IDNEUF - REVERSE PROXY

DOCUMENTATION D'INSTALLATION

IDNEUF

AGENCE UNIVERSITAIRE DE LA FRANCOPHONIE

VERSION 1.0

J.P NAULET

2016/06/13

HISTORIQUE DES RÉVISIONS

VERSION	DESCRIPTION	DATE	AUTEUR
1.0	Document initial	2016/6/13	J.P Naulet

INTRODUCTION

Le présent document décrit l'architecture fonctionnelle et technique du Reverse Proxy frontal du service IDNEUF, ainsi que les étapes d'installation et de configuration.

Note: le CMS Drupal et le moteur ORI-OAI font l'objet de documentations séparées.

01

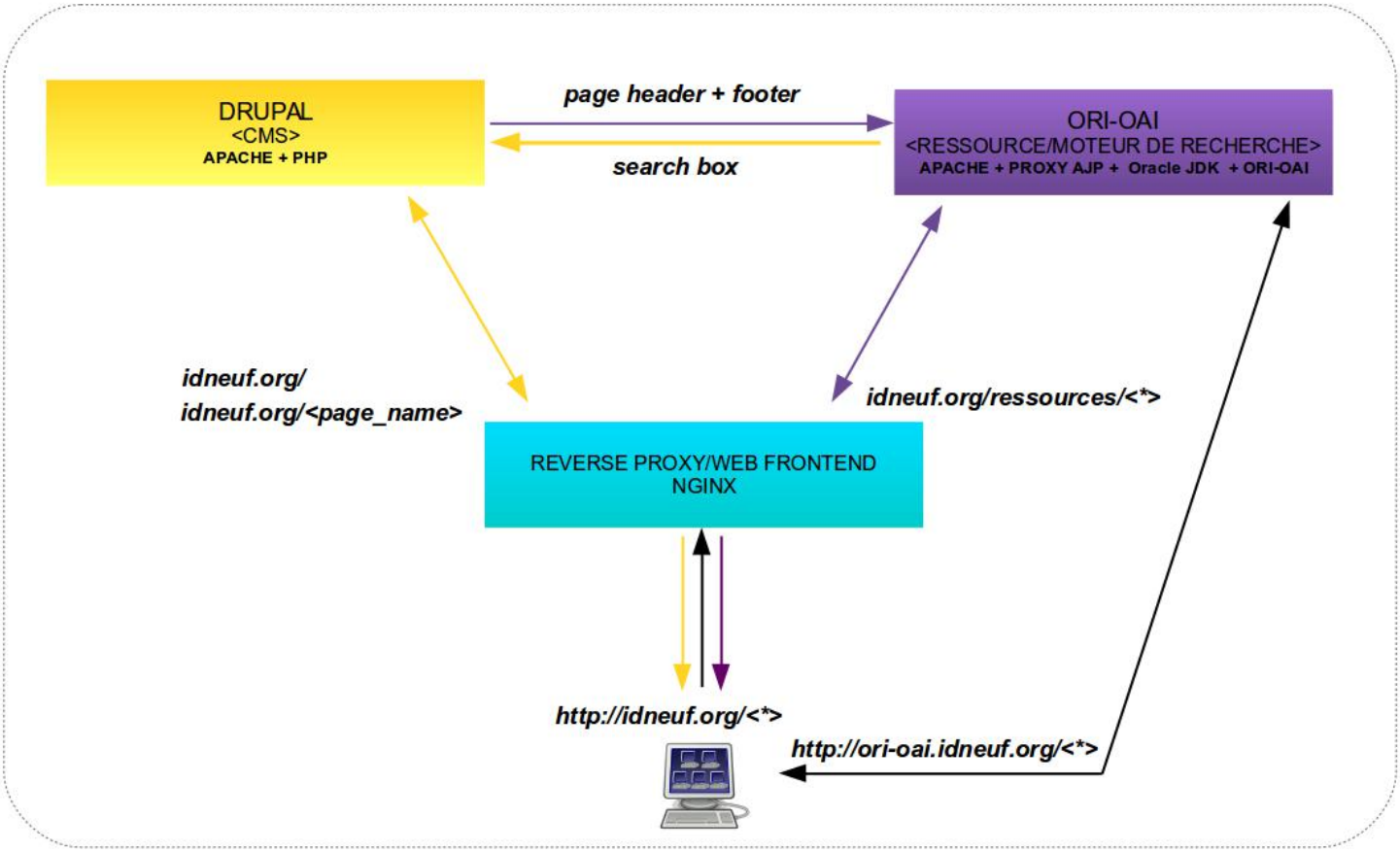
ARCHITECTURE FONCTIONNELLE DU SERVICE IDNEUF

Le service IDNEUF se compose d'un serveur Web Frontal (NGINX) configuré en mode "Reverse Proxy" qui distribue les requettes faites au service IDNEUF vers un CMS (Drupal) pour la partie contenu et présentation, et vers un MOTEUR ORI-OAI pour la partie recherche de ressources.

Ainsi l'accès aux ressources, le routage et la topologie du service IDNEUF sont gérés via le Reverse Proxy.

Enfin le Reverse Proxy permet des fonctions avancées en matière de restriction d'accès, de sécurité, de manipulation d'URL et de performance.

Ci-après un schéma fonctionnel décrivant la topologie du service IDNEUF:



