# Raspberry pi xplore image

Dit is een readme van de basic image die werd geconfigureerd voor xplore group. Deze image heeft een Raspian stretch lite OS en werd geconfigureerd met de nodige programma’s en de nodige configuraties voor een Container image.

## Credentials

IP address: Deze word weergegeven tijdens de boot. Voor dat je u credentials moet invoeren.  
Gebruikersnaam : xplore  
Wachtwoord : kubernetes  
Default hostnaam: xploreGroup

# Prerequisites

## Te installeren software op host machine

* + <https://www.raspberrypi.org/downloads/>
  + <https://etcher.io/>
  + <https://www.putty.org/>
  + <https://sourceforge.net/projects/win32diskimager/>
  + 2 Bash scripts voor het automatiseren van de initialisatie en de beveiliging nadat je een ssh key hebt gegenereerd.
    - Init.sh
    - xplore

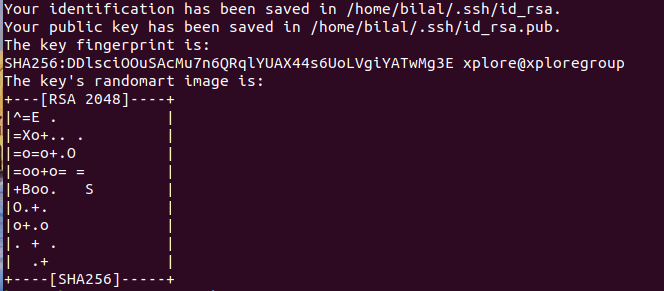
Voor de setup heb je de Rasbian stretch lite nodig die je vind in de downloads pagina van raspberry. Om deze rasbian stretch lite image te burnen op een sd kaart gebruik je etcher. Dit is een programma dat in Linux , macOS en windows kan draaien. Je selecteert je image en je sd kaart en etcher zal al het werk verichten van flashen tot burnen en unmounten van je sd kaart. Wanneer je via een windows host machine werkt en geen linux of mac kan je putty gebruiken om te connecteren via ssh. Voor het burnen van een gepersonaliseerde image voor xplore group gebruikte ik win32diskimager.

## SSH verbinding

SSH service staat default open voor alle pc’s voor de raspberri pi. Om keys aan te maken dat je kan inloggen zonder credentials mee te geven kan je ssh-keygen voor linux en mac en putty keygen voor windows gebruiken. De publieke keys moet je na het aanmaken kopieren naar de ~/.ssh/authorized\_keys file kopieren zodat de raspberry pi jouw pc als authorized kan instellen.

## SSH key aanmaken in linux

Met de commando *ssh-keygen -t rsa -C comment*(Geef als comment de naam van jouw pc of jou naam mee zodat je in de raspberry pi later de keys van de verschillende pc’s makkelijker kan achterhalen.)ga je de ssh keys genereren. Volg de instructies op het scherm. Je zal gevraagd worden om de keys op te slaan in een map naar keuze of de default home folder. Verder krijg je de vraag om een wachtwoord in te geven , deze dient om de private key te beveiligen.  
Bij een succesvolle creatie van een ssh key krijg je soortgelijk scherm te zien



Nu zal je de public key van je hostmachine moeten kopiëren om deze in je raspberri pi op te slaan en dat je raspberri pi jouw host machine als authorized host kan zien. Dit kan je doen met volgende commando:

*cat ~/.ssh/id\_rsa.pub | ssh* ***xplore@xploreGroup*** *'cat >> .ssh/authorized\_keys'*

Als je nu inlogt via ssh (met de commando ***ssh xplore@xploreGroup***) zal je direct ingelogd zijn zonder eerst de credentials in te moeten geven.

