**Project Fasten Your Seatbelts**

**Handleiding IPtables**

Klas: IN104

Groep: 4

Door: Sander de Jong

Inhoudsopgave

[Versiebeheer 3](#_Toc408259501)

[Inleiding 4](#_Toc408259502)

[Doel 4](#_Toc408259503)

[Voorbereidingen 5](#_Toc408259504)

[Software installeren 5](#_Toc408259505)

[Captive Portal uploaden naar de Raspberry 5](#_Toc408259506)

[Configureren 7](#_Toc408259507)

# Versiebeheer

|  |  |  |
| --- | --- | --- |
| **Naam** | **Versie:** | **Aangepast:** |
| Sander de Jong | 1 | Document aangemaakt |
| Sander de Jong | 2 | IPtable regel aangepast |

# Inleiding

Deze handleiding gaat er vanuit dat je een werkende Raspberry Pi Access Point hebt, mocht dit niet zo zijn verwijs ik naar de handleiding die gemaakt is door Ahish en Gian.

In dit document zullen we de Captive Portal die gemaakt is door Errol en Solaiman werkend krijgen op onze Raspberry Pi accesspoints.

## Doel

Wanneer we klaar zijn met dit document moet er een wifi netwerk aanwezig zijn, wanneer er met dit netwerk wordt verbonden zal er een webpagina worden geopend waar de gebruiker moet inloggen en algemene voorwaarden moet accepteren voordat er toegang naar het internet mogelijk is.

# Voorbereidingen

Voordat we iets kunnen moeten we eerst een aantal software pakketten installeren doe het volgende:

## Software installeren

*sudo apt-get update*

*sudo apt-get install openjdk-7-jre*

*sudo apt-get install tomcat7-docs tomcat7-admin*

*sudo apt-get install tomcat7*

Door de bovenste twee commado’s uit te voeren wordt alle software die we nodig hebben geïnstalleerd.

## Captive Portal uploaden naar de Raspberry

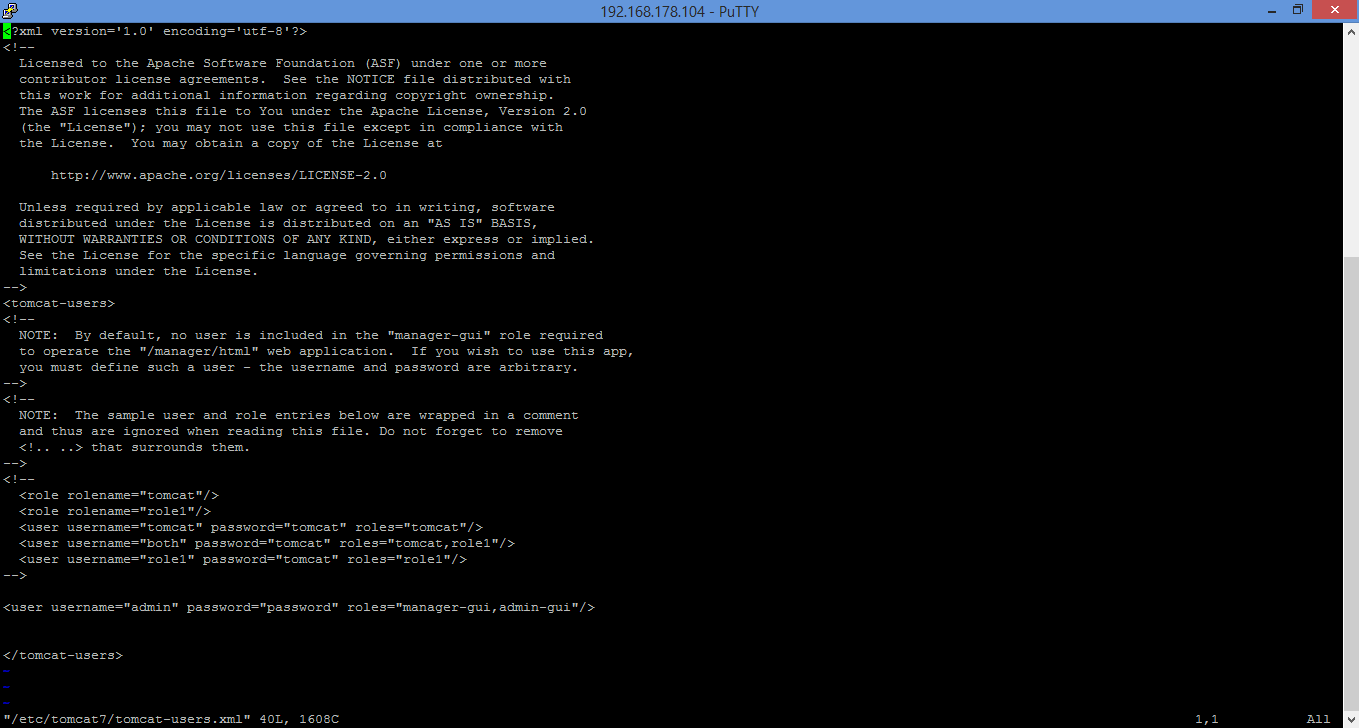
In Dropbox staat in de captive portal map een .war bestand. Dit bestand kunnen we uploaden in Tomcat, dit doen we via de manager.