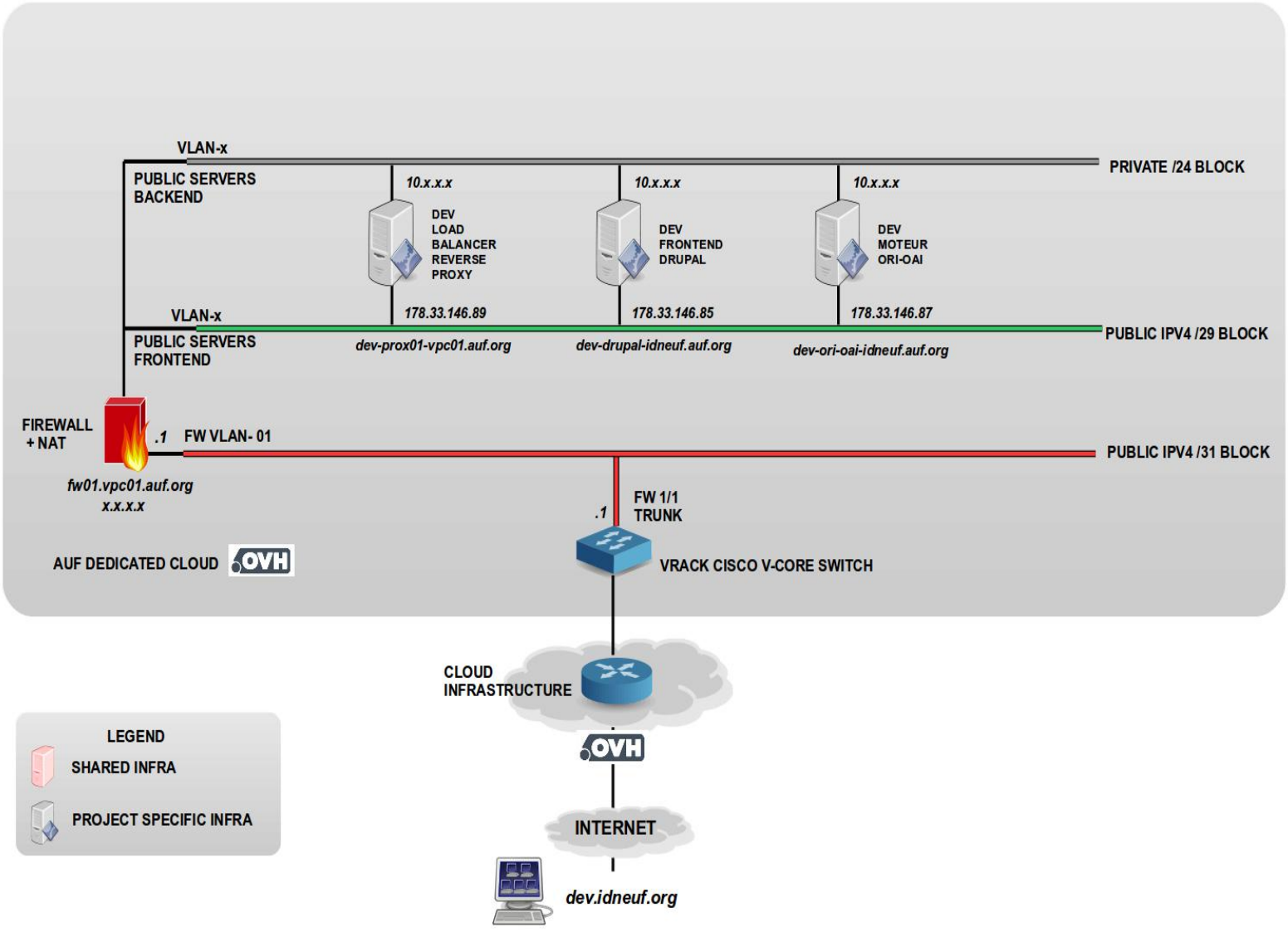
REVERSE PROXY IDNEUF

02

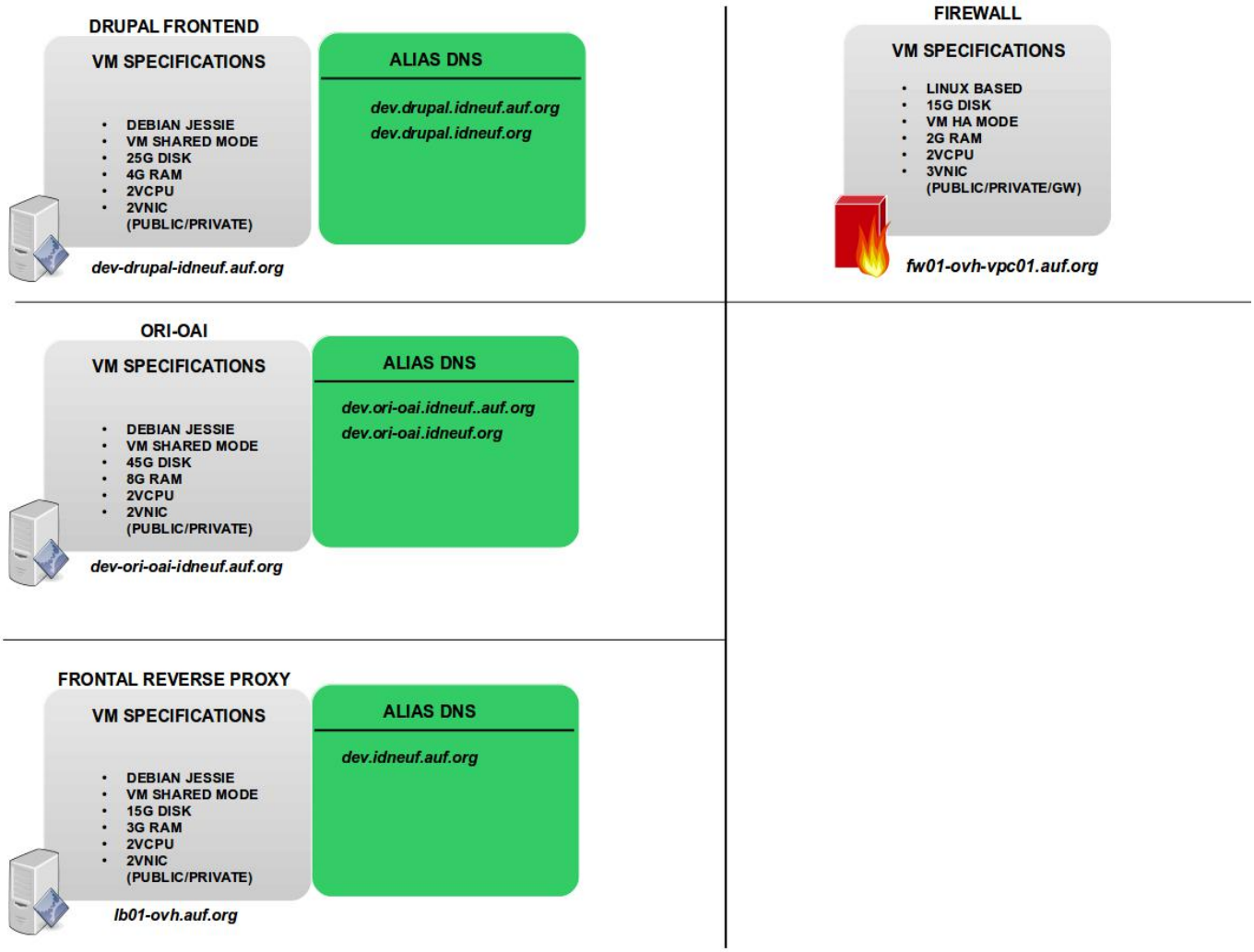
ARCHITECTURE TECHNIQUE DU SERVICE IDNEUF

Ci-après l'architecture cible de l'infra OVH Cloud entourant le projet IDNEUF

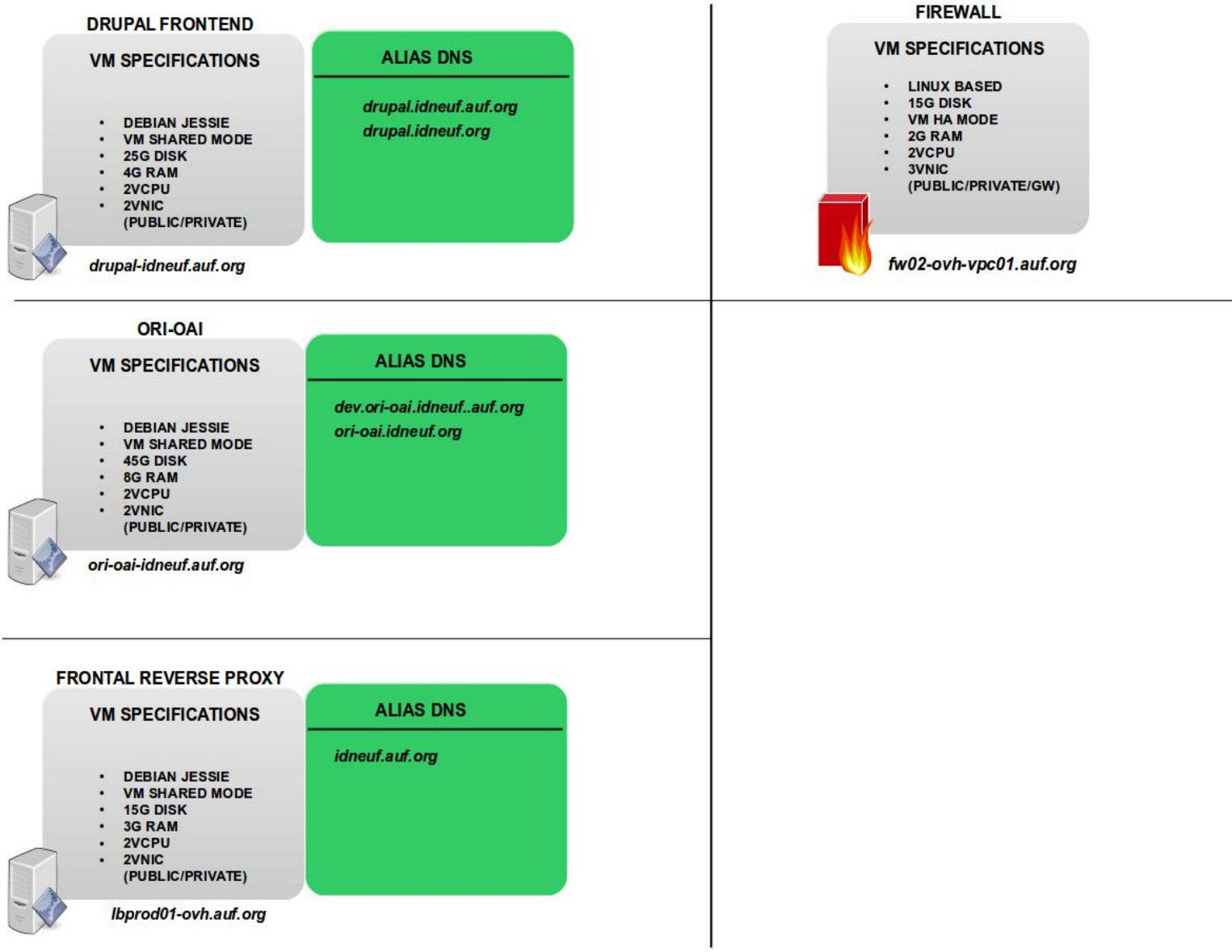
IDNEUF DEV – ARCHITECTURE TECHNIQUE – PHASE 1



IDNEUF DEV – DESIGN TECHNIQUE



IDNEUF PROD – DESIGN TECHNIQUE



03

PROCÉDURE D'INSTALLATION
DU REVERSE PROXY

PRÉREQUIS

Dans le cadre de l'installation du Reverse Proxy IDNEUF sur les serveurs de l'AUF, les prérequis suivants sont à observer.

PRÉREQUIS SYSTÈME

DEV
Debian jessie 25GB HDD
2G RAM
1VCPU

PROD
Debian jessie 45GB HDD
