

Produits Entr'ouvert - HowDoWeDoPublikDomainNameChange - # 9

NE PAS UTILISER, préférez <https://dev.entrouvert.org/projects/prod-eo/wiki/HowDoWeDoPublikDomainNameChangeSurLeSaas>

HowDoWeDoPublikDomainNameChange (pas sur le SaaS)

DNS

S'assurer que les noms de domaine existent. Sur un hébergement on-premise, si besoin, taper les noms dans /etc/hosts.

Certificats

Obtenir le certificat pour le nouveau domaine. Placer dans /etc/ssl/{private,certs} ou /etc/nginx/ssl/.

NGINX

Créer le fichier de conf déclarant le nouveau certificat et sa clé. Ex:

/etc/nginx/includes/wildcard.demarches.grenoblealpesmetropole.fr.conf

```
ssl_certificate /etc/nginx/ssl/wildcard.demarches.grenoblealpesmetropole.fr.crt;
ssl_certificate_key /etc/nginx/ssl/wildcard.demarches.grenoblealpesmetropole.fr.key;
```

Page de maintenance

- prévoir la modification de la conf nginx pour déclarer les noms de domaine supplémentaires:
/etc/nginx/conf.d/server-names-hash-bucket-size.conf:
server_names_hash_bucket_size 128;
- rajouter le nouveau nom de domaine dans les directions de port 80 => 443

```
server {
    listen 80;
    server_name statistiques.demarches.lametro.fr statistiques.demarches.grenoblealpesmetropole.fr;

    access_log /var/log/nginx/bijoe-access.log combined;
    error_log /var/log/nginx/bijoe-error.log;

    return 302 https://$host$request_uri;
}
```

Configurer le mode maintenance de Nginx:

Créer un fichier de configuration du mode maintenance: /etc/nginx/includes/maintenance.conf

```
if (-f $document_root/maintenance.html) {
    set $maintenance 1;
}

if ($maintenance = 1) {
    return 503;
}

error_page 503 @maintenance;

location @maintenance {
    rewrite ^(.*)$ /maintenance.html break;
}
```

Créer le fichier `/usr/share/nginx/html/maintenance.html` et y poser le message de maintenance en HTML.

Déclarer un vhost pour l'ancien nom de domaine, avec la conf SSL, et de la page de maintenance. Ex:

```
server {
    listen 443 ssl;
    server_name accueil.demarches.lametro.fr;

    include includes/ssl.conf;
    include includes/wildcard.demarches.lametro.fr.conf;

    include includes/maintenance.conf;
}
```

Test de la config:

```
sudo nginx -t
```

et reload si tout va bien.

Services

- stop services:

```
sudo systemctl stop authentic2-multitenant bijoe chrono combo fargo hobo passerelle wcs welco
```

- stop cron jobs:

```
sudo vi /etc/cron.d/wcs
```

Tenants

Rénommer les répertoires des tenants:

```
sudo -u authentic-multitenant mv /var/lib/authentic2-multitenant/tenants/connexion.demarches.lametro.fr{,.invalid.migration}
sudo -u bijoe mv /var/lib/bijoe/tenants/statistiques.demarches.lametro.fr{,.invalid.migration}
sudo -u chrono mv /var/lib/chrono/tenants/agendas.demarches.lametro.fr{,.invalid.migration}
sudo -u combo mv /var/lib/combo/tenants/portail-agent.demarches.lametro.fr{,.invalid.migration}
sudo -u combo mv /var/lib/combo/tenants/demarches.lametro.fr{,.invalid.migration}
sudo -u hobo mv /var/lib/hobo/tenants/hobo.demarches.lametro.fr{,.invalid.migration}
sudo -u fargo mv /var/lib/fargo/tenants/porte-documents.demarches.lametro.fr{,.invalid.migration}
}
sudo -u passerelle mv /var/lib/passerelle/tenants/passerelle.demarches.lametro.fr{,.invalid.migration}
sudo -u wcs mv /var/lib/wcs/services.demarches.lametro.fr{,.invalid.migration}
sudo -u welco mv /var/lib/welco/tenants/accueil.demarches.lametro.fr{,.invalid.migration}
```

Schémas des bases des données

Exporter les schemas pour toutes les briques, sauf wcs, en remplaçant l'ancien nom de domaine par le nouveau:

- hobo:

```
sudo -u hobo pg_dump -n hobo_demarches_lametro_fr | sed 's/demarches_lametro_fr/demarches_grenoblealpesmetropole_fr/g' | sed 's/demarches.lametro.fr/demarches.grenoblealpesmetropole.fr/g' > hobo.sql
```

- combo:

```
sudo -u combo pg_dump -n demarches_lametro_fr -n portail_agent_demarches_lametro_fr | sed 's/demarches_lametro_fr/demarches_grenoblealpesmetropole_fr/g' | sed 's/demarches.lametro.fr/demarches.grenoblealpesmetropole.fr/g' > combo.sql
```

