Documentation technique Serveur Web

Table des matières

[Introduction 3](#_Toc135492599)

[1. Configuration de la machine 3](#_Toc135492600)

[2. Docker compose de traefik, authelia et nextcloud 3](#_Toc135492601)

[2.1 Docker compose 3](#_Toc135492602)

[2.2 Traefik 7](#_Toc135492603)

[2.3 Authelia 8](#_Toc135492604)

[2.4 Nextcloud 10](#_Toc135492605)

[Configuration de nextcloud 10](#_Toc135492606)

[Application SSO 12](#_Toc135492607)

[Intégration avec l’AD 13](#_Toc135492608)

[Intégration avec Authelia 14](#_Toc135492609)

# Introduction

Notre serveur web est sous ubuntu 22.0.4.

Sur ce serveur nous allons, avec docker, host nextcloud, traefik et authelia.

# Configuration de la machine

Voici les caractéristiques de la machine web :

2 Processeur

1 Cœur par processeur

4GB de memoire ram

Disque de 100 Go

# Docker compose de traefik, authelia et nextcloud

## 2.1 Docker compose

Le docker compose se trouve dans /home/appdata

version: "3.8"

volumes:

  nextcloud:

  db:

secrets:

  JWT\_SECRET:

    file: authelia/secrets/JWT\_SECRET

  SESSION\_SECRET:

    file: authelia/secrets/SESSION\_SECRET

  STORAGE\_PASSWORD:

    file: authelia/secrets/STORAGE\_PASSWORD

  STORAGE\_ENCRYPTION\_KEY:

    file: authelia/secrets/STORAGE\_ENCRYPTION\_KEY

  PASSWORD:

    file: authelia/secrets/PASSWORD

networks:

  net:

    external: true

    name: nextcloud

services:

   db:

    image: mariadb:10.6

    restart: always

    command: --transaction-isolation=READ-COMMITTED --log-bin=binlog --binlog-format=ROW

    networks:

      net: {}

    volumes:

      - db:/var/lib/mysql

    environment:

      - MYSQL\_ROOT\_PASSWORD=\*\*\*

      - MYSQL\_PASSWORD=\*\*\*

      - MYSQL\_DATABASE=nextcloud

      - MYSQL\_DATABASE=authelia

      - MYSQL\_USER=nextcloud

  app:

    image: nextcloud

    restart: always

    links:

      - db

    networks:

      net: {}

    volumes:

      - nextcloud:/var/www/html/

    environment:

      - MYSQL\_PASSWORD=\*\*\*

      - MYSQL\_DATABASE=nextcloud

      - MYSQL\_USER=nextcloud

      - MYSQL\_HOST=db

      - NEXTCLOUD\_URL=nextcloud.maxcaptab.fr

    labels:

      - 'traefik.enable=true'

      #- 'traefik.http.routers.test-redirectscheme.redirectscheme.scheme=https'

      #- 'traefik.http.routers.test-redirectscheme.redirectscheme.permanent=true'

      - 'traefik.http.routers.nextcloud.rule=Host(`nextcloud.maxcaptab.fr`)'

      - 'traefik.http.routers.nextcloud.entryPoints=https'

      - 'traefik.http.routers.nextcloud.tls=true'

      - 'traefik.http.routers.nextcloud.middlewares=authelia@docker'

      #- "traefik.http.routers.nextcloud.tls.certresolver=myresolver"

  authelia:

    container\_name: authelia

    image: docker.io/authelia/authelia:latest

    restart: unless-stopped

    networks:

      net:

        aliases:

          - "auth.maxcaptab.fr"

    expose:

      - 9091

    secrets: [JWT\_SECRET, SESSION\_SECRET, STORAGE\_PASSWORD, STORAGE\_ENCRYPTION\_KEY]

    environment:

      AUTHELIA\_JWT\_SECRET\_FILE: /run/secrets/JWT\_SECRET

      AUTHELIA\_SESSION\_SECRET\_FILE: /run/secrets/SESSION\_SECRET

      AUTHELIA\_STORAGE\_ENCRYPTION\_KEY\_FILE: /run/secrets/STORAGE\_ENCRYPTION\_KEY

    volumes:

