Project: Bayer PID

Nginx Installation with   
keepalived (nginx-ha)

For: Bayer AG in Leverkusen / Germany

Name: Dariusz Czajka  
Company: Capgemini  
Date: 03/2019  
Version: 1.0

Changes

|  |  |  |
| --- | --- | --- |
| Date | Name | Change |
| 28/03/2019 | Dariusz Czajka (Capgemini) | Initial Doku |
| 15/05/2019 | Dariusz Czajka (Capgemini) | QA – HA configuration |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Systems

|  |  |  |  |
| --- | --- | --- | --- |
| System | IP/Mask | Environment | State |
| by0uf0.bayer.cnb | 10.205.112.134/21 | Prod | Nginx Master |
| by0uf1.bayer.cnb | 10.205.112.152/21 | Prod | Nginx Backup |
| by0uey.bayer.cnb | 10.205.112.132/21 | QA | Nginx Master |
| by0wlx.bayer.cnb | 10.205.116.211/21 | QA | Nginx Backup |

Software

OS: Red Hat Enterprise Linux Server 7.5  
Webserver: Nginx Plus 17.1  
IP Failover: keepalived 2.0.10 (nginx-ha)  
Other: Systemd Unit Files

Short description:

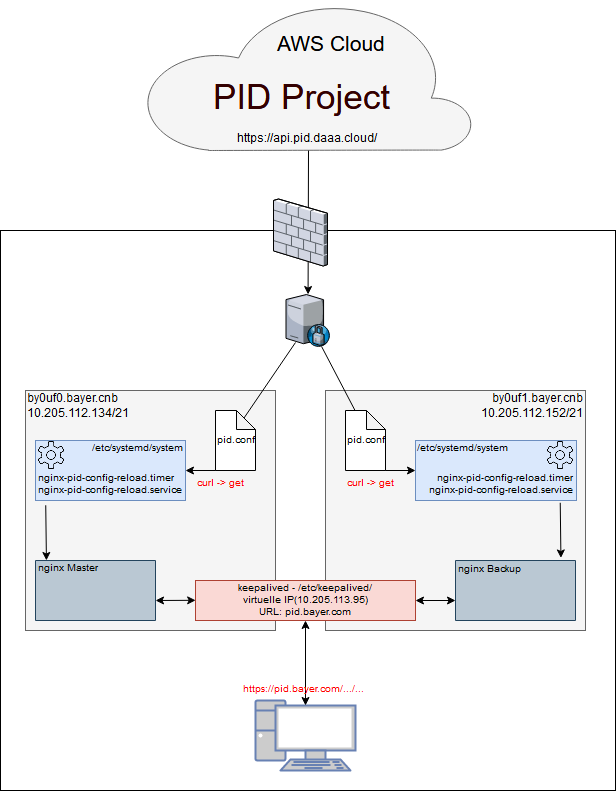
For the redirects created in the PID project (system in the AWS Cloud), the pid.conf file is retrieved at a fixed interval via the provided API. The used nginx plus will be reloaded at the same time as the new configuration file.

Between the two nginx servers was set up an HA solution using the by nginx implemented keepalived.

In event of a failure of the master node, the IP address is transferred to the backup node, thus ensuring fail-safety.

Further information can be found in the enclosed diagram and the scripts used.

# Production



Cluster IP

|  |  |  |
| --- | --- | --- |
| IP | FQDN | Environment |
| *10.205.113.95* | **pid.bayer.com** | Prod |

Installed Versions:

Red Hat Enterprise Linux Server release 7.5 (Maipo)  
nginx-ha-keepalived-2.0.10-1.el7\_4.ngx.x86\_64  
nginx-plus-17-1.el7\_4.ngx.x86\_64

Configuration Files:

/opt/pid/reload\_nginx.conf: (technical User for Internet Connect)

http\_proxy=http://MZYSQ:[PASSWORD]@10.185.190.100:8080/  
https\_proxy=https://MZYSQ: [PASSWORD]@10.185.190.100:8080/

/opt/pid/reload\_nginx\_config.sh: (Script to load pid.conf from API)

