[Hiren Sathwara and Harpalsinh Gohil]

[V 1.0]| [2020-10-09]



Apache Reverse Proxy Operation Guide



Document Management Information

|  |  |
| --- | --- |
| **Site** | <xxx> |
| **Document Code** |  |
| **Title** | Apache Reverse Proxy Operation Guide |
| **Zodiac Version** |  |
| **Security** | *Confidential* |
| **Owner** | <Team> / <Team Member Name> |
| **Type** | Word |
| **Published (in Repository)** |  |
| **Added to Repository Date** | 2020-10-09 |
| **Retention Period** |  |

Version Controls

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Prepared By** | **Reviewed By** | **Change Description** |
| <v.1.0> | 2020-10-09 | Hiren Sathwara, Harpalsinh Gohil |  |  |
|  |  |  |  |  |
|  |  |
|  |  |
|  |  |

Contents

[0. Introduction 3](#_Toc53153323)

[0.1. Concept and Requirement of Apache Reverse Proxy 3](#_Toc53153324)

[0.2. Prerequisites 3](#_Toc53153325)

[1. REVERSE PROXY CONFIGURATION 4](#_Toc53153326)

[1.1. CREATE REVERSE PROXY IN DOCKER CONTAINER 4](#_Toc53153327)

[2. CREATE SELF SIGN CERTIFICATE 7](#_Toc53153328)

[2.1. Create RSA Key Pair 7](#_Toc53153329)

[2.2. Extract Private Key into “httpd” folder 7](#_Toc53153330)

[2.3. Creating a “Certificate Signing Request” or CSR file 7](#_Toc53153331)

[2.4. Creating the Certificate .crt file 8](#_Toc53153332)

[2.5. Configure Apache file to use Self Signed Certificate 8](#_Toc53153333)

[3. Troubleshooting 10](#_Toc53153334)

[3.1. Restart Apache reverse Proxy 10](#_Toc53153335)

[3.2. How to Check Reverse Proxy Container Log? 10](#_Toc53153336)

[3.3. Auto Start Container After Reboot 10](#_Toc53153337)

[3.4. Replace existing Certificate 10](#_Toc53153338)

[3.5. 502 Error in Reverse Proxy 11](#_Toc53153339)

[3.6. Reverse Proxy show 503 service Unavailable error 11](#_Toc53153340)

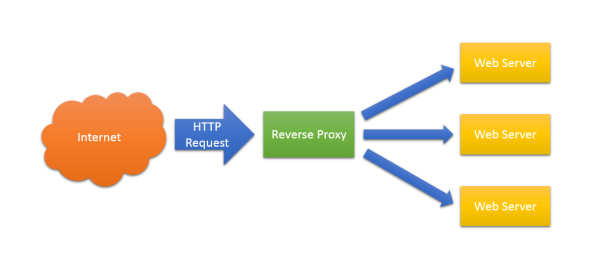
[3.7. Check Reverse Proxy Container status 11](#_Toc53153341)

# Introduction

This Operation Guide contains step-by-step configuration and troubleshooting of Apache Reverse Proxy. It will help support team to setup Apache Reverse Proxy.

## Concept and Requirement of Apache Reverse Proxy

* A reverse proxy is a server that act as a mediator in front of web servers and forwards client (e.g. web browser) requests to backend web or application servers. Reverse proxies are typically implemented to help increase security, performance, and reliability
* We have multiple Zodiac Application server, to distribute traffic for Zodiac application from the client, we require Apache Reverse Proxy Server



## Prerequisites

* Linux base machine with apache role and proxy module
* Reverse Proxy Rules
* SSL certificate [Self signed or Domain Base]
* Docker module
* DNS Name Resolution

# REVERSE PROXY CONFIGURATION

## CREATE REVERSE PROXY IN DOCKER CONTAINER

* Pull the container image from internet

# docker pull httpd:latest

* To verify httpd images use below docker images command.

# docker images   


* Create httpd folder in /opt/zodiac/local/

# mkdir httpd

* Create logs folder in /opt/zodiac/local/

# mkdir logs

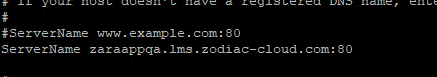
* Copy conf folder local machine to docker machine using tool like WINSCP
* Stop existing container running in 80 and 443 port if any

# docker container stop <container ID>

* After Upload the conf folder access httpd.conf file and changes the server Name.