      - ./authelia/config:/config

    labels:

      - 'traefik.enable=true'

      - 'traefik.http.routers.authelia.rule=Host(`auth.maxcaptab.fr`)'

      - 'traefik.http.routers.authelia.entryPoints=https'

      - 'traefik.http.routers.authelia.tls=true'

      #- traefik.http.routers.authelia-insecure.entrypoints=web

      #- traefik.http.routers.authelia-insecure.rule=Host(`auth.maxcaptab.fr`)

      #- traefik.http.routers.authelia-insecure.middlewares=force-secure

      - 'traefik.http.middlewares.authelia.forwardAuth.address=http://authelia:9091/api/verify?rd=https%3A%2F%2Fauth.maxcaptab.fr%2F'

      - 'traefik.http.middlewares.authelia.forwardAuth.trustForwardHeader=true'

      - 'traefik.http.middlewares.authelia.forwardAuth.authResponseHeaders=Remote-User,Remote-Groups,Remote-Name,Remote-Email'

      - 'traefik.http.middlewares.authelia-basic.forwardAuth.address=http://authelia:9091/api/verify?auth=basic'

      - 'traefik.http.middlewares.authelia-basic.forwardAuth.trustForwardHeader=true'

      - 'traefik.http.middlewares.authelia-basic.forwardAuth.authResponseHeaders=Remote-User,Remote-Groups,Remote-Name,Remote-Email'

      #- "traefik.http.routers.authelia.tls.certresolver=myresolver"

  traefik:

    container\_name: traefik

    image: traefik:v2.9

    restart: unless-stopped

    command:

      - '--api=true'

      - '--api.dashboard=true'

      - '--api.insecure=false'

      - '--pilot.dashboard=false'

      - '--global.sendAnonymousUsage=false'

      - '--global.checkNewVersion=false'

      - '--log=true'

      - '--log.level=DEBUG'

      - '--log.filepath=/config/traefik.log'

      - '--providers.docker=true'

      - '--providers.docker.exposedByDefault=false'

      - '--entryPoints.http=true'

      - '--entryPoints.http.http.redirections.entryPoint.to=https'

      - '--entryPoints.http.http.redirections.entryPoint.scheme=https'

      #- '--entrypoints.web.address=:80'

      #- '--entrypoints.web.http.redirections.entryPoint.to=websecure'

      #- '--entrypoints.web.http.redirections.entryPoint.scheme=https'

      #- '--entrypoints.web.http.redirections.entrypoint.permanent=true'

      #- '--entrypoints.websecure.address=:443'

      - '--entryPoints.http.address=:80/tcp'

      ## Please see the Forwarded Header Trust section of the Authelia Traefik Integration documentation.

      - '--entryPoints.http.forwardedHeaders.trustedIPs=10.0.1.0/24, 10.0.8.0/24,192.168.10.0/24,192.168.20.0/24,127.0.0.0/8,172.0.0.0/8'

      - '--entryPoints.http.proxyProtocol.trustedIPs=10.0.1.0/24, 10.0.8.0/24,192.168.10.0/24,192.168.20.0/24,127.0.0.0/8,172.0.0.0/8'

      - '--entryPoints.http.forwardedHeaders.insecure=false'

      - '--entryPoints.http.proxyProtocol.insecure=false'

      - '--entryPoints.https=true'

      - '--entryPoints.https.address=:443/tcp'

      ### Please see the Forwarded Header Trust section of the Authelia Traefik Integration documentation.

      - '--entryPoints.https.forwardedHeaders.trustedIPs=10.0.1.0/24, 10.0.8.0/24,192.168.10.0/24,192.168.20.0/24,127.0.0.0/8,172.0.0.0/8'

      - '--entryPoints.https.proxyProtocol.trustedIPs=10.0.1.0/24, 10.0.8.0/24,192.168.10.0/24,192.168.20.0/24,127.0.0.0/8,172.0.0.0/8'

      - '--entryPoints.https.forwardedHeaders.insecure=false'

      - '--entryPoints.https.proxyProtocol.insecure=false'

      - "--certificatesresolvers.letsencrypt.acme.email=maxoucaparros@gmail.com"