Voordat we kunnen inloggen op de manager moeten we eerst een account aanmaken, een wachtwoord en rechten. Dit doen we met vim[[1]](#footnote-1) /etc/tomcat7/tomcat-users.xml

Hierin zetten we de volgende regel:

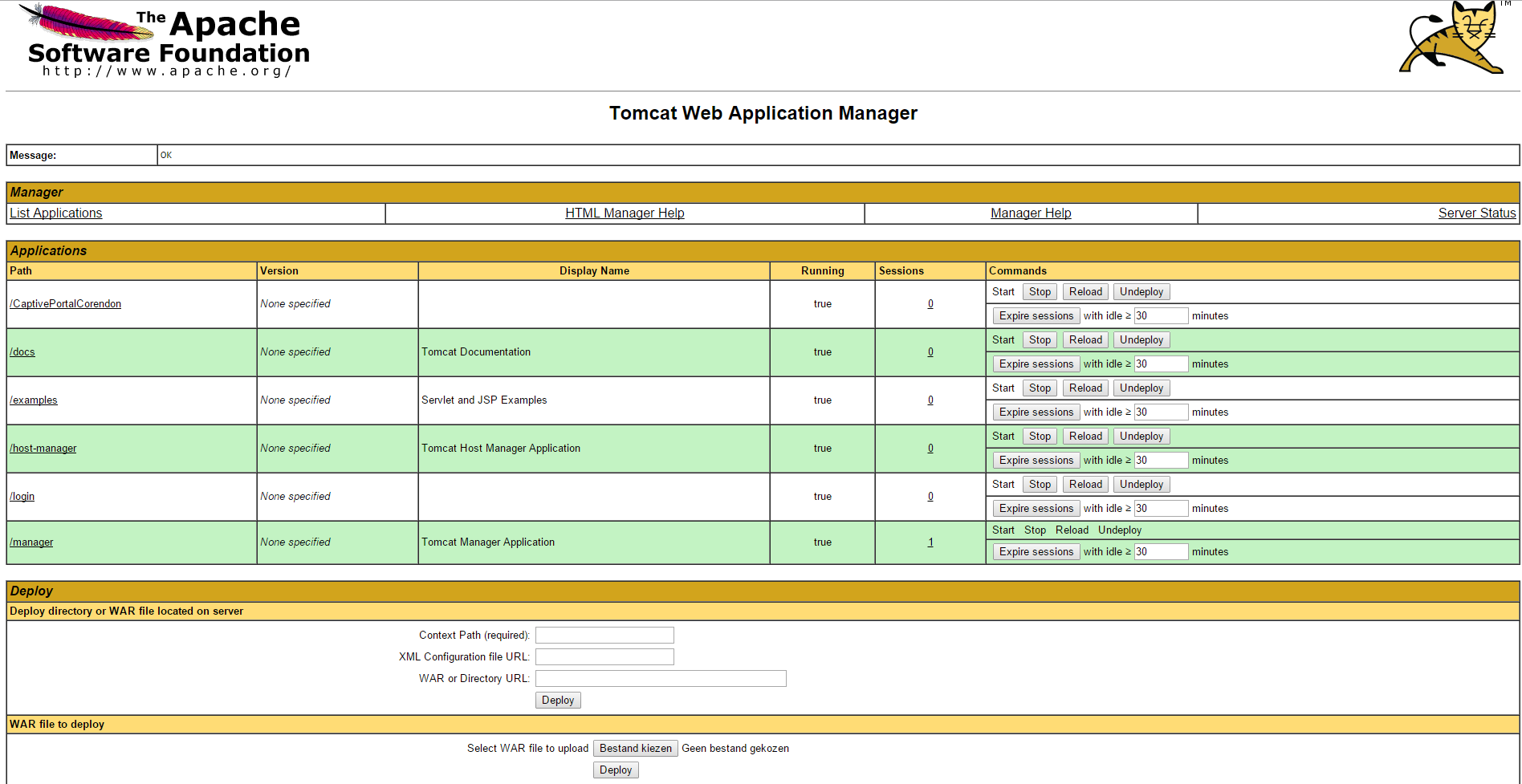
*<user username="admin" password="password" roles="manager-gui,admin-gui"/>*