# vi /opt/zodiac/local/httpd/conf/httpd.conf

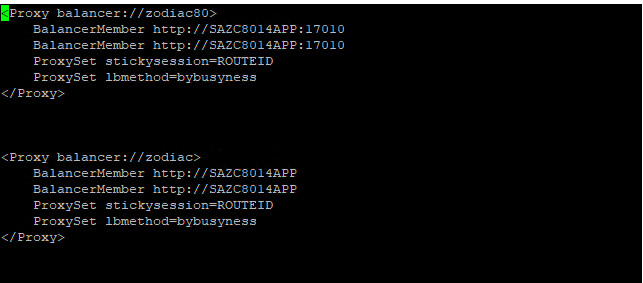
* Change the server Name



* After changes in httpd.conf Save file and exit
* Go to the /opt/zodiac/local/httpd/conf/extra folder and change the Proxy rule

# vi /opt/zodiac/local/httpd/conf/extra/httpd-proxy-zodiac.conf

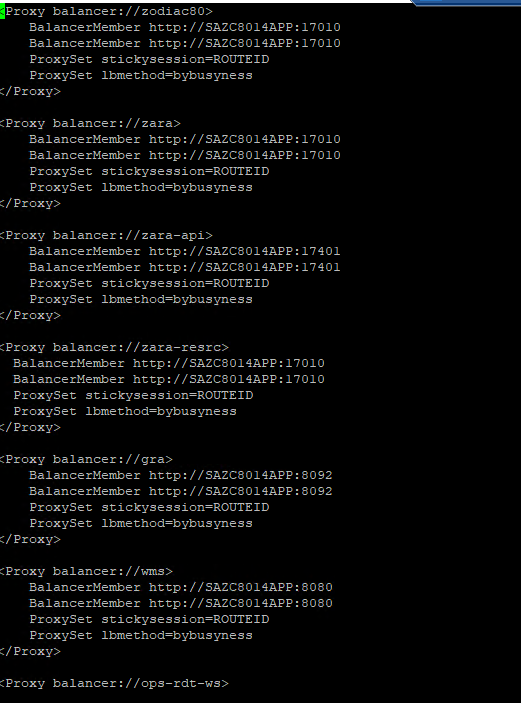
Note:- Change Server Name as per our service running .like <Zodiac, OPS>



* After changes in httpd-proxy-zodiac.conf Save file and exit
* Go to the /opt/zodiac/local/httpd/conf/extra folder and change the httpd-ssl-proxy-zodiac.conf file

# vi /opt/zodiac/local/httpd/conf/extra/ httpd-ssl-proxy-zodiac.conf

Note:- Change Server Name as per our service running .like <Zodiac, OPS>



* After changes in httpd-ssl-proxy-zodiac.conf Save file and exit
* Use below command to start httpd container and map httpd and logs folder

# docker run –td –p 80:80 –p 443:443

–v /opt/zodiac/local/httpd/conf:/usr/local/apache2/conf/:Z

–v /opt/zodiac/local/httpd/logs:/usr/local/apache2/logs/:Z httpd

Note:-

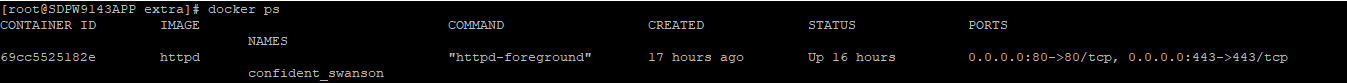
-p for using Port number

-v for using Bind or map the folder in docker container

Z for using bind selinux context in docker container

* After run this command verify container running using docker ps command

# docker ps



**Note:- If you need to change in http configuration, you need to change in local httpd.conf file (/opt/zodiac/local/httpd/) and restart the container using below command.**

# docker container restart <container ID>

# CREATE SELF SIGN CERTIFICATE

# Create RSA Key Pair

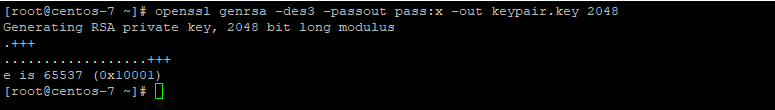
* First step to use openssl package on Linux/Centos to create RSA Key pair. To do this you need to make sure SSL package install, if not then install using below command

# yum install openssl

* Once you verify or install openssl package, generate keypair using below command

# openssl genrsa -des3 -passout pass:x -out keypair.key 2048

This command uses 2048 bit encryption and output as file keypair.key as below output. Key file place on current working directory.