      - "--certificatesresolvers.letsencrypt.acme.storage=/config/acme.json"

      - "--certificatesresolvers.letsencrypt.acme.caserver=https://acme-v02.api.letsencrypt.org/directory"

      - "--certificatesresolvers.letsencrypt.acme.keytype=RSA4096"

      - "--certificatesresolvers.letsencrypt.acme.dnschallenge=true"

      - "--certificatesresolvers.letsencrypt.acme.dnschallenge.provider=cloudflare"

      - "--certificatesresolvers.letsencrypt.acme.dnschallenge.delaybeforecheck=0"

      - "--certificatesresolvers.letsencrypt.acme.dnschallenge.resolvers=1.1.1.1:53,8.8.8.8:53"

    networks:

          net: {}

    ports:

      - "80:80"

      - "443:443"

      - "8443:443"

      - "8080:80"

    volumes:

      - /var/run/docker.sock:/var/run/docker.sock

      - ./traefik/data/traefik:/config

      #- "./cert/:/certs/"

      #- ./letsencrypt:/letsencrypt

      #- ./acme.json:/acme.json

      #- ./traefik.yml:/etc/traefik/traefik.yml

    labels:

      - 'traefik.enable=true'

      # middleware redirect

      - traefik.http.middlewares.force-secure.redirectscheme.scheme=https

      - traefik.http.middlewares.force-secure.redirectscheme.permanent=true

      #- 'traefik.http.routers.reverse-proxy.rule=Host(`maxcaptab.fr`)'

      - 'traefik.http.routers.api.rule=Host(`traefik.maxcaptab.fr`)'

      - 'traefik.http.routers.api.entryPoints=https'

      - 'traefik.http.routers.api.tls=true'

      - 'traefik.http.routers.api.service=api@internal'

      - 'traefik.http.routers.api.middlewares=authelia@docker'

      #- "traefik.http.routers.api.tls.certresolver=myresolver"

    depends\_on:

      - authelia

## Traefik

Pour traefik voici la configuration qu’on a mis en place :

* Redirection http -> https
* Port 80 pour http et 443 pour https
* Trusted IP 10.0.1.0/24 pour le VPN admin et 10.0.8.0/24 pour le VPN User. Ensuite les IPs local
* Nous avons aussi essayé de récupérer un certificat avec letsencrypt pour notre nom de domaine : maxcaptab.fr
* Nous avons configuré le middleware authelia@docker pour utiliser le SSO d’authelia
* Nous stockons les logs dans /home/appdata/traefik/traefik/data/traefik
* Nous avons utilisé depends\_on : authelia, pour pouvoir lancer traefik après authelia.

## Authelia

Nous avons tout d’abord créé des clés secrètes pour encrypter Authelia.

Les secrets se trouvent dans /home/appdata/authelia/secrets

Ensuite nous avons créé un alias pour que les autres containers puissent utiliser l’alias afin de communiquer avec authelia.

Nous avons configuré le middleware pour qu’il fonctionne.

Pour la configuration d’authelia nous avons utilisé les configurations suivantes :

default\_redirection\_url: "https://nextcloud.maxcaptab.fr"

authentication\_backend:

 ldap:

 implementation: activedirectory

 url: ldap://192.168.10.10:389

start\_tls: false

 tls:

  server\_name: server-AD

  base\_dn: dc=contoso,dc=adds

  username\_attribute: sAMAccountName

  users\_filter: (&({username\_attribute}={input})(objectCategory=person)(objectClass=user))

  groups\_filter: (&(member:1.2.840.113556.1.4.1941:={dn})(objectClass=group)(objectCategory=group))

  group\_name\_attribute: cn

  mail\_attribute: mail

  display\_name\_attribute: displayName

  permit\_referrals: false

  user: CN=pfsense admin,OU=admin,OU=AllUser;DC=contoso,DC=adds

  password: \*\*\*

rules :

access\_control:

  default\_policy: one\_factor

  networks:

    - name: internal

      networks:

        - 192.168.99.0/24

        - 192.168.20.0/24

        - 192.168.10.0/24

    - name: VPN

      networks: 10.0.1.0/24

  rules:

