="YES"
```

Rys 3.7.2: Dodanie do pliku `/etc/rc.conf` wpisów wyłączających sendmaila oraz wpisu włączającego postfixa.

Postfix został zainstalowany podczas instalacji pakietu Maia-Mailguard.

```
37.187.124.66 - PuTTY
===>>> pkg-message for postfix-3.6.0,1
On install:
To use postfix instead of sendmail:
  - clear sendmail queue and stop the sendmail daemons

Run the following commands to enable postfix during startup:
  - sysrc postfix_enable="YES"
  - sysrc sendmail_enable="NONE"

If postfix is *not* already activated in /usr/local/etc/mail/mailer.conf
  - mv /usr/local/etc/mail/mailer.conf /usr/local/etc/mail/mailer.conf.old
  - install -m 0644 /usr/local/share/postfix/mailer.conf.postfix /usr/local/etc/
mail/mailer.conf

Disable sendmail(8) specific tasks,
add the following lines to /etc/periodic.conf(.local):
  daily_clean_hoststat_enable="NO"
  daily_status_mail_rejects_enable="NO"
  daily_status_include_submit_mailq="NO"
  daily_submit_queuerun="NO"

If you are using SASL, you need to make sure that postfix has access to read
:
[brylka][ 0-$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6$ csh ][06/07/2
```

Rys 3.7.3: Zainstalowany Postfix.

Tworzymy certyfikaty SSL dla usługi SMTP oraz zabezpieczamy pliki przez odczytem przez niepowołanych użytkowników.

```
37.187.124.66 - PuTTY
root@brylka:/usr/local/etc/ssl/dovecot # cd /usr/local/etc/ssl/postfix
root@brylka:/usr/local/etc/ssl/postfix # openssl req -new -x509 -nodes -out smtpd.pem -keyout smt
pd.pem -days 3650
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'smtpd.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:dolnyslask
Locality Name (eg, city) []:Jelenia Gora
Organization Name (eg, company) [Internet Widgits Pty Ltd]:brylka.net
Organizational Unit Name (eg, section) []:brylka.net
Common Name (e.g. server FQDN or YOUR name) []:projekt.brylka.net
Email Address []:bartosz@bryniarski.pl
root@brylka:/usr/local/etc/ssl/postfix # chmod 640 /usr/local/etc/ssl/postfix/*
root@brylka:/usr/local/etc/ssl/postfix # chgrp -R postfix /usr/local/etc/ssl/postfix
root@brylka:/usr/local/etc/ssl/postfix #
[brylka][ 0-$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6$ csh ][06/10/21 12:30 AM]
```

Rys 3.7.4: Tworzenie certyfikatu oraz zabezpieczenie plików.

Do pliku /usr/local/etc/postfix/main.cf dodajemy następujące ustawienia:

```
soft_bounce = no

# SASL CONFIG
broken_sasl_auth_clients = yes
smtpd_delay_reject = yes
smtpd_helo_required = yes
smtpd_helo_restrictions =
    permit_mynetworks,
    permit_sasl_authenticated,
    reject_invalid_hostname,
    reject_unknown_hostname,
    reject_non_fqdn_hostname,
    reject_non_fqdn_helo_hostname,
    reject_invalid_helo_hostname,
    permit
smtpd_sender_restrictions =
    permit_mynetworks,
    permit_sasl_authenticated,
    reject_non_fqdn_sender,
    reject_unknown_sender_domain,
    reject_unlisted_sender,
    permit
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated
defer_unauth_destination
smtpd_recipient_restrictions =
    permit_mynetworks,
    permit_sasl_authenticated,
    reject_non_fqdn_hostname,
    reject_non_fqdn_sender,
    reject_non_fqdn_recipient,
    reject_unauth_destination,
    reject_unauth_pipelining,
    reject_invalid_hostname,
    reject_rbl_client bl.spamcop.net,
    reject_rbl_client sbl-xbl.spamhaus.org,
    reject_rbl_client zen.spamhaus.org,
    reject_rbl_client dnsbl.sorbs.net,
    reject_rbl_client rhsbl.sorbs.net,
    reject_rbl_client db.wpbl.info,
    reject_rbl_client cbl.abuseat.org,
    reject_rbl_client proxies.blackholes.wirehub.net,
    reject_rbl_client query.bondedsender.org
    permit
smtpd_sasl_auth_enable = yes
smtpd_sasl_authenticated_header = yes
smtpd_sasl_local_domain = $myhostname
smtpd_sasl_security_options = noanonymous
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth

# TLS CONFIG
smtp_use_tls = yes
smtpd_use_tls = yes
```

```
smtp_tls_note_starttls_offer = yes
smtpd_tls_key_file = /usr/local/etc/ssl/postfix/smtpd.pem
smtpd_tls_cert_file = /usr/local/etc/ssl/postfix/smtpd.pem
smtpd_tls_CAfile = /usr/local/etc/ssl/postfix/smtpd.pem
smtpd_tls_loglevel = 0
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
smtpd_tls_mandatory_protocols=!SSLv2,!SSLv3
tls_random_source = dev:/dev/urandom

#MySQL Configuration
virtual_alias_maps =
proxy:mysql:/usr/local/etc/postfix/mysql_virtual_alias_maps.cf
virtual_gid_maps = static:125
virtual_mailbox_base = /usr/local/virtual
virtual_mailbox_domains =
proxy:mysql:/usr/local/etc/postfix/mysql_virtual_domains_maps.cf
virtual_mailbox_limit = 51200000
virtual_mailbox_maps =
proxy:mysql:/usr/local/etc/postfix/mysql_virtual_mailbox_maps.cf
virtual_minimum_uid = 125
virtual_transport = dovecot
virtual_uid_maps = static:125

# Additional for quota support
virtual_mailbox_limit_maps =
proxy:mysql:/usr/local/etc/postfix/mysql_virtual_mailbox_limit_maps.cf
proxy_read_maps = $local_recipient_maps $mydestination $virtual_alias_maps
    $virtual_alias_domains $virtual_mailbox_maps $virtual_mailbox_domains
    $relay_recipient_maps $relay_domains $canonical_maps $sender_canonical_maps
    $recipient_canonical_maps $relocated_maps $transport_maps $mynetworks
    $virtual_mailbox_limit_maps

maximal_queue_lifetime = 1d
bounce_queue_lifetime = 1d

# Adjusted message size limit.
message_size_limit = 25600000

myhostname = projekt.brylka.net
mydomain = projekt.brylka.net
mydestination = localhost.$mydomain, localhost
relay_domains = proxy:mysql:/usr/local/etc/postfix/mysql_relay_domains_maps.cf
relay_recipient_maps =
proxy:mysql:/usr/local/etc/postfix/mysql_virtual_mailbox_maps.cf

dovecot_destination_recipient_limit = 1
```

```
37.187.124.66 - PuTTY
GNU nano 5.7 /usr/local/etc/postfix/main.cf
soft_bounce = no

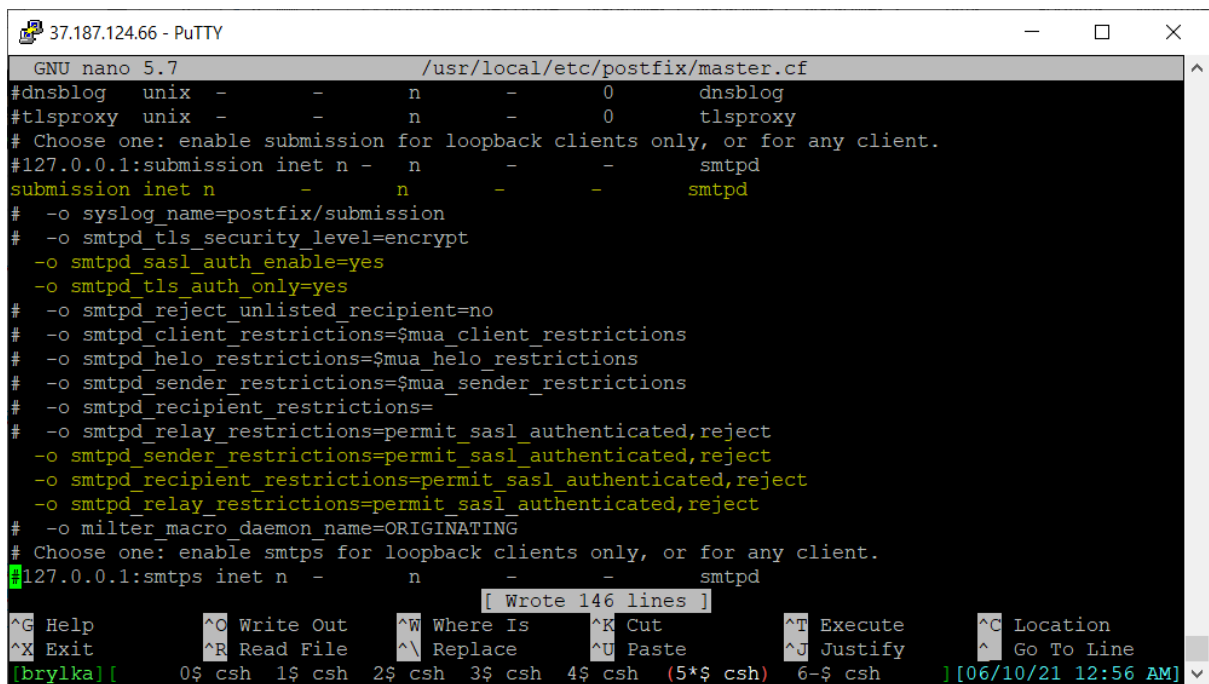
# SASL CONFIG
broken_sasl_auth_clients = yes
smtpd_delay_reject = yes
smtpd_helo_required = yes
smtpd_helo_restrictions =
  permit_mynetworks,
  permit_sasl_authenticated,
  reject_invalid_hostname,
  reject_unknown_hostname,
  reject_non_fqdn_hostname,
  reject_non_fqdn_helo_hostname,
  reject_invalid_helo_hostname,
  permit
smtpd_sender_restrictions =
  permit_mynetworks,
  permit_sasl_authenticated,
  reject_non_fqdn_sender,
  reject_unknown_sender_domain,
  reject_unlisted_sender,

^G Help      ^O Write Out  ^W Where Is   ^R Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
[brylka] 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/21 12:51 AM]
```

Rys 3.7.5: Fragment pliku /usr/local/etc/postfix/main.cf

Do pliku /usr/local/etc/postfix/master.cf dodajemy ustawienia:

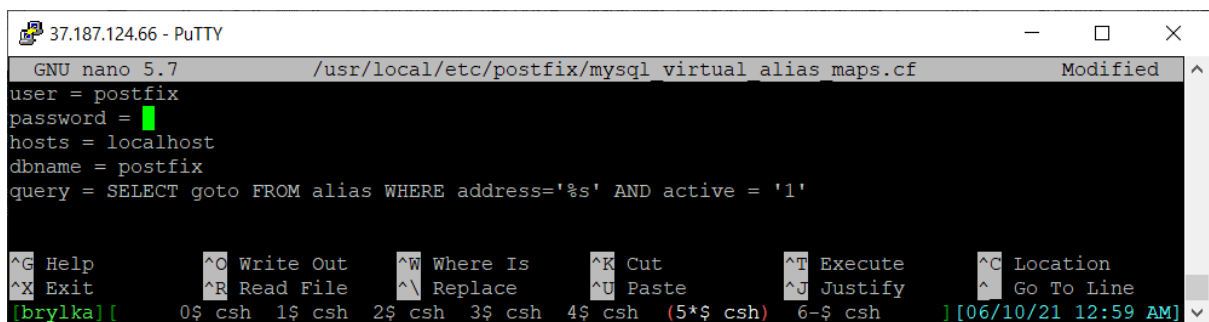
```
submission inet n      -      n      -      -      smtpd
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_tls_auth_only=yes
  -o smtpd_sender_restrictions=permit_sasl_authenticated,reject
  -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
smtps      inet n      -      n      -      -      smtpd
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_sender_restrictions=permit_sasl_authenticated,reject
  -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
dovecot    unix  -      n      n      -      -      pipe
  flags=DRhu user=vscan:vscan argv=/usr/local/libexec/dovecot/deliver -f ${sender}
  -d ${recipient}
```



```
GNU nano 5.7 /usr/local/etc/postfix/master.cf
#dnsblog unix - - n - 0 dnsblog
#tlsproxy unix - - n - 0 tlsproxy
# Choose one: enable submission for loopback clients only, or for any client.
#127.0.0.1:submission inet n - n - - smtpd
submission inet n - n - - smtpd
# -o syslog_name=postfix/submission
# -o smtpd_tls_security_level=encrypt
-o smtpd_sasl_auth_enable=yes
-o smtpd_tls_auth_only=yes
# -o smtpd_reject_unlisted_recipient=no
# -o smtpd_client_restrictions=$mua_client_restrictions
# -o smtpd_helo_restrictions=$mua_helo_restrictions
# -o smtpd_sender_restrictions=$mua_sender_restrictions
# -o smtpd_recipient_restrictions=
# -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
-o smtpd_sender_restrictions=permit_sasl_authenticated,reject
-o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
-o smtpd_relay_restrictions=permit_sasl_authenticated,reject
# -o milter_macro_daemon_name=ORIGINATING
# Choose one: enable smtps for loopback clients only, or for any client.
#127.0.0.1:smtps inet n - n - - smtpd
[ Wrote 146 lines ]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line
[brylka] 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/21 12:56 AM]
```

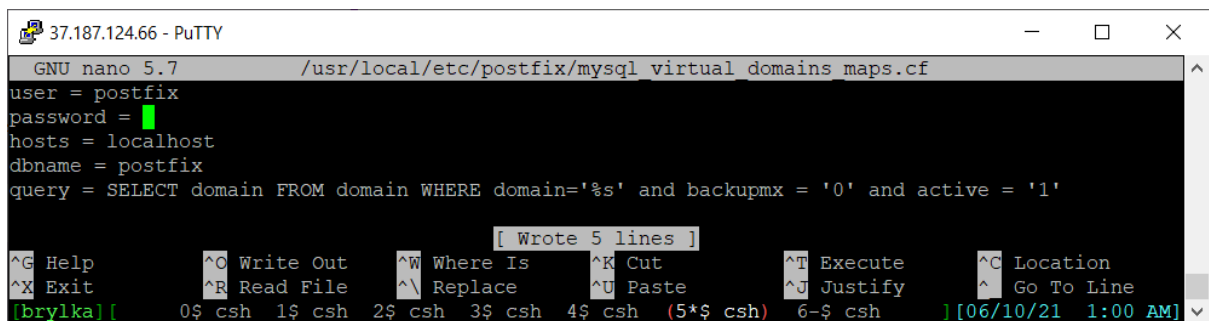
Rys 3.7.6: Fragment pliku /usr/local/etc/postfix/master.cf

Tworzymy pliki do obsługi połączeń z bazą danych i zapytań.



```
GNU nano 5.7 /usr/local/etc/postfix/mysql_virtual_alias_maps.cf Modified
user = postfix
password =
hosts = localhost
dbname = postfix
query = SELECT goto FROM alias WHERE address='%s' AND active = '1'
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line
[brylka] 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/21 12:59 AM]
```

Rys 3.7.7: Plik /usr/local/etc/postfix/mysql_virtual_alias_maps.cf



```
GNU nano 5.7 /usr/local/etc/postfix/mysql_virtual_domains_maps.cf
user = postfix
password =
hosts = localhost
dbname = postfix
query = SELECT domain FROM domain WHERE domain='%s' and backupmx = '0' and active = '1'
[ Wrote 5 lines ]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line
[brylka] 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/21 1:00 AM]
```

Rys 3.7.8: Plik /usr/local/etc/postfix/mysql_virtual_domains_maps.cf


```
37.187.124.66 - PuTTY
GNU nano 5.7 /usr/local/etc/postfix/mysql_virtual_mailbox_maps.cf
user = postfix
password = █
hosts = localhost
dbname = postfix
query = SELECT maildir FROM mailbox WHERE username='%s' AND active = '1'
[Wrote 5 lines]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
[brylka] 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/21 1:01 AM]
```

Rys 3.7.9: Plik /usr/local/etc/postfix/mysql_virtual_mailbox_maps.cf

```
37.187.124.66 - PuTTY
GNU nano 5.7 /usr/local/etc/postfix/mysql_virtual_mailbox_limit_maps.cf
user = postfix
password = █
hosts = localhost
dbname = postfix
query = SELECT quota FROM mailbox WHERE username='%s'
[Wrote 5 lines]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
[brylka] 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/21 1:03 AM]
```

Rys 3.7.10: Plik /usr/local/etc/postfix/mysql_virtual_mailbox_limit_maps.cf

```
37.187.124.66 - PuTTY
GNU nano 5.7 /usr/local/etc/postfix/mysql_relay_domains_maps.cf
user = postfix
password = █
hosts = localhost
dbname = postfix
query = SELECT domain FROM domain WHERE domain='%s' and backupmx = '1'
[Wrote 5 lines]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
[brylka] 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/21 1:04 AM]
```

Rys 3.7.11: Plik /usr/local/etc/postfix/mysql_relay_domains_maps.cf

Nadajemy odpowiednie prawa stworzonym plikom.

```
37.187.124.66 - PuTTY
root@brylka:/usr/local/etc/postfix # chmod 640 /usr/local/etc/postfix/mysql_*
root@brylka:/usr/local/etc/postfix # chgrp postfix /usr/local/etc/postfix/mysql_*
root@brylka:/usr/local/etc/postfix # ls -la | grep mysql_
-rw-r----- 1 root postfix 144 Jun 10 01:04 mysql_relay_domains_maps.cf
-rw-r----- 1 root postfix 140 Jun 10 00:58 mysql_virtual_alias_maps.cf
-rw-r----- 1 root postfix 161 Jun 10 01:00 mysql_virtual_domains_maps.cf
-rw-r----- 1 root postfix 127 Jun 10 01:03 mysql_virtual_mailbox_limit_maps.cf
-rw-r----- 1 root postfix 146 Jun 10 01:02 mysql_virtual_mailbox_maps.cf
root@brylka:/usr/local/etc/postfix # █
[brylka] 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/21 1:06 AM]
```

Rys 3.7.12: Zabezpieczenie przed przeglądaniem plików przez niepowołanych użytkowników.

```
37.187.124.66 - PuTTY
# >>>>>>>> show through to sendmail.
#
# See also RFC 2142, 'MAILBOX NAMES FOR COMMON SERVICES, ROLES
# AND FUNCTIONS', May 1997
# http://tools.ietf.org/html/rfc2142
#
# Pretty much everything else in this file points to "root", so
# you would do well in either reading root's mailbox or forwarding
# root's email from here.
#
# root: me@my.domain
root: brylka@projekt.brylka.net
#
# Basic system aliases -- these MUST be present
MAILER-DAEMON: postmaster
postmaster: root

root@brylka:/usr/local/etc/postfix # /usr/bin/newaliases
WARNING: local host name (brylka) is not qualified; see cf/README: WHO AM I?
/etc/mail/aliases: 30 aliases, longest 25 bytes, 326 bytes total
root@brylka:/usr/local/etc/postfix # █
[brylka] 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/21 1:10 AM]
```

Rys 3.7.13: Dodanie aliasu użytkownika root.

3.8. INSTALACJA I KONFIGURACJA POSTFIXADMIN

PostfixAdmin został zainstalowany podczas instalacji pakietu Maia-Mailguard.

```
37.187.124.66 - PuTTY
===>>> pkg-message for postfixadmin-3.2.4
On install:
If you are upgrading, you may need to update your existing database.
You can do so by browsing to [URL]/setup.php where [URL] is the
postfixadmin root.

To avoid checksum errors when uninstalling or upgrading postfixadmin,
do not edit config.inc.php. Instead, put your configuration settings
in config.local.php in the postfixadmin webroot. That file will be
included automatically by config.inc.php.

For detailed information, please see the complete installation steps
in /usr/local/share/doc/postfixadmin/INSTALL.TXT.

On upgrade:
For upgrade-related details, including configuration changes, see
/usr/local/share/doc/postfixadmin/CHANGELOG.TXT.

===>>> pkg-message for spamassassin-3.4.5
On install:
You should complete the following post-installation tasks:

:█
[brylka] 0-$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6$ csh ] [06/07/21 1:10 AM]
```

Rys 3.8.1: Zainstalowany PostfixAdmin.

Dodajemy ustawienia w pliku /usr/local/www/postfixadmin/config.local.php

```
<?php
$CONF['configured'] = true;
```

```
$CONF['setup_password'] = 'hasło';
$CONF['database_type'] = 'mysqli';
$CONF['database_host'] = 'localhost';
$CONF['database_user'] = 'postfix';
$CONF['database_password'] = 'hasło';
$CONF['database_name'] = 'postfix';
$CONF['admin_email'] = 'brylka@projekt.brylka.net';
$CONF['smtp_server'] = 'localhost';
$CONF['smtp_port'] = '25';
$CONF['encrypt'] = 'md5crypt';
$CONF['dovecotpw'] = "/usr/sbin/doveadm pw";
$CONF['page_size'] = '50';
$CONF['default_aliases'] = array (
    'abuse' => 'abuse@projekt.brylka.net',
    'hostmaster' => 'hostmaster@projekt.brylka.net',
    'postmaster' => 'postmaster@projekt.brylka.net',
    'webmaster' => 'webmaster@projekt.brylka.net'
);
$CONF['domain_path'] = 'NO';
$CONF['domain_in_mailbox'] = 'YES';
$CONF['aliases'] = '50';
$CONF['mailboxes'] = '50';
$CONF['maxquota'] = '102400';
$CONF['domain_quota_default'] = '1024000';
$CONF['quota'] = 'YES';
$CONF['domain_quota'] = 'YES';
$CONF['quota_multiplier'] = '1048576';
$CONF['transport'] = 'NO';
$CONF['vacation'] = 'YES';
$CONF['vacation_domain'] = 'autoreply.projekt.brylka.net';
$CONF['vacation_control'] = 'YES';
$CONF['vacation_control_admin'] = 'YES';
$CONF['alias_control'] = 'YES';
$CONF['alias_control_admin'] = 'YES';
$CONF['show_header_text'] = 'NO';
$CONF['header_text'] = ':: Postfix Admin ::';
$CONF['show_footer_text'] = 'YES';
$CONF['footer_text'] = 'Projekt brylka.net';
$CONF['footer_link'] = 'https://projekt.brylka.net/';
$CONF['welcome_text'] = <<<EOM
Hello,
```

Welcome to your new email account!

For questions or comments regarding your mail account, please feel free to send an email to hostmaster@projekt.brylka.net. Likewise, any other inquiries regarding the Company Name or our affiliates can be sent to the same address.

Also, don't forget to check your mail settings via Maia-Mailguard located at <https://projekt.brylka.net/maia/>. Simply log into your account using your email address and password. That's it! From Maia-Mailguard, you can adjust your spam, virus, malware, whitelists, blacklists, etc... This will put you in full control of your email so

you never miss anything important.

Thank you for using projekt.brylka.net and enjoy your new email account!

Regards,

projekt.brylka.net

hostmaster@projekt.brylka.net

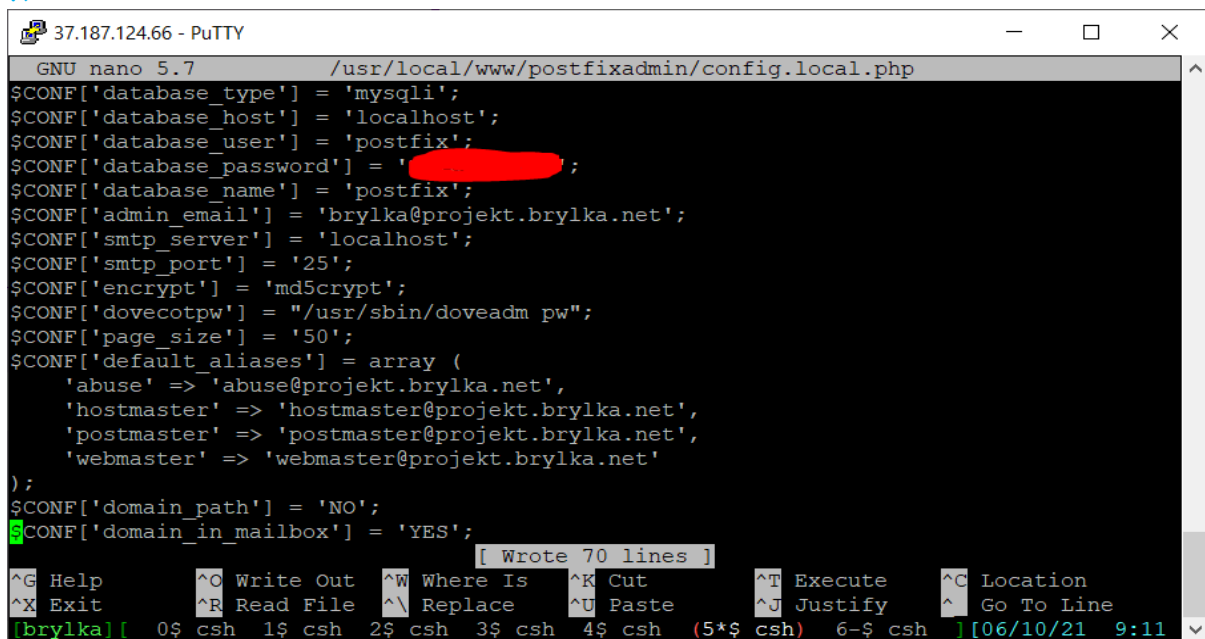
EOM;

```
$CONF['emailcheck_resolve_domain']='NO';
```

```
$CONF['mailbox_postdeletion_script'] = '/usr/local/bin/sudo -u vscan /root/bin/postfixa>
```

```
$CONF['domain_postdeletion_script'] = '/usr/local/bin/sudo -u vscan /root/bin/postfixad>
```

```
?>
```

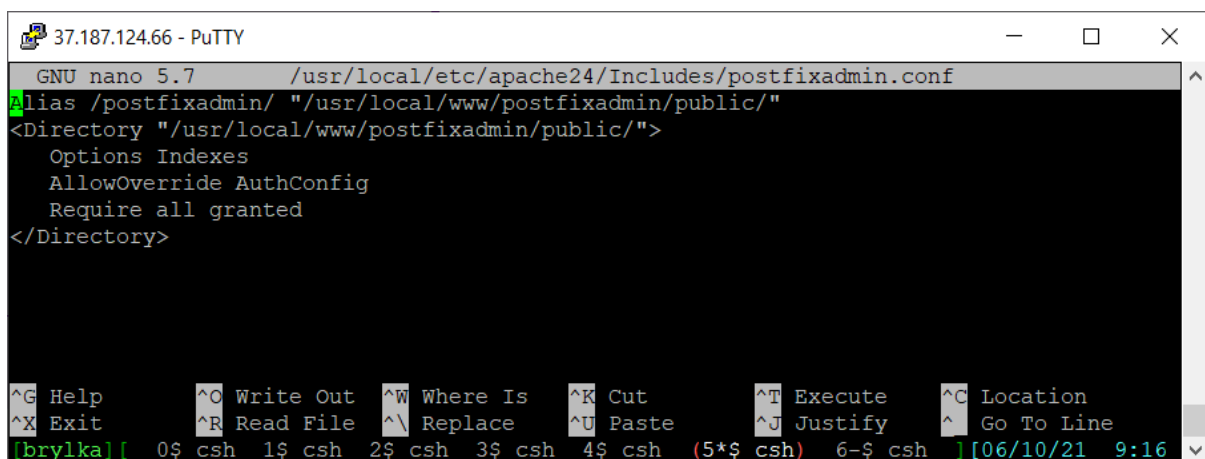


The screenshot shows a terminal window titled "37.187.124.66 - PuTTY" with a nano editor editing the file "/usr/local/www/postfixadmin/config.local.php". The configuration includes database settings, email server settings, and a list of aliases. A red highlight is visible over the database password field. The terminal shows the user is in the nano editor, and the prompt is [brylka] [0\$ csh 1\$ csh 2\$ csh 3\$ csh 4\$ csh (5*\$ csh) 6-\$ csh] [06/10/21 9:11].