## Extract Private Key into “httpd” folder

* Copy keypair.key file to /opt/zodiac/local/httpd/conf/ file location. All ssl certificate will store in same location
* Extract private key from keypair.key file using below command

# openssl rsa -passin pass:x -in keypair.key -out /opt/zodiac/local/httpd/conf/selfsrv.key

Note:- Selfsrv.key file is your private key file you can use any name. After private key file generated remove keypair.key file

# rm keypair.key

## Creating a “Certificate Signing Request” or CSR file

* Create certificate signing request to submit “Certificate Authority” using below command

# openssl req -new -key /opt/zodiac/local/httpd/conf/selfsrv.key -out /opt/zodiac/local/httpd/conf/selfsrv.csr

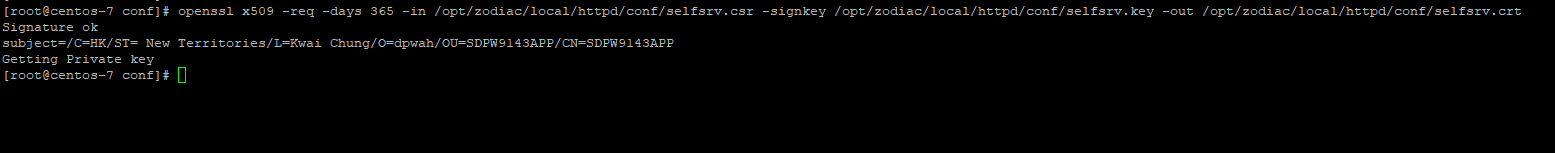
You need to give some details as like Country Code, State, Locality or City, Organization Name, Organizational Unit, Common Name and Email Address.



## Creating the Certificate .crt file

* Create Certificate file using csr and key file

# openssl x509 -req -days 365 -in /opt/zodiac/local/httpd/conf/selfsrv.csr -signkey /opt/zodiac/local/httpd/conf/selfsrv.key -out /opt/zodiac/local/httpd/conf/selfsrv.crt



* You will find 3 files selfsrv.key, selfsrv.csr and selfsrv.crt file in given location /opt/zodiac/local/httpd/conf/

## Configure Apache file to use Self Signed Certificate

* Once all file generated you need to change file path from default value in of SSLCertificateFile and SSLCertificateKeyFile as follow.

# vi /opt/zodiac/local/httpd/conf/extra/httpd-ssl.conf

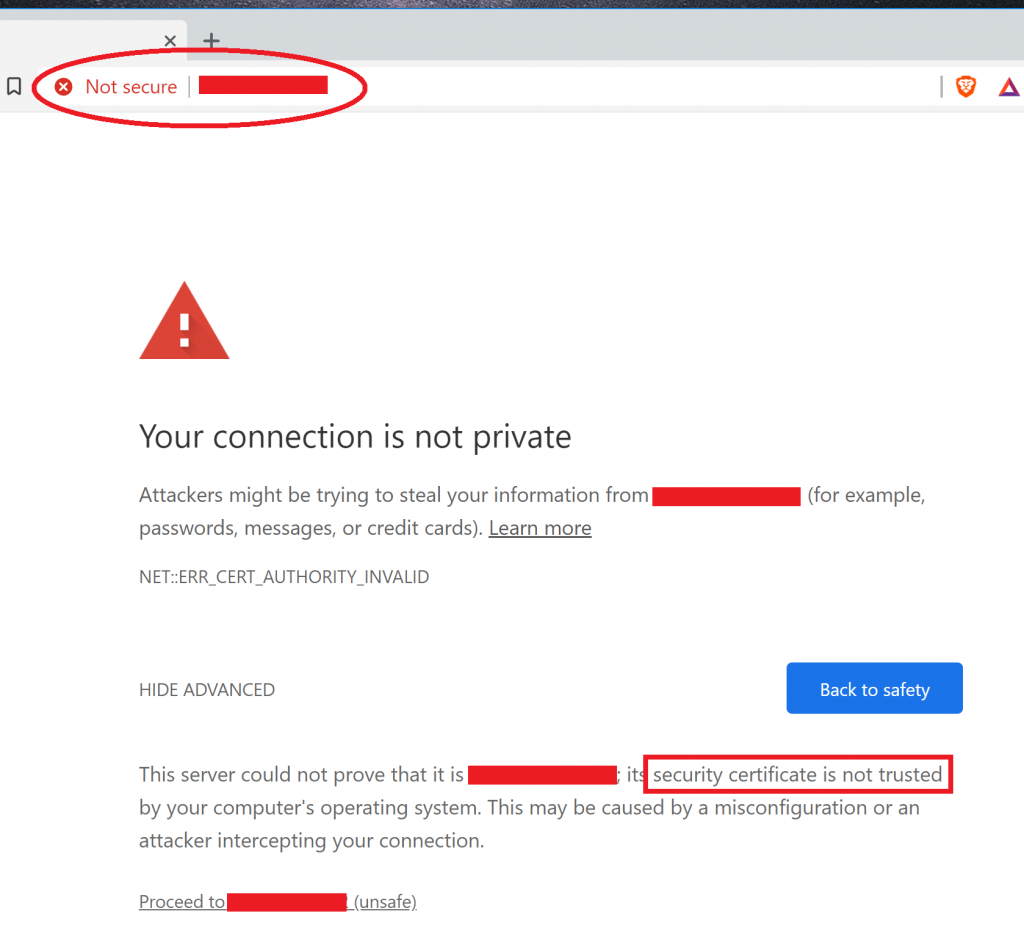
**SSLCertificateFile "/usr/local/apache2/conf/selfsrv.crt"**