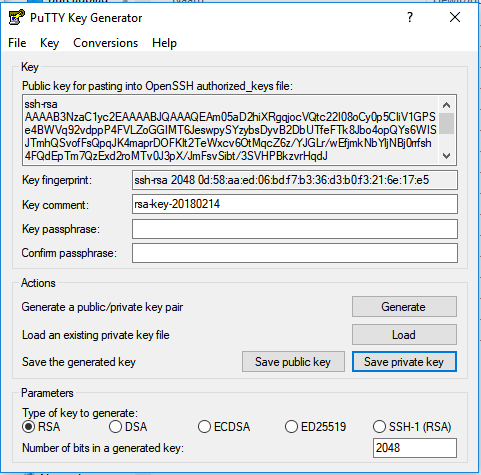
## SSH key in mac

Aangezien mac met dezelfde unix terminal werkt als linux zijn de commando’s identiek namelijk:

* *ssh-keygen -t rsa -C comment (Geef als comment de naam van je pc of jouw naam mee)*
* Stel hierna in waar de keys moeten worden opgeslagen
* Voor een extra beveiliging kan je een wachtwoord instellen op de private key. Dit is optioneel
* Ten slotte kopieer je de publieke key naar de raspberri pi *cat ~/.ssh/id\_rsa.pub | ssh* ***xplore@xploreGroup*** *'cat >> .ssh/authorized\_keys'*

## SSH key in windows

In Windows gebruik je niet de ssh keygen maar de Putty Key Generator.  
Daar kies je in het tabblad key voor de optie “SSH-2 RSA key” en klik je op Generate. Beweeg je muis over het lege grijze vlak zodat de keygenerator zijn werk kan uitvoeren en een random key kan genereren. Nadat putty een ssh key heeft uitgevoerd krijg je volgend scherm te zien. SLA ZEKER JE KEYS GOED OP. De private key en de public key sla je veilig op je host machine.

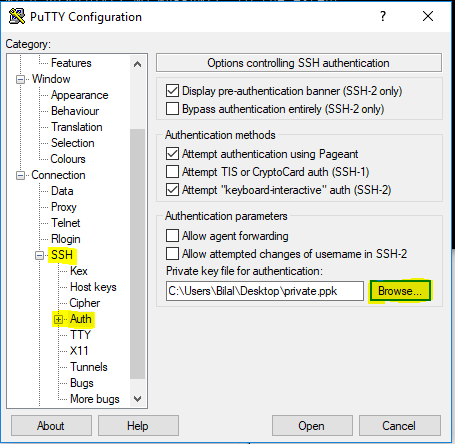


De bovenstaande key die je in het textvak kunt zien moet je kopieren en plakken in de authorized\_keys file van je raspberry pi(LET OP DE SCROLBAR, KOPIEER ZEKER ALLES MEEE). Hiervoor ga je in putty verbinden (TYP DIT NIET OVER KOPIEER) met de raspberry pi om naar volgende bestand te gaan ~/.ssh/authorized\_keys (Wanneer dit bestand niet bestaat maak je dit aan). Dit bestand kan al andere keys bevatten van andere pc’s je plakt hierin de publiek key van jouw pc op een nieuwe lijn(in Putty kan je plakken vanuit je windows klembord met de shortkey *shift+insert).* Sla het bestand ~/.ssh/authorized\_keys op en sluit de editor.

## Verbinden met de raspberry vanuit windows host.

Wanneer je nu wilt verbinden met de Raspberry pi via putty ga je de private key meegeven in putty dit doe je door in putty het volgende in te stellen.

Bij opstart van putty kies je in het linkerscherm voor -->SSH-->Auth daar zie je de Browse knop moet je de private key aanduiden die je daarnet in de Putty Key Generator hebt opgeslagen.



Wanneer je nu verbind met je raspberry zal je geen passwoord vraag meer krijgen. Je kan zelf de default gebruikersnaam instellen. Door in het tabblad Connection--> Date de auto-login username in te stellen. Zo zal je bij je volgende sessie direct verbonden zijn met je raspberry pi. Vergeet zeker niet om deze instellingen in putty op te slaan zodat je niet steeds de keys en de default gebruikersnaam moet meegeven.

## Extra beveiliging

Om je beveiliging te verbeteren ga je het wachtwoord uitschakelen nadat je verbonden bent met je ssh zodat enkel de pc’s die verbonden zijn met de ssh key kunnen verbinden. Er zijn hiervoor 3 lijnen in het configuratie bestand dat je hiervoor moet aanpassen.