```
GNU nano 5.7 /usr/local/www/postfixadmin/config.local.php
$CONF['database_type'] = 'mysqli';
$CONF['database_host'] = 'localhost';
$CONF['database_user'] = 'postfix';
$CONF['database_password'] = 'XXXXXXXXXX';
$CONF['database_name'] = 'postfix';
$CONF['admin_email'] = 'brylka@projekt.brylka.net';
$CONF['smtp_server'] = 'localhost';
$CONF['smtp_port'] = '25';
$CONF['encrypt'] = 'md5crypt';
$CONF['dovecotpw'] = "/usr/sbin/doveadm pw";
$CONF['page_size'] = '50';
$CONF['default_aliases'] = array (
  'abuse' => 'abuse@projekt.brylka.net',
  'hostmaster' => 'hostmaster@projekt.brylka.net',
  'postmaster' => 'postmaster@projekt.brylka.net',
  'webmaster' => 'webmaster@projekt.brylka.net'
);
$CONF['domain_path'] = 'NO';
$CONF['domain_in_mailbox'] = 'YES';
[ Wrote 70 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
[brylka] [ 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/21 9:11]
```

Rys 3.8.2: Edycja pliku /usr/local/www/postfixadmin/config.local.php

Dodajemy do pliku konfiguracyjnego apache wpis powodujący dodanie aplikacji PostfixAdmin.



The screenshot shows a terminal window titled "37.187.124.66 - PuTTY" with a nano editor editing the file "/usr/local/etc/apache24/Includes/postfixadmin.conf". The configuration includes an alias and a directory block. The terminal shows the user is in the nano editor, and the prompt is [brylka] [0\$ csh 1\$ csh 2\$ csh 3\$ csh 4\$ csh (5*\$ csh) 6-\$ csh] [06/10/21 9:16].

```
GNU nano 5.7 /usr/local/etc/apache24/Includes/postfixadmin.conf
Alias /postfixadmin/ "/usr/local/www/postfixadmin/public/"
<Directory "/usr/local/www/postfixadmin/public/">
  Options Indexes
  AllowOverride AuthConfig
  Require all granted
</Directory>
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
[brylka] [ 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/21 9:16]
```

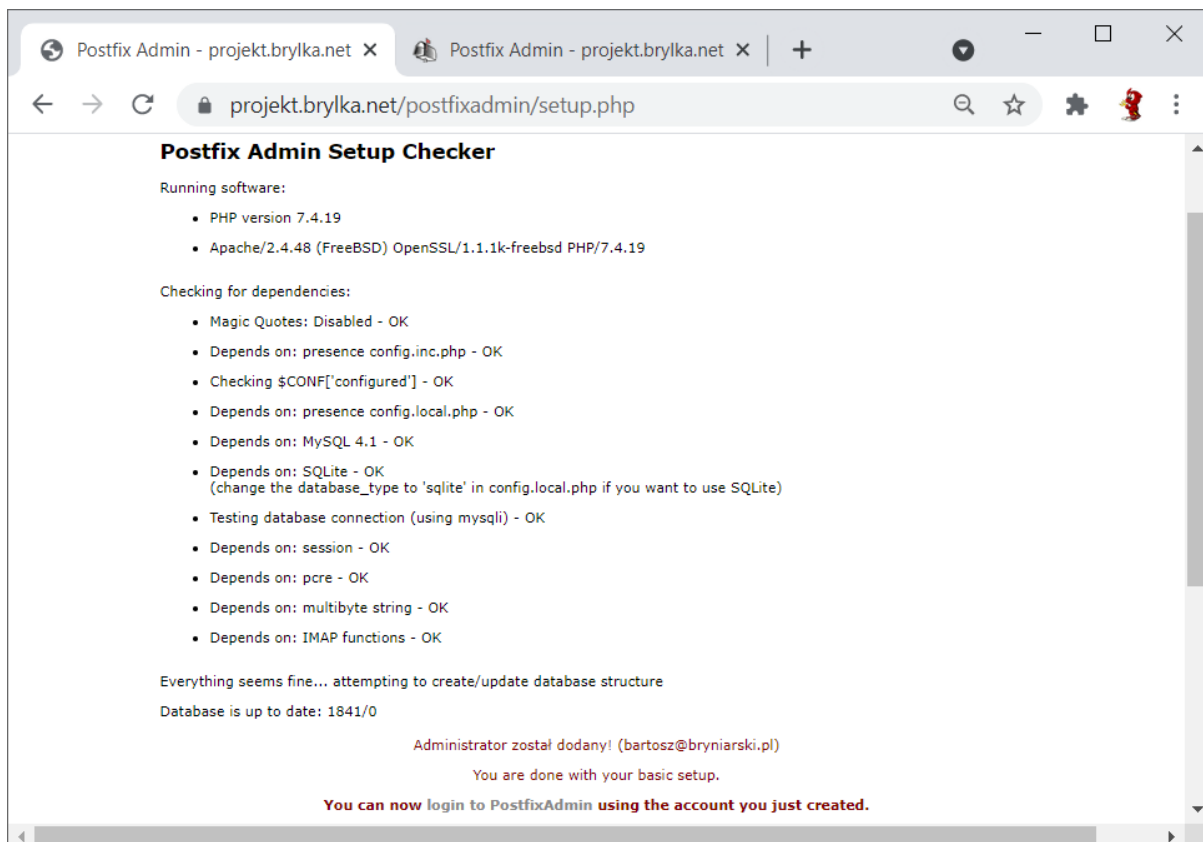
Rys 3.8.3: Dodanie pliku /usr/local/etc/apache24/Includes/postfixadmin.conf z konfiguracją apache.

```
37.187.124.66 - PuTTY
</Directory>

root@brylka:/usr/local/etc/apache24/Includes # apachectl configtest
Performing sanity check on apache24 configuration:
Syntax OK
root@brylka:/usr/local/etc/apache24/Includes # sercive apache 24 restart
sercive: Command not found.
root@brylka:/usr/local/etc/apache24/Includes # service apache 24 restart
apache does not exist in /etc/rc.d or the local startup
directories (/usr/local/etc/rc.d), or is not executable
root@brylka:/usr/local/etc/apache24/Includes # service apache24 restart
Performing sanity check on apache24 configuration:
Syntax OK
Stopping apache24.
Waiting for PIDS: 34637.
Performing sanity check on apache24 configuration:
Syntax OK
Starting apache24.
root@brylka:/usr/local/etc/apache24/Includes # █
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/21 9:19
```

Rys 3.8.4: Przeladowujemy apache.

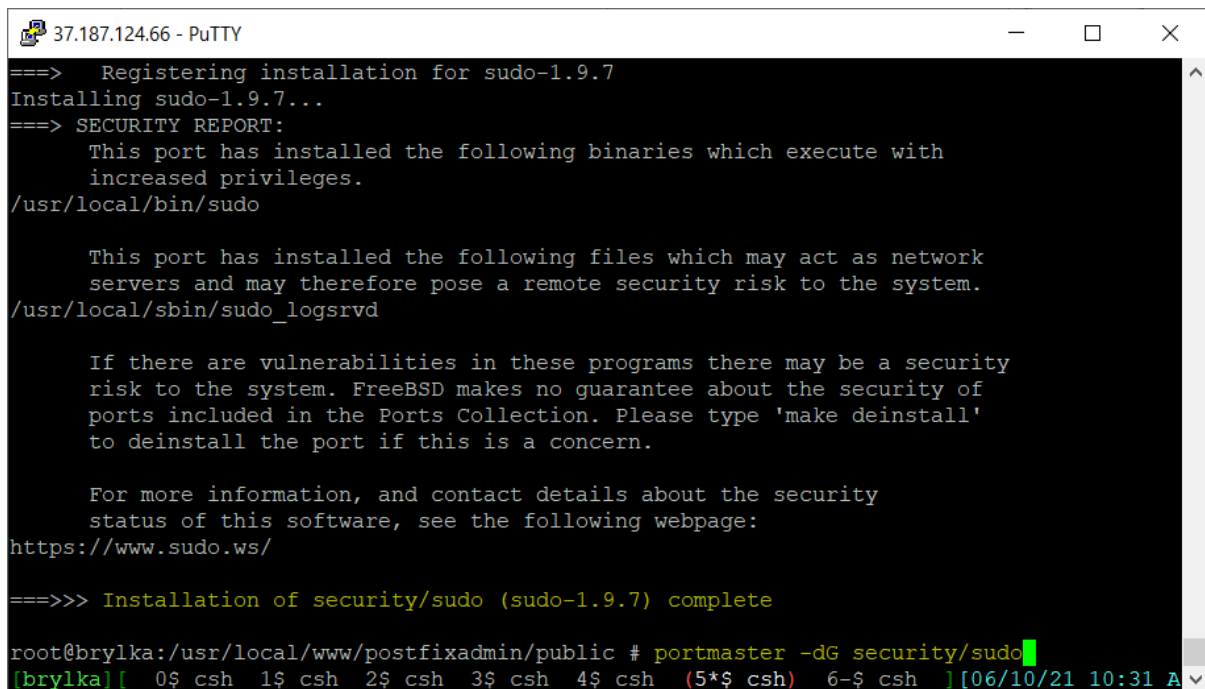
Przechodzimy na stronę <https://projekt.brylka.net/postfixadmin/setup.php> na której sprawdzana jest konfiguracja PostfixAdmina. Na stronie tej podajemy dane administratora, który będzie zarządzał systemem pocztowym.



Rys 3.8.5: Dodanie administratora systemu pocztowego PostfixAdmin.

Instalujemy dodatek, który umożliwił będzie usuwanie użytkowników z systemu pocztowego wraz z czyszczeniem katalogów. Wydajemy polecenie:

```
portmaster -dG security/sudo
```



```
37.187.124.66 - PuTTY
==> Registering installation for sudo-1.9.7
Installing sudo-1.9.7...
==> SECURITY REPORT:
    This port has installed the following binaries which execute with
    increased privileges.
/usr/local/bin/sudo

    This port has installed the following files which may act as network
    servers and may therefore pose a remote security risk to the system.
/usr/local/sbin/sudo_logsrvd

    If there are vulnerabilities in these programs there may be a security
    risk to the system. FreeBSD makes no guarantee about the security of
    ports included in the Ports Collection. Please type 'make deinstall'
    to deinstall the port if this is a concern.

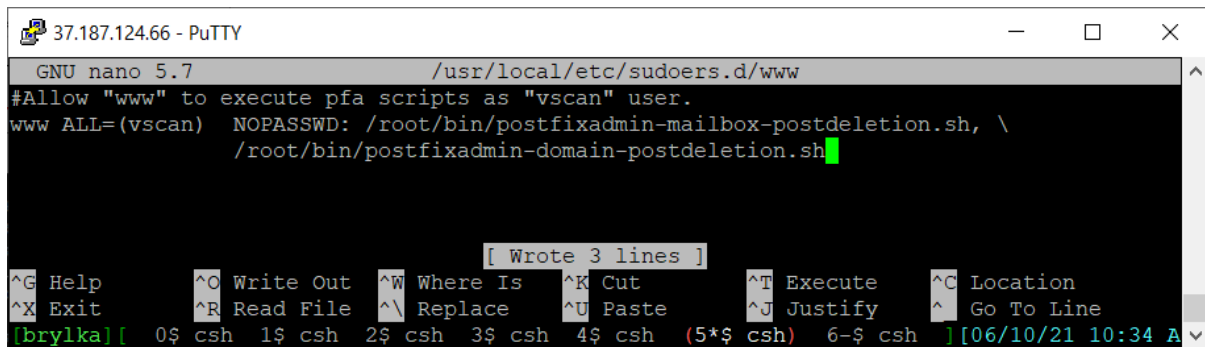
    For more information, and contact details about the security
    status of this software, see the following webpage:
https://www.sudo.ws/

==>>> Installation of security/sudo (sudo-1.9.7) complete

root@brylka:/usr/local/www/postfixadmin/public # portmaster -dG security/sudo
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/21 10:31 A
```

Rys 3.8.6: Dodanie pakietu security/sudo.

Tworzymy plik /usr/local/etc/sudoers.d/www z konfiguracją.



```
37.187.124.66 - PuTTY
GNU nano 5.7 /usr/local/etc/sudoers.d/www
#Allow "www" to execute pfa scripts as "vscan" user.
www ALL=(vscan) NOPASSWD: /root/bin/postfixadmin-mailbox-postdeletion.sh, \
    /root/bin/postfixadmin-domain-postdeletion.sh
[ Wrote 3 lines ]
^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/21 10:34 A
```

Rys 3.8.7: Dodanie pliku /usr/local/etc/sudoers.d/www.

Wykonujemy kilka poleceń tworzących katalogi oraz kopiujące pliki przykładowe.

```
37.187.124.66 - PuTTY
root@brylka:/var/mail/vhosts # mkdir /root/bin
root@brylka:/var/mail/vhosts # mkdir -p /var/mail/vhosts/deleted/{mailboxes,domains}
root@brylka:/var/mail/vhosts # chown -R vscan:vscan /var/mail/vhosts/default.sieve default.svbin deleted/
root@brylka:/var/mail/vhosts # chown -R vscan:vscan /var/mail/vhosts/deleted
root@brylka:/var/mail/vhosts # chmod -R 0700 /var/mail/vhosts/deleted
root@brylka:/var/mail/vhosts # cp /usr/local/share/postfixadmin/ADDITIONS/postfixadmin-*deletion.sh /root/bin/
root@brylka:/var/mail/vhosts # chmod +x /root/bin/postfixadmin*
root@brylka:/var/mail/vhosts #
```

[brylka] [0\$ csh 1\$ csh 2\$ csh 3\$ csh 4\$ csh (5*\$ csh) 6-\$ csh] [06/10/2024 10:00:00]

Rys 3.8.8: Polecenia tworzące katalogi i kopiujące przykładowe pliki konfiguracyjne.

Edytujemy dwa pliki wcześniej skopiowane i wstawiamy odpowiednie ustawienia.

```
37.187.124.66 - PuTTY
GNU nano 5.7 /root/bin/postfixadmin-domain-postdeletion.sh
# the script is actually run by the apache user (e.g. through PHP),
# then you could use "sudo" to grant apache the rights to run
# this script as the relevant user.
# Assume this script has been saved as
# /usr/local/bin/postfixadmin-domain-postdeletion.sh and has been
# made executable. Now, an example /etc/sudoers line:
# apache ALL=(courier) NOPASSWD: /usr/local/bin/postfixadmin-domain-postdeletion.sh
# The line states that the apache user may run the script as the
# user "courier" without providing a password.

# Change this to where you keep your virtual mail users' maildirs.
#basedir=/var/spool/maildirs
basedir=/var/mail/vhosts

# Change this to where you would like deleted maildirs to reside.
#trashbase=/var/spool/deleted-maildirs
trashbase=/var/mail/vhosts/deleted/domains

[ Wrote 64 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
[brylka] [ 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/2024 10:00:00]
```

Rys 3.8.9: Edytujemy plik /root/bin/postfixadmin-domain-postdeletion.sh

```
37.187.124.66 - PuTTY
GNU nano 5.7 /root/bin/postfixadmin-mailbox-postdeletion.sh
# this script as the relevant user.
# Assume this script has been saved as
# /usr/local/bin/postfixadmin-mailbox-postdeletion.sh and has been
# made executable. Now, an example /etc/sudoers line:
# apache ALL=(courier) NOPASSWD: /usr/local/bin/postfixadmin-mailbox-postdeleti
# The line states that the apache user may run the script as the
# user "courier" without providing a password.

# Change this to where you keep your virtual mail users' maildirs.
#basedir=/var/spool/maildirs
basedir=/var/mail/vhosts

# Change this to where you would like deleted maildirs to reside.
#trashbase=/var/spool/deleted-maildirs
trashbase=/var/mail/vhosts/deleted/mailboxes

if [ ! -e "$trashbase" ]; then
    [ Wrote 79 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/2
```

Rys 3.8.10: Edytujemy plik /root/bin/postfixadmin-mailbox-postdeletion.sh

Tworzymy użytkownika i grupę vacation.

```
37.187.124.66 - PuTTY
root@brylka:/var/mail/vhosts # pw groupadd vacation
root@brylka:/var/mail/vhosts # pw useradd vacation -c Virtual\ Vacation -d /nonexistent -g vacation -s /sbin/nologin
root@brylka:/var/mail/vhosts #
```

Rys 3.8.11: Dodanie grupy i użytkownika vacation.

Wykonujemy kilka komend tworzących katalogi oraz nadające prawa do tych katalogów.


```
37.187.124.66 - PuTTY
root@brylka:/var/mail/vhosts # mkdir /var/spool/vacation
root@brylka:/var/mail/vhosts # cp /usr/local/share/postfixadmin/VIRTUAL_VACATION/vacation.pl /var/spool/vacation/
root@brylka:/var/mail/vhosts # chown -R vacation:vacation /var/spool/vacation/
root@brylka:/var/mail/vhosts # chmod 700 /var/spool/vacation/
root@brylka:/var/mail/vhosts # chmod 750 /var/spool/vacation/vacation.pl
root@brylka:/var/mail/vhosts # touch /var/log/vacation.log /var/log/vacation-debug.log
root@brylka:/var/mail/vhosts # chown vacation:vacation /var/log/vacation*
root@brylka:/var/mail/vhosts # █

[brylka] [ 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/2
```

Rys 3.8.12: Tworzenie katalogów i nadawanie praw.

W pliku /var/spool/vacation/vacation.pl należy wstawić odpowiednie ustawienia.

```
our $db_type = 'mysql';
our $db_host = 'localhost';
our $db_username = 'postfix';
our $db_password = 'hasło';
our $db_name = 'postfix';
our $vacation_domain = 'autoreply.projekt.brylka.net';
our $smtp_ssl = '';
our $logfile = "/var/log/vacation.log"; # specify a file name here for example:
vacation.log
our $log_level = 0;
our $log_to_file = 1;
```

```
37.187.124.66 - PuTTY
GNU nano 5.7 /var/spool/vacation/vacation.pl
our $db_type = 'mysql';

# leave empty for connection via UNIX socket
our $db_host = 'localhost';

# connection details
our $db_username = 'postfix';
our $db_password = '██████████';
our $db_name = 'postfix';

our $vacation_domain = 'autoreply.projekt.brylka.net';

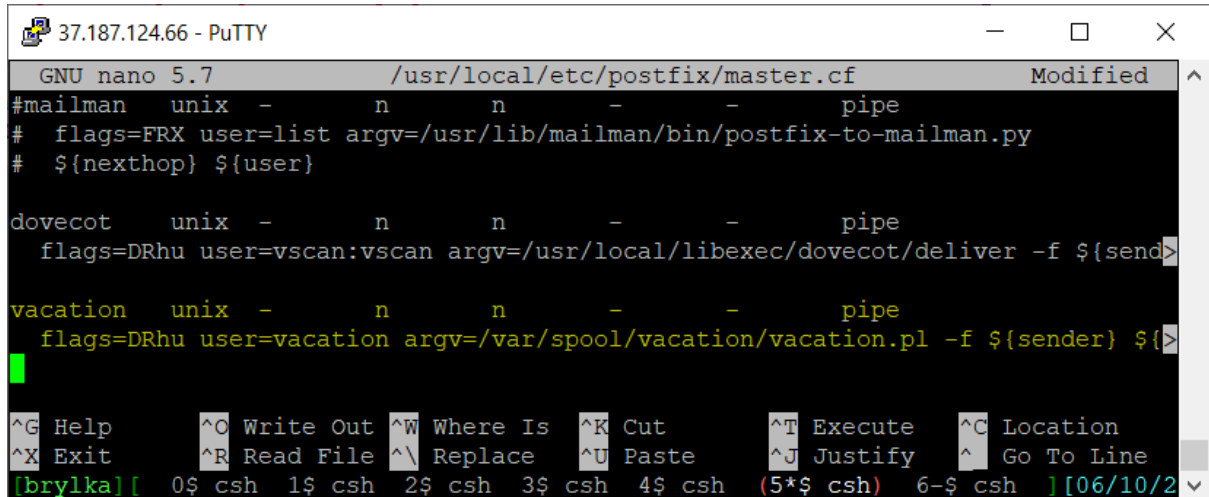
# smtp server used to send vacation e-mails
our $smtp_server = 'localhost';
# port to connect to █ defaults to 25 for non-SSL, 465 for 'ssl', 587 for 'start

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
[brylka] [ 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/2
```

Rys 3.8.13: Edycja pliku /var/spool/vacation/vacation.pl.

Do pliku `/usr/local/etc/postfix/master.cf` dodajemy następujące ustawienia:

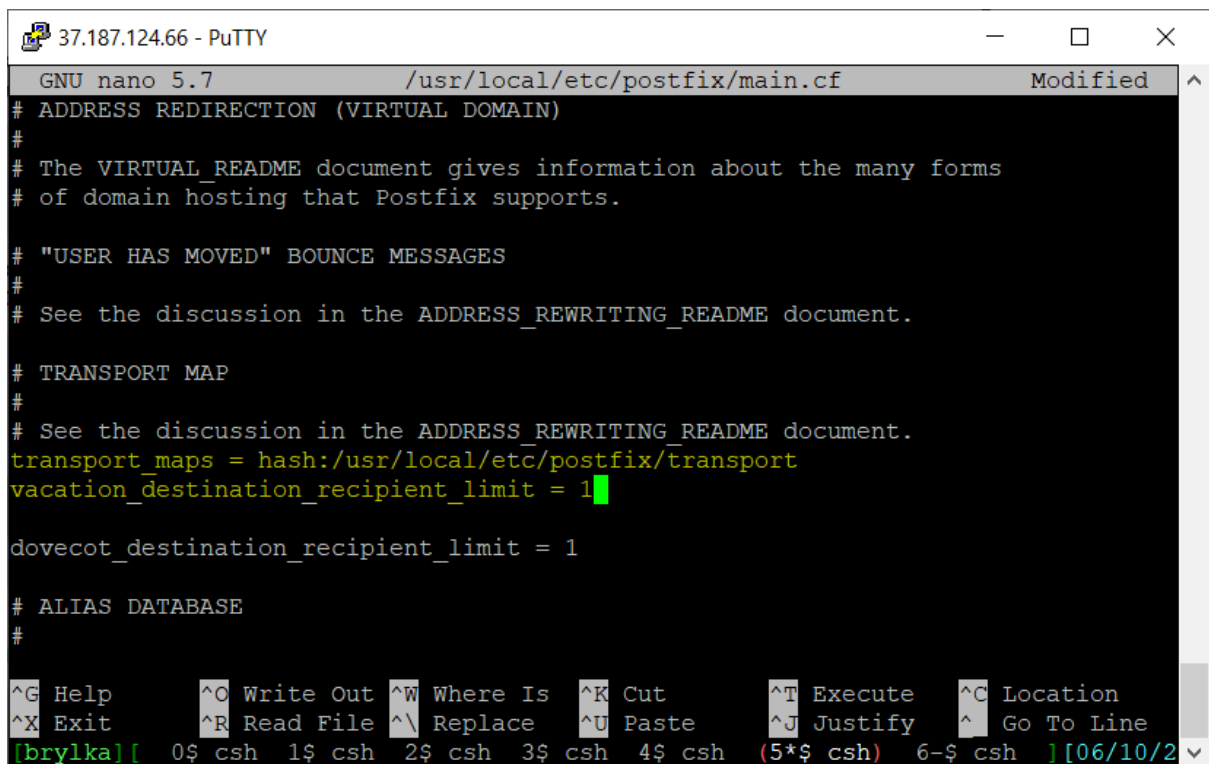
```
vacation unix - n n - - pipe
    flags=DRhu user=vacation argv=/var/spool/vacation/vacation.pl -f ${sender}
    ${recipient}
```



```
GNU nano 5.7 /usr/local/etc/postfix/master.cf Modified
#mailman unix - n n - - pipe
# flags=FRX user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
# ${nexthop} ${user}

dovecot unix - n n - - pipe
    flags=DRhu user=vscan:vscan argv=/usr/local/libexec/dovecot/deliver -f ${send>
vacation unix - n n - - pipe
    flags=DRhu user=vacation argv=/var/spool/vacation/vacation.pl -f ${sender} ${>
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line
[brylka] [ 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/24
```

Rys 3.8.14: Dodanie ustawień do pliku `/usr/local/etc/postfix/master.cf`.