#!/bin/sh

general\_nginx\_config=/etc/nginx/nginx.conf  
pid\_nginx\_config=/etc/nginx/conf.d/pid.conf  
old\_pid\_nginx\_config=/etc/nginx/conf.d/pid.conf.old

if [ -f $pid\_nginx\_config ]; then  
 echo "Backing up old config file"  
 sudo mv $pid\_nginx\_config $old\_pid\_nginx\_config  
fi

echo "Get new config from backend"  
curl https://api.pid.daaa.cloud/api/proxyconfig --output $pid\_nginx\_config

echo "Validate new config"  
sudo nginx -t -c $general\_nginx\_config

if [ $? == 0 ]; then  
 echo "Validation successfully"  
 echo "Reload server"  
 sudo nginx -s reload  
else  
 echo "VALIDATE nginx config failed"  
 rm $pid\_nginx\_config

if [ -f $old\_pid\_nginx\_config ]; then  
 echo "Rename old file"  
 sudo mv $old\_pid\_nginx\_config $pid\_nginx\_config  
 fi  
fi

/etc/nginx/conf.d/pid.conf   
(Configuration File will be reloaded every min from API - <https://api.pid.daaa.cloud/api/proxyconfig>)

server {

listen 80;  
 server\_name pid.bayer.com www.pid.bayer.com;  
 return 301 https://$server\_name$request\_uri;  
}

server {  
 listen 443 ssl http2;  
 include snippets/self-signed.conf;  
 include snippets/ssl-params.conf;  
 server\_name pid.bayer.com www.pid.bayer.com;  
 proxy\_set\_header 'Access-Control-Allow-Origin' "\*";  
 proxy\_set\_header 'Access-Control-Allow-Credentials' 'true';  
 proxy\_set\_header 'Access-Control-Allow-Methods' 'GET, POST, PUT, DELETE, OPTIONS';  
 proxy\_set\_header 'Access-Control-Allow-Headers' 'Accept,Authorization,Cache-Control,Content-Type,DNT,If-Modified-Since,Keep-Alive,Origin,User-Agent,X-Requested-With';

location /kos/k0000068 {  
 rewrite ^.\* https://ui.pid.daaa.cloud/resource/1e9e20ee-1e2c-47eb-ab4b-96dc378750a5;  
 }  
 location /kos/k0000008 {  
 rewrite ^.\* https://indigo-explorer.intranet.cnb/edg/tbl/k0000008\_v1.editor;  
 }  
...  
 location / {  
 rewrite ^.\* https://ui.pid.daaa.cloud/;  
 }  
}

SSL Configuration

The Path for SSL can be set in /etc/nginx/conf.d/pid.conf:

…

include snippets/self-signed.conf;

include snippets/ssl-params.conf;

…

/etc/systemd/system/nginx-pid-config-reload.service

[Unit]  
Description=Downloads NGINX configuration from PID Web API, validates it and reloads the NGINX server

[Service]  
EnvironmentFile=/opt/pid/reload\_nginx.conf  
Type=oneshot  
ExecStart=/bin/bash /opt/pid/reload\_nginx\_config.sh

/etc/systemd/system/nginx-pid-config-reload.timer

[Unit]  
Description=Reloads the NGINX config every minutes

[Timer]  
OnBootSec=10s  
OnCalendar=\*:0/1

[Install]  
WantedBy=timers.target

/etc/keepalived/keepalived.conf (HA Configuration Master Node)

global\_defs {  
 vrrp\_version 3  
}

vrrp\_script chk\_manual\_failover {  
 script "/usr/libexec/keepalived/nginx-ha-manual-failover"  
 interval 10  
 weight 50  
}

vrrp\_script chk\_nginx\_service {  
 script "/usr/libexec/keepalived/nginx-ha-check"  
 interval 3  
 weight 50  
}

vrrp\_instance VI\_1 {  
 interface eth0  
 priority 101  
 virtual\_router\_id 51  
 advert\_int 1  
 accept  
 garp\_master\_refresh 5  
 garp\_master\_refresh\_repeat 1  
 unicast\_src\_ip 10.205.112.134  
 unicast\_peer {  
 10.205.112.152  
 }  
 virtual\_ipaddress {  
 10.205.113.95  
 }  
 track\_script {  
 chk\_nginx\_service  
 chk\_manual\_failover  
 }  
 notify "/usr/libexec/keepalived/nginx-ha-notify"

/etc/keepalived/keepalived.conf (HA Configuration Backup Node)