Config file : /etc/ssh/sshd\_config

* ChallengeResponseAuthentication no
* PasswordAuthentication no
* UsePAM no

Sla zeker de veranderingen op. Restart de ssh service nadat je het bestand hebt opgeslagen zodat de veranderingen toegepast worden.

### *Automatiseren van de extra beveiliging*

In de home folder zit er een bash script “xplore”. Dit bash script zal de 3 lijnen die nodig zijn voor het wachtwoord uit te schakelen voor zijn werk nemen. Het heeft 2 parameters genaamd lock en unlock. Lock zal de configuratie gegevens veranderen zodat je wachtwoord wordt uitgeschakeld. Je kan deze terugzetten naar default instellingen door de parameter unlock mee te geven. Zie wel dat je deze bash script met sudo runt aangezien je bezig bent in de /etc/ folder en het de service ssh opnieuw opstart.

Sudo verplichten om

### Wees altijd up-to-date

Wanneer je er een gewoonte van maakt om je raspberry op een regelmatige basis te updaten zorg je er ook voor dat je de nodige beveiliging fixes van linux meekrijgt. Voor linux zijn hiervoor 3 commando’s voorzien.

* Sudo apt-get update
* Sudo apt-get upgrade
* Sudo apt-get dis-upgrade

Omdat deze 3 commando’s op een regelmatige basis moeten worden uitgevoerd is er hiervoor een bash script “update” voorzien in de home folder. Dit script bevat de 3 commando’s om je systeem up te daten en kan op een latere tijdstip altijd worden aangevuld of worden aangepast om de update te vervolledigen.

## Programma’s die extra geinstalleerd zijn

* Vim
* Docker
  + installeren
    - curl -sSL get.docker.com | sh
  + toevoegen aan groep via usermod
    - sudo usermod -aG xplore docker
* Swap uitschakelen
  + De reden waarom we swap uitschakelen is omdat we kubernetes gaan gebruiken en kubernetes niet gemaakt is om de swap geheugen te gaan gebruiken. Dit zorgt voor problemen waardoor het nodig is swap uit te schakelen in een linux omgeving
* Control groups of Cgroups
  + Cgroups zorgen voor het managen van resources zoals CPU , system memory(RAM) , netwerk bandwith of een combinatie van deze resources.
  + Cgroups in kubernetes
  + Met Cgroups kan je instellen hoeveel cpu en hoeveel Ram geheugen elke container/ node nodig ga hebben. Hiervoor moet je dit wel aanzetten in het boot bestand
* Kubernetes
  + Aangezien kubeadm op elke node word geinstalleerd is het handig dat dit al is gebeurt in de basic os
    - apt-get install -y kubeadm
  + Het initialiseren van de master en de nodes gaan we later instellen want dit gebeurt nadat je de basic image hebt opgestart zodat je onderscheid kan maken van een master en van een node

## Initialiseren

IP address tonen in boot menu

Dit word al default gedaan , de code die hiervoor word gebruikt   
 staat in de file /etc/rc.local

Automatisatie initialiseren van image (init.sh)

* Installeren van vim
* Ssh verbinding automatisch inschakelen
* Aanmaken van ssh folder in home folder en de nodige permissies geven
* User toevoegen aan sudo group
* Initialiseren van kubernetes via een bash script dat het volgende gaat uitvoeren
  + - Installeren van docker
    - Swap uitschakelen
    - Cgroup gegevens aanpassen in boot config
    - Download kubeadm repo en toevoegen aan repo lijst
    - Updaten van repo list
    - Installeren van kubeadm

## What did i do ?

* Rasbian stretch lite burnen op sd kaart
  + De reden dat ik Rasbian lite heb gebruikt is omdat dit de ideale os is voor een server omgeving. Bij de gewone Rasbian zijn er te veel utilities die we zowiezo niet nodig hebben. De rasbian heeft ook standaard een gui geinstalleerd ookal kan je instellen om te booten in de cli omgeving. Al deze benodigdheden die we niet nodig hebben zijn al weggehaald door Raspberry zelf in een mooie gui loze omgeving: Rasbian lite.
* Default credentials
  + Gebruikersnaam : pi
  + Wachtwoord : raspberry
  + **//opgelet default keyboard is qwerty//**
    - Dit verander je in de config menu , zie verder hoe je dit doet.
* Verander de gebruikersnaam en wachtwoord
  + Gebruikersnaam: ***xplore***
  + Wachwoord: ***kubernetes***

In linux kan je de gebruikersnaam niet veranderen als je ingelogd bent met deze gebruikersnaam. Daarom zal je even moeten inloggen als de root gebruiker.