```
GNU nano 5.7 /usr/local/etc/postfix/main.cf Modified
# ADDRESS REDIRECTION (VIRTUAL DOMAIN)
#
# The VIRTUAL_README document gives information about the many forms
# of domain hosting that Postfix supports.
#
# "USER HAS MOVED" BOUNCE MESSAGES
#
# See the discussion in the ADDRESS_REWRITING_README document.
#
# TRANSPORT MAP
#
# See the discussion in the ADDRESS_REWRITING_README document.
transport_maps = hash:/usr/local/etc/postfix/transport
vacation_destination_recipient_limit = 1
dovecot_destination_recipient_limit = 1
# ALIAS DATABASE
#
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line
[brylka] [ 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/24
```

Rys 3.8.15: Do pliku `/usr/local/etc/postfix/main.cf` dodajemy ustawienia.

```
37.187.124.66 - PuTTY
root@brylka:/var/mail/vhosts # echo "autoreply.projekt.brylka.net vacation:" >>
/usr/local/etc/postfix/transport
root@brylka:/var/mail/vhosts # postmap /usr/local/etc/postfix/transport
root@brylka:/var/mail/vhosts # █

[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6-$ csh ] [06/10/2
```

Rys 3.8.16: Wykonujemy dwa polecenia. Pierwsze tworzy plik /usr/local/etc/postfix/transport, drugie aktualizuje tabelę Postfixa.

3.9. KONFIGURACJA SPAMASSASSIN'A I CLAM ANTI-VIRUS'A

SpamAssassin oraz Clam Anti-Virus zostały zainstalowane podczas instalacji Maia-Mailguard.

```
37.187.124.66 - PuTTY
===>>> pkg-message for spamassassin-3.4.5
On install:
You should complete the following post-installation tasks:

1) Read /usr/local/share/doc/spamassassin/INSTALL
and /usr/local/share/doc/spamassassin/UPGRADE
BEFORE enabling SpamAssassin for important changes

2) Edit the configuration in /usr/local/etc/mail/spamassassin,
in particular /usr/local/etc/mail/spamassassin/init.pre
You may get lots of annoying (but harmless) error messages
if you skip this step.

3) To run spamd, add the following to /etc/rc.conf:
spamd_enable="YES"

4) If this is a new installation, you should run sa-update
and sa-compile. If this isn't a new installation, you
should probably run those commands on a regular basis
anyway.

5) Install mail/spamass-rules if you want some third-party
:
█
[brylka][ 0-$ csh 1$ csh 2$ csh 3$ csh 4$ csh (5*$ csh) 6$ csh ] [06/07/2
```

Rys 3.9.1. Zainstalowany SpamAssassin

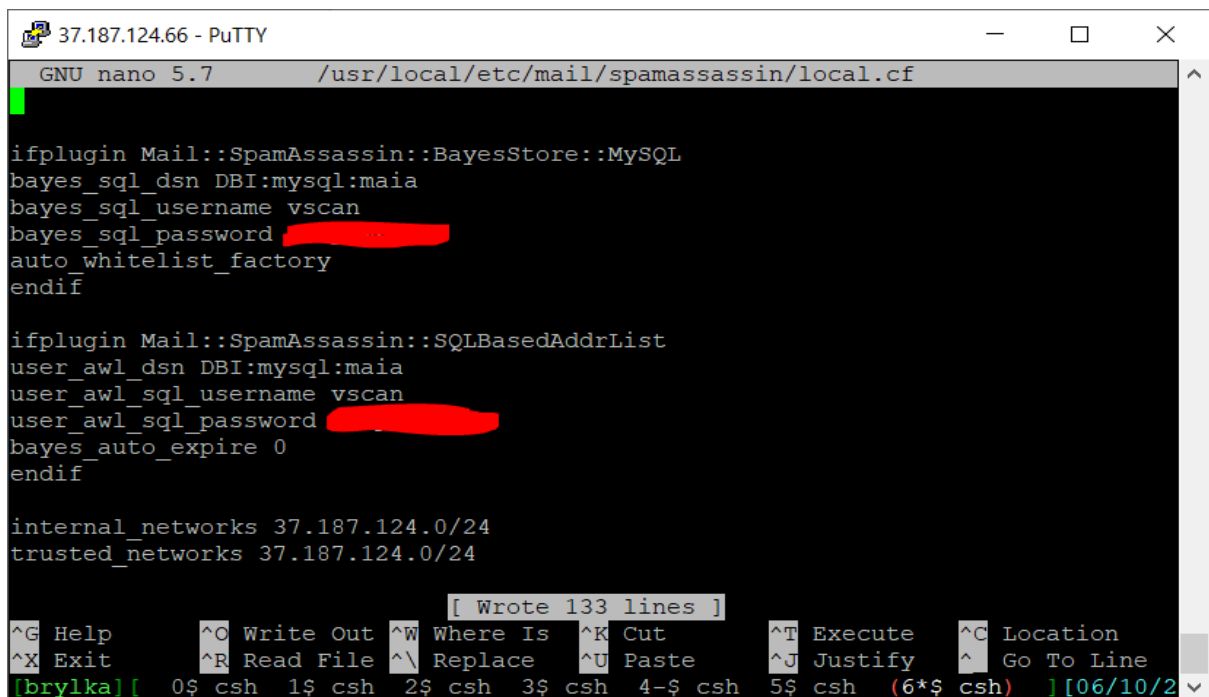
Konfiguracja SpamAssassina sprowadza się do edycji pliku /usr/local/etc/mail/spamassassin/local.cf, dodajemy w nim następujące ustawienia odpowiedzialne za łączność z bazą danych:

```
ifplugin Mail::SpamAssassin::BayesStore::MySQL
bayes_sql_dsn DBI:mysql:maia
bayes_sql_username vscan
```

```
bayes_sql_password hasło
auto_whitelist_factory
endif

ifplugin Mail::SpamAssassin::SQLBasedAddrList
user_awl_dsn DBI:mysql:maia
user_awl_sql_username vscan
user_awl_sql_password hasło
bayes_auto_expire 0
endif

internal_networks 37.187.124.0/24
trusted_networks 37.187.124.0/24
```



```
37.187.124.66 - PuTTY
GNU nano 5.7 /usr/local/etc/mail/spamassassin/local.cf

ifplugin Mail::SpamAssassin::BayesStore::MySQL
bayes_sql_dsn DBI:mysql:maia
bayes_sql_username vscan
bayes_sql_password ██████████
auto_whitelist_factory
endif

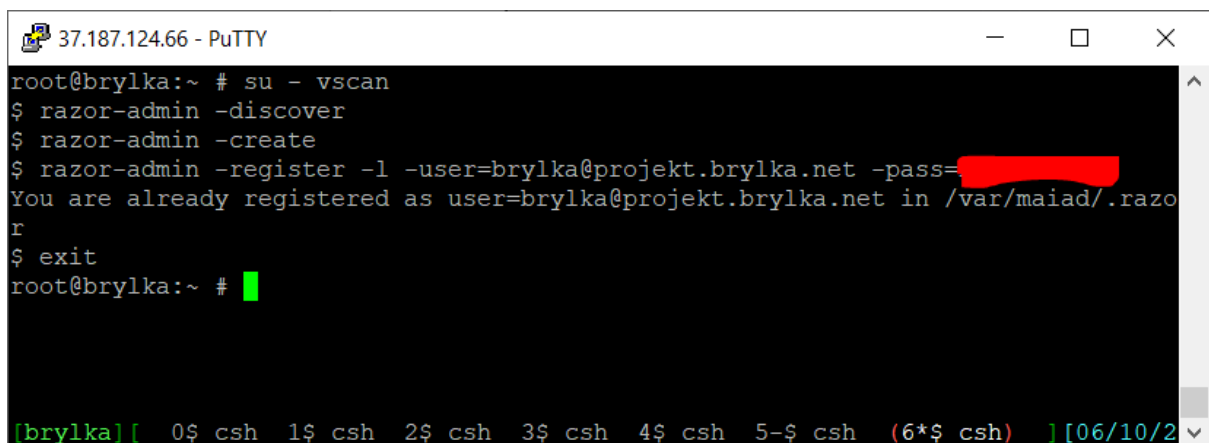
ifplugin Mail::SpamAssassin::SQLBasedAddrList
user_awl_dsn DBI:mysql:maia
user_awl_sql_username vscan
user_awl_sql_password ██████████
bayes_auto_expire 0
endif

internal_networks 37.187.124.0/24
trusted_networks 37.187.124.0/24

[Wrote 133 lines]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4-$ csh 5$ csh (6*$ csh) ][06/10/2
```

Rys 3.9.2: Konfiguracja SpamAssassina.

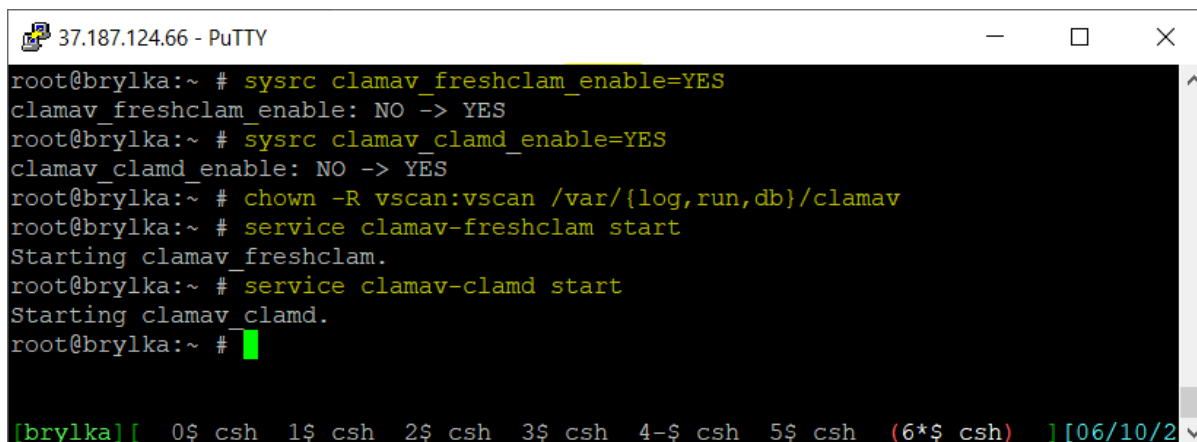
Następnie wykonujemy kilka komend Razor'a, które odpowiadają za konfigurację raportowania spamu.



```
37.187.124.66 - PuTTY
root@brylka:~ # su - vscan
$ razor-admin -discover
$ razor-admin -create
$ razor-admin -register -l -user=brylka@projekt.brylka.net -pass=██████████
You are already registered as user=brylka@projekt.brylka.net in /var/maiad/.razor
$ exit
root@brylka:~ #
```

Rys 3.9.3: Komendy Razor'a.

Konfiguracja Clam Anti-Virus'a sprowadza się do dodania do uruchamianych przy starcie usług, zmiany uprawnień do katalogów, oraz uruchomienie demonów.



```
37.187.124.66 - PuTTY
root@brylka:~ # sysrc clamav_freshclam_enable=YES
clamav_freshclam_enable: NO -> YES
root@brylka:~ # sysrc clamav_clamd_enable=YES
clamav_clamd_enable: NO -> YES
root@brylka:~ # chown -R vscan:vscan /var/{log,run,db}/clamav
root@brylka:~ # service clamav-freshclam start
Starting clamav_freshclam.
root@brylka:~ # service clamav-clamd start
Starting clamav clamd.
root@brylka:~ #
```

Rys 3.9.4: Konfiguracja i uruchomienie Clam Anti-Virus'a.

3.10. INSTALACJA I KONFIGURACJA MAIA-MAILGUARD

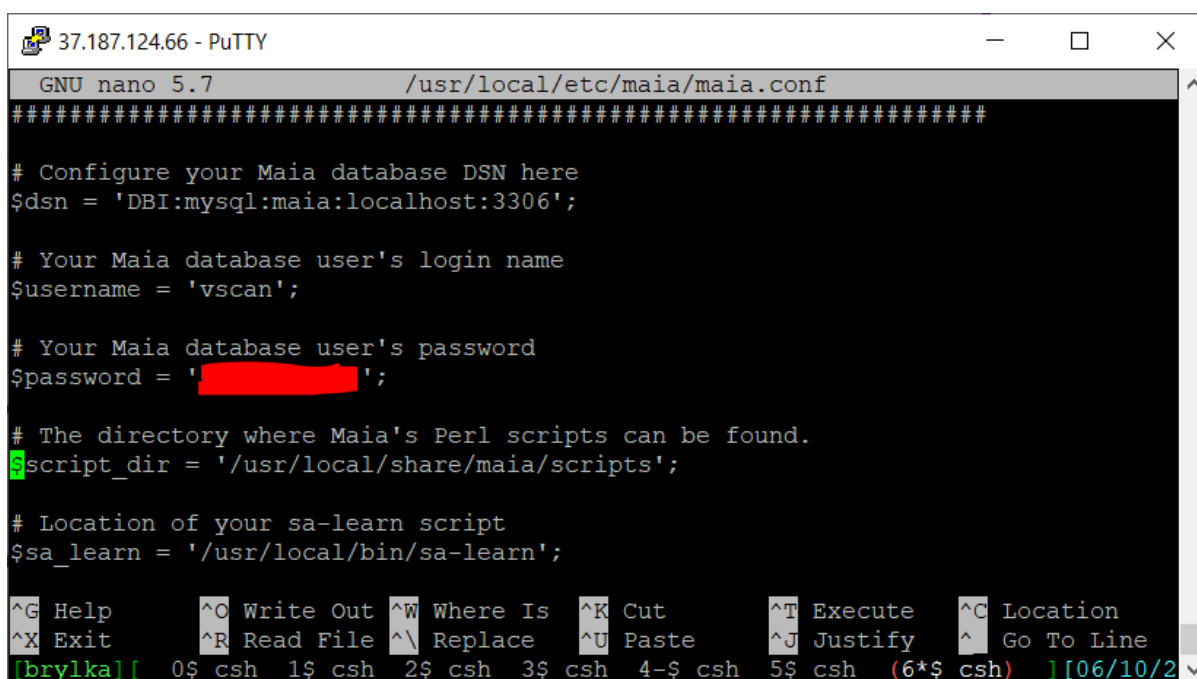
Maia-Mailguard został zainstalowany jeszcze przez konfiguracją Dovecota. Aby pakiet działał poprawnie należy w pliku php.ini dodać następujące ustawienie:

```
include_path = " ./usr/local/share/pear"
```

i zresetować apache. Następnie wykonujemy polecenia:

```
cd /usr/local/share/maia/scripts/
sed -i.bak 's|/usr/bin/perl.*$|/usr/bin/env perl|' *.pl
rm -f *.bak
```

Edytujemy plik /usr/local/etc/maia/maia.conf wprowadzając ustawienia bazy danych.



```
37.187.124.66 - PuTTY
GNU nano 5.7 /usr/local/etc/maia/maia.conf
#####
# Configure your Maia database DSN here
$dsn = 'DBI:mysql:maia:localhost:3306';

# Your Maia database user's login name
$username = 'vscan';

# Your Maia database user's password
$password = 'XXXXXXXXXX';

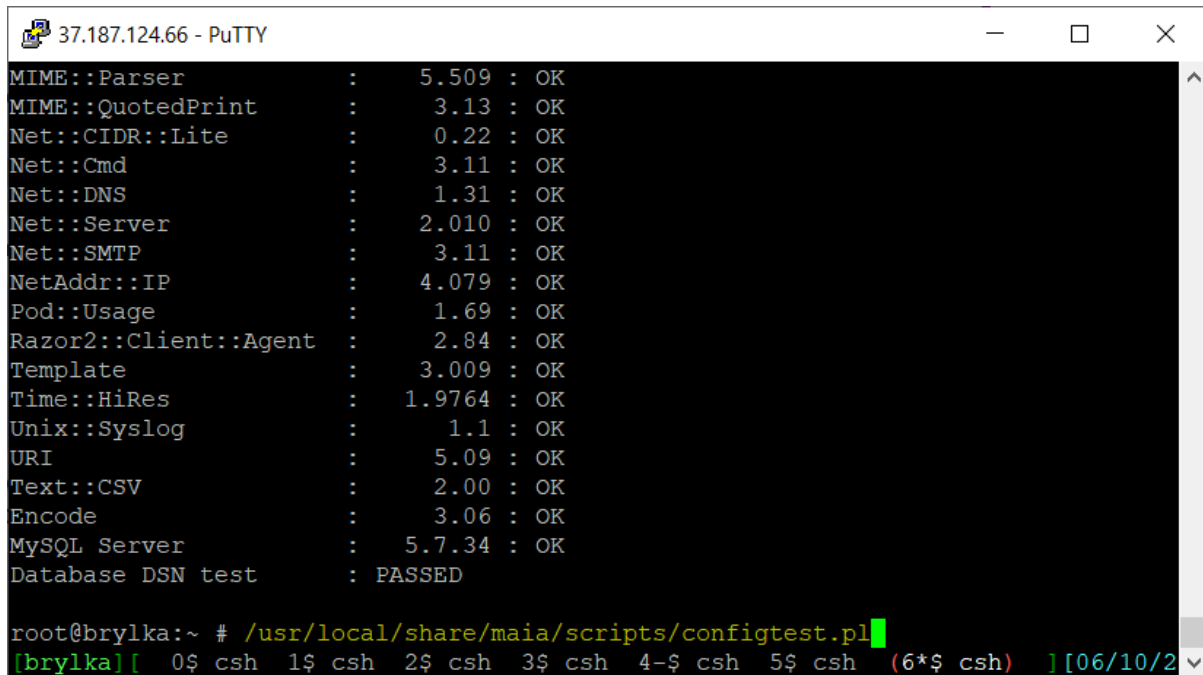
# The directory where Maia's Perl scripts can be found.
$script_dir = '/usr/local/share/maia/scripts';

# Location of your sa-learn script
$sa_learn = '/usr/local/bin/sa-learn';

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4-$ csh 5$ csh (6*$ csh) ][06/10/2
```

Rys 3.10.1: Ustawienia Maia-Mailguard.

Uruchamiamy skrypt `/usr/local/share/maia/scripts/configtest.pl`, który testuje konfigurację i wymagania.



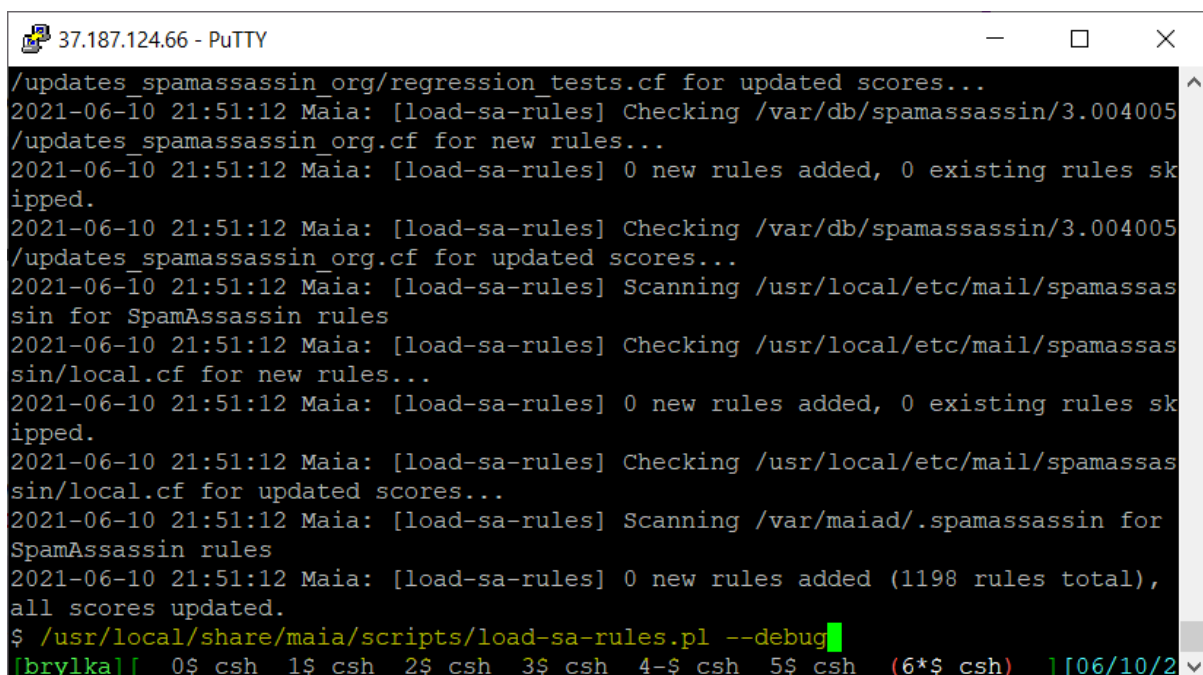
```
37.187.124.66 - PuTTY
MIME::Parser : 5.509 : OK
MIME::QuotedPrint : 3.13 : OK
Net::CIDR::Lite : 0.22 : OK
Net::Cmd : 3.11 : OK
Net::DNS : 1.31 : OK
Net::Server : 2.010 : OK
Net::SMTP : 3.11 : OK
NetAddr::IP : 4.079 : OK
Pod::Usage : 1.69 : OK
Razor2::Client::Agent : 2.84 : OK
Template : 3.009 : OK
Time::HiRes : 1.9764 : OK
Unix::Syslog : 1.1 : OK
URI : 5.09 : OK
Text::CSV : 2.00 : OK
Encode : 3.06 : OK
MySQL Server : 5.7.34 : OK
Database DSN test : PASSED

root@brylka:~ # /usr/local/share/maia/scripts/configtest.pl
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4-$ csh 5$ csh (6*$ csh) ] [06/10/2
```

Rys 3.10.2: Sprawdzenie wymagań Maia-Mailguard.

Wykonujemy aktualizację reguł SpamAssassina:

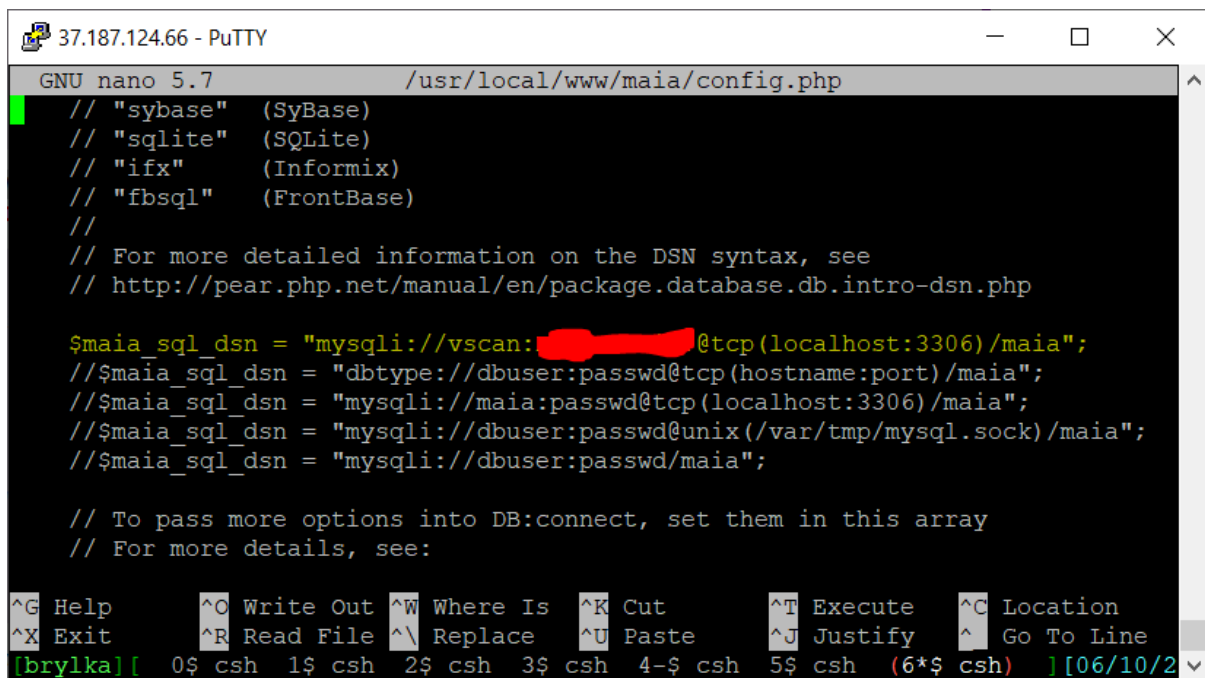
```
# sa-update
# su - vscan
$ /usr/local/share/maia/scripts/load-sa-rules.pl --debug
$ exit
```



```
37.187.124.66 - PuTTY
/updates_spamassassin_org/regression_tests.cf for updated scores...
2021-06-10 21:51:12 Maia: [load-sa-rules] Checking /var/db/spamassassin/3.004005
/updates_spamassassin_org.cf for new rules...
2021-06-10 21:51:12 Maia: [load-sa-rules] 0 new rules added, 0 existing rules sk
ipped.
2021-06-10 21:51:12 Maia: [load-sa-rules] Checking /var/db/spamassassin/3.004005
/updates_spamassassin_org.cf for updated scores...
2021-06-10 21:51:12 Maia: [load-sa-rules] Scanning /usr/local/etc/mail/spamassas
sin for SpamAssassin rules
2021-06-10 21:51:12 Maia: [load-sa-rules] Checking /usr/local/etc/mail/spamassas
sin/local.cf for new rules...
2021-06-10 21:51:12 Maia: [load-sa-rules] 0 new rules added, 0 existing rules sk
ipped.
2021-06-10 21:51:12 Maia: [load-sa-rules] Checking /usr/local/etc/mail/spamassas
sin/local.cf for updated scores...
2021-06-10 21:51:12 Maia: [load-sa-rules] Scanning /var/maid/.spamassassin for
SpamAssassin rules
2021-06-10 21:51:12 Maia: [load-sa-rules] 0 new rules added (1198 rules total),
all scores updated.
$ /usr/local/share/maia/scripts/load-sa-rules.pl --debug
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4-$ csh 5$ csh (6*$ csh) ] [06/10/2
```

Rys 3.11.3: Aktualizacja reguł SpamAssassina.

Edytujemy ustawienia Maia-Mailguard – aplikacji internetowej, wstawiając przede wszystkim ustawienia bazy danych.