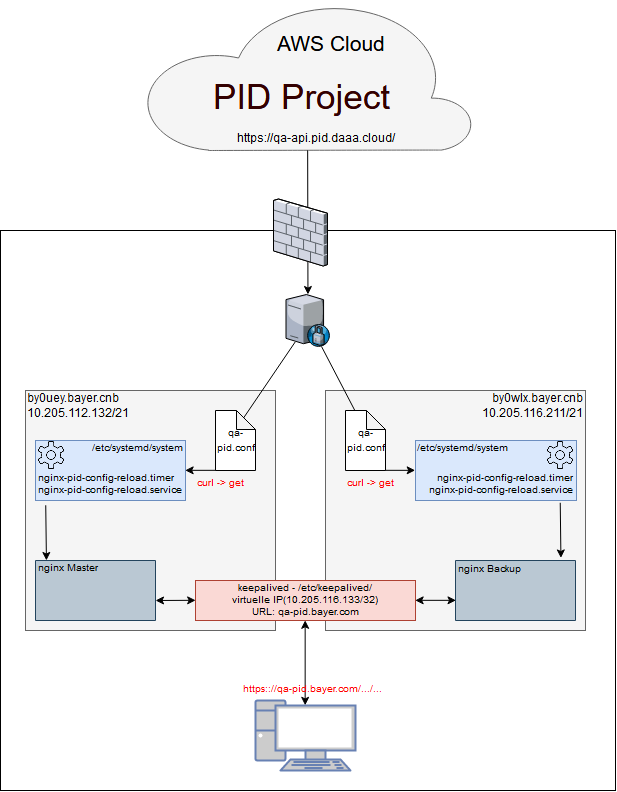
global\_defs {  
 vrrp\_version 3  
}

vrrp\_script chk\_manual\_failover {  
 script "/usr/libexec/keepalived/nginx-ha-manual-failover"  
 interval 10  
 weight 50  
}

vrrp\_script chk\_nginx\_service {  
 script "/usr/libexec/keepalived/nginx-ha-check"  
 interval 3  
 weight 50  
}

vrrp\_instance VI\_1 {  
 interface eth0  
 priority 100  
 virtual\_router\_id 51  
 advert\_int 1  
 accept  
 garp\_master\_refresh 5  
 garp\_master\_refresh\_repeat 1  
 unicast\_src\_ip 10.205.112.152  
 unicast\_peer {  
 10.205.112.134  
 }  
 virtual\_ipaddress {  
 10.205.113.95  
 }  
 track\_script {  
 chk\_nginx\_service  
 chk\_manual\_failover  
 }  
 notify "/usr/libexec/keepalived/nginx-ha-notify"

# QA



The QA System is configured identical to Production.

Cluster IP

|  |  |  |
| --- | --- | --- |
| IP | FQDN | Environment |
| *10.205.116.133* | **qa-pid.bayer.com** | QA |

Installed Versions:

Red Hat Enterprise Linux Server release 7.5 (Maipo)  
nginx-ha-keepalived-2.0.14-1.el7\_4.ngx.x86\_64  
nginx-plus-18-1.el7\_4.ngx.x86\_64

The here used configuration Files are:

/opt/pid/reload\_nginx.conf: (technical User for Internet Connect)

http\_proxy=http://MZYSQ:[PASSWORD]@10.185.190.100:8080/  
https\_proxy=https://MZYSQ: [PASSWORD]@10.185.190.100:8080/

/opt/pid/reload\_nginx\_config.sh: (Script to load pid.conf from API)

#!/bin/sh

general\_nginx\_config=/etc/nginx/nginx.conf  
pid\_nginx\_config=/etc/nginx/conf.d/qa-pid.conf  
old\_pid\_nginx\_config=/etc/nginx/conf.d/qa-pid.conf.old

if [ -f $pid\_nginx\_config ]; then  
 echo "Backing up old config file"  
 sudo mv $pid\_nginx\_config $old\_pid\_nginx\_config  
fi

echo "Get new config from backend"  
curl https://qa-api.pid.daaa.cloud/api/proxyconfig --output $pid\_nginx\_config

echo "Validate new config"  
sudo nginx -t -c $general\_nginx\_config

if [ $? == 0 ]; then  
 echo "Validation successfully"  
 echo "Reload server"  
 sudo nginx -s reload  
else  
 echo "VALIDATE nginx config failed"  
 rm $pid\_nginx\_config

if [ -f $old\_pid\_nginx\_config ]; then  
 echo "Rename old file"  
 sudo mv $old\_pid\_nginx\_config $pid\_nginx\_config  
 fi  
fi