8G RAM
2VCPU

PRÉREQUIS LOGICIELS

Les paquets suivants sont à installer avant de procéder à l'installation du moteur

`nginx` > 1.6.2 (Nginx Full)
+dependances
```
fontconfig-config fonts-dejavu-core libfontconfig1 libgd3 libjbig0 libtiff5
libvpx1 libxpm4 nginx nginx-common nginx-full
libgd-tools fcgiwrap nginx-doc ssl-cert
```

`nginx-extras` > 1.6.2 (Nginx Extra)
+dependances
```
liblua5.1-0 libperl5.20 perl perl-base perl-modules
rename libarchive-extract-perl libmodule-pluggable-perl libpod-latex-perl
libterm-ui-perl libtext-soundex-perl libcgi-pm-perl libmodule-build-perl
libpackage-constants-perl
liblua5.1-0 libperl5.20 nginx-extras
```

Note:
Nginx Extra propose l'intégralité des modules précompilés pour Nginx (utilisé pour la maniplation des headers), à installer en suivant de Nginx Full

Différences entre les versions de nginx:
http://askubuntu.com/questions/553937/what-is-the-difference-between-the-core-full-extras-and-light-packages-for-ngi

Activation des scripts de démarrage par défaut (optionnel)
```
update-rc.d nginx default
```

CONFIGURATION GÉNÉRIQUE

CHEMINS

Créer le chemin par défaut, utilisér pour servir des fichiers statiques ou mettre en cache (au besoin) sous `/var/www/reverse_proxy`

exp:
```
/var/www/reverse_proxy/www.idneuf.org
/var/www/reverse_proxy/dev.idneuf.org
```

NGINX

Emplacement par défaut des fichiers Nginx

```
cors_support                --> fichier d'activation du module CORS
conf.d/                     --> configurations additionnelles de Nginx
fastcgi_params              --> configuration interface FastCGI
nginx.conf                  --> configuration principale de Nginx
fastcgi.conf                --> configuration interface FastCGI
sites-available             --> définition des virtualhosts
sites-enabled               --> activation des virtualhosts
proxy_params                --> paramètres proxy
```

1) Configuration de `nginx.conf`

Laisser la configuration par défaut.

