Configurer Nginx pour GeoNature

Installer les domaines de GeoNature

- Notes : dans notre exemple, nous utiliserons un adresse web de type *<alias>.<domaine-sinp>* (Ex. : expert.silene.eu) comme adresse principale de GeoNature. L'adresse web *geonature.<domaine-sinp>* (Ex: geonature.silene.eu) devra être redirigé vers *<alias>.<domaine-sinp>*.
- Créer un fichier de configuration : `vi /etc/nginx/sites-available/geonature.conf`
- Y placer le contenu suivant :

```
server {
    listen 80;
    listen [::]:80;

    server_name <alias>.<domaine-sinp>;
    root /home/geonat/www/geonature/frontend/dist;

    location ^~ "/api/" {
        proxy_set_header X-Forwarded-Host $host:$server_port;
        proxy_set_header X-Forwarded-Server $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;

        # WARNING: up timeout to 300s for Synthese downloading (See bug
)
        # Set timeout like Gunicorn in GeoNature config/settings.ini
file
        proxy_read_timeout 300s;
        proxy_connect_timeout 75s;
        proxy_pass http://127.0.0.1:8000/;# ATTENTION : bien mettre un
slash final ! Sinon => 404
    }
}
```

- Créer un lien depuis les sites actifs : `cd /etc/nginx/sites-enabled/ ; ln -s ../sites-available/geonature.conf geonature.conf`
- Tester la config et relancer Nginx si OK : `nginx -t && nginx -s reload`
- Tester l'URL http://geonature.<domaine-sinp>/ qui doit afficher une erreur 502 si le serveur *Gunicorn* de GeoNature n'est pas lancé.
  - Vérifier les services supervisés par Supervisor : `supervisorctl status`
  - Démarrer le service *GeoNature* : `supervisorctl start geonature2`
  - Arrêter le service *GeoNature* : `supervisorctl stop geonature2`

Ajout de la page de maintenance auto

- Il est possible d'ajouter une page web qui sera automatiquement affichée par Nginx quand le

dossier `dist` de GeoNature n'existe pas.
- Lorsque nous lançons le build du frontend de GeoNature le dossier `dist` est supprimé puis recréé uniquement à la fin du build.
- Ajouter sur le serveur les fichiers de la page de maintenance :

```
rsync -av --size-only  ./maintenance geonat@web-<region>-
sinp:/home/geonat/www/
```

- En ajoutant, le code suivant au fichier de config Nginx de GeoNature, la page de maintenance sera automatiquement affiché durant chaque build :

```
    # Set root path
    set $root_path /home/geonat/www/geonature/frontend/dist;
    if (!-d /home/geonat/www/geonature/frontend/dist) {
       set $root_path /home/geonat/www/maintenance/geonature;
    }
    root $root_path;
```

Activer SSL et HTTP2 pour GeoNature

- Installer un certificat SSL via Certbot (Letsencrypt) : `certbot --nginx -d <alias>.<domaine-sinp> -d geonature.<domaine-sinp>`
    - Ex. pour PACA : `certbot –nginx -d expert.silene.eu -d geonature.silene.eu`
    - Ex. pour AURA :

```
  certbot --nginx \
    -d donnees.biodiversite-auvergne-rhone-alpes.fr -d
geonature.biodiversite-auvergne-rhone-alpes.fr \
    -d donnees.biodiversite-auvergne-rhone-alpes.com -d
geonature.biodiversite-auvergne-rhone-alpes.com \
    -d donnees.biodiversite-auvergne-rhone-alpes.eu -d
geonature.biodiversite-auvergne-rhone-alpes.eu \
    -d donnees.biodiversite-auvergne-rhone-alpes.net -d
geonature.biodiversite-auvergne-rhone-alpes.net \
    -d donnees.biodiversite-auvergne-rhone-alpes.org -d
geonature.biodiversite-auvergne-rhone-alpes.org \
    -d donnees.biodiversite-aura.com -d geonature.biodiversite-
aura.com \
    -d donnees.biodiversite-aura.eu -d geonature.biodiversite-
aura.eu \
    -d donnees.biodiversite-aura.fr -d geonature.biodiversite-
aura.fr \
    -d donnees.biodiversite-aura.net -d geonature.biodiversite-
aura.net \
    -d donnees.biodiversite-aura.org -d geonature.biodiversite-
aura.org \
    -d donnees.observatoire-biodiversite-auvergne-rhone-alpes.com
```

```
-d geonature.observatoire-biodiversite-auvergne-rhone-alpes.com \
    -d donnees.observatoire-biodiversite-auvergne-rhone-alpes.eu -
d geonature.observatoire-biodiversite-auvergne-rhone-alpes.eu \
    -d donnees.observatoire-biodiversite-auvergne-rhone-alpes.fr -
d geonature.observatoire-biodiversite-auvergne-rhone-alpes.fr \
    -d donnees.observatoire-biodiversite-auvergne-rhone-alpes.net
-d geonature.observatoire-biodiversite-auvergne-rhone-alpes.net \
    -d donnees.observatoire-biodiversite-auvergne-rhone-alpes.org
-d geonature.observatoire-biodiversite-auvergne-rhone-alpes.org
```