**SSLCertificateKeyFile "/usr/local/apache2/conf/selfsrv.key"**

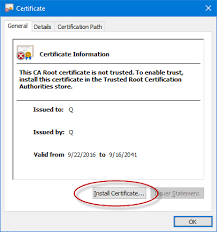
* Restart httpd container using below command

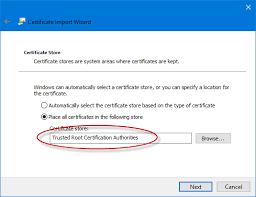
# docker container restart <Contaier\_ID>

* SSL has been installed now on server. When you tried to browse it on Internet Explorer it showing SSL is not trusted



* Click on proceed and then you will site with “Certificate Error” in address bar and click on “View Certificate”
* Click on Install Certificate on Trusted location





Once you added certificate again try to browse site using https it will working fine

# Troubleshooting

# Restart Apache reverse Proxy

* After Make changes in Reverse Proxy configuration file need to restart Docker Container using below command

# docker ps (List of running Container)

# docker container restart <Container ID>

# How to Check Reverse Proxy Container Log?

* Run the below command to check the Docker Container Log

# docker logs <Container ID>

# Auto Start Container After Reboot

* This command help to automatically start container on every reboot. Perform the below command

# docker ps –q (this command show the Only display numeric IDs then run below command)

# docker update --restart always $(docker ps -q)

# Replace existing Certificate

* Store your certificate on given path /opt/zodiac/local/httpd/conf/
* Change directory to /opt/zodiac/local/httpd/conf/extra/ and modify file using below command

# vi /opt/zodiac/local/httpd/conf/extra/httpd-ssl.conf

* After Replace the below value

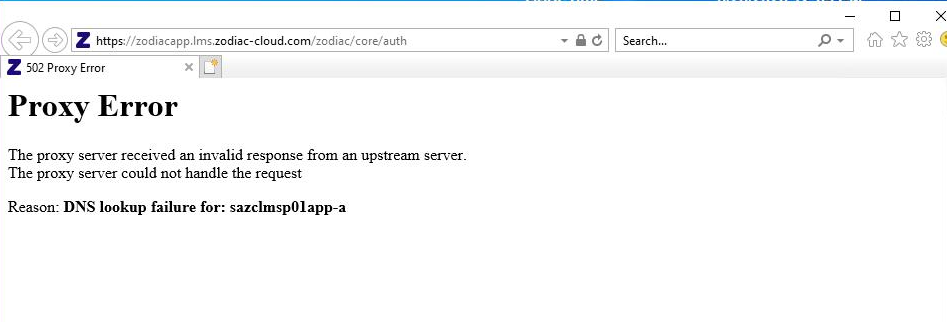
SSLCertificateFile "/usr/local/apache2/conf/**<certificate name>.crt**"

SSLCertificateKeyFile "/usr/local/apache2/conf/**<key name>.key**"

* After Replace the Certificate restart the container using below command

# docker container restart <Container ID>

# 502 Error in Reverse Proxy



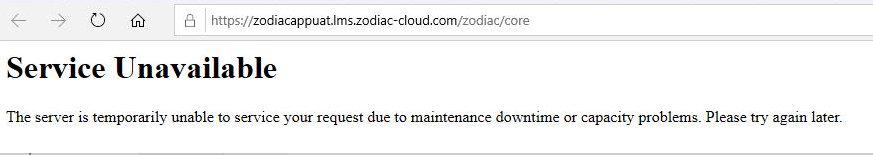
* Perform the below steps to troubleshoot
  + Verify the DNS name resolution using below command

# nslookup <backend\_Servername>

# nslookup <backend\_Servername.example.com>

* Perform Ping command to Check connection and DNS name Resolution
  + Ping <Backend Server Name>

# Reverse Proxy show 503 service Unavailable error



* Verify your Zodiac services is running or not in Backend Server
* Verify Application in IIS of Application Server

# Check Reverse Proxy Container status

* Run **docker ps** command to verify the status of docker container. 