```
GNU nano 5.7 /usr/local/www/maia/config.php
// "sybase" (SyBase)
// "sqlite" (SQLite)
// "ifx" (Informix)
// "fbsql" (FrontBase)
//
// For more detailed information on the DSN syntax, see
// http://pear.php.net/manual/en/package.database.db.intro-dsn.php

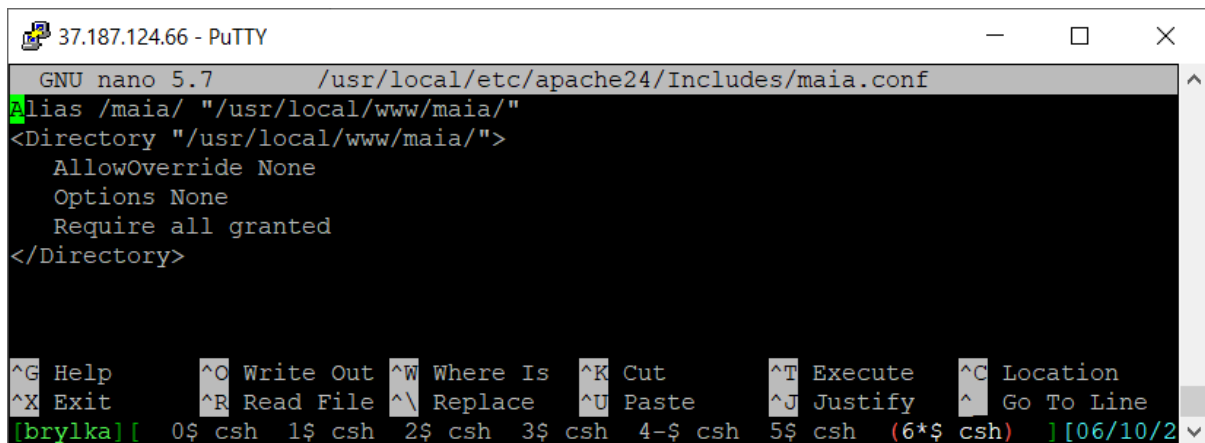
$maia_sql_dsn = "mysql://vscan:[REDACTED]@tcp(localhost:3306)/maia";
//$maia_sql_dsn = "dbtype://dbuser:passwd@tcp(hostname:port)/maia";
//$maia_sql_dsn = "mysql://maia:passwd@tcp(localhost:3306)/maia";
//$maia_sql_dsn = "mysql://dbuser:passwd@unix(/var/tmp/mysql.sock)/maia";
//$maia_sql_dsn = "mysql://dbuser:passwd/maia";

// To pass more options into DB:connect, set them in this array
// For more details, see:

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4-$ csh 5$ csh (6*$ csh) ] [06/10/2
```

Rys 3.11.4: Ustawienia aplikacji Maia-Mailguard.

Dodajemy plik /usr/local/etc/apache24/Includes/maia.conf z ustawieniami do aplikacji internetowej dla Maia-Mailguard. Resetujemy apache.

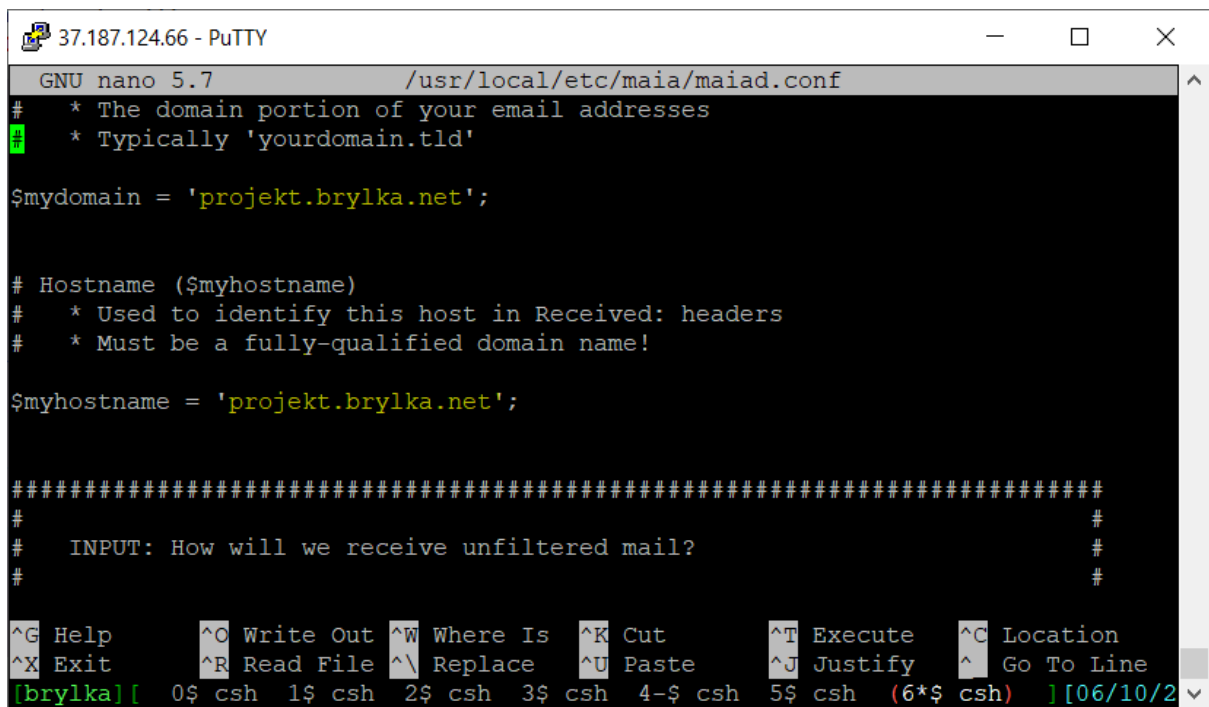


```
GNU nano 5.7 /usr/local/etc/apache24/Includes/maia.conf
Alias /maia/ "/usr/local/www/maia/"
<Directory "/usr/local/www/maia/">
  AllowOverride None
  Options None
  Require all granted
</Directory>

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4-$ csh 5$ csh (6*$ csh) ] [06/10/2
```

Rys 3.11.5: Konfiguracja Maia-Mailguard w apache.

Edytujemy plik /usr/local/etc/maia/maiad.conf wprowadzając między innymi nazwę hosta.



```
37.187.124.66 - PuTTY
GNU nano 5.7 /usr/local/etc/maia/maiad.conf
# * The domain portion of your email addresses
# * Typically 'yourdomain.tld'

$mydomain = 'projekt.brylka.net';

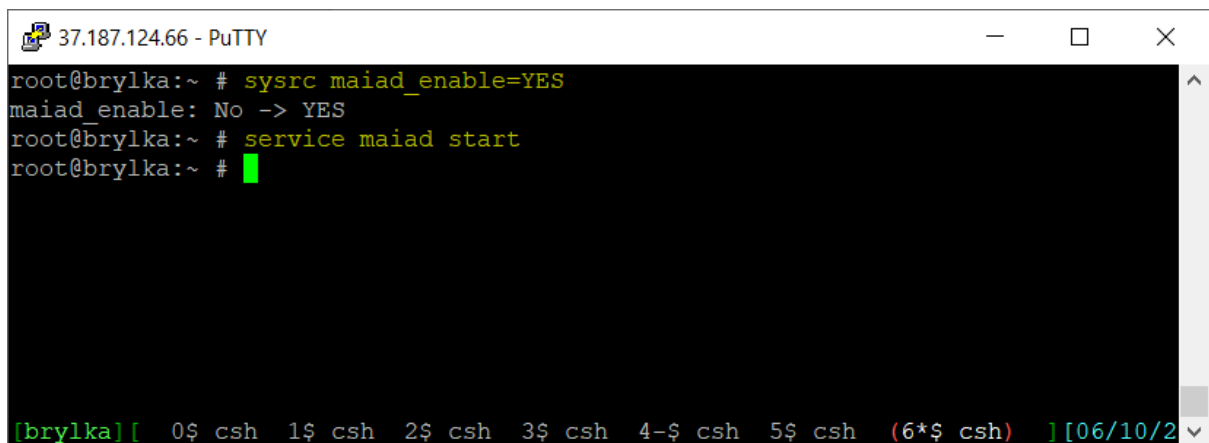
# Hostname ($myhostname)
# * Used to identify this host in Received: headers
# * Must be a fully-qualified domain name!

$myhostname = 'projekt.brylka.net';

#####
#
# INPUT: How will we receive unfiltered mail?
#
#####
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4-$ csh 5$ csh (6*$ csh) ][06/10/2
```

Rys 3.11.6: Edytujemy plik /usr/local/etc/maia/maiad.conf.

Dodajemy Maia-Mailguard do usług uruchamianych przy starcie systemu, uruchamiamy demona.



```
37.187.124.66 - PuTTY
root@brylka:~ # sysrc maiaad_enable=YES
maiaad_enable: No -> YES
root@brylka:~ # service maiaad start
root@brylka:~ #
```

Rys 3.11.7: Dodanie Maia-Mailguard do startu systemu, uruchomienie demona.

Następnie do konfiguracji postfixa dodajemy kilka ustawień. Edytujemy plik /usr/local/etc/postfix/main.cf i dodajemy wpis:

```
# Maia-Mailguard
#
content_filter=smtp-amavis:[127.0.0.1]:10024
```



```
37.187.124.66 - PuTTY
GNU nano 5.7 /usr/local/etc/postfix/main.cf
maximal_queue_lifetime = 1d
bounce_queue_lifetime = 1d

# Adjusted message size limit.
message_size_limit = 25600000

# Maia-Mailguard
#
content_filter=smtp-amavis:[127.0.0.1]:10024

# LOCAL PATHNAME INFORMATION
#
# The queue_directory specifies the location of the Postfix queue.
# This is also the root directory of Postfix daemons that run chrooted.
# See the files in examples/chroot-setup for setting up Postfix chroot
# environments on different UNIX systems.
#
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4-$ csh 5$ csh (6*$ csh) ][06/10/2
```

Rys 3.11.8: Edycja pliku /usr/local/etc/postfix/main.cf.

Do pliku /usr/local/etc/postfix/master.cf wstawiamy ustawienia:

```
smtp-amavis unix - - n - 2 smtp
  -o smtp_data_done_timeout=2400
  -o smtp_send_xforward_command=yes
  -o disable_dns_lookups=yes
  -o max_use=20
127.0.0.1:10025 inet n - n - - smtpd
  -o content_filter=
  -o local_recipient_maps=
  -o relay_recipient_maps=
  -o smtpd_restriction_classes=
  -o smtpd_delay_reject=no
  -o smtpd_client_restrictions=permit_mynetworks,reject
  -o smtpd_helo_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_recipient_restrictions=permit_mynetworks,reject
  -o mynetworks_style=host
  -o mynetworks=127.0.0.0/8
  -o strict_rfc821_envelopes=yes
  -o smtpd_error_sleep_time=0
  -o smtpd_soft_error_limit=1001
  -o smtpd_hard_error_limit=1000
  -o smtpd_client_connection_count_limit=0
  -o smtpd_client_connection_rate_limit=0
  -o
receive_override_options=no_header_body_checks,no_unknown_recipient_checks,no_address_mappings
```

```
37.187.124.66 - PuTTY
GNU nano 5.7 /usr/local/etc/postfix/master.cf

smtp-amavis unix - - n - 2 smtp
-o smtp_data_done_timeout=2400
-o smtp_send_xforward_command=yes
-o disable_dns_lookups=yes
-o max_use=20
127.0.0.1:10025 inet n - n - - smtpd
-o content_filter=
-o local_recipient_maps=
-o relay_recipient_maps=
-o smtpd_restriction_classes=
-o smtpd_delay_reject=no
-o smtpd_client_restrictions=permit_mynetworks,reject
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,reject
-o mynetworks_style=host
-o mynetworks=127.0.0.0/8
-o strict_rfc821_envelopes=yes

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4-$ csh 5$ csh (6*$ csh) ][06/10/2
```

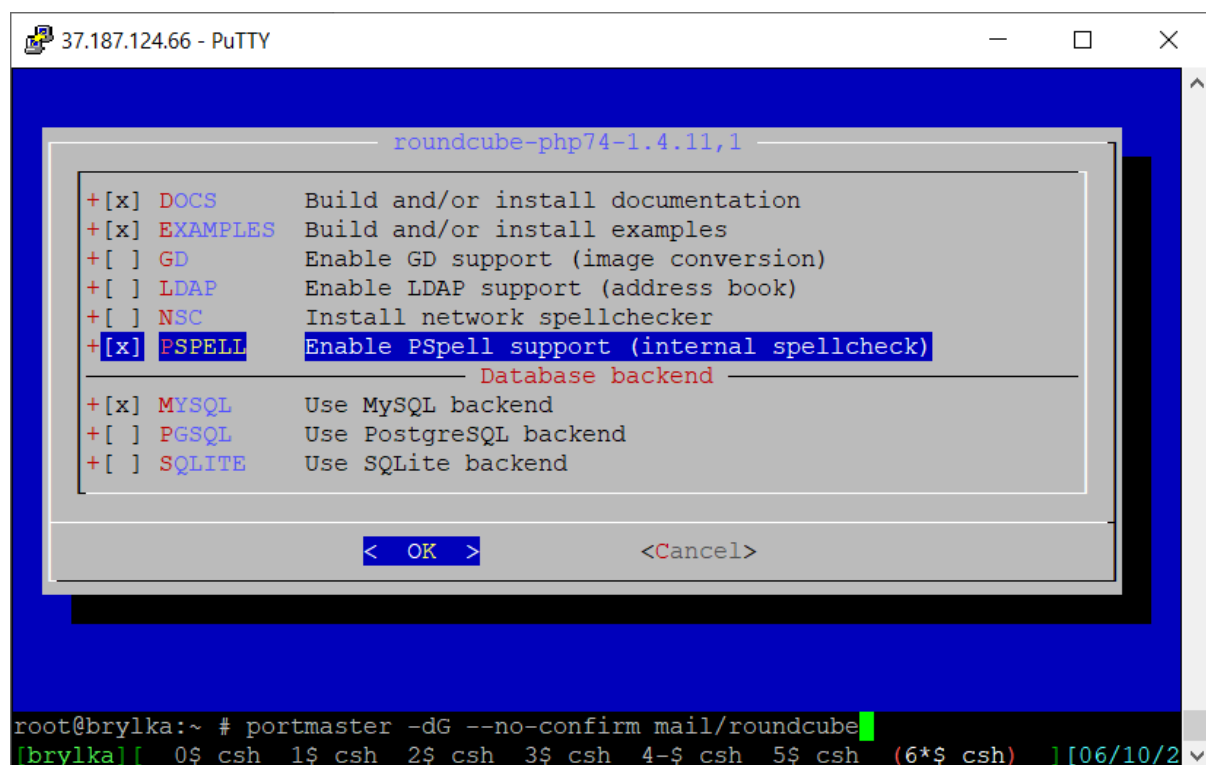
Rys 3.11.9: Edycja pliku /usr/local/etc/postfix/master.cf.

Dodajemy użytkownikowi vscan do crontaba skrypty niezbędne między innymi do aktualizacji regułek SpamAssassina.

```
37.187.124.66 - PuTTY
#Load new rules and store into Maia database.
30 4 * * * /usr/local/share/maia/scripts/load-sa-rules.pl > /dev/null
#Train Spam Assassin.
0 * * * * /usr/local/share/maia/scripts/process-quarantine.pl --learn --report >
/dev/null
#Take a snapshot of the stats at the start of every hour.
0 * * * * /usr/local/share/maia/scripts/stats-snapshot.pl > /dev/null
#Purge mail that has not been confirmed.
0 23 * * * /usr/local/share/maia/scripts/expire-quarantine-cache.pl > /dev/null
#Send quarantine reminders.
0 15 * * * /usr/local/share/maia/scripts/send-quarantine-reminders.pl > /dev/nul
l
#Send quarantine digests.
0 15 * * * /usr/local/share/maia/scripts/send-quarantine-digests.pl > /dev/null
#Force bayesian auto-expiry during off-peak hours.
25 2 * * * /usr/local/bin/sa-learn --sync --force-expire > /dev/null
~
~
~
~
~
/tmp/crontab.dPImlCZEFi: unmodified: line 1
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4-$ csh 5$ csh (6*$ csh) ][06/10/2
```

Rys 3.11.10: Regułki crontab użytkownika vscan.

3.11. INSTALACJA I KONFIGURACJA ROUNDUCUBE



```
37.187.124.66 - PuTTY

roundcube-php74-1.4.11,1

+ [x] DOCS      Build and/or install documentation
+ [x] EXAMPLES  Build and/or install examples
+ [ ] GD        Enable GD support (image conversion)
+ [ ] LDAP      Enable LDAP support (address book)
+ [ ] NSC       Install network spellchecker
+ [x] PSPELL    Enable PSpell support (internal spellcheck)

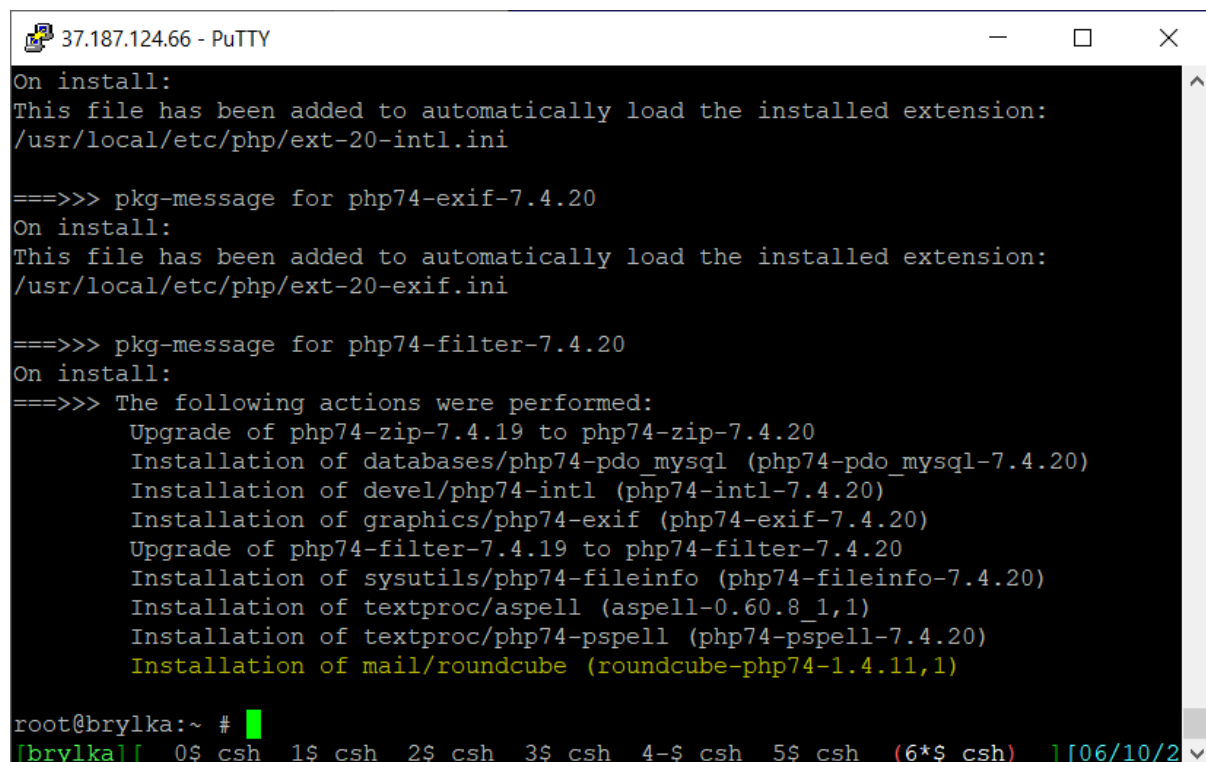
----- Database backend -----
+ [x] MYSQL     Use MySQL backend
+ [ ] PGSQL     Use PostgreSQL backend
+ [ ] SQLITE    Use SQLite backend

< OK >      <Cancel>

root@brylka:~ # portmaster -dG --no-confirm mail/roundcube
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4-$ csh 5$ csh (6*$ csh) ] [06/10/2024]
```

Rys 3.11.1: Dodanie do kompilacji Roundcube: MySQL i Pspell.

Wraz z Roundcube zainstalowały się inne pakiety.



