

Mise en place d'un serveur de monitoring Icinga

Gitea - Git with a cup of tea



Dans cette documentation nous installerons une solution de supervision nommée Icinga 2.

Cette documentation est réalisée dans le cadre d'un TP guidé, il peut donc y avoir d'autre méthode plus ou moins simple pour y parvenir. Pour mieux s'y retrouver cette documentation disposera de plusieurs screenshots illustrant les consignes.

Préambule

Nous considérons que vous êtes équipé de cette manière :

1. Une VM sous Debian 11 vierge **[GITEA]**

Les allocations de matériel (CPU/RAM...) sont à allouer selon vos envies, attention à respecter la configuration minimale. C'est à dire :

Pour **Icinga** :

1. 2GB de ram
2. 2 cœurs de CPU
3. 60GB d'espace disque
4. *Debian 11*

Nos IP pour notre infrastructure seront :

1. [Icinga] : **10.192.43.58**

Mot de passe par défaut sur toutes les sessions : **Not24get**

Rappel des deux commandes essentielles :

1. ip a (connaitre son adresse IP)
2. nano /etc/network/interfaces (configuration de l'interface réseau)

Conseil : Ajouter les deux machines dans un logiciel tel que mRemoteNG pour faciliter

l'administration.

Installation de Icinga

Ajouter dans les sources.list le repo

```
apt-get update  
apt-get -y install apt-transport-https wget gnupg  
  
wget -O - https://packages.icinga.com/icinga.key | gpg --dearmor -o  
/usr/share/keyrings/icinga-archive-keyring.gpg  
  
DIST=$(awk -F"[\n ]+" '/VERSION=/ {print $2}' /etc/os-release); \  
echo "deb [signed-by=/usr/share/keyrings/icinga-archive-keyring.gpg]  
https://packages.icinga.com/debian icinga-${DIST} main" > \  
/etc/apt/sources.list.d/${DIST}-icinga.list  
echo "deb-src [signed-by=/usr/share/keyrings/icinga-archive-keyring.gpg]  
https://packages.icinga.com/debian icinga-${DIST} main" >> \  
/etc/apt/sources.list.d/${DIST}-icinga.list
```

Terminer avec :

```
apt-get update
```

Vérification GPG

```
apt install gpg  
gpg --keyserver keys.openpgp.org --recv  
7C9E68152594688862D62AF62D9AE806EC1592E2  
gpg --verify gitea-1.17.3-linux-amd64.asc gitea-1.17.3-linux-amd64
```

Installation des dépendances

GIT

```
apt install git
```

Vérifier avec :

```
git --version
```

MariaDB

```
apt install mariadb-server
```

```
mysql_secure_installation
```

Suivez la procédure d'installation de MariaDB.

Vérifier la bonne exécution avec :

```
systemctl status mariadb
```

apache2

```
apt-get install apache2
```

Création utilisateur

Dans le système

snippet.sh

```
adduser \
--system \
--shell /bin/bash \
--gecos 'Git Version Control' \
--group \
--disabled-password \
--home /home/git \
gitea
```

Dans le SGBD

```
mysql -uroot -p
```

snippet.sql

```
CREATE USER giteaDBuser IDENTIFIED BY 'Not24get';
CREATE DATABASE giteaDB DEFAULT CHARACTER SET utf8 DEFAULT COLLATE
utf8_general_ci;
GRANT ALL PRIVILEGES ON giteaDB.* TO giteaDBuser;
FLUSH PRIVILEGES;
```

- Tester la connexion :

```
mysql -u giteaDBuser -p -e "SHOW DATABASES;"
```

Création structure de dossier

Dossiers Gitea conf

```
mkdir -p /var/lib/giteadir/{custom,data,log}
chown -R gitea:gitea /var/lib/giteadir/
chmod -R 750 /var/lib/giteadir/
mkdir /var/lib/giteadir/custom/conf
ln -s /var/lib/giteadir/custom/conf /etc/gitea
chown root:gitea /etc/gitea
chmod 770 /etc/gitea
```

Permissions dossiers

```
chmod 750 /etc/gitea
chmod 640 /etc/gitea/app.ini
```

Définition des variables

snippet.sh

```
export GITEA_WORK_DIR=/var/lib/giteadir/
```

Copie de Gitea

snippet.sh

```
cp gitea /usr/local/bin/gitea
```

Essai de Gitea (exécution du binary)

- Changer d'utilisateur :

```
su gitea
```

- Exécuter Gitea

```
GITEA_WORK_DIR=/var/lib/giteadir/ /usr/local/bin/gitea web -c
/etc/gitea/app.ini
```

Reset mot de passe compte administrateur "gitea"