Dit zorgt ervoor dat we kunnen inloggen met “admin” als gebruikersnaam en “password” als wachtwoord.



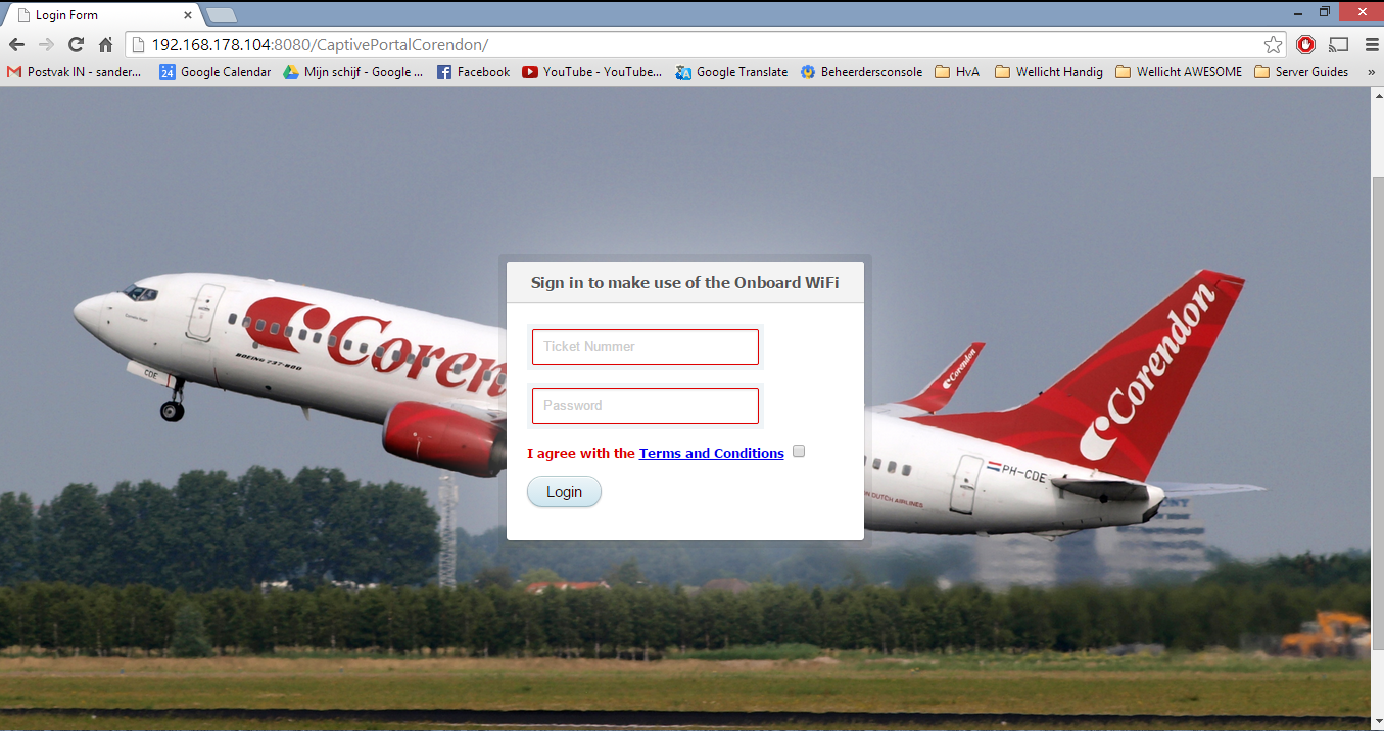
Afbeelding 20 – de inhoud van tomcat.xml