Note: S'assurer que le protocol SSLV3 n'est pas activé, en raison de failles de sécurité connues et non résolues (directive `ssl_protocols`)

Vérifier que l'on a bien
```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
```

2) custom.conf

Créer le fichier `conf.d/custom.conf`

Ajouter la configuration suivante:

```
# indexes
index index.php index.htm index.html;

# rate limiting
limit_req_zone $binary_remote_addr zone=per_ip:10m rate=3r/s;
limit_req_zone $server_name zone=per_server:10m rate=200r/s;
```

La première ligne ajoute différents fichiers index que le serveur pourrait être amené à servir.

Les autres lignes activent le "rate limiting" qui pourra êtte utilisé et modfié en cas de besoin pour protéger les services en aval du Reverse Proxy

Pour plus d'informations cf: http://nginx.org/en/docs/http/ngx_http_limit_req_module.html

3) Serveur par défaut

Le serveur par défault du Reverse Proxy est configuré sous `/etc/nginx/sites-available/default`

Notes:
En PROD, aucun serveur non actif ne devrait être exposé et activé.

Comme pour le serveur Web Apache, l'activation/désactivation d'un Virtualhost se fait par création/suppression d'un lien symbolique entre les répertoires sites-available et sites-enabled

```
default -> /etc/nginx/sites-available/default
dev.idneuf.org -> /etc/nginx/sites-available/dev.idneuf.org
www.idneuf.org -> /etc/nginx/sites-available/www.idneuf.org
```

4) Vérification des configurations et des Virtualhosts activés

```
nginx -t

nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

Le Reverse Proxy constitue le point d'accès frontal et de distribution de un ou plusieurs services (dont IDNeuf).

Cependant, les services en **DEV** et en **PROD** devront être gérés par des Reverse Proxy **différents** afin d'isoler la PROD de tout risque, telles les modifications pouvant survenir en DEV.

IDNEUF DEV

Pour le service IDNEUF DEV le Virtualhost `dev.idneuf.org` a été créé avec la configuration suivante:

`/etc/nginx/sites-available/dev.idneuf.org`

```
server {
    listen 80;
    listen [::]:80;
    server_name dev.idneuf.org;
    root /var/www/reverse_proxy/;

    # log level
    error_log   /var/log/nginx/dev.idneuf.org.error debug; #debug
    #error_log   /var/log/nginx/dev.idneuf.org.error; #normal

    location / {
      proxy_set_header Host dev.idneuf.org;
      proxy_set_header X-Real-IP $remote_addr;
      #proxy_set_header X-Forwarded-For $remote_addr;
      proxy_pass http://dev.drupal.idneuf.org:80;
    }

    location /ressources/ {
      #try_files $uri $uri/ $uri/index.html =404;
      proxy_set_header Host dev.idneuf.org;
      proxy_set_header X-Real-IP $remote_addr;
      #proxy_set_header X-Forwarded-For $remote_addr;
      proxy_pass http://dev.ori-oai.idneuf.org:80;
    }

    location /ori-oai-thumbnail/ {
      proxy_set_header Host dev.idneuf.org;
      proxy_set_header X-Real-IP $remote_addr;
      #proxy_set_header X-Forwarded-For $remote_addr;
      proxy_pass http://dev.ori-oai.idneuf.org:80;
    }
}
```

Notes:

La directive `location` contient la configuration pour répondre aux requêtes sur l'URL dev.idneuf.org

* Log level par défaut est au niveau `error`. Passer en mode debug si besoin (et redémarrer le serveur)

```
# log level
#error_log   /var/log/nginx/www.idneuf.org.error debug; #debug
error_log   /var/log/nginx/www.idneuf.org.error error; #normal
```

* La transmission des requêtes au serveur Drupal et au moteur ORI-OAI en aval nécessite une modification des headers.