```
37.187.124.66 - PuTTY

On install:
This file has been added to automatically load the installed extension:
/usr/local/etc/php/ext-20-intl.ini

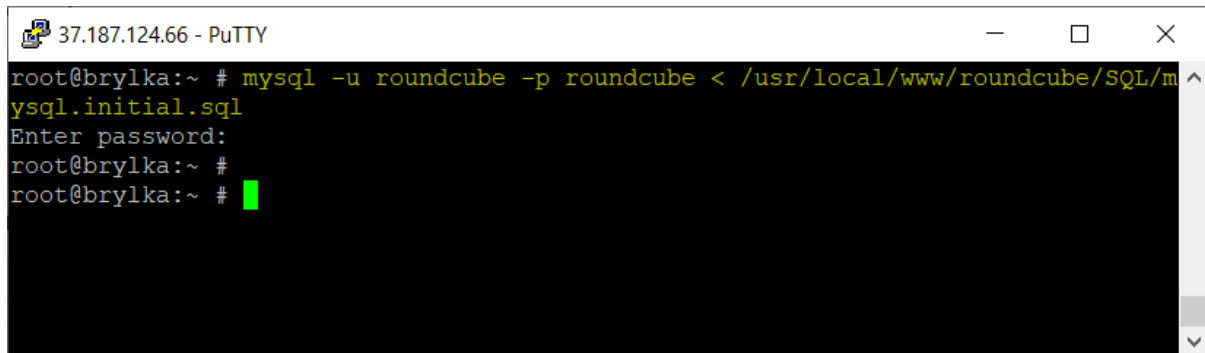
===>>> pkg-message for php74-exif-7.4.20
On install:
This file has been added to automatically load the installed extension:
/usr/local/etc/php/ext-20-exif.ini

===>>> pkg-message for php74-filter-7.4.20
On install:
===>>> The following actions were performed:
  Upgrade of php74-zip-7.4.19 to php74-zip-7.4.20
  Installation of databases/php74-pdo_mysql (php74-pdo_mysql-7.4.20)
  Installation of devel/php74-intl (php74-intl-7.4.20)
  Installation of graphics/php74-exif (php74-exif-7.4.20)
  Upgrade of php74-filter-7.4.19 to php74-filter-7.4.20
  Installation of sysutils/php74-fileinfo (php74-fileinfo-7.4.20)
  Installation of textproc/aspell (aspell-0.60.8_1,1)
  Installation of textproc/php74-pspell (php74-pspell-7.4.20)
  Installation of mail/roundcube (roundcube-php74-1.4.11,1)

root@brylka:~ #
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4-$ csh 5$ csh (6*$ csh) ] [06/10/2024]
```

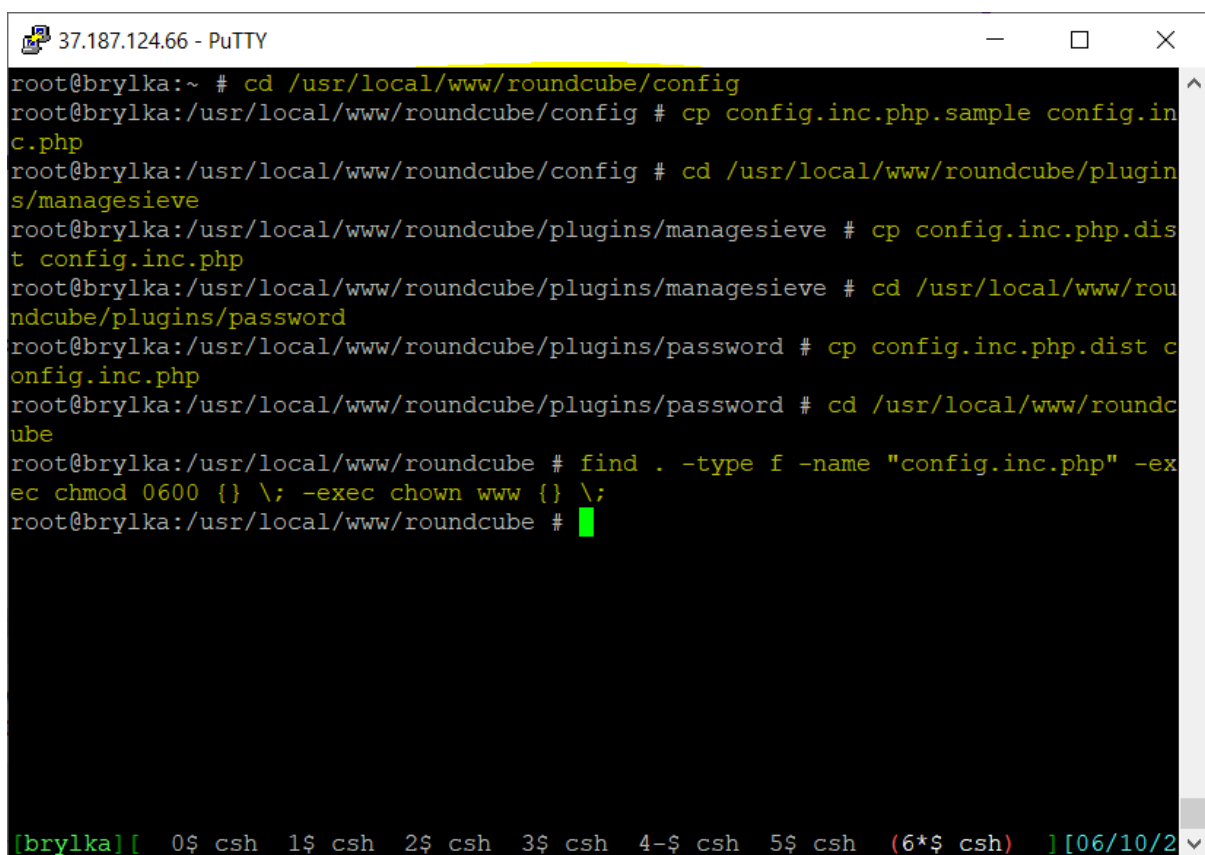
Rys 3.11.2: Instalacja Roundcube.

Importujemy zawartość pliku `/usr/local/www/roundcube/SQL/mysql.initial.sql` do bazy danych.



```
37.187.124.66 - PuTTY
root@brylka:~ # mysql -u roundcube -p roundcube < /usr/local/www/roundcube/SQL/mysql.initial.sql
Enter password:
root@brylka:~ #
root@brylka:~ #
```

Rys 3.11.3: Import danych do bazy danych.



```
37.187.124.66 - PuTTY
root@brylka:~ # cd /usr/local/www/roundcube/config
root@brylka:/usr/local/www/roundcube/config # cp config.inc.php.sample config.inc.php
root@brylka:/usr/local/www/roundcube/config # cd /usr/local/www/roundcube/plugins/managesieve
root@brylka:/usr/local/www/roundcube/plugins/managesieve # cp config.inc.php.dist config.inc.php
root@brylka:/usr/local/www/roundcube/plugins/managesieve # cd /usr/local/www/roundcube/plugins/password
root@brylka:/usr/local/www/roundcube/plugins/password # cp config.inc.php.dist config.inc.php
root@brylka:/usr/local/www/roundcube/plugins/password # cd /usr/local/www/roundcube
root@brylka:/usr/local/www/roundcube # find . -type f -name "config.inc.php" -exec chmod 0600 {} \; -exec chown www {} \;
root@brylka:/usr/local/www/roundcube #
```

[brylka][0\$ csh 1\$ csh 2\$ csh 3\$ csh 4-\$ csh 5\$ csh (6*\$ csh)] [06/10/2024]

Rys 3.11.4: Kopiujemy pliki konfiguracyjne Roundcube.

Dodajemy dane do bazy danych oraz kilka ustawień dodatkowych w pliku konfiguracyjnym Roundcube `/usr/local/www/roundcube/config/config.inc.php`.

```
37.187.124.66 - PuTTY
GNU nano 5.7 /usr/local/www/roundcube/config/config.inc.php

// This key is used to encrypt the users imap password which is stored
// in the session record. For the default cipher method it must be
// exactly 24 characters long.
// YOUR KEY MUST BE DIFFERENT THAN THE SAMPLE VALUE FOR SECURITY REASONS
$config['des_key'] = 'rcmail-!24ByteDESkey*Str';

// List of active plugins (in plugins/ directory)
$config['plugins'] = array(
    'archive',
    'zipdownload',
    'managesieve',
    'password',
);

// skin name: folder from skins/
$config['skin'] = 'elastic';

$config['spellcheck_engine'] = 'pspell';
$config['preview_pane'] = true;
$config['mime_types'] = '/usr/local/etc/apache24/mime.types';
$config['enable_installer'] = false;

[ Wrote 93 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4-$ csh 5$ csh (6*$ csh) ][06/10/2
```

Rys 3.11.5: Edycja pliku konfiguracyjnego Roundcube.

```
37.187.124.66 - PuTTY
/usr/local/www/roundcube/plugins/managesieve/config.inc.php

// $config['managesieve_conn_options'] = array(
//     'ssl' => array(
//         'verify_peer' => true,
//         'verify_depth' => 3,
//         'cafile' => '/etc/openssl/certs/ca.crt',
//     ),
// );
// Note: These can be also specified as an array of options indexed by hostname
$config['managesieve_conn_options'] = null;

// A file with default script content (eg. spam filter)
#$config['managesieve_default'] = '/etc/dovecot/sieve/global';
$config['managesieve_default'] = '/var/mail/vhost/default.sieve';

// The name of the script which will be used when there's no user script
$config['managesieve_script_name'] = 'managesieve';

// Sieve RFC says that we should use UTF-8 encoding for mailbox names,
// but some implementations does not covert UTF-8 to modified UTF-7.
// Defaults to UTF7-IMAP
$config['managesieve_mbox_encoding'] = 'UTF-8';

root@brylka:/usr/local/www/roundcube #
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4-$ csh 5$ csh (6*$ csh) ][06/10/2
```

Rys 3.11.6: Edycja pliku /usr/local/www/roundcube/plugins/managesieve/config.inc.php.

```
37.187.124.66 - PuTTY
/usr/local/www/roundcube/plugins/password/config.inc.php
// %d is replaced with the domain part of the username
// (in case the username is an email address)
// Deprecated macros:
// %c is replaced with the crypt version of the new password, MD5 if avail
// otherwise DES. More hash function can be enabled using the password
// configuration parameter.
// %D is replaced with the dovecotpw-crypted version of the new password
// %n is replaced with the hashed version of the new password
// %q is replaced with the hashed password before the change
// Escaping of macros is handled by this module.
// Default: "SELECT update_passwd(%c, %u)"
$config['password_query'] = 'SELECT update_passwd(%c, %u)';
$config['password_query'] = 'UPDATE mailbox SET password=%c, modified=now() WHE
[ Wrote 495 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4-$ csh 5$ csh (6*$ csh) ][06/10/2
```

Rys 3.11.7: Edytujemy plik `/usr/local/www/roundcube/plugins/password/config.inc.php`.

```
37.187.124.66 - PuTTY
GNU nano 5.7 /usr/local/etc/apache24/Includes/roundcube.conf
Alias /roundcube "/usr/local/www/roundcube/"
<Directory "/usr/local/www/roundcube">
  Options Indexes FollowSymLinks
  AllowOverride All
  Require all granted
</Directory>
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh 4-$ csh 5$ csh (6*$ csh) ][06/10/2
```

Rys 3.11.8: Dodajemy ustawienia do apache. Resetujemy apache.

3.12. URUCHOMIENIE I SPRAWDZENIE DZIAŁANIA USŁUG LOKALNIE

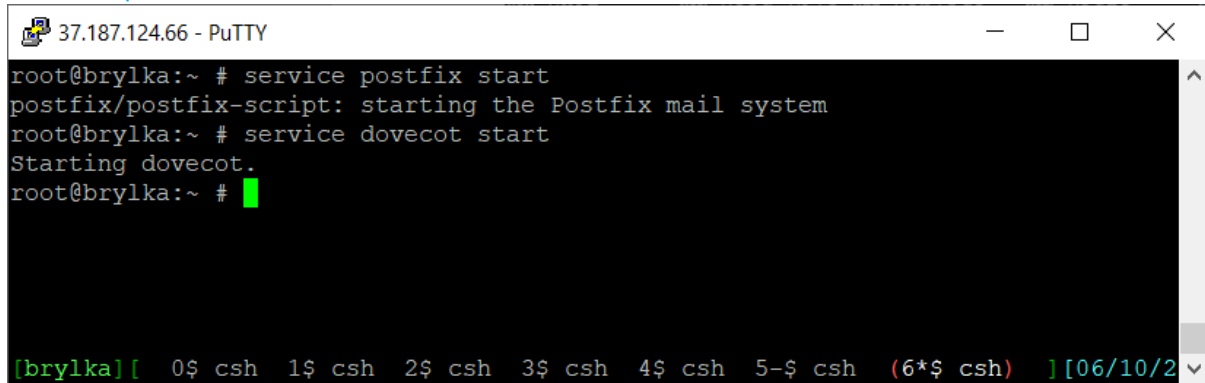
Sprawdzamy działanie usług lokalnie. Dokładne testy działania usług z zewnątrz, sprawdzające np. podatność na OpenRelay zostaną przeprowadzone w rozdziale czwartym.

3.12.1. URUCHOMIENIE I TEST POSTFIX I DOVECOT

Postfixa i Dovecota uruchamiamy poleceniami:

```
service dovecot start
```

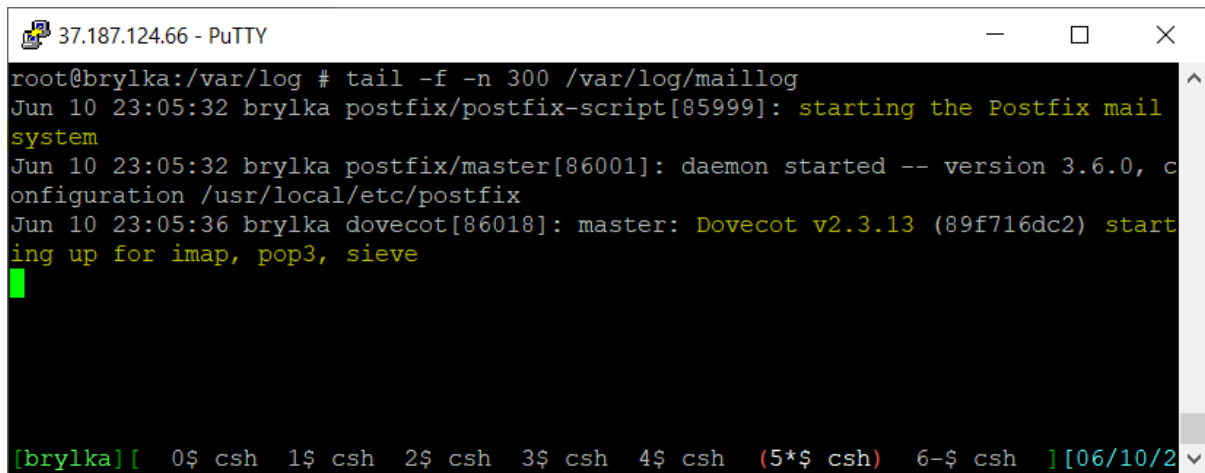
service postfix start



```
37.187.124.66 - PuTTY
root@brylka:~ # service postfix start
postfix/postfix-script: starting the Postfix mail system
root@brylka:~ # service dovecot start
Starting dovecot.
root@brylka:~ #
```

[brylka][0\$ csh 1\$ csh 2\$ csh 3\$ csh 4\$ csh 5-\$ csh (6*\$ csh)][06/10/2

Rys 3.12.1.1: Uruchomienie Postfixa i Dovecota.



```
37.187.124.66 - PuTTY
root@brylka:/var/log # tail -f -n 300 /var/log/maillog
Jun 10 23:05:32 brylka postfix/postfix-script[85999]: starting the Postfix mail
system
Jun 10 23:05:32 brylka postfix/master[86001]: daemon started -- version 3.6.0, c
onfiguration /usr/local/etc/postfix
Jun 10 23:05:36 brylka dovecot[86018]: master: Dovecot v2.3.13 (89f716dc2) start
ing up for imap, pop3, sieve

```

[brylka][0\$ csh 1\$ csh 2\$ csh 3\$ csh 4\$ csh (5*\$ csh) 6-\$ csh][06/10/2

Rys 3.12.1.2: Sprawdzenie logów systemowych pokazuje uruchomienie usług.

Testujemy połączenie do usług uruchamianych przez demony.

```
37.187.124.66 - PuTTY
root@brylka:~ # telnet localhost 25
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 projekt.brylka.net ESMTP Postfix
EHLO testuje.com.pl
250-projekt.brylka.net
250-PIPELINING
250-SIZE 25600000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
STARTTLS
220 2.0.0 Ready to start TLS
^CConnection closed by foreign host.
root@brylka:~ #
```

[brylka] [0\$ csh 1\$ csh 2\$ csh 3\$ csh 4\$ csh 5-\$ csh (6*\$ csh)] [06/10/2

Rys 3.12.1.3 Test komunikacji SMTP na porcie 25.

```
37.187.124.66 - PuTTY
root@brylka:~ # telnet localhost 465
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
^CConnection closed by foreign host.
root@brylka:~ #
```

[brylka] [0\$ csh 1\$ csh 2\$ csh 3\$ csh 4\$ csh 5-\$ csh (6*\$ csh)] [06/10/2

Rys 3.12.1.4: Test komunikacji SMTP na porcie 465.


```
37.187.124.66 - PuTTY
root@brylka:~ # telnet localhost 587
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^'.
220 projekt.brylka.net ESMTP Postfix
quit
221 2.0.0 Bye
Connection closed by foreign host.
root@brylka:~ #
```

Rys 3.12.1.5: Test komunikacji SMTP na porcie 587.

```
37.187.124.66 - PuTTY
root@brylka:~ # telnet localhost 110
Trying ::1...
Connected to localhost.
Escape character is '^'.
+OK projekt.brylka.net Mail Server Ready...
quit
+OK Logging out
Connection closed by foreign host.
root@brylka:~ #
```

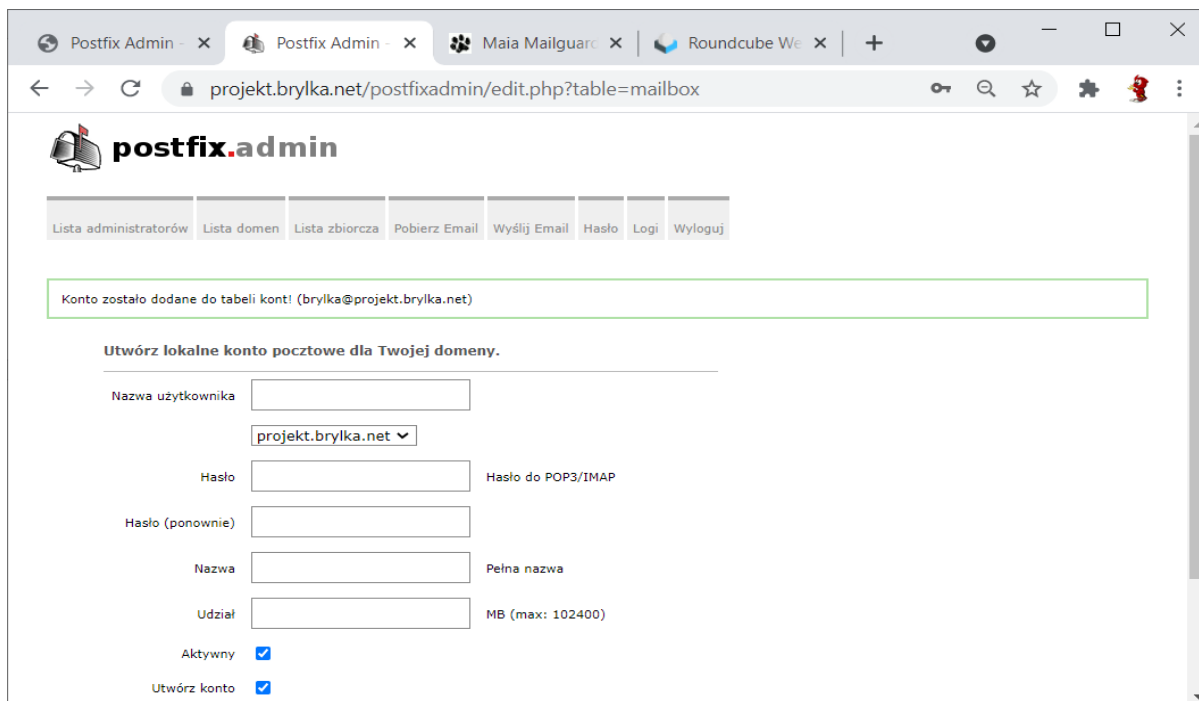
Rys 3.12.1.6: Test komunikacji POP3 na porcie 110.

```
37.187.124.66 - PuTTY
root@brylka:~ # telnet localhost 143
Trying ::1...
Connected to localhost.
Escape character is '^'.
* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+ START
TLS AUTH=PLAIN AUTH=LOGIN] projekt.brylka.net Mail Server Ready...
^C^C
^C^X^C
Connection closed by foreign host.
root@brylka:~ #
```

Rys 3.12.1.7: Test komunikacji IMAP na porcie 143.

3.12.2. TEST POSTFIXADMIN

Po zalogowaniu się do PostfixAdmina dodaję domenę projekt.brylka.net, a następnie konto brylka@projekt.brylka.net.



Konto zostało dodane do tabeli kont! (brylka@projekt.brylka.net)

Utwórz lokalne konto pocztowe dla Twojej domeny.

Nazwa użytkownika

Hasło Hasło do POP3/IMAP

Hasło (ponownie)

Nazwa Pełna nazwa

Udział MB (max: 102400)

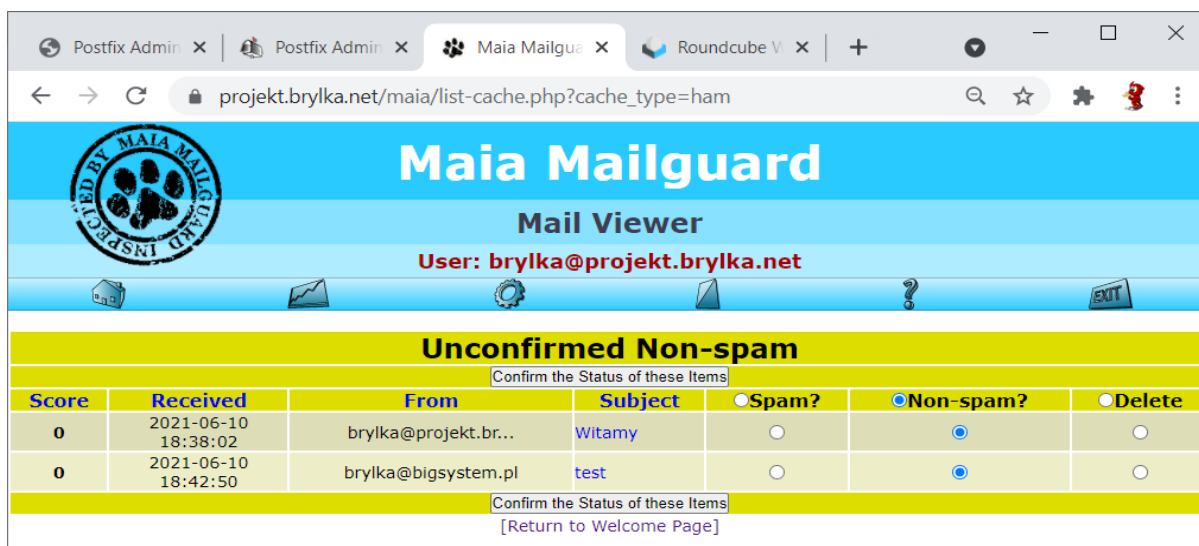
Aktywny

Utwórz konto

Rys 3.12.2.1: Dodanie konta do systemu pocztowego.

3.12.3. TEST MAIA-MAILGUARD

Po zalogowaniu się do aplikacji Mail-Mailguard widzimy poprawne działanie pakietu (na konto brylka@projekt.brylka.net dostarczone zostały dwie wiadomości: powitalna z systemu i testowa wysłana przeze nie z innego serwera).



Maia Mailguard

Mail Viewer

User: brylka@projekt.brylka.net

Unconfirmed Non-spam

Confirm the Status of these Items

Score	Received	From	Subject	Spam?	Non-spam?	Delete
0	2021-06-10 18:38:02	brylka@projekt.br...	Witamy	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
0	2021-06-10 18:42:50	brylka@bigsystem.pl	test	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

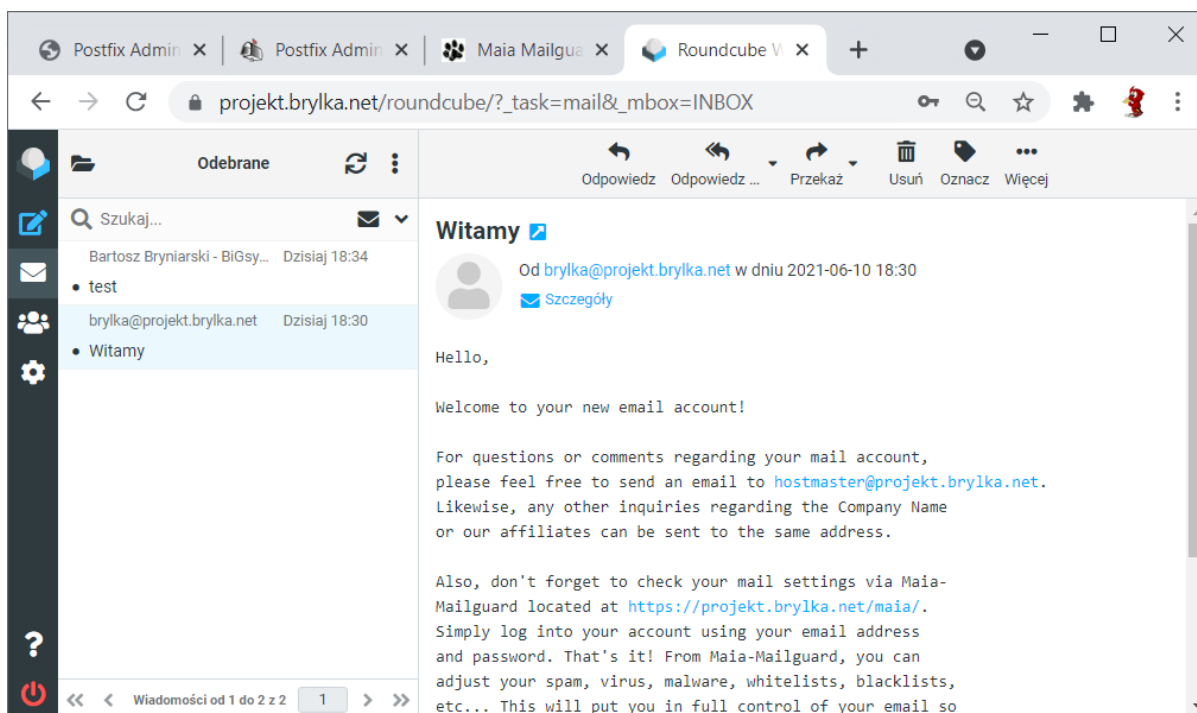
Confirm the Status of these Items

[Return to Welcome Page]

Rys 3.12.3.1: Strona aplikacji Maia-Mailguard.

3.12.4. TEST ROUNDUCUBE

Po zalogowaniu się do Roundcube możemy przeglądać wiadomości.



Rys 3.12.4.1: Test Roundcube.

3.13. INSTALACJA I KONFIGURACJA FAIL2BAN

Instalujemy Fail2Ban z paczek. Podczas instalacji doinstalowane zostaną trzy dodatkowe pakiety.