/etc/nginx/conf.d/pid.conf   
(Configuration File will be reloaded every min from API - <https://qa-api.pid.daaa.cloud/api/proxyconfig>)

server {

listen 80;  
 server\_name qa-pid.bayer.com www.qa-pid.bayer.com;  
 return 301 https://$server\_name$request\_uri;  
}

server {  
 listen 443 ssl http2;  
 include snippets/self-signed.conf;  
 include snippets/ssl-params.conf;  
 server\_name qa-pid.bayer.com www.qa-pid.bayer.com;  
 proxy\_set\_header 'Access-Control-Allow-Origin' "\*";  
 proxy\_set\_header 'Access-Control-Allow-Credentials' 'true';  
 proxy\_set\_header 'Access-Control-Allow-Methods' 'GET, POST, PUT, DELETE, OPTIONS';  
 proxy\_set\_header 'Access-Control-Allow-Headers' 'Accept,Authorization,Cache-Control,Content-Type,DNT,If-Modified-Since,Keep-Alive,Origin,User-Agent,X-Requested-With';

location /kos/k0000068 {  
 rewrite ^.\* https://ui.pid.daaa.cloud/resource/1e9e20ee-1e2c-47eb-ab4b-96dc378750a5;  
 }  
 location /kos/k0000008 {  
 rewrite ^.\* https://indigo-explorer.intranet.cnb/edg/tbl/k0000008\_v1.editor;  
 }  
...  
 location / {  
 rewrite ^.\* https://ui.pid.daaa.cloud/;  
 }  
}

SSL Configuration

The Path for SSL can be set in /etc/nginx/conf.d/pid.conf:

…

include snippets/self-signed.conf;

include snippets/ssl-params.conf;

…

/etc/systemd/system/nginx-pid-config-reload.service

[Unit]  
Description=Downloads NGINX configuration from PID Web API, validates it and reloads the NGINX server

[Service]  
EnvironmentFile=/opt/pid/reload\_nginx.conf  
Type=oneshot  
ExecStart=/bin/bash /opt/pid/reload\_nginx\_config.sh

/etc/systemd/system/nginx-pid-config-reload.timer

[Unit]  
Description=Reloads the NGINX config every minutes

[Timer]  
OnBootSec=10s  
OnCalendar=\*:0/1

[Install]  
WantedBy=timers.target

/etc/keepalived/keepalived.conf (HA Configuration Master Node)

global\_defs {  
 vrrp\_version 3  
}

vrrp\_script chk\_manual\_failover {  
 script "/usr/libexec/keepalived/nginx-ha-manual-failover"  
 interval 10  
 weight 50  
}

vrrp\_script chk\_nginx\_service {  
 script "/usr/libexec/keepalived/nginx-ha-check"  
 interval 3  
 weight 50  
}

vrrp\_instance VI\_1\_QA {  
 interface eth0  
 priority 101  
 virtual\_router\_id 53  
 advert\_int 1  
 accept  
 garp\_master\_refresh 5  
 garp\_master\_refresh\_repeat 1  
 unicast\_src\_ip 10.205.112.132  
 unicast\_peer {  
 10.205.16.211  
 }  
 virtual\_ipaddress {  
 10.205.116.133  
 }  
 track\_script {  
 chk\_nginx\_service  
 chk\_manual\_failover  
 }  
 notify "/usr/libexec/keepalived/nginx-ha-notify"

/etc/keepalived/keepalived.conf (HA Configuration Backup Node)

global\_defs {  
 vrrp\_version 3  
}

vrrp\_script chk\_manual\_failover {  
 script "/usr/libexec/keepalived/nginx-ha-manual-failover"  
 interval 10  
 weight 50  
}

vrrp\_script chk\_nginx\_service {  
 script "/usr/libexec/keepalived/nginx-ha-check"  
 interval 3  
 weight 50  
}

vrrp\_instance VI\_1\_QA {  
 interface eth0  
 priority 100  
 virtual\_router\_id 53  
 advert\_int 1  
 accept  
 garp\_master\_refresh 5  
 garp\_master\_refresh\_repeat 1  
 unicast\_src\_ip 10.205.116.211  
 unicast\_peer {  
 10.205.112.132  
 }  
 virtual\_ipaddress {  
 10.205.116.133  
 }  
 track\_script {  
 chk\_nginx\_service  
 chk\_manual\_failover  
 }  
 notify "/usr/libexec/keepalived/nginx-ha-notify"

# Handling examples

cat /var/run/nginx-ha-keepalived.state (Show state of keepalive Node)

STATE=MASTER

systemctl status keepalived (start / stop / restart / status of Service )

● keepalived.service - LVS and VRRP High Availability Monitor  
 Loaded: loaded (/usr/lib/systemd/system/keepalived.service; enabled; vendor preset: disabled)  
 Active: active (running) since Sun 2019-03-24 20:15:14 CET; 3 days ago  
 Process: 29120 ExecStart=/usr/sbin/keepalived $KEEPALIVED\_OPTIONS (code=exited, status=0/SUCCESS)  
 Main PID: 29121 (keepalived)  
 CGroup: /system.slice/keepalived.service  
 ├─29121 /usr/sbin/keepalived –D  
 └─29122 /usr/sbin/keepalived –D

systemctl status nginx (start / stop / restart / status of Service )