Nu we dit hebben gedaan kunnen we inloggen via de webbrowser. Ga naar <ip-adres>:8080/manager/, wanneer we hier heen gaat wordt er gevraagd om een gebruikersnaam en wachtwoord, dit is natuurlijk “admin” en “password”. Wanneer je hebt ingelogd kom op de volgende webpagina



Afbeelding 21 – Manager van Tomcat

In het midden van de webpagina staat: “Select WAR file to upload”, selecteer hier het .war bestand wat op dropbox staat en kies er voor om het te deployen. Nu is de captive portal beschikbaar via <ipadres>:8080/CaptivePortalCorendon.



Afbeelding 22 – De captive portal op de Raspberry

## Configureren

Nu we de captive portal kunnen benaderen vanaf de access point gaan we regels toevoegen zodat verkeer vanuit port 80(HTTP) en 443(HTTPS) wordt doorgestuurd naar de captive portal.

Eerst verplaatsen we de map CaptivePortalCorendon naar de ROOT map. Dit doen we door dit commando in te voeren:

*rm –r /var/lib/ROOT | Mv /var/lib/CaptivePortalCorendon /var/lib/ROOT*

Dit commando zal de huidige inhoud van ROOT verwijderen en de CaptivePortalCorendon map verplaatsen naar de map ROOT.

Vervolgens kunnen we de eerste iptable regels in de access point zetten. De eerste paar regels zullen er voor zorgen dat de access point al het netwerk verkeer zal weigeren behalve ssh verbindingen, dit is belangrijk om de access point te kunnen beheren

*iptables -A INPUT -p tcp --dport 22 -j ACCEPT*

*iptables -P INPUT DROP*

Vervolgens gaan we ervoor zorgen dat al het http en https verkeer wordt gerouteerd naar de captive portal, dit doen we met de volgende regels:

*iptables -A PREROUTING -t nat -p tcp --dport 80 -j REDIRECT --to-port 8080*

*iptables -A PREROUTING -t nat -p tcp --dport 443 -j REDIRECT --to-port 8443*

Beide iptable regels zijn hetzelfde, het enige wat verschilt is de destination port en de port waar het verkeer naar wordt doorgestuurd.

Dit zorgt er voor dat al het verkeer dat op weg is naar port 80/443 naar port 8080/8443wordt gestuurd van de access point.

1. Ik gebruik vrijwel altijd vi, nano kan natuurlijk ook. [↑](#footnote-ref-1)