```
proxy_set_header Host dev.idneuf.org;
proxy_set_header X-Real-IP $remote_addr;
```

* Pour des raisons de sécurité le header Host est forcé à `dev.idneuf.org` afin de prévenir des risques de spoofing et de débordement de la pile d'exécution côté Drupal.

* La transmission des requêtes vers un serveur se fait via la directive `proxy_pass` (pour les requêtes http)

```
proxy_pass http://dev.drupal.idneuf.org:80;
```

* Les requêtes par défaut sont envoyées au frontend Drupal via la directive

```
location /
```

* Les requêtes au moteur sont envoyées au backend ORI-OAI via les directives

```
location /ressources
location /ori-oai-thumbnail/
```

* D'autres directives peuvent être ajoutées pour aouter des fonctionnalités et augmenter la sécurité

exp: rate limiting, réécriture d'URL, cache et buffers

IDNEUF PROD

Pour le service IDNEUF PROD le Virtualhost www.idneuf.org a été créé avec la configuration suivante:

/etc/nginx/sites-available/www.idneuf.org

```
server {
    listen 80;
    listen [::]:80;
    server_name www.idneuf.org;
    server_name idneuf.org;

    root /var/www/reverse_proxy/;

    # log level
    #error_log   /var/log/nginx/www.idneuf.org.error debug; #debug
    error_log   /var/log/nginx/www.idneuf.org.error error; #normal


    if ($host = 'idneuf.org'){
       return 301 $scheme://www.idneuf.org$request_uri;
    }

    location /
      proxy_set_header Host www.idneuf.org;
      proxy_set_header X-Real-IP $remote_addr;
      #proxy_set_header X-Forwarded-For $remote_addr;
      proxy_pass http://dev.drupal.idneuf.org:80;
      #limit_req zone=per_ip burst=10 nodelay;
      #limit_req zone=per_server burst=1000;
    }

    location /ressources/ {
      proxy_set_header Host www.idneuf.org;
      proxy_set_header X-Real-IP $remote_addr;
      #proxy_set_header X-Forwarded-For $remote_addr;
      proxy_pass http://dev.ori-oai.idneuf.org:80;
      #limit_req zone=per_ip burst=5 nodelay;
      #limit_req zone=per_server burst=1500;
    }

    location /ori-oai-thumbnail/ {
      proxy_set_header Host www.idneuf.org;
      proxy_set_header X-Real-IP $remote_addr;
      #proxy_set_header X-Forwarded-For $remote_addr;
      proxy_pass http://dev.ori-oai.idneuf.org:80;
      #limit_req zone=per_ip burst=5 nodelay;
      #limit_req zone=per_server burst=1500;
    }
}
```

Notes:

La configuration de www.idneuf.org est très similaire à celle de dev.idneuf.org (se référer à cette dernière pour davantage de détails)

Pour la PROD certaines directives on été ajoutées

* Redirection de idneuf.org vers www.idneuf.org pour satisfaire aux contraintes techniques du moteur ORI-OAI

```
if ($host = 'idneuf.org'){
      return 301 $scheme://www.idneuf.org$request_uri;
}
```

Redirection permanente (301) en http/https

* Dans cette configuration le frontend Drupal et le backend ORI-OAI utilisés sont ceux de DEV, pour des raison de disponibilité au moment de la configuration. Il conviendra de modifier la configuration en fonction des frontend et backend de PROD qui seront utilisés au final

```
proxy_pass http://dev.drupal.idneuf.org:80;
```

sera à remplacer par

```
proxy_pass http://drupal.idneuf.org:80;
```

Ainsi,

```
proxy_pass http://dev.ori-oai.idneuf.org:80;
```

sera à remplacer par

```
proxy_pass http://ori-oai.idneuf.org:80;
```

* Les directives de rate limiting ont été pré-incluses (mais non activées), dans l'éventualité ou il faudrait limiter le nombre de requêtes par secondes faite au service IDNEUF en PROD (à adapter avec le retour d'expérience).