1. Om dit te doen activeer je de root gebruiker. Geef de gebruiker een passwoord door het commando “sudo passwd root” in te geven.
2. Volg vervolgens de instructies op het scherm.
3. Nadat je alles succesvol hebt uitgevoerd ga je uitloggen uit de gebruiker pi dit doe je met de commando “logout”.
4. Je logt terug in als de gebruiker root door de credentials gebruikersnaam “root” en ww die je net hebt ingesteld in te geven.
5. Met de commando “usermod -l nieweNaam pi” zal je een nieuwe naam geven aan de pi user.
6. In linux voldoet het niet om de naam van de gebruiker alleen te veranderen je zal de naam van de home directory ook moeten aanpassen.
7. Dit doe je met de commando “usermod -m -d /home/nieweNaam nieuweNaam”.

Nu kan je inloggen met de nieuwe gebruikersnaam. Weet dat je nog steeds de default wachtwoord raspberry gebruikt.

1. Deze pas je aan door de commando “passwd” toe te passen en de instructies op het scherm te volgen.
2. Nu kan je de root gebruiker terug uitschakelen.

Kijk ZEKER na of je nieuwe gebruiker nog steeds administrator rechten heeft door een sudo commando uit te voeren

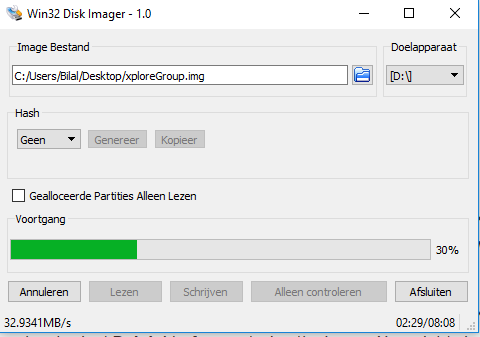
* Configuratie scherm (sudo raspi-config)
  + Veranderen van keyboard layout
    - Localisation options
    - Change keyboard Layout
  + Verander hostname
    - Nieuwe hostname: ***xploreGroup***
      * Network options
      * Change hostname
* 2 Bashscriptjes die het initialiseren en de security automatiseren
  + - Voor portable redenen beginnen deze scriptjes met #!/usr/bin/env bash
* **SCRIPT1**:init.sh
* Rasbian lite volledig updaten
  + Apt-get update #alle mogelijke updates ophalen
  + Apt-get upgrade #upgraden van de huidige packages
  + Apt -get dist-upgrade #installeren van de nieuwe updates
* Vim installeren
* SSH folder aanmaken en authorized keys file aanmaken
* Xplore toevoegen aan sudo group
* Zet ssh verbinding op auto start
* ssh folder in home folder voor de authorized keys in op te slaan
* ssh verbinding key’s opzetten (dit gebeurt niet op de rasberry pi maar in de host)
* **SCRIPT2**: xplore
* Extra beveiliging , wachtwoorden uitschakelen nadat je bent ingelogd met een ssh key. Hiervoor is er een bash script ter beschikking gesteld. Zodat je na het inloggen je pc kan “locken” en de wachtwoorden authenticatie uit zet. Met de parameter lock mee te geven aan dit script zal je de raspberry in lock modus plaatsen , unlocken gebeurt wanneer je de parameter unlock meegeeft.
* Ter info: Root login uitschakelen via ssh

Als extra beveiliging is het zeker van belang dat je niet kan inloggen met root in je ssh. Deze zit er default in. Wanneer je dit toch wilt instellen wat niet aangeraden word moet je de lijn PermitRootLogin veranderen naar yes. Dan zal je met root kunnen inloggen. Aangezien deze lijn niet in de default configuratie zit word er dit default uitgeschakeld

* + - De configuratie gebeurt in de config file van ssh
    - /etc/ssh/sshd\_config

Image clonen/backuppen

Via het programma “Win32 Disk imager” (zie “te installeren software”)

In het zoekveld zoek je de image waar je het naar zal schrijven zorg er zeker voor dat de schijfletter rechtsboven klopt met de schijfletter van de sd kaart. Klik vervolgens op “Lezen” en het programma zal je sd kaart clonen naar een image bestand.  