En cas de perte du mot de passe voici la commande à utiliser :

```
gitea -c /etc/gitea/app.ini admin user change-password -u gitea -p
"motdepasse"
```

Création d'un service systemd

- Copier dans /etc/systemd/system/gitea.service :

[snippet.sh](#)

```
[Unit]
Description=Gitea (Git with a cup of tea)
After=syslog.target
After=network.target
Wants=mariadb.service
After=mariadb.service

[Service]
RestartSec=2s
Type=simple
User=gitea
Group=
WorkingDirectory=/var/lib/giteadir/
ExecStart=/usr/local/bin/gitea web --config /etc/gitea/app.ini
Restart=always
Environment=USER=gitea HOME=/home/git GITEA_WORK_DIR=/var/lib/giteadir

[Install]
WantedBy=multi-user.target
```

- Activer le service et démarrer le avec :

```
systemctl enable gitea
systemctl start gitea
systemctl status gitea
```

Configuration du serveur SQL sur Gitea

- Type : mysql
- Hôte : 127.0.0.1:3306
- Nom : giteaDB
- Nom d'utilisateur : giteaDBuser

Gitea nécessite MySQL, PostgreSQL, MSSQL, SQLite3 ou TiDB (avec le protocole MySQL).

Type de base de données * MySQL

Hôte * 127.0.0.1:3306

Nom d'utilisateur * giteaDBuser

Mot de passe * *****

Nom de base de données * giteaDB

Note aux utilisateurs de MySQL : utilisez le moteur de stockage InnoDB et si vous utilisez "utf8mb4", votre version InnoDB doit être supérieure à 5.6.

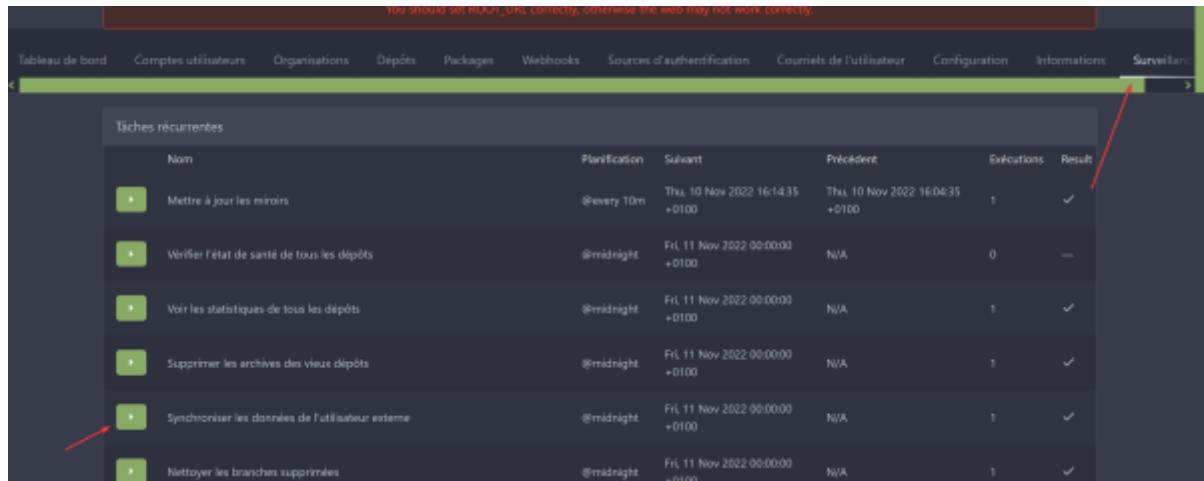
Jeu de caractères * utf8mb4

Ajout authentification LDAP

Type d'authentification LDAP (via BindDN)