```
37.187.124.66 - PuTTY
root@brylka:~ # pkg search fail2ban
py38-fail2ban-0.11.2          Scans log files and bans IP that makes too many p
password failures
root@brylka:~ # pkg install py38-fail2ban
Updating FreeBSD_latest repository catalogue...
FreeBSD_latest repository is up to date.
All repositories are up to date.
The following 4 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:
  libinotify: 20180201_2
  py38-fail2ban: 0.11.2
  py38-pyinotify: 0.9.6
  py38-sqlite3: 3.8.10_7

Number of packages to be installed: 4

The process will require 3 MiB more space.
687 KiB to be downloaded.

Proceed with this action? [y/N]: y
[brylka][ 0$ csh 1$ csh 2$ csh 3$ csh (4*$ csh) 5-$ csh 6$ csh ] [06/11/2
```

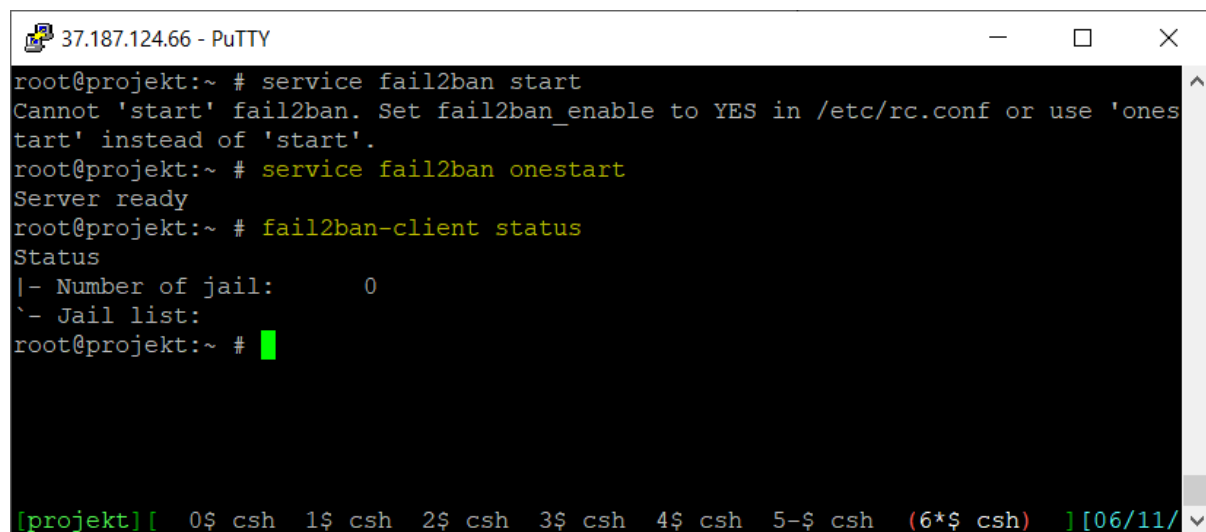
Rys 3.13.1: Inicjowanie instalacji Fail2Ban.

Podczas konfiguracji firewalla trzeba być bardzo ostrożnym, szczególnie konfigurując to na zdalnej maszynie, nie mając do niej fizycznego dostępu, gdyż jedna nieprzemyślana komenda może zablokować nam dostęp do maszyny. Dla własnego bezpieczeństwa, aby nie stracić dostępu do maszyny komendy będą wykonywać „z palca”, bez dodawania firewalla do startu systemu – jakkolwiek pomyłkę będzie można naprawić przez zdalny „hard reset” maszyny.

Uruchamiamy Fail2Ban poleceniem:

```
service fail2ban onestart
```

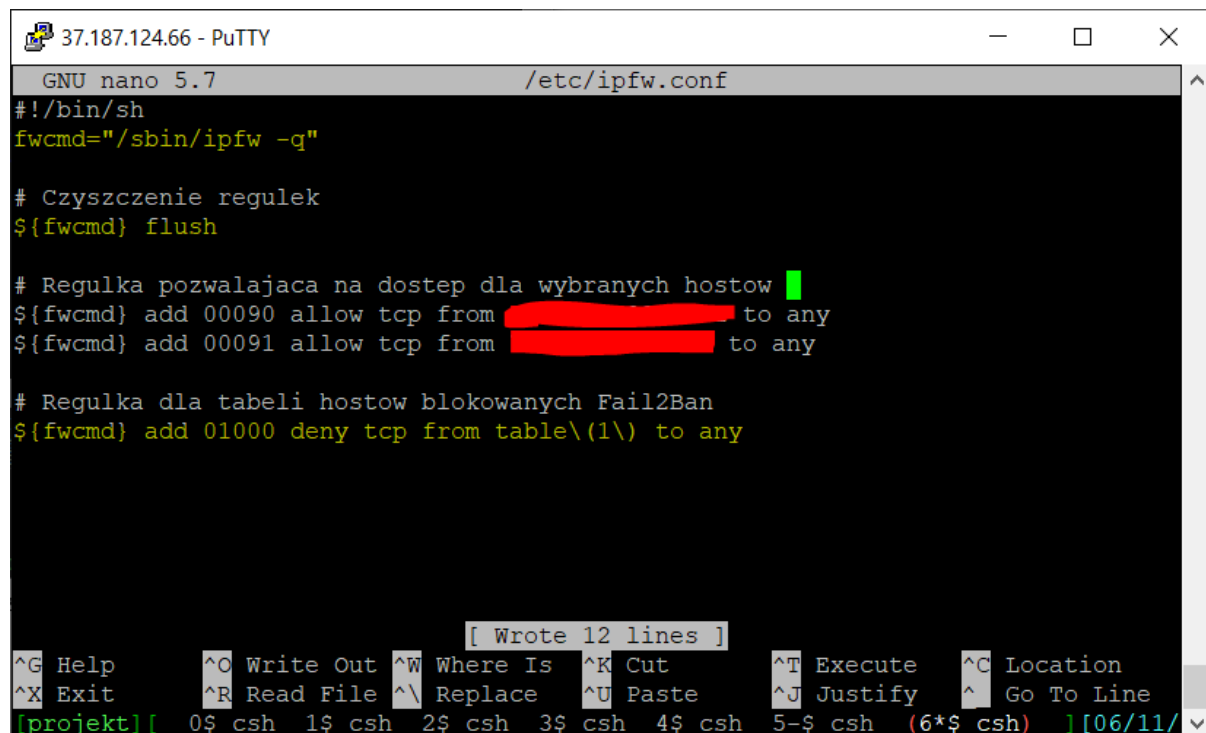
i sprawdzamy status.



```
37.187.124.66 - PuTTY
root@projekt:~ # service fail2ban start
Cannot 'start' fail2ban. Set fail2ban_enable to YES in /etc/rc.conf or use 'onestart' instead of 'start'.
root@projekt:~ # service fail2ban onestart
Server ready
root@projekt:~ # fail2ban-client status
Status
|- Number of jail:      0
`- Jail list:
root@projekt:~ #
```

Rys 3.13.1: Uruchomienie Fail2Ban i sprawdzenie statusu.

Dodajemy regułki firewalla w pliku /etc/ipfw.conf



```
37.187.124.66 - PuTTY
GNU nano 5.7 /etc/ipfw.conf
#!/bin/sh
fwcmd="/sbin/ipfw -q"

# Czyszczenie regulek
${fwcmd} flush

# Regułka pozwalająca na dostęp dla wybranych hostów
${fwcmd} add 00090 allow tcp from [redacted] to any
${fwcmd} add 00091 allow tcp from [redacted] to any

# Regułka dla tabeli hostów blokowanych Fail2Ban
${fwcmd} add 01000 deny tcp from table\{1\} to any

[ Wrote 12 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
[projekt][ 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh 5-$ csh (6*$ csh) ][06/11/
```

Rys 3.13.2: Dodanie regułek ipfw.

Uruchamiamy regułki firewalla komendą:

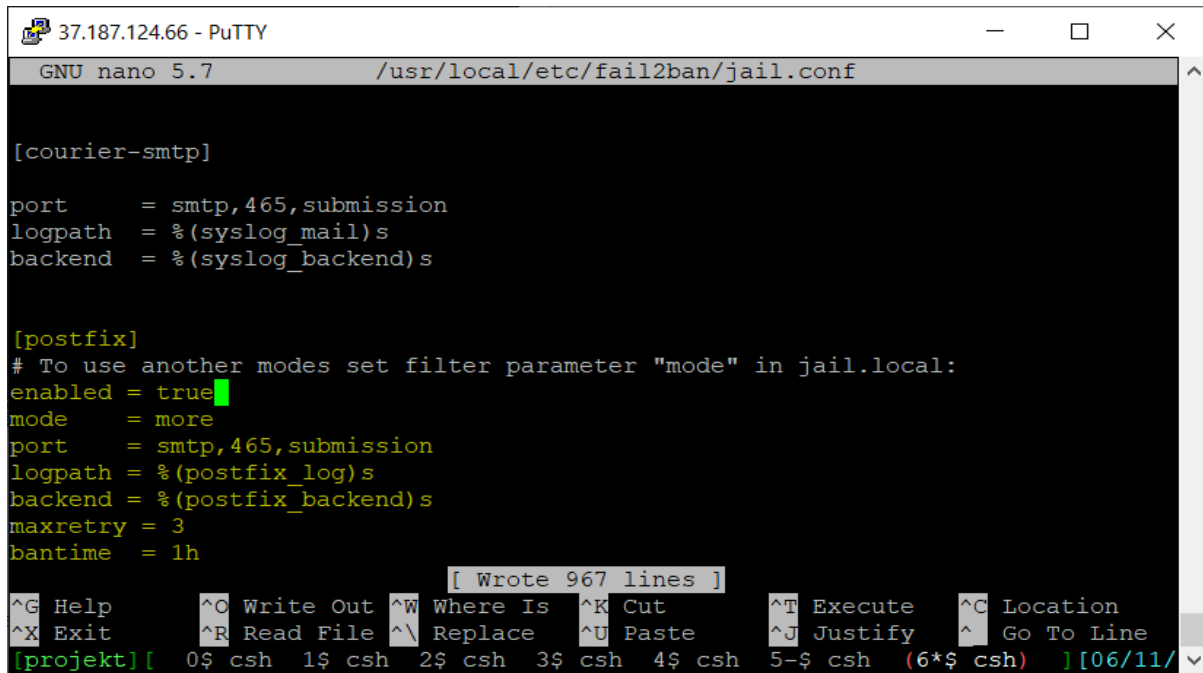
```
sh /etc/ipfw.conf
```

sprawdzamy czy się załadowały:

```
ipfw list
```

Wszystko w porządku, dostępu do maszyny sobie nie zablokowałem.

Konfigurujemy jail'a w Fail2Ban dla usługi SMTP.



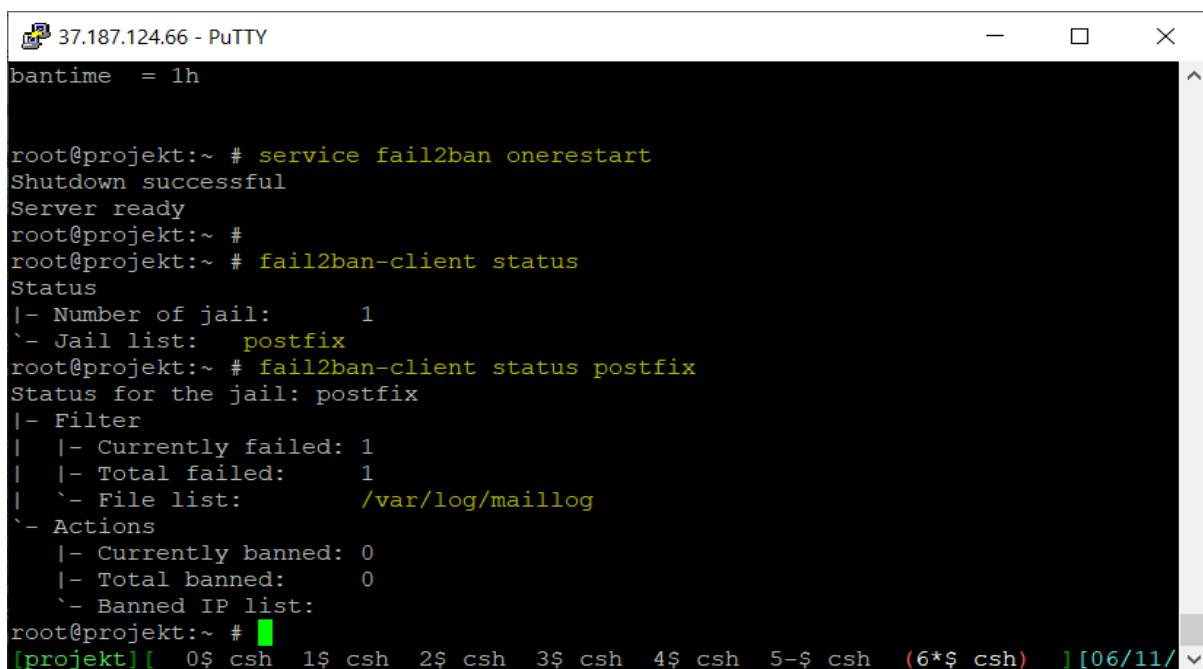
```
37.187.124.66 - PuTTY
GNU nano 5.7 /usr/local/etc/fail2ban/jail.conf

[courier-smtp]
port      = smtp,465,submission
logpath   = %(syslog_mail)s
backend   = %(syslog_backend)s

[postfix]
# To use another modes set filter parameter "mode" in jail.local:
enabled   = true
mode      = more
port      = smtp,465,submission
logpath   = %(postfix_log)s
backend   = %(postfix_backend)s
maxretry  = 3
bantime   = 1h

[ Wrote 967 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
[projekt][ 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh 5-$ csh (6*$ csh) ][06/11/
```

Rys 3.13.3: Konfiguracja Fail2Ban jail dla usługi SMTP.



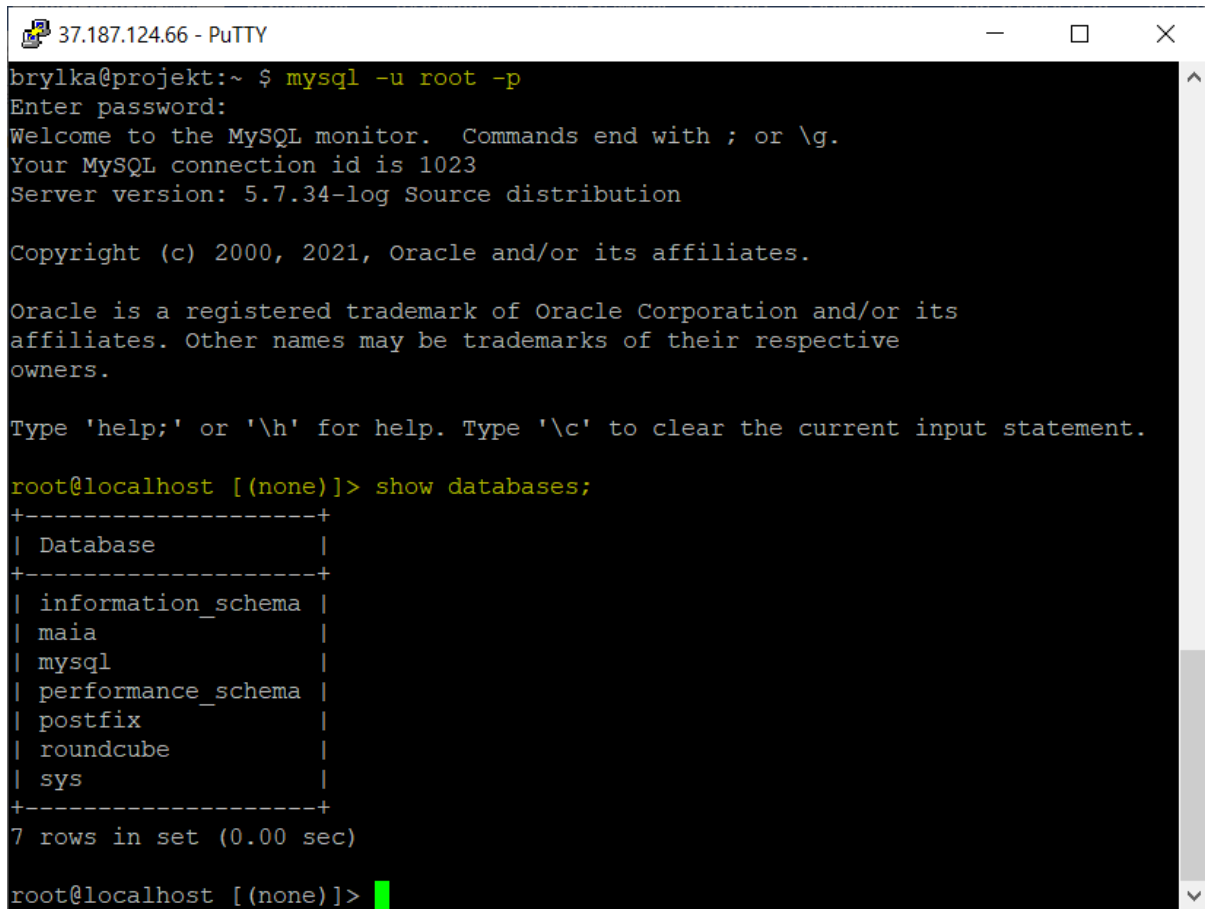
```
37.187.124.66 - PuTTY
bantime   = 1h

root@projekt:~ # service fail2ban onerestart
Shutdown successful
Server ready
root@projekt:~ #
root@projekt:~ # fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:          postfix
root@projekt:~ # fail2ban-client status postfix
Status for the jail: postfix
|- Filter
| |- Currently failed: 1
| |- Total failed:    1
| `-- File list:      /var/log/maillog
`- Actions
   |- Currently banned: 0
   |- Total banned:    0
   `-- Banned IP list:
root@projekt:~ #
[projekt][ 0$ csh 1$ csh 2$ csh 3$ csh 4$ csh 5-$ csh (6*$ csh) ][06/11/
```

Rys 3.13.4: Sprawdzenie statusu Fail2Ban.

4.2. TEST SYSTEMU ZARZĄDZANIA BAZĄ DANYCH MYSQL

Lokalny test Systemu Zarządzania Bazą Danych MySQL – logowanie na konto administratora.



```
37.187.124.66 - PuTTY
brylka@projekt:~ $ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1023
Server version: 5.7.34-log Source distribution

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.

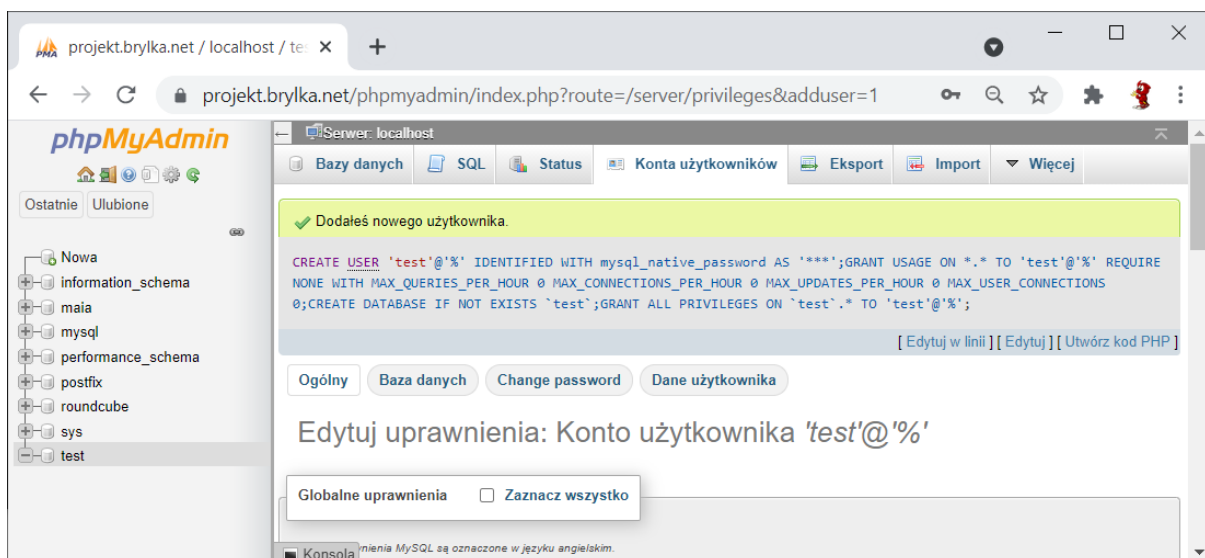
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

root@localhost [(none)]> show databases;
+-----+
| Database                |
+-----+
| information_schema      |
| maia                    |
| mysql                   |
| performance_schema     |
| postfix                 |
| roundcube               |
| sys                     |
+-----+
7 rows in set (0.00 sec)

root@localhost [(none)]>
```

Rys 4.2.1: Zalogowanie się lokalnie na konto administratora.

Test phpMyAdmin – aplikacji do zarządzania SZBD MySQL.



Rys 4.2.2: Test phpMyAdmin – dodanie konta test.

```
jupiter.wiedzmin.net - PuTTY
root@jupiter:~ # mysql -u test -h 37.187.124.66 -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3
Server version: 5.7.34-log Source distribution

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

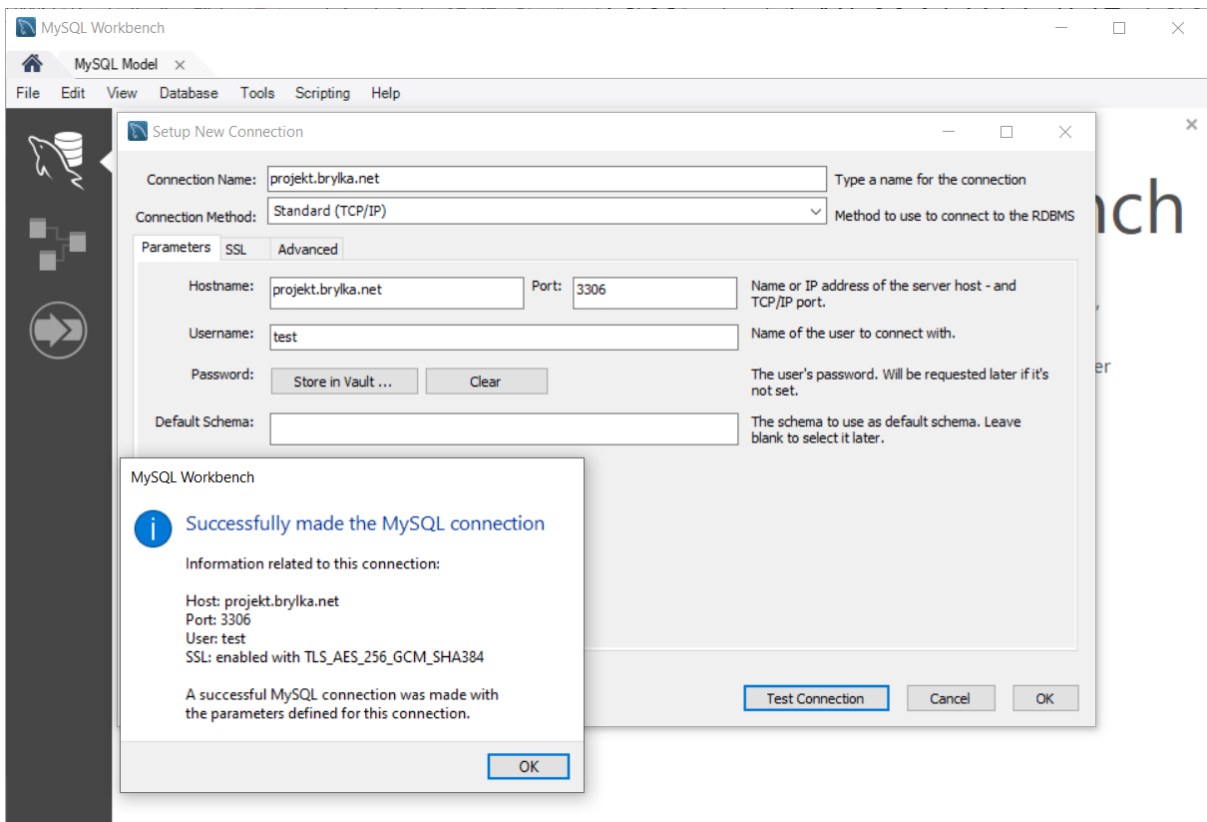
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