  - Email à fournir : adminsys@<domaine-sinp>
  - Répondre : A → N → 2
  - Tester ensuite la redirection auto de HTTP vers HTTPS : http://<alias>.<domaine-sinp>/ → doit rediriger vers HTTPS automatiquement
- Tester les configurations SSL :
  - https://www.ssllabs.com/ssltest/analyze.html?d=<alias>.<domaine-sinp>
  - https://www.ssllabs.com/ssltest/analyze.html?d=geonature.<domaine-sinp>
- Préparer les fichiers de maintenances dans `~/www/maintenance/` en les transférant depuis le dépôt *sinp-<region>-srv* à l'aide de *rsync*.
- Modifier les redirections (geonature.<domaine-sinp> → <alias>.<domaine-sinp>) et l'UUID pour la maintenance (*<uuid-maintenance-disable>*) pour qu'au final le fichier *geonature.conf* contienne :

```
server {
    listen 443 ssl http2; # managed by Certbot
    listen [::]:443 ssl http2; # managed by Certbot

    server_name <alias>.<domaine-sinp>;

    # Set maintenance mode
    # Define root paths
    set $base_root_path /home/geonat/www;
    set $geonature_root_path $base_root_path/geonature/frontend/dist;
    set $maintenance_root_path $base_root_path/maintenance/geonature;
    # Disable maintenance mode by default
    set $maintenance off;

    # Activate maintenance mode ("short") if GeoNatue is being
recompiled
    if (!-d $geonature_root_path) {
        set $maintenance on;
        set $maintenance_duration "short";
    }

    # Activate maintenance mode ("long") if file "maintenance.enable"
exists
    if (-f $maintenance_root_path/maintenance.enable) {
        set $maintenance on;
        set $maintenance_duration "long";
    }
```

```
    # Disable maintenance mode if user browser send a cookie named
"maintenance_disable" with a specific UUID value
    if ($cookie_maintenance_disable = "<uuid-maintenance-disable>") {
        set $maintenance off;
    }

    # Disable maintenance mode for specific IP (default web server IP)
    if ($remote_addr ~ (51.91.137.130)) {
        set $maintenance off;
    }

    # Disable maintenance mode for the URI with the path to the shared
CSS, JS, or images used in the maintenance page.
    if ($uri ~ "^/maintenance/shared/") {
        set $maintenance off;
    }

    # Return HTTP code 503 (service unavailable) if maintenance is on
    if ($maintenance = on) {
        return 503;
    }

    error_page 503 @maintenance;

    # Display the long or short term maintenance page.
    location @maintenance {
        root $maintenance_root_path;
        rewrite ^(.*)$ "/maintenance.$maintenance_duration.html" break;
    }

    # Set root path
    root $geonature_root_path;

    # Change root path for shared files used in the maintenance page.
    location ~ "^/maintenance/shared/" {
        root $base_root_path;
    }

    # GeoNature Angular App
    # No cache for index.html Angular App and config/locale json files
    location ~* "^/index.html|.*\.json$" {
        expires -1;
        add_header Cache-Control "no-store";
    }
    # Favicon
    location "/favicon.ico" {
        expires 1y;
        add_header Cache-Control "public, no-transform";
    }
```

```
    # JS and CSS
    location ~* "^/[^/]+\.[0-9a-f]{20}\.(?:js|css)$" {
        expires 1y;
        add_header Cache-Control "public, immutable";
    }
    # Images
    location ~* "^/[^/]+\.[0-9a-f]{20}\.(?:gif|jpe?g|png|svg)$" {
        expires 1y;
        add_header Cache-Control "public, no-transform, immutable";
    }
    # Fonts
    location ~* "^/[^/]+\.[0-9a-f]{20}\.(?:woff2?|eot|ttf)$" {
        expires 1y;
        add_header Cache-Control "public, immutable";
    }

    # GeoNature API
    location ^~ "/api/" {
        proxy_set_header X-Forwarded-Host $host:$server_port;
        proxy_set_header X-Forwarded-Server $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;

        # WARNING: up timeout to 300s for Synthese downloading (See bug
)
        # Set timeout like Gunicorn in GeoNature config/settings.ini
file
        proxy_read_timeout 300s;
        proxy_connect_timeout 75s;
        proxy_pass http://127.0.0.1:8000/;# ATTENTION : bien mettre un
slash final ! Sinon => 404
    }

    # Alias for Export module
    location "/exports/schedules" {
        alias
/home/geonat/www/geonature/backend/static/exports/schedules;
    }
    location "/exports/users" {
        alias
/home/geonat/www/geonature/backend/static/exports/usr_generated;
    }

    ssl_certificate /etc/letsencrypt/live/<alias>.<domaine-
sinp>/fullchain.pem; # managed by Certbot
    ssl_certificate_key /etc/letsencrypt/live/<alias>.<domaine-
sinp>/privkey.pem; # managed by Certbot
    include /etc/letsencrypt/options-ssl-nginx.conf; # managed by
Certbot
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot
}
```

```
server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;
    server_name geonature.<domaine-sinp>;

    ssl_certificate /etc/letsencrypt/live/<alias>.<domaine-
sinp>/fullchain.pem; # managed by Certbot
    ssl_certificate_key /etc/letsencrypt/live/<alias>.<domaine-
sinp>/privkey.pem; # managed by Certbot
    include /etc/letsencrypt/options-ssl-nginx.conf; # managed by
Certbot
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot

    return 302 https://<alias>.<domaine-sinp>$request_uri;
}

server {
    listen 80;
    listen [::]:80;
    server_name <alias>.<domaine-sinp> geonature.<domaine-sinp>;
    return 302 https://<alias>.<domaine-sinp>$request_uri;
}
```