```
#limit_req zone=per_ip burst=5 nodelay;
#limit_req zone=per_server burst=1500;
```

DNS

Renseigner l'adresse IP publique du serveur (directe ou pre-NAT) dans le DNS de l'AUF.

Associer le CNAME dev.idneuf.org à dev-proxy01.vpc01.auf.org
Associer le CNAME idneuf.org à prod-proxy01.vpc01.auf.org

MONITORING/MANAGEMENT

Afin d'assurer la bonne surveillance du service, le reverse proxy NGINX devra être monitoré à plusieurs niveaux:

1) Ajouter le serveur aux systèmes de monitoring (disque, ressources, réseau) et de déploiement de l'AUF (niveau système)

2) Monitorer le bon fonctionnement du Reverse Proxy (niveau NGINX) (logs nginx + processus)

3) Monitorer les URLs de service dev.idneuf.org et www.idneuf.org (code retour normal 200)
Tests spécifiques à mettre en place sur ces URLs

4) Monitorer les URLs dev.drupal.idneuf.org et dev.ori-oai.idneuf.org/ressources

5) Monitorer les URLs drupal.idneuf.org et ori-oai.idneuf.org

6) Monitorer les erreurs dans les logs

BACKUP

Ajouter le serveur au système de backup des VM dans nos clouds (cloud OVH privé dans ce cas ici)

SCRIPTS DE DÉMARRAGE

Les scripts démarrage des web applications sont dans:

```
/etc_init.d /nginx

Usage: nginx {start|stop|restart|reload|force-reload|status|configtest|
rotate|upgrade}
```

URLS

DEV

dev.idneuf.org
dev.drupal.idneuf.org
dev.ori-oai.idneuf.org/ressources/

PROD

idneuf.org
drupal.idneuf.org
ori-oai.idneuf.org/ressources/

DÉPANNAGE

A) Vérifier dans les logs la nature des messages d'erreur

/var/log/nginx/www.idneuf.org
/var/log/nginx/dev.idneuf.org

Le cas échéant passer en mode debug dans la configuration Nginx

exp: `#error_log  /var/log/nginx/www.idneuf.org.error debug; #debug`

On peut également utiliser les commandes suivantes:

```
systemctl status
```

ou

```
journalctl -xn
```

B) Vérifier dans les processus NGINX sont bien lancés

```
ps -ef | grep nginx

www-data 15881 15880  0 jun10 ?        00:00:10 nginx: worker
process
www-data 15882 15880  0 jun10 ?        00:00:10 nginx: worker
process
www-data 15883 15880  0 jun10 ?        00:00:09 nginx: worker
process
www-data 15884 15880  0 jun10 ?        00:00:06 nginx: worker process
```

C) Vérifier les flux entre le Reverse Proxy, le serveur Drupal et le moteur ORI-OAI

```
Internet --> Reverse Proxy (port 80)
Reverse Proxy --> Drupal (port 80)
Reverse Proxy --> Moteur ORI-OAI (port 80)
Drupal <--> Moteur ORI-OAI (port 80)
```

D) Vérifier le logs et le bon lancement des serveurs Drupal et moteur ORI-OAI

SÉCURITÉ

→ Le frontend drupal et le moteur devraient être sur le même réseau local pour optimiser les temps de réponse et sécuriser les accès via un reverse proxy et firewall commun au service IDneuf

(Le frontend Drupal et le moteur ORI-OAI communiquent entre eux via des appels croisés sur des URLs spécifiques, avant de servir le contenu au client web qui effectue une requête de connexion sur le frontend ou le moteur)

→ Bloquer l'accès sur le web aux URLs de management de s'il y en a

ADDENDUM

- Le frontend Drupal fera l'objet d'une autre documentation

- Le backend moteur ORI-OAI fera l'objet d'une autre documentation

- Se référer au dossier Design_Technique du projet IDneuf pour l'architecture globale du projet sur owncloud

https://nuage.auf.org/index.php/apps/files/?dir=%2F[[AUF-partage-ARI]]%2FI-Ressources-informatiques%20%28global%29%2Fi-3000-activite-specifique%2Fi-3400-systemes-communication%2FProjets%20SI%2FIDneuf%2FDocumentation_Technique

ANNEXES

Différences entre les versions de nginx
http://askubuntu.com/questions/553937/what-is-the-difference-between-the-core-full-extras-and-light-packages-for-ngi

Config générique NGINX
https://www.nginx.com/resources/wiki/start/topics/tutorials/config_pitfalls/
http://wiki.nginx.org/QuickStart
http://wiki.nginx.org/Configuration

Variables NGINX
http://nginx.org/en/docs/http/ngx_http_core_module.html#variables