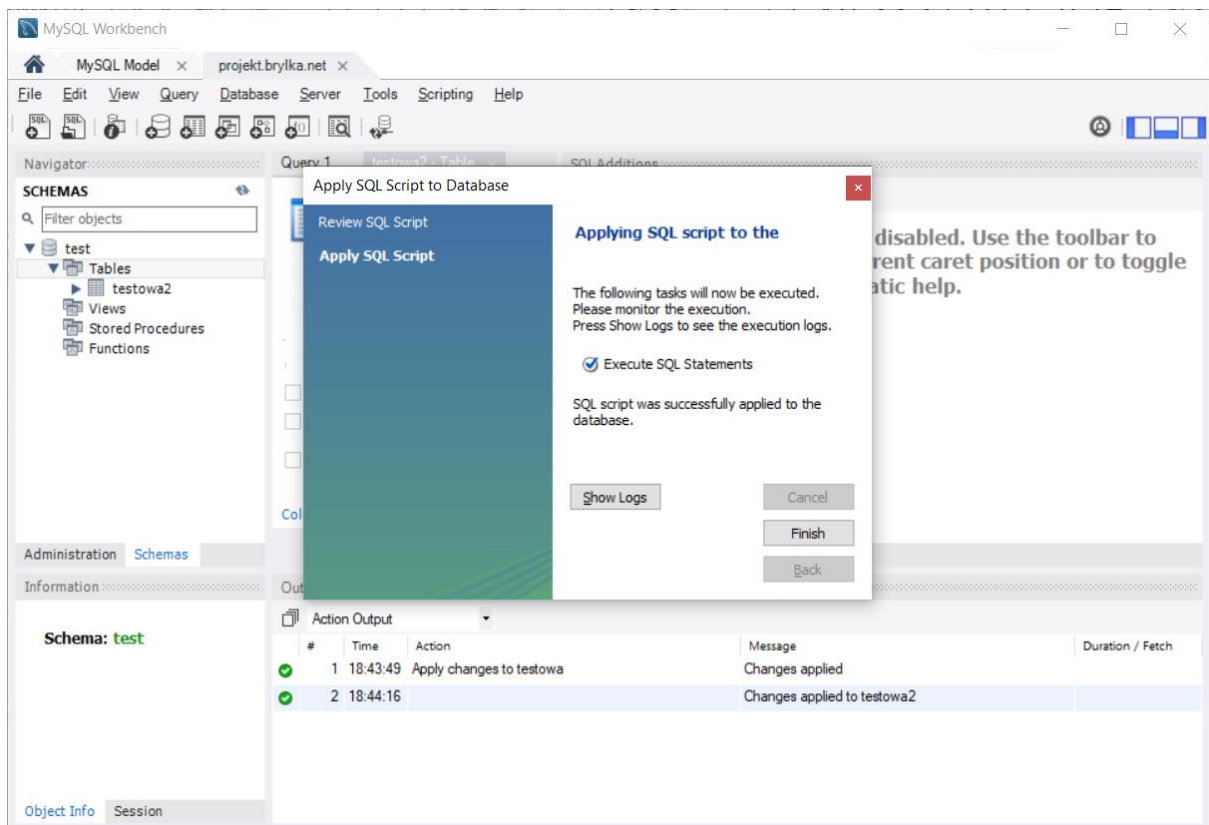
test@37.187.124.66 [(none)]> show databases;
+-----+
| Database                |
+-----+
| information_schema      |
| test                    |
+-----+
2 rows in set (0.00 sec)

test@37.187.124.66 [(none)]>
```

Rys 4.2.3: Zalogowanie się do MySQL ze zdalnego urządzenia na użytkownika „test”.



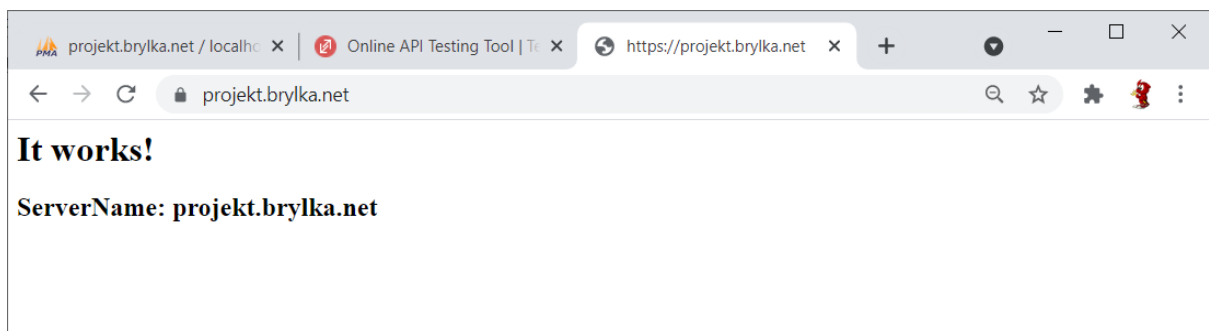
Rys 4.2.4: Test połączenia do bazy danych z programie MySQL Workbench.



Rys 4.2.5: Operacje na bazie danych w programie MySQL Workbench.

4.3. TEST HTTP | HTTPS

Wpisanie w przeglądarkę adresu <http://projekt.brylka.net> powoduje przekierowanie na <https://projekt.brylka.net>



Rys 4.3.1: Strona startowa serwera widziana w przeglądarce.

projekt.brylka.net / localhost | ph x Online API Testing Tool | Test You x +

reqbin.com

REQBIN Request Examples Articles & Tutorials REST API Library Curl Online Contact Login Sign Up

REST API EXAMPLES
 REST API POST Example
 POST HTML Form
 POST JSON Example
 POST Request Example
 GET Request Example
 Bearer Token Auth
 Weather REST API

ARTICLES & TUTORIALS
 POST GET DELETE

sematext
 Real-time infrastructure and API monitoring

Xceed
 The Best Tools for WPFI.NET/Javascript
 Try it Now!

Fully featured easy to use Word API
 ADS VIA CARBON

Status: 200 (OK) Time: 376 ms Size: 0.08 kb

Content (8) Headers (8) Raw (10) HTML Timings

```
HTTP/1.1 200 OK
Date: Fri, 11 Jun 2021 08:34:25 GMT
Server: Apache/2.4.48 (FreeBSD) OpenSSL/1.1.1k-freebsd PHP/7.4.19
Last-Modified: Fri, 04 Jun 2021 21:23:47 GMT
ETag: "54-5c3f74ea9bbdc"
Accept-Ranges: bytes
Content-Length: 84
Content-Type: text/html

<html><body><h1>It works!</h1><h2>ServerName: projekt.brylka.net</h2></body></html>
```

What is API?
 API (Application Programming Interface) is a computing interface that defines how software components interact with each other. It is a way of programmatically interacting with a separate software component or resource and expose functionality for internal or external use and testing. API defines what requests can be made, how they will be made and hides complexity from

Rys 4.3.2: Test usługi https w serwisie REQBIN.

projekt.brylka.net x Online API Testin x https://projekt.brylka.net x SSL Server Test: x +

ssllabs.com/ssltest/analyze.html?d=projekt.brylka.net

Qualys SSL Labs Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > projekt.brylka.net

SSL Report: projekt.brylka.net (37.187.124.66)
 Assessed on: Fri, 11 Jun 2021 08:40:13 UTC | Hide | Clear cache Scan Another »

Summary

Overall Rating

A

Certificate 100
 Protocol Support 100
 Key Exchange 85
 Cipher Strength 85

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server supports TLS 1.3.

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	projekt.brylka.net Fingerprint SHA256: 0f7a4d5b4d69d09e3379303637465981390a54148ab78e7bfa9cab6590ff6bd Pin SHA256: 03679Kf8G8lv7bQrCHAdGSbAQT3zqK9jco+Zf98w=
Common names	projekt.brylka.net

Rys 4.3.3: Test certyfikatów ssl w serwisie SSL Labs.

4.4. TEST SMTP

W pierwszej kolejności testuję czy konfiguracja postfixa nie przepuszcza nieautoryzowanych meili – test Open Relay. Narzędzie appriver pokazało, że serwer przeszedł test pozytywnie – nie jest Open Relay.

AppRiver SpamLab - Open R... Network Tools: DNS,IP,Email

tools.appriver.com/OpenRelay.aspx

appriver a ZIX company RBL Test Whois Headers SMTP DNS RegEx Encoding

Open Relay Test

Mail Server

projekt.brylka.net

✓ Check for Open Relay

R: 220 projekt.brylka.net ESMTP Postfix
S: HELO appriver.com
R: 250 projekt.brylka.net

Test #1
S: RSET
R: 250 2.0.0 Ok
S: MAIL FROM: <spamtest@appriver.com>
R: 250 2.1.0 Ok
S: RCPT TO: <relaytest@appriver.com>
R: 454 4.7.1 <relaytest@appriver.com>: Relay access denied
Relay NOT Accepted

Test #2
S: RSET
R: 250 2.0.0 Ok
S: MAIL FROM: <spamtest>
R: 250 2.1.0 Ok
S: RCPT TO: <relaytest@appriver.com>
R: 504 5.5.2 <spamtest>: Sender address rejected: need fully-qualified address
Relay NOT Accepted

Test #3
S: RSET
R: 250 2.0.0 Ok
S: MAIL FROM: <>
R: 250 2.1.0 Ok
S: RCPT TO: <relaytest@appriver.com>
R: 454 4.7.1 <relaytest@appriver.com>: Relay access denied
Relay NOT Accepted

Test #4
S: RSET
R: 250 2.0.0 Ok
S: MAIL FROM: <spamtest@projekt.brylka.net>
R: 250 2.1.0 Ok
S: RCPT TO: <relaytest@appriver.com>
R: 550 5.1.0 <spamtest@projekt.brylka.net>: Sender address rejected: User unknown in virtual mailbox table
Relay NOT Accepted

Rys 4.4.1: Test SMTP Open Relay.

Network Tools: DNS,IP,Email

mxtoolbox.com/SuperTool.aspx?action=smtp%3aprojekt.brylka.ne...

smtp

220 projekt.brylka.net ESMTP Postfix

Status	Test	Result
✓	NameSMTP Reverse DNS Mismatch	ResponseOK - 37.187.124.66 resolves to projekt.brylka.net
✓	NameSMTP Valid Hostname	ResponseOK - Reverse DNS is a valid Hostname
✓	NameSMTP Banner Check	ResponseOK - Reverse DNS matches SMTP Banner
✓	NameSMTP TLS	ResponseOK - Supports TLS.
✓	NameSMTP Connection Time	Response0.920 seconds - Good on Connection time
✓	NameSMTP Open Relay	ResponseOK - Not an open relay.
✓	NameSMTP Transaction Time	Response1.661 seconds - Good on Transaction Time

Session Transcript:

```
Connecting to 37.187.124.66

220 projekt.brylka.net ESMTP Postfix [818 ms]
EHLO keeper-us-east-1c.mxtoolbox.com
250-projekt.brylka.net
250-PIPELINING
250-SIZE 25600000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING [189 ms]
MAIL FROM:<supertool@mxtoolboxsmtpdiag.com>
250 2.1.0 Ok [259 ms]
RCPT TO:<test@mxtoolboxsmtpdiag.com>
454 4.7.1 <test@mxtoolboxsmtpdiag.com>: Relay access denied [215 ms]

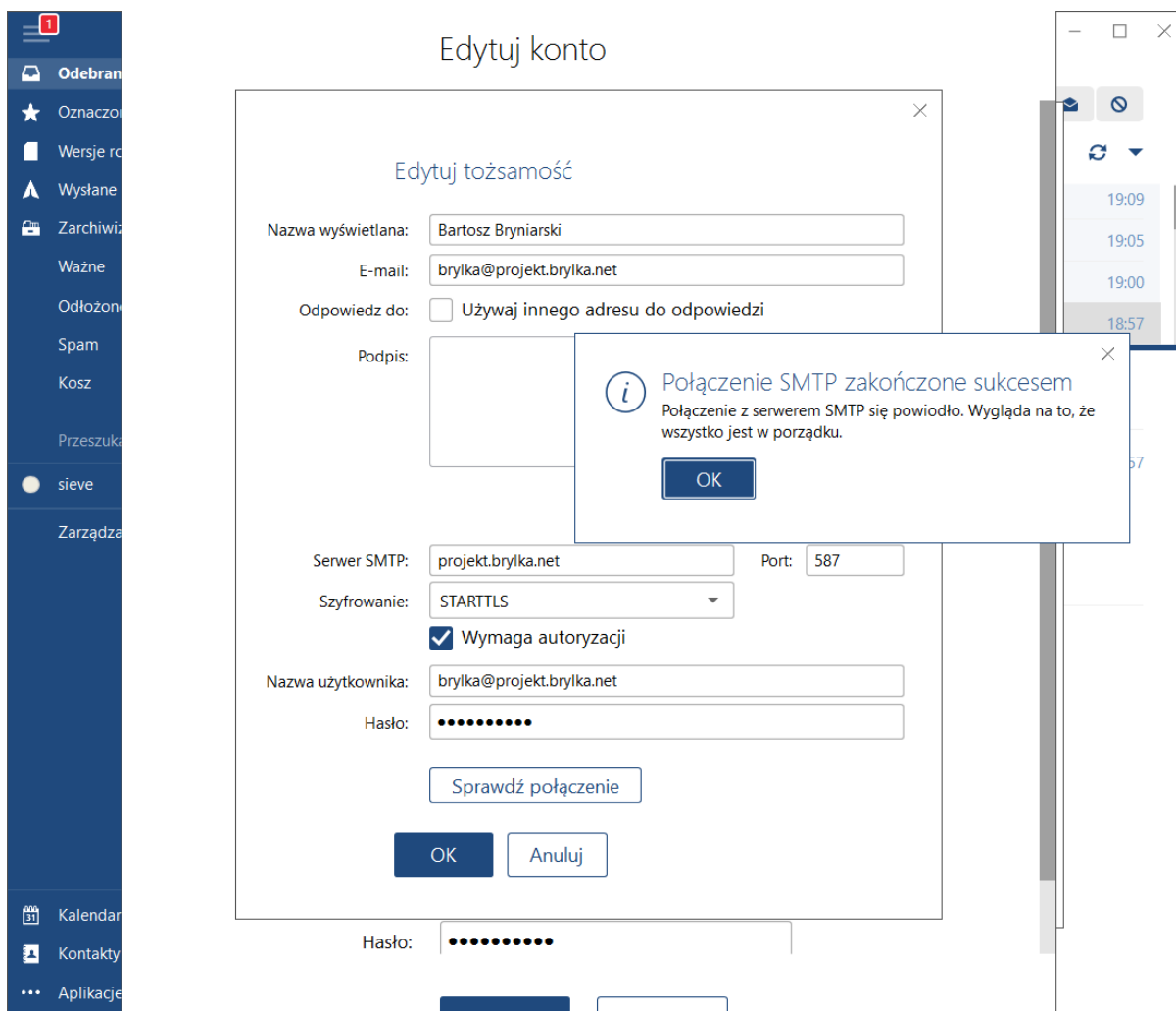
LookupServer 2565ms
```

[Feedback](#) [Contact](#) [Terms & Conditions](#) [Site Map](#) [API](#) [Privacy](#)

Your IP is: 176.114.238.102
Phone: (866)-MXTOOLBOX / (866)-698-6652 | feedback@mxtoolbox.com
© Copyright 2004-2021, MXToolBox, Inc. All rights reserved

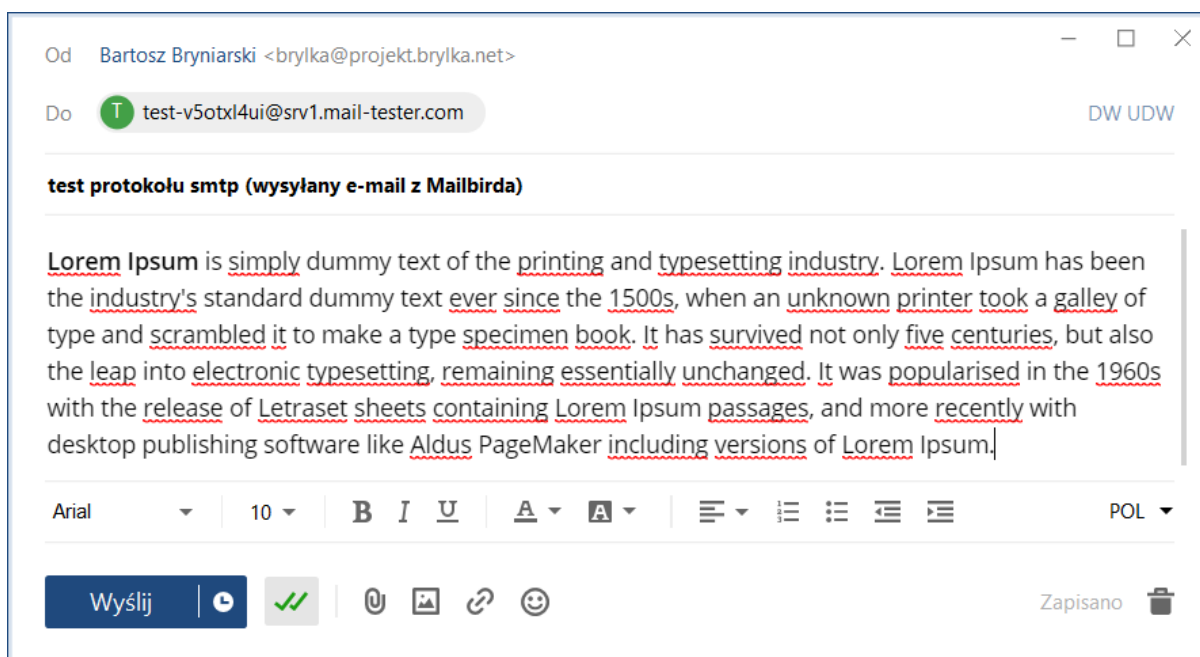
Rys 4.4.2: Test przy pomocy mxtoolbox wskazuje na poprawną konfigurację protokołu smtp.

Konfiguruję klienta pocztowego Mailbird do obsługi skrzynki pocztowej
brylka@projekt.brylka.net



Rys 4.4.3: Konfiguracja smtp w programie Mailbird.

Wysłałam e-maila testowego na serwer testujący wiadomości mail-tester.com.



Rys 4.4.4: Przygotowanie e-maila testowego do usługi mail-tester.com.

W logach serwera pocztowego widzimy odebranie wiadomości i kolejne fazy przekazywania jej przez różne procesy, aż do przekazania na serwer docelowy.

```
37.187.124.66 - PuTTY
Jun 11 22:45:20 projekt postfix/smtpd[2446]: connect from home.brylka.net[176.114.238.102]
Jun 11 22:45:20 projekt postfix/smtpd[2446]: DF7F918EF8: client=home.brylka.net[176.114.238.102], sasl_method=PLAIN, sasl_userna
me=brylka@projekt.brylka.net
Jun 11 22:45:21 projekt postfix/cleanup[2449]: DF7F918EF8: message-id=<Mailbird-11a6a7b8-0abb-4b1b-bf0f-3b99e4b0acca@projekt.bry
lka.net>
Jun 11 22:45:21 projekt postfix/qmgr[86003]: DF7F918EF8: from=<brylka@projekt.brylka.net>, size=4599, nrcpt=1 (queue active)
Jun 11 22:45:21 projekt postfix/smtpd[2446]: disconnect from home.brylka.net[176.114.238.102] ehlo=2 starttls=1 auth=1 mail=1 rc
pt=1 data=1 noop=1 commands=8
Jun 11 22:45:21 projekt dovecot[86020]: imap(brylka@projekt.brylka.net)<2426><mARkKIPeEwSwcu5m>: delete: box=Drafts, uid=8, msgi
d=<Mailbird-11a6a7b8-0abb-4b1b-bf0f-3b99e4b0acca@projekt.brylka.net>, size=2443
Jun 11 22:45:21 projekt dovecot[86020]: imap(brylka@projekt.brylka.net)<2426><mARkKIPeEwSwcu5m>: expunge: box=Drafts, uid=8, msg
id=<Mailbird-11a6a7b8-0abb-4b1b-bf0f-3b99e4b0acca@projekt.brylka.net>, size=2443
Jun 11 22:45:21 projekt postfix/smtpd[2452]: connect from localhost[127.0.0.1]
Jun 11 22:45:21 projekt postfix/smtpd[2452]: 61F5318EFB: client=localhost[127.0.0.1]
Jun 11 22:45:21 projekt postfix/cleanup[2449]: 61F5318EFB: message-id=<Mailbird-11a6a7b8-0abb-4b1b-bf0f-3b99e4b0acca@projekt.bry
lka.net>
Jun 11 22:45:21 projekt postfix/qmgr[86003]: 61F5318EFB: from=<brylka@projekt.brylka.net>, size=5018, nrcpt=1 (queue active)
Jun 11 22:45:21 projekt postfix/smtpd[2452]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5
Jun 11 22:45:21 projekt maiad[99750]: (99750-03) Passed CLEAN, [176.114.238.102] [176.114.238.102] <brylka@projekt.brylka.net> -
> <test-v5otxl4ui@srv1.mail-tester.com>, Message-ID: <Mailbird-11a6a7b8-0abb-4b1b-bf0f-3b99e4b0acca@projekt.brylka.net>, Hits: -,
386 ms
Jun 11 22:45:21 projekt maiad[99750]: (99750-03) Passed CLEAN, <brylka@projekt.brylka.net> -> <test-v5otxl4ui@srv1.mail-tester.c
om>, Hits: -, tag=999, tag2=999, kill=999, 0/0/0/0
Jun 11 22:45:21 projekt postfix/smtp[2450]: DF7F918EF8: to=<test-v5otxl4ui@srv1.mail-tester.com>, relay=127.0.0.1[127.0.0.1]:100
24, delay=0.71, delays=0.24/0.04/0.01/0.43, dsn=2.6.0, status=sent (250 2.6.0 Ok, id=99750-03, from MTA: 250 2.0.0 Ok: queued as
61F5318EFB)
Jun 11 22:45:21 projekt postfix/qmgr[86003]: DF7F918EF8: removed
Jun 11 22:45:21 projekt dovecot[86020]: imap-login: Login: user=<brylka@projekt.brylka.net>, method=PLAIN, rip=176.114.238.102,
lip=37.187.124.66, mpid=2455, TLS, session=<svIcIoPERgSwcu5m>
^C
root@projekt:~ #
[projekt] 0$ csh 1$ csh (2*$ csh) 3-$ csh 4$ csh 5$ csh 6$ csh [06/11/21 10:47 PM]
```

Rys 4.4.5: Logi serwera pocztowego.

Wyniki Spam Testu

mail-tester.com/test-v5otxl4ui

Twój e-mail jest prawie perfekcyjny

Wynik: **7.2/10**

Temat: test protokołu smtp (wysłany e-mail z Mailbirda) Otrzymano 0 minut/y temu

- ✓ Kliknij tutaj aby zobaczyć swoją wiadomość
- 1.3 SpamAssassin uważa, że powienes się poprawić
- 1 Nie jesteś w pełni uwierzytelniony

Sprawdzamy czy serwer, z którego wysyłasz jest uwierzytelniony.

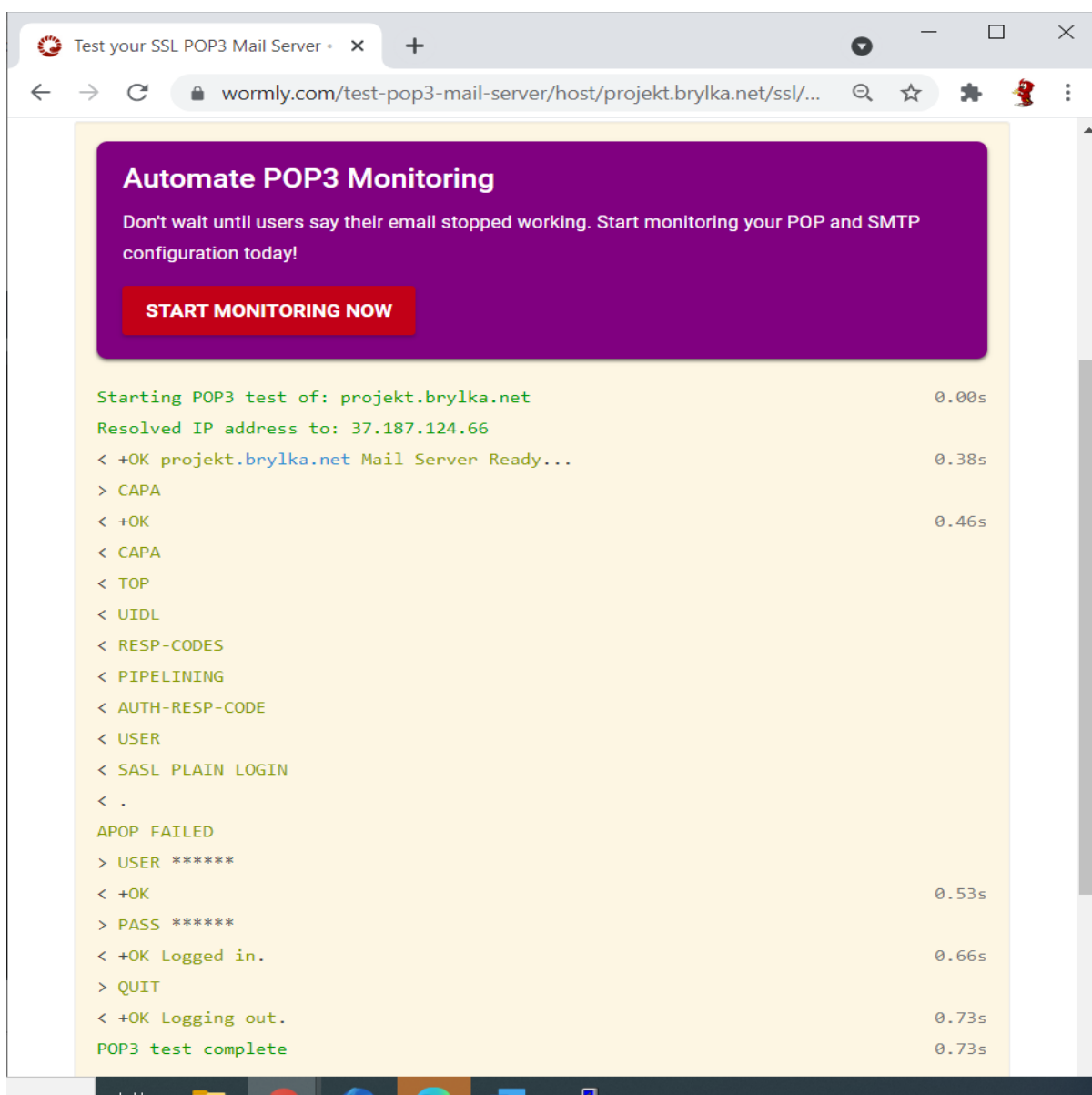
- ✓ [SPF] Serwer 37.187.124.66 jest upoważniony do używania brylka@projekt.brylka.net
- 1 Twoja wiadomość nie została podpisana kluczem DKIM
- ✓ Nie posiadasz rekordu DMARC
- ✓ Twój serwer 37.187.124.66 jest powiązany z projekt.brylka.net

Rys 4.4.6: Wynik mail-tester.com wskazuje na poprawną konfigurację.

Test wykonany przez mail-tester.com wskazuje, że konfiguracja protokołu SMTP jest poprawna. Kilka punktów zostało odjętych za zbyt skąpą treść wiadomości (regułka ApamAssassina), oraz niepełną autoryzację – brakuje DKIM i DMARC. Konfiguracja np. DMARCa jest trochę uciążliwa – niezbędna jest założenie skrzynki e-mailowej dla tej usługi gdzie inne serwery będą dostarczały wiadomości, oraz nasz serwer musi wysyłać co 24h wiadomości ze statystykami o otrzymywanych oraz blokowanych wiadomościach. Brak tych mechanizmów nie wpływa znacząco na dostarczanie e-maili, więc ich nie instalowałem i nie konfigurowałem.

4.5. TEST POP3

Przy pomocy narzędzia wormly.com sprawdziłem komunikację pop3, jest poprawna, można zalogować się na skrzynkę. Nie będę konfigurował programu pocztowego do obsługi pop3, zamiast tego protokołu skonfiguruję IMAP.

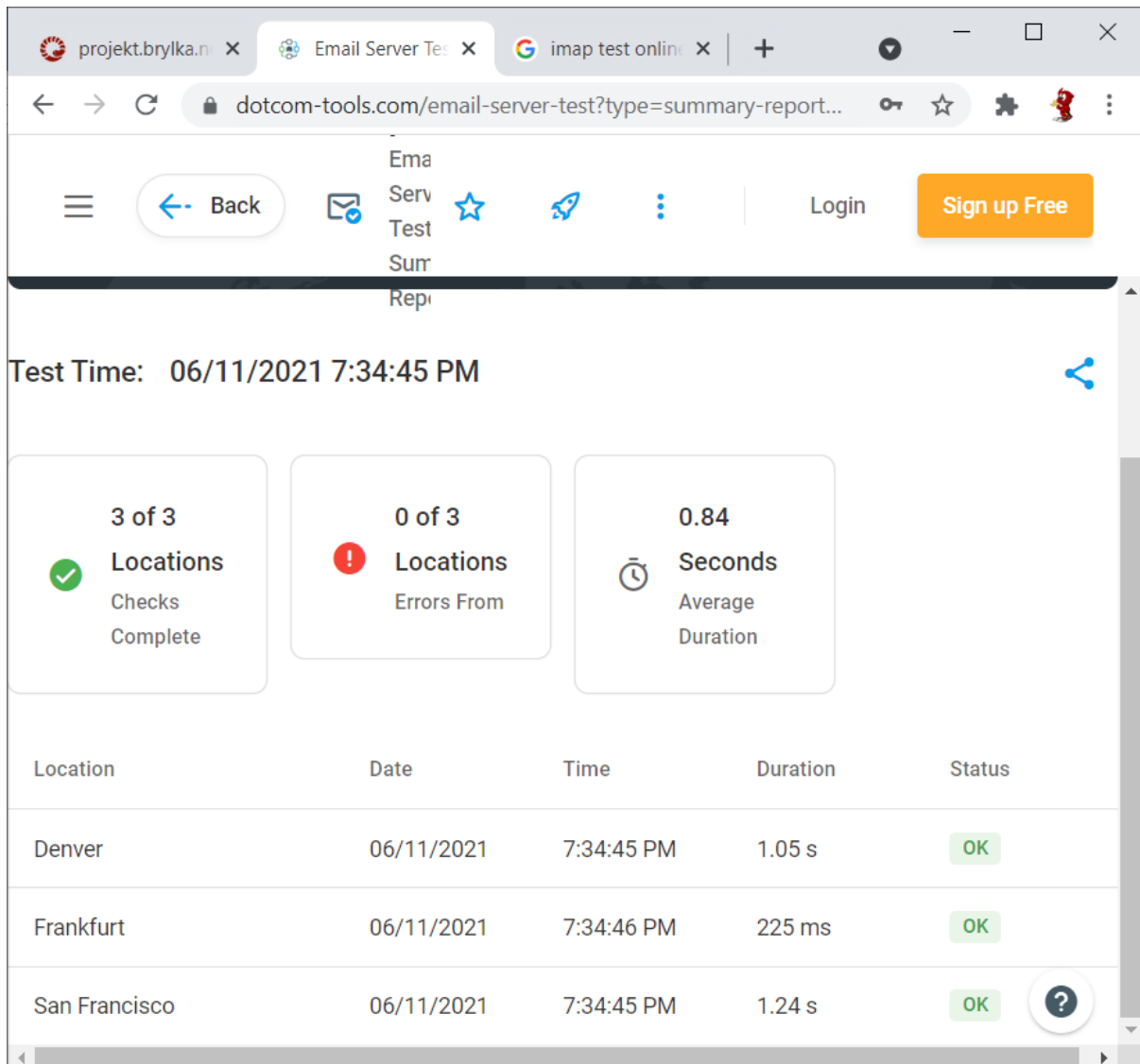