● nginx.service - NGINX Plus - high performance web server  
 Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor preset: disabled)  
 Active: active (running) since Tue 2019-03-19 15:09:59 CET; 1 weeks 1 days ago  
 Docs: https://www.nginx.com/resources/  
 Main PID: 3661 (nginx)  
 CGroup: /system.slice/nginx.service  
 ├─3661 nginx: master process /usr/sbin/nginx –c  
/etc/nginx/nginx.conf  
 ├─6451 nginx: worker process  
 └─6452 nginx: worker proces

If a configuration will not be updated/refreshed it can be an error in the configuration File:

systemctl status nginx-pid-config-reload.service

● nginx-pid-config-reload.service - Downloads NGINX configuration from PID Web API, validates it and reloads the NGINX server

Loaded: loaded (/etc/systemd/system/nginx-pid-config-reload.service; static; vendor preset: disabled)

Active: inactive (dead) since Thu 2019-03-28 12:56:02 CET; 25s ago

Process: 11491 ExecStart=/bin/bash /opt/pid/reload\_nginx\_config.sh (code=exited, status=0/SUCCESS)

Main PID: 11491 (code=exited, status=0/SUCCESS)  
Mar 28 12:56:01 by0uey.bayer.cnb bash[11491]: [313B blob data]  
Mar 28 12:56:01 by0uey.bayer.cnb bash[11491]: Validate new config  
Mar 28 12:56:01 by0uey.bayer.cnb sudo[11502]: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/sbin/nginx -t -c /etc/nginx/nginx.conf  
Mar 28 12:56:01 by0uey.bayer.cnb bash[11491]: nginx: [warn] "ssl\_stapling" ignored, issuer certificate not found for certificate "/etc/ssl/certs/pid.bayer.com\_serial-6261436448204992404\_valid-05.12.2023.crt"  
**Mar 28 12:56:01 by0uey.bayer.cnb bash[11491]: nginx: [emerg] duplicate location "/constraint/c0000005" in /etc/nginx/conf.d/qa-pid.conf:648  
Mar 28 12:56:01 by0uey.bayer.cnb bash[11491]: nginx: configuration file /etc/nginx/nginx.conf test failed**Mar 28 12:56:01 by0uey.bayer.cnb bash[11491]: VALIDATE nginx config failed  
Mar 28 12:56:01 by0uey.bayer.cnb bash[11491]: Rename old file  
Mar 28 12:56:01 by0uey.bayer.cnb sudo[11505]: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/mv /etc/nginx/conf.d/qa-pid.conf.old /etc/nginx/conf.d/qa-pid.conf  
Mar 28 12:56:02 by0uey.bayer.cnb systemd[1]: Started Downloads NGINX configuration from PID Web API, validates it and reloads the NGINX server.

This failure is even to find in System Log:

/var/log/messages

Mar 28 00:04:00 by0uey bash: nginx: [emerg] duplicate location "/constraint/c0000005" in /etc/nginx/conf.d/qa-pid.conf:648  
Mar 28 00:04:00 by0uey bash: nginx: configuration file /etc/nginx/nginx.conf test failed  
Mar 28 00:04:00 by0uey bash: VALIDATE nginx config failed

Manuel IP failover:

touch /var/run/keepalived-manual-failover

or

systemctl stop keepalived

# Links

GIT

Git Repo PID: <https://bayer.githost.io/daaa/pid>

Frontend PID

PID Dev UI: <https://dev-ui.pid.daaa.cloud/>

PID QA UI: <https://qa-ui.pid.daaa.cloud/>

PID Productive UI: <https://ui.pid.daaa.cloud/>

Backend Swagger UI

Dev: <https://dev-api.pid.daaa.cloud/swagger/index.html>

QA: <https://qa-api.pid.daaa.cloud/swagger/index.html>

Prod: <https://api.pid.daaa.cloud/swagger/index.html>

Generated Configuration Files:

Dev: <https://dev-api.pid.daaa.cloud/api/proxyconfig>

QA: <https://qa-api.pid.daaa.cloud/api/proxyconfig>

Prod: <https://api.pid.daaa.cloud/api/proxyconfig>

Nginx Plus Documentation

Installing nginx Plus: <https://docs.nginx.com/nginx/admin-guide/installing-nginx/installing-nginx-plus/>

Installing nginx HA: <https://docs.nginx.com/nginx/admin-guide/high-availability/ha-keepalived/>