- passerelle:

```
sudo -u passerelle pg_dump -n passerelle_demarches_lametro_fr | sed 's/demarches_lametro_fr/demarches_grenoblealpesmetropole_fr/g' | sed 's/demarches.lametro.fr/demarches.grenoblealpesmetropole.fr/g' > passerelle.sql
```

- welco:

```
sudo -u welco pg_dump -n accueil_demarches_lametro_fr | sed 's/demarches_lametro_fr/demarches_grenoblealpesmetropole_fr/g' | sed 's/demarches.lametro.fr/demarches.grenoblealpesmetropole.fr/g' > welco.sql
```

- authentic:

```
sudo -u authentic-multitenant pg_dump -n connexion_demarches_lametro_fr authentic2_multitenant | sed 's/demarches_lametro_fr/demarches_grenoblealpesmetropole_fr/g' | sed 's/demarches.lametro.fr/demarches.grenoblealpesmetropole.fr/g' > authentic.sql
```

- fargo:

```
sudo -u fargo pg_dump -n porte_documents_demarches_lametro_fr | sed 's/demarches_lametro_fr/demarches_grenoblealpesmetropole_fr/g' | sed 's/demarches.lametro.fr/demarches.grenoblealpesmetropole.fr/g' > fargo.sql
```

- chrono:

```
sudo -u chrono pg_dump -n agendas_demarches_lametro_fr | sed 's/demarches_lametro_fr/demarches_grenoblealpesmetropole_fr/g' | sed 's/demarches.lametro.fr/demarches.grenoblealpesmetropole.fr/g' > chrono.sql
```

- bijoe:

```
sudo -u bijoe pg_dump -n services_demarches_lametro_fr -n statistiques_demarches_lametro_fr | sed 's/demarches_lametro_fr/demarches_grenoblealpesmetropole_fr/g' | sed 's/demarches.lametro.fr/demarches.grenoblealpesmetropole.fr/g' > bijoe.sql
```

cela permet d'automatiquement renommer les issues dans mellon.UserSAMLIdentifier, les métadonnées des SP dans la base d'Authentic.

Pour chaque service

Authentic

- modifier le nom de domaine dans
 - hobo.json
 - settings.json (s'il existe) !\ attention à ne pas modifier le nom de domaine dans la conf LDAP s'il est utilisé dans le realm

Combo, Welco, Passerelle, Chrono, Fargo, Bijoe

- modifier le nom de domaine dans
 - idp-metadata-1.xml
 - hobo.json

Hobo

- modifier le nom de domaine dans
 - idp-metadata-1.xml
 - base_url

Bijoe

- modifier le nom de domaine dans
 - wcs-olap.ini
 - schemas/services_demarches_lametro_fr.model
 - sudo -u bijoe mv schemas/services_demarches_{lametro,grenoblealpesmetropole}_fr.model

WCS

Renommer les fichiers avec les métadonnées d'authentification

```
mv idp-https-connexion.demarches.lametro.fr-idp-saml2-metadata-metadata.xml idp-https-connexion.demarches.grenoblealpesmetropole.fr-idp-saml2-metadata-metadata.xml
```

et y remplacer l'ancien nom de domaine par le nouveau. Ex: lametro par grenoblealpesmetropole

- dans saml2-metadata.xml remplacer l'ancien nom de domaine par le nouveau: Ex: lametro par grenoblealpesmetropole
- dans site-options.cfg remplacer l'ancien nom de domaine par le nouveau: Ex: lametro par grenoblealpesmetropole
 - [options]
 - modifier: theme_skeleton_url
 - [variables]
 - modifier: idp_url
 - modifier: portal_user_url
 - modifier: portal_agent_url
 - etc...

Mettre à jour le fichier config.pck du tenant (en faisant une sauvegarde au préalable):

```
import pickle
data = pickle.load(file('config.pck'))

data['idp']['https-connexion.demarches.grenoblealpesmetropole.fr-idp-saml2-metadata'] = data['idp']['https-connexion.demarches.lametro.fr-idp-saml2-metadata']
data['idp']['https-connexion.demarches.grenoblealpesmetropole.fr-idp-saml2-metadata']['metadata'] = data['idp']['https-connexion.demarches.grenoblealpesmetropole.fr-idp-saml2-metadata']['metadata'].replace('lametro', 'grenoblealpesmetropole')
data['idp']['https-connexion.demarches.grenoblealpesmetropole.fr-idp-saml2-metadata']['metadata_url'] = data['idp']['https-connexion.demarches.grenoblealpesmetropole.fr-idp-saml2-metadata']['metadata_url'].replace('lametro', 'grenoblealpesmetropole')
data['idp'].pop('https-connexion.demarches.lametro.fr-idp-saml2-metadata')

data['saml_identities']['registration-url'] = data['saml_identities']['registration-url'].replace('lametro', 'grenoblealpesmetropole')

data['sp']['saml2_base_url'] = data['sp']['saml2_base_url'].replace('lametro', 'grenoblealpesmetropole')
data['sp']['saml2_providerid'] = data['sp']['saml2_providerid'].replace('lametro', 'grenoblealpesmetropole')

data['misc']['frontoffice-url'] = data['misc']['frontoffice-url'].replace('lametro', 'grenoblealpesmetropole')
data['misc']['homepage-redirect-url'] = data['misc']['homepage-redirect-url'].replace('lametro', 'grenoblealpesmetropole')

# optionnel
data['postgresql']['database'] = data['postgresql']['database'].replace('lametro', 'grenoblealpesmetropole')
```

```
with open('new_config.pck', 'w') as conf:
    pickle.dump(data, conf)
```