```
Starting POP3 test of: projekt.brylka.net 0.00s
Resolved IP address to: 37.187.124.66
< +OK projekt.brylka.net Mail Server Ready... 0.38s
> CAPA
< +OK 0.46s
< CAPA
< TOP
< UIDL
< RESP-CODES
< PIPELINING
< AUTH-RESP-CODE
< USER
< SASL PLAIN LOGIN
< .
APOP FAILED
> USER *****
< +OK 0.53s
> PASS *****
< +OK Logged in. 0.66s
> QUIT
< +OK Logging out. 0.73s
POP3 test complete 0.73s
```

Rys 4.5.1: Test protokołu pop3 przy pomocy wormly.com.

4.6. TEST IMAP

Przy pomocy narzędzia dotcom-tools.com sprawdziłem komunikację imap, jest poprawna, można zalogować się na skrzynkę.

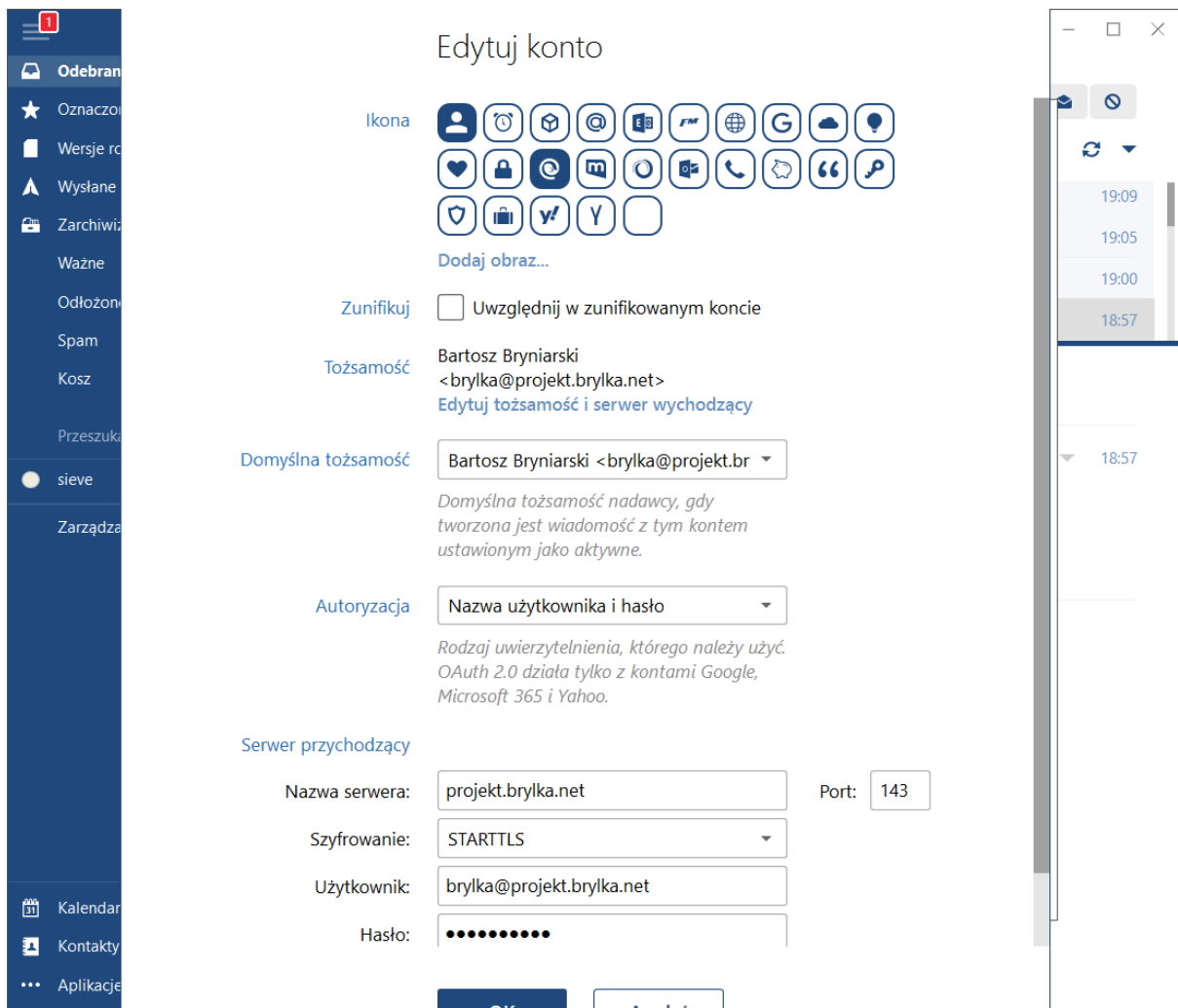


Test Time: 06/11/2021 7:34:45 PM

3 of 3 Locations Checks Complete	0 of 3 Locations Errors From	0.84 Seconds Average Duration		
Location	Date	Time	Duration	Status
Denver	06/11/2021	7:34:45 PM	1.05 s	OK
Frankfurt	06/11/2021	7:34:46 PM	225 ms	OK
San Francisco	06/11/2021	7:34:45 PM	1.24 s	OK

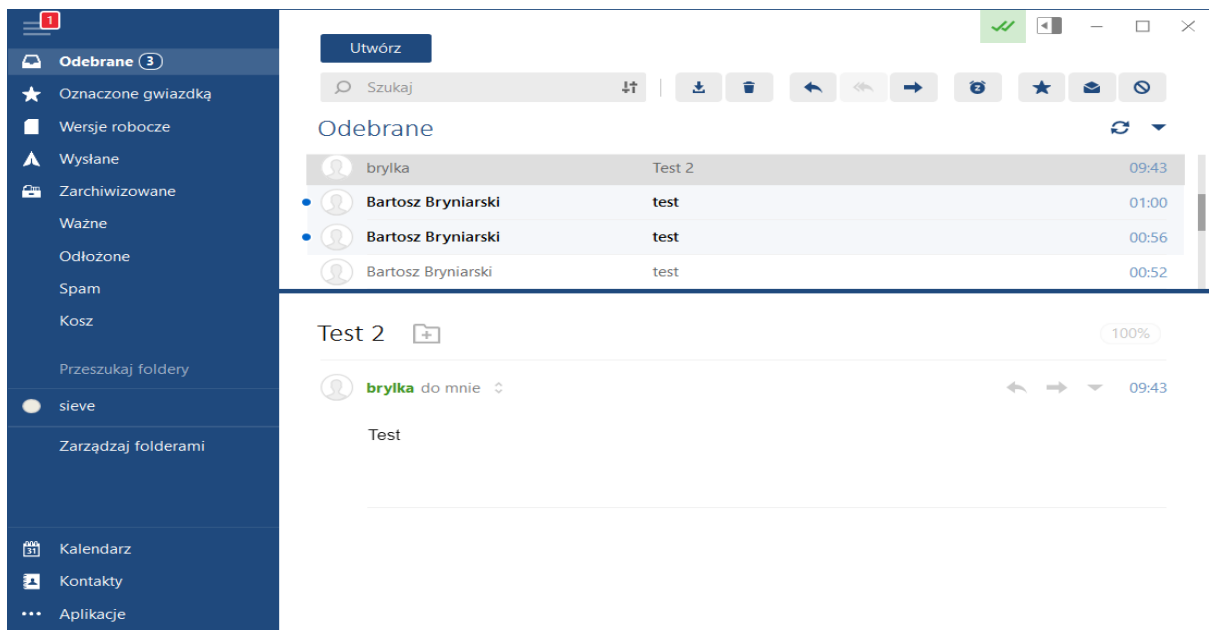
Rys 4.6.1: Test protokołu imap narzędziem dotcom-tools.com.

Konfiguruję program pocztowy Mailbird do obsługi konta pocztowego brylka@projekt.brylka.net

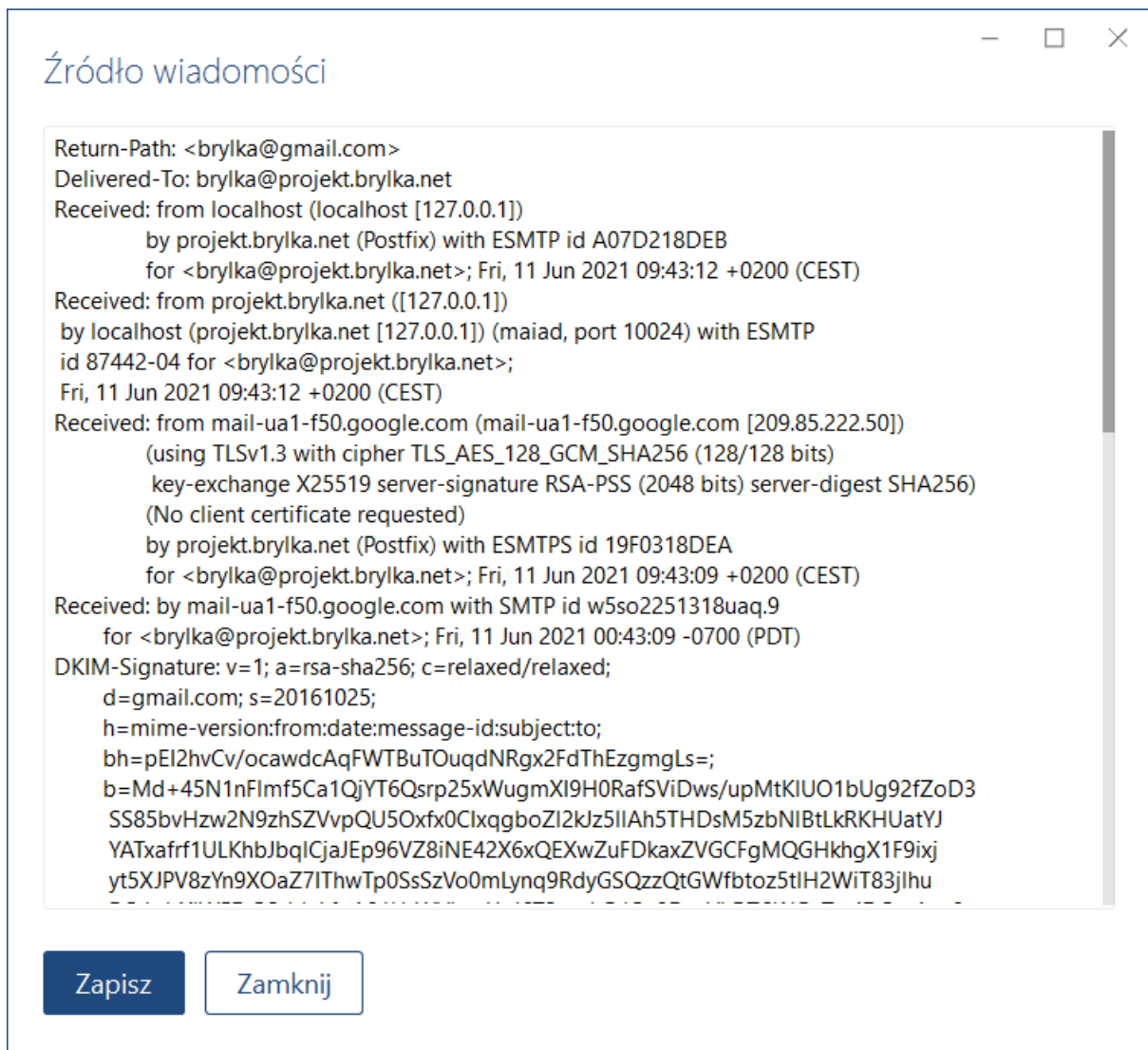


Rys 4.6.2: Konfiguracja imap w programie Mailbird.

Konfiguracja Mailbird do obsługi konta brylka@projekt.brylka.net jest poprawna co widać po wiadomościach, jakie zostały poprane z serwera przez protokół IMAP. Wysłłem kilka testowych wiadomości.



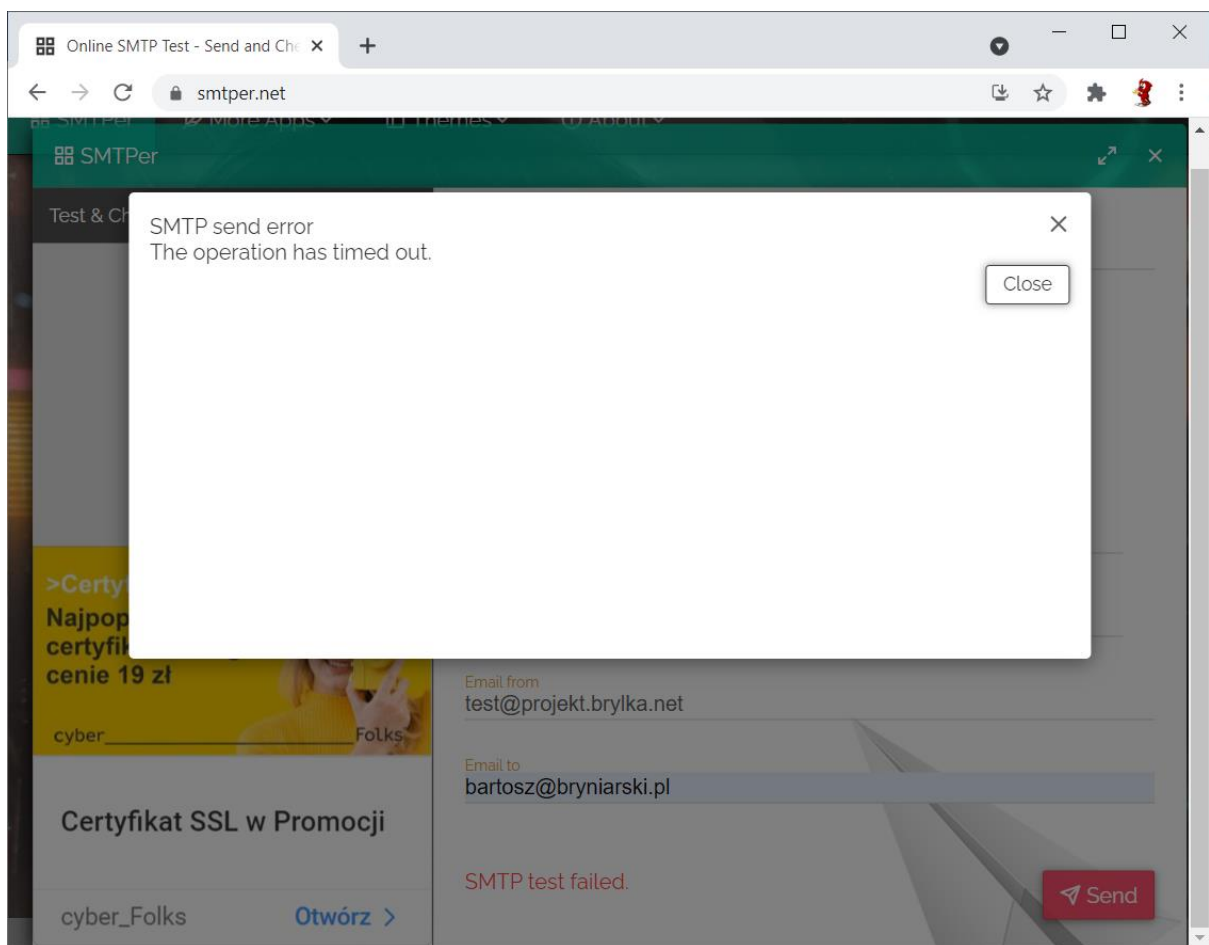
Rys 4.6.3: Skrzynka pocztowa obsługiwana przez IMAP.



Rys 4.6.4: Źródło wiadomości otrzymanej z serwera gmail.com.


```
37.187.124.66 - PuTTY
root@projekt:/usr/local/etc/fail2ban # fail2ban-client status postfix
Status for the jail: postfix
|- Filter
| |- Currently failed: 1
| |- Total failed: 4
| `-- File list: /var/log/maillog
`- Actions
   |- Currently banned: 1
   |- Total banned: 1
   `-- Banned IP list: 167.114.117.203
root@projekt:/usr/local/etc/fail2ban #
```

Rys 4.7.3: Status Fail2Ban dla postfixa z zablokowanym jednym adresem IP.



Rys 4.7.4: Kolejna próba wysłania e-maila zakończyła się niepowodzeniem – przekroczenie czasu.

5. PODSUMOWANIE

System pocztowy przy użyciu Postfixa oraz Dovecota został skonfigurowany poprawnie, co zostało potwierdzone testami. Konfiguracja usług pocztowych – protokołów SMTP oraz POP3/IMAP jest dosyć pracochłonna, szczególnie przez współdzielenie danych autoryzacyjnych użytkowników przez oba serwery. Dodatkowo serwer MTA ma sporo zadań do wykonania, od takich najprostszyc jak przesyłanie e-maili na inne serwery, czy już bardziej skomplikowaną jak autoryzację użytkowników, detekcję spamu, przeszukiwanie baz RBL, itp. Oba serwery (poczty wychodzącej i przychodzącej) w przedstawionej konfiguracji współpracują z bazą danych MySQL – ma to swoje zalety, np. administracja użytkownikami jest łatwiejsza (można edytować wpisy w bazie), w przypadku plików konfiguracyjnych, może wystąpić problem nadpisania danych. Do zarządzania użytkownikami systemu pocztowego użyłem narzędzia PostfixAdmin, dostępnego z poziomu strony www. Dla łatwiejszego użytkowania skrzynek pocztowych zainstalowałem Roundcube – aplikację z poziomu przeglądarki.

Aby w pełni skonfigurować system pocztowy należało by jeszcze doinstalować i skonfigurować kilka rzeczy, np.: mechanizmy DKIM oraz DMARC, GrayList, limitowanie poczty wychodzącej.

6. BIBLIOGRAFIA

1. Postfix Nowoczesny system przesyłania wiadomości. Ralf Hildebrandt Patrick Koetter, Helion 2006
2. Postfix Przewodnik encyklopedyczny. Kyle D. Dent, Helion 2004
3. Apache Przewodnik encyklopedyczny. Ben Laurie, Peter Laurie, Helion 2003
4. FreeBSD Podstawy administracji systemem. Michael M. Lucas, Helion 2009

Dokumentacja internetowa:

1. FreeBSD Handbook
<https://docs.freebsd.org/en/books/handbook/>
2. Postfix Documentation
<http://www.postfix.org/documentation.html>
3. Dovecot Manual
<https://doc.dovecot.org/>
4. OpenSSH Manual Page
<https://www.openssh.com/manual.html>
5. MySQL Documentation
<https://dev.mysql.com/doc/>
6. phpMyAdmin Documentation
<https://www.phpmyadmin.net/docs/>
7. Documentation: Apache HTTP Server
<https://httpd.apache.org/docs/>
8. Documentation Let's Encrypt
<https://letsencrypt.org/docs/>
9. roundcube/roundcubemail Wiki
<https://github.com/roundcube/roundcubemail/wiki>
10. Documentation Maia-Mailguard
<http://www.maiamailguard.com/docs.php>
11. PostfixAdmin Wiki
<https://sourceforge.net/p/postfixadmin/wiki/Home/>