- **Notes** : la configuration Nginx de GeoNature active la mise en cache définitive des fichiers comprenant un hash dans leur nom (JS, CSS, polices et images). Angular Cli génère des fichiers comprenant le hash de leur contenu dans leur nom. Tout nouveau build génère une nouveau hash pour les fichiers modifiés. Les fichiers peuvent donc être mis en cache définitivement à l'exception du fichier *index.html*.

Création config Nginx maintenance GeoNature

- **Notes** : le fichier de configuration *geonature_maintenance.conf* pointe vers un fichier *index.html* indiquant que GeoNature est en maintenance
- Copier la config de GeoNature : cp /etc/nginx/sites-available/geonature.conf /etc/nginx/sites-available/geonature_maintenance.conf
- Éditer le fichier : `vi /etc/nginx/sites-available/geonature_maintenance.conf`
- Modifier le fichier de config ainsi :

```
server {
    listen [::]:443 ssl http2; # managed by Certbot
    listen 443 ssl http2; # managed by Certbot

    server_name <alias>.<domaine-sinp>;
    root /home/geonat/www/geonature/frontend/src/app/maintenance;

    ssl_certificate
/etc/letsencrypt/live/<alias>.<domaine>/fullchain.pem; # managed by
```

```
Certbot
    ssl_certificate_key
/etc/letsencrypt/live/<alias>.<domaine>/privkey.pem; # managed by
Certbot
    include /etc/letsencrypt/options-ssl-nginx.conf; # managed by
Certbot
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot
}

server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;
    server_name geonature.<domaine-sinp>;

    ssl_certificate /etc/letsencrypt/live/<alias>.<domaine-
sinp>/fullchain.pem; # managed by Certbot
    ssl_certificate_key /etc/letsencrypt/live/<alias>.<domaine-
sinp>/privkey.pem; # managed by Certbot
    include /etc/letsencrypt/options-ssl-nginx.conf; # managed by
Certbot
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot

    return 302 https://<alias>.<domaine-sinp>$request_uri;
}

server {
    listen 80;
    listen [::]:80;
    server_name <alias>.<domaine-sinp> geonature.<domaine-sinp>;
    return 302 https://<alias>.<domaine-sinp>$request_uri;
}
```