Vérifier les dans /formsdefs/, /workflows/, /mail-templates/ s'il y a des références en dur vers le nom de domaine et le remplacer.

Création des nouveaux schémas

Importer les dumps créés plus haut:

```
sudo -u hobo psql < hobo.sql
sudo -u combo psql < combo.sql
sudo -u passerelle psql < passerelle.sql
sudo -u welco psql < welco.sql
sudo -u authentic-multitenant psql authentic2_multitenant < authentic.sql
sudo -u fargo psql < fargo.sql
sudo -u chrono psql < chrono.sql
sudo -u bijoe psql < bijoe.sql
```

Renommer les répertoires des tenants

```
sudo -u authentic-multitenant mv /var/lib/authentic2-multitenant/tenants/connexion.demarches.lametro.fr.invalid.migration /var/lib/authentic2-multitenant/tenants/connexion.demarches.grenoblealpesmetropole.fr
sudo -u bijoe mv /var/lib/bijoe/tenants/statistiques.demarches.lametro.fr.invalid.migration /var/lib/bijoe/tenants/statistiques.demarches.grenoblealpesmetropole.fr
sudo -u chrono mv /var/lib/chrono/tenants/agendas.demarches.lametro.fr.invalid.migration /var/lib/chrono/tenants/agendas.demarches.grenoblealpesmetropole.fr
sudo -u combo mv /var/lib/combo/tenants/portail-agent.demarches.lametro.fr.invalid.migration /var/lib/combo/tenants/portail-agent.demarches.grenoblealpesmetropole.fr
sudo -u combo mv /var/lib/combo/tenants/demarches.lametro.fr.invalid.migration /var/lib/combo/tenants/demarches.grenoblealpesmetropole.fr
sudo -u hobo mv /var/lib/hobo/tenants/hobo.demarches.lametro.fr.invalid.migration /var/lib/hobo/tenants/hobo.demarches.grenoblealpesmetropole.fr
sudo -u fargo mv /var/lib/fargo/tenants/porte-documents.demarches.lametro.fr.invalid.migration /var/lib/fargo/tenants/porte-documents.demarches.grenoblealpesmetropole.fr
sudo -u passerelle mv /var/lib/passerelle/tenants/passerelle.demarches.lametro.fr.invalid.migration /var/lib/passerelle/tenants/passerelle.demarches.grenoblealpesmetropole.fr
sudo -u wcs mv /var/lib/wcs/services.demarches.lametro.fr.invalid.migration /var/lib/wcs/services.demarches.grenoblealpesmetropole.fr
sudo -u welco mv /var/lib/welco/tenants/accueil.demarches.lametro.fr.invalid.migration /var/lib/welco/tenants/accueil.demarches.grenoblealpesmetropole.fr
```

Démarrer les services et les crons:

```
sudo systemctl start authentic2-multitenant bijoe chrono combo fargo hobo passerelle wcs welco
```

```
sudo vi /etc/cron.d/wcs
```

Retrait de la page de maintenance et redirection vers le nouveau domaine:

```
server {
    listen 443 ssl;
    server_name accueil.demarches.lametro.fr;

    include includes/ssl.conf;
    include includes/wildcard.demarches.lametro.fr.conf;

    # include includes/maintenance.conf;
    return 302 https://accueil.demarches.lametro.fr$request_uri;
}
```

Test de la config:

```
sudo nginx -t
```

et reload si tout va bien.

Warnings

FranceConnect

Il suffit de déclarer les nouvelles URLs de retour (callback et redirection de déconnexion) en plus des anciennes, puis de retirer les anciennes un fois la migration faite. Il n'y a pas de validation faites sur ces URLs dans le back-office de FranceConnect donc pas de blocage possible.

WCS

Les demandes peuvent contenir des URLs avec l'ancien nom de domaine (typiquement les URLs vers les résas dans Chrono). Les appels webservice vers ces URLs vont échouer car ne seront pas signés.

Il faut identifier toutes les demandes ayant des URLs avec l'ancien nom de domaine dans data et workflow_data et mettre à jour.