## Extra veiligheidsopties voor betere security (optioneel) *DEZE ZITTEN NIET IN DE BASIC IMAGE*

### Ervoor zorgen dat sudo steeds een wachtwoord vraagt

Wanneer je sudo gebruikt ben je een superuser en default heb je hiervoor geen wachtwoord voor nodig. Dit is voor normale gebruik en gemak geen probleem. Maar dit word een probleem wanneer een onbevoegd persoon toegang krijgt tot jouw systeem. Om dit te vermijden kan je ervoor zorgen dat je bij elke keer dat je sudo gaat intypen er een wachtwoord word aangevraagd. Dit doe je door in het bestand */etc/sudoers.d/0.10\_pi-nopasswd* het volgende aan te passen.

**xplore** ALL=(ALL) PASSWD:ALL  
  
Sla dit bestand op , en bij de volgende login / boot zal je de veranderingen waarnemen.

### Firewall installeren

Dit zit niet in de basic image omdat een firewall niet voor elke node en voor de master hetzelfde moet zijn. De firewall moet worden toegepast om een globale methode.

Hoe we de firewall gaan instellen voor de gehele cluster ***AANVULLEN TIJDENS HET CREEEREN VAN DE CLUSTE zie hiervoor link in bronnenlijst***

### Installeren van fail2ban

Dit is een optie nadat je de firewall hebt ingesteld. Omdat je u Pi gebruikt als een server en deze toegankelijk is voor mensen die ermee verbinden met ssh hebben gebruikers toegang aan de Pi. Fail2ban is een scanner dat de log files gaat bekijken en nakijken op ongewone activiteiten. Het zal aangeven wanneer er bijvoorbeeld meerdere brute force pogingen hebben plaats gevonden om in te loggen in je pi. En heeft zelf de mogelijkheid om elke firewall die is ingesteld in te stellen dat bepaalde ip-addressen niet meer mogen inloggen. Dit is een automatische tool dat word aangeboden zodat de gebruiker niet steeds de log bestanden moet bekijken voor ongewone aanmeldingen. Het grijpt ook in na een ongewone situatie zodat jij dit zelf niet manueel meer hoeft te doen.

***ZIE BRON HOE JE DIT INSTELT/ INSTALLEERT. AANVULLEN TIJDENS HET CREEEREN VAN DE CLUSTER OM DAN NADAT JE DE FIREWALL HEBT INGESTELD DE FAIL2BIN , IN TE STELLEN.***

Bronnenlijst

* installeren van raspberry os en clonen van os in windows

<https://www.makeuseof.com/tag/install-operating-system-raspberry-pi/>

<https://www.raspberrypi.org/magpi/pi-sd-etcher/>

* ssh keys instellen via putty en putty key gen

<https://devops.profitbricks.com/tutorials/use-ssh-keys-with-putty-on-windows/>  
<https://www.raspberrypi.org/forums/viewtopic.php?f=36&t=181846>  
<https://www.ssh.com/ssh/putty/windows/puttygen>

* disable password login bash script

<https://www.cyberciti.biz/faq/how-to-disable-ssh-password-login-on-linux/>  
<http://support.hostgator.com/articles/specialized-help/technical/how-to-disable-password-authentication-for-ssh>  
<https://stackoverflow.com/questions/20898384/ssh-disable-password-authentication>  
<https://lani78.com/2008/08/08/generate-a-ssh-key-and-disable-password-authentication-on-ubuntu-server/>

* Initialisatie script

<https://kubecloud.io/setup-a-kubernetes-1-9-0-raspberry-pi-cluster-on-raspbian-using-kubeadm-f8b3b85bc2d1>  
<https://stackoverflow.com/questions/21612980/why-is-usr-bin-env-bash-superior-to-bin-bash>

* Beveiliging van de raspberry pi

<https://www.raspberrypi.org/documentation/configuration/security.md>