How to bring up a reverse proxy using the jwilder/nginx-proxy

Last Modified on 09/24/2024 11:28 am EDT

Introduction

Exalate on-premise (such as Azure DevOps, ServiceNow) is deployed as Docker images. There is no built-in ssl support as it is much simpler to bring up a reverse proxy which can terminate SSL connections.

Our preference is the jwilder/Nginx-proxy image, which is a customization of the Nginx proxy. This article gives you a quick run down of the setup process.

> **Note**: For an in-depth tutorial on this topic, please see the article here.

Setting up jwilder/nginx-proxy with the letsencrypt SSL configuration

> **Warning**: Despite our best efforts, code can change without notice due to a variety of factors. If you encounter an issue in any of the code shown here and find that a specific block of code is not correct, or is causing errors, please check with the Community to find an updated version.

docker-compose.yml

```
version: "2"

services:
 nginx-proxy:
   image: jwilder/nginx-proxy
   container_name: nginx-proxy
   ports:
     - "80:80"
     - "443:443"
   volumes:
    - /etc/nginx/vhost.d
     - /etc/nginx/certs
     - /usr/share/nginx/html
     - /var/run/docker.sock:/tmp/docker.sock:ro
   networks:
     - proxy

 ssl-generator:
   image: jrcs/letsencrypt-nginx-proxy-companion
   volumes_from:
     - nginx-proxy
   volumes:
     - /var/run/docker.sock:/var/run/docker.sock:ro
   networks:
     - proxy

networks:
 proxy:
```

Using it in the container

The next step is to configure a DNS name which points to the host with the jwilder container running - assume **exalate.acme.com**

In the service definition of the exalate configure the following environment variables:

```
...
   environment:
     - LETSENCRYPT_HOST=exalate.acme.com
     - VIRTUAL_HOST=exalate.acme.com
...
```

Now, cycle the container.

The jwilder proxy will detect that the container has the VIRTUAL_HOST environment variable. This will automatically add in the nginx configuration:

```
# exalate.acme.com
upstream exalate.acme.com {
                        # Cannot connect to network of this container
                        server 127.0.0.1 down;
                        ## Can be connected with "nginx-proxy" network
                # francisexalatenet_bluejira_1
                server 172.18.0.8:8080;
}
server {
        server_name exalate.acme.com;
        listen 80 ;
        access_log /var/log/nginx/access.log vhost;
        return 301 https://$host$request_uri;
}
server {
        server_name exalate.acme.com;
        listen 443 ssl http2 ;
        access_log /var/log/nginx/access.log vhost;
        ssl_protocols TLSv1.2 TLSv1.3;
        ssl_ciphers 'ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM
-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:D
HE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SH
A256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA3
84:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-A
ES256-SHA256:DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:A
ES128-SHA:AES256-SHA:!DSS';
        ssl_prefer_server_ciphers on;
        ssl_session_timeout 5m;
        ssl_session_cache shared:SSL:50m;
        ssl_session_tickets off;
        ssl_certificate /etc/nginx/certs/exalate.acme.com.crt;
        ssl_certificate_key /etc/nginx/certs/exalate.acme.com.key;
        ssl_dhparam /etc/nginx/certs/exalate.acme.com.dhparam.pem;
        ssl_stapling on;
        ssl_stapling_verify on;
        ssl_trusted_certificate /etc/nginx/certs/exalate.acme.com.chain.pem;
        add_header Strict-Transport-Security "max-age=31536000" always;
        include /etc/nginx/vhost.d/default;
        location / {
                proxy_pass http://exalate.acme.com;
        }
}
```

The letsencrypt integration will automatically generate a LetEncrypt SSL certificate and add it into the configuration.

Warning: It is important that the letsencrypt service has a clear path to exalate.acme.com as it will check if that service does exist with the right settings.

Warning: In order for Let's Encrypt to generate and renew SSL Certificates, make sure the proxy server is reachable from the internet on the provided FQDN (for example, exalate.acme.com). For more information on how Let´s Encrypt works, please check the documentation here.

Warning: We recommend always including the full certificate chain, rather than just the server certificate, to avoid potential installation failures. Additionally, ensure that your certificates have an A or A+ rating.

ON THIS PAGE