    ## Rules applied to everyone

    - domain: '\*.maxcaptab.fr'

      policy: one\_factor

      networks:

        - internal

        - VPN

    - domain: '\*'

      policy: one\_factor

identity\_providers:

  oidc:

    hmac\_secret: Slj^2tvRREiA86Rgaw%G^1E1%mC8H\*o#rq#jWU0vkwFHCa\*

issuer\_private\_key: | \*\*\*\*

 clients:

      -

        id: nextcloudID

        description: Nextcloud

        secret: '!HydLZ2RcQwvOzwwlgqr2epM0S\*!XrmaMG@rcc5\*ebFc3z4$UciBOV5zl7BCHZJklu@7IsOQd4IhI'

        public: false

        authorization\_policy: one\_factor

        consent\_mode: auto

        pre\_configured\_consent\_duration: 1w

        audience: []

        scopes:

          - openid

          - groups

          - email

          - profile

        redirect\_uris:

        - https://nextcloud.maxcaptab.fr/apps/oidc\_login/oidc

## Nextcloud

### Configuration de nextcloud

Une image contenant texte, capture d’écran, Police, Système d’exploitation

Description générée automatiquement

On installe ensuite les applications recommandées :

Une image contenant texte, capture d’écran, multimédia, logiciel

Description générée automatiquement

Puis on se dirige dans l’es options d’administrations

Une image contenant texte, capture d’écran, logiciel, multimédia

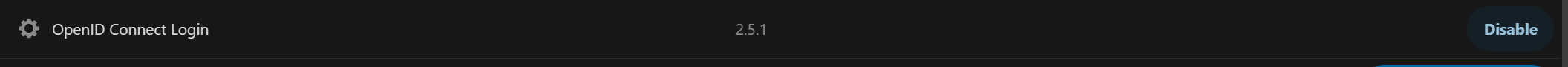
Description générée automatiquement

### Application SSO

Pour l’application SSO nous utiliserons OpenId connect login qui va nous permettre de lier les logins Authelia avec nextcloud.

Une image contenant texte, capture d’écran, logiciel, Système d’exploitation

Description générée automatiquement



### Intégration avec l’AD

Nextcloud permet une intégration dans l’AD très facile il suffit de faire la conf suivante :

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

### Intégration avec Authelia

Il faut changer le fichier config.php d’Authelia et rentrer la config suivante :

$CONFIG = **array** (

'allow\_user\_to\_change\_display\_name' => false,

'lost\_password\_link' => 'disabled',

'oidc\_login\_provider\_url' => 'https://auth.maxcaptab.fr,

'oidc\_login\_client\_id' => 'nextcloud',

'oidc\_login\_client\_secret' => 'insecure\_secret',

'oidc\_login\_auto\_redirect' => false,

'oidc\_login\_end\_session\_redirect' => false,

'oidc\_login\_button\_text' => 'Log in with Authelia',

'oidc\_login\_hide\_password\_form' => false,

'oidc\_login\_use\_id\_token' => true,

'oidc\_login\_attributes' => **array** (

'id' => 'preferred\_username',

'name' => 'name',

'mail' => 'email',

'groups' => 'groups',

),

'oidc\_login\_default\_group' => 'oidc',

'oidc\_login\_use\_external\_storage' => false,

'oidc\_login\_scope' => 'openid profile email groups',

'oidc\_login\_proxy\_ldap' => false,

'oidc\_login\_disable\_registration' => true,

'oidc\_login\_redir\_fallback' => false,

'oidc\_login\_alt\_login\_page' => 'assets/login.php',

'oidc\_login\_tls\_verify' => true,

'oidc\_create\_groups' => false,

'oidc\_login\_webdav\_enabled' => false,

'oidc\_login\_password\_authentication' => false,

'oidc\_login\_public\_key\_caching\_time' => 86400,

'oidc\_login\_min\_time\_between\_jwks\_requests' => 10,

'oidc\_login\_well\_known\_caching\_time' => 86400,

'oidc\_login\_update\_avatar' => false,

);

Avec cette configuration nous allons pouvoir nous connecter à Nextcloud avec les logins d’Authelia.