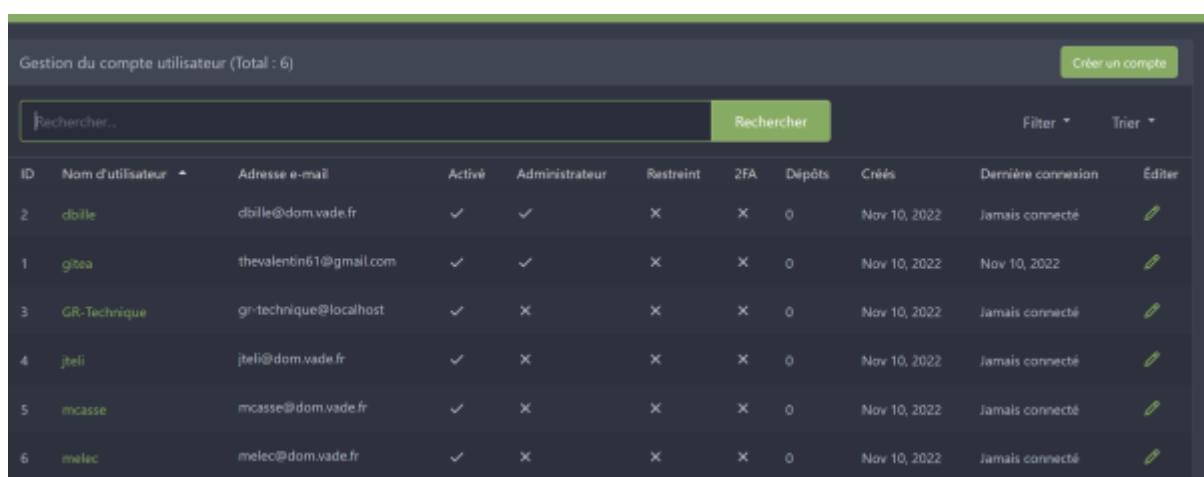
- Hôte : 10.192.43.10
- Port : 389
- Bind DN : CN=srv-gitea,OU=LDAP,OU=Utilisateurs,DC=dom,DC=vade,DC=fr
- Bind mot de passe : password
- Utilisateur Search Base : DC=dom,DC=vade,DC=fr
- Filtre utilisateur : (&(memberof:1.2.840.113556.1.4.1941:=cn=GG-Git-Users,ou=GG,ou=Groupes,dc=dom,dc=vade,dc=fr)(|(userPrincipalName=%[1]\$)(sAMAccountName=%[1]\$)))
- Filtre administrateur : (memberof=cn=GG-Git-Admins,ou=GG,ou=Groupes,dc=dom,dc=vade,dc=fr)
- Attribut nom d'utilisateur : sAMAccountName
- Attribut prénom : givenName
- Attribut nom de famille : sn
- Attribut e-mail : userPrincipalName

Une fois les champs remplis, mettre à jour manuellement la BDD en allant :



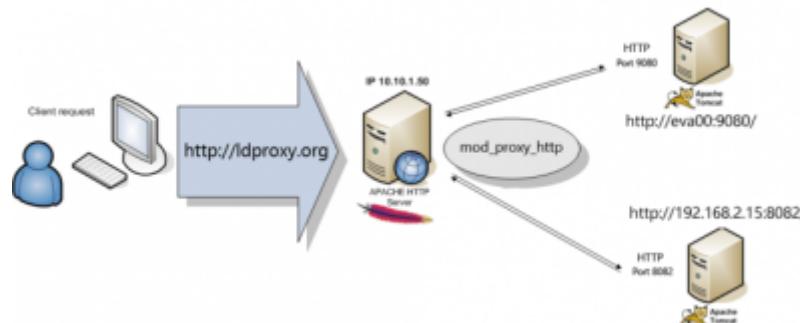
Nom	Planification	Suivant	Précédent	Exécutions	Résultat
Mettre à jour les miroirs	@every 10m +0100	Thu, 10 Nov 2022 16:14:35 +0100	Thu, 10 Nov 2022 16:04:35 +0100	1	✓
Vérifier l'état de santé de tous les dépôts	@midnight +0100	Fri, 11 Nov 2022 00:00:00 +0100	N/A	0	—
Voir les statistiques de tous les dépôts	@midnight +0100	Fri, 11 Nov 2022 00:00:00 +0100	N/A	1	✓
Supprimer les archives des vieux dépôts	@midnight +0100	Fri, 11 Nov 2022 00:00:00 +0100	N/A	1	✓
Synchroniser les données de l'utilisateur externe	@midnight +0100	Fri, 11 Nov 2022 00:00:00 +0100	N/A	1	✓
Nettoyer les branches supprimées	@midnight +0100	Fri, 11 Nov 2022 00:00:00 +0100	N/A	1	✓

Voici les utilisateurs une fois synchronisés :



ID	Nom d'utilisateur	Adresse e-mail	Activé	Administrateur	Restreint	2FA	Dépôts	Créés	Dernière connexion	Editer
2	dbille	dbille@dom.vade.fr	✓	✓	✗	✗	0	Nov 10, 2022	Jamais connecté	✍
1	gitea	thevalentin61@gmail.com	✓	✓	✗	✗	0	Nov 10, 2022	Nov 10, 2022	✍
3	GR-Technique	gr-technique@localhost	✓	✗	✗	✗	0	Nov 10, 2022	Jamais connecté	✍
4	jtel	jtel@dom.vade.fr	✓	✗	✗	✗	0	Nov 10, 2022	Jamais connecté	✍
5	mcasse	mcasse@dom.vade.fr	✓	✗	✗	✗	0	Nov 10, 2022	Jamais connecté	✍
6	melec	melec@dom.vade.fr	✓	✗	✗	✗	0	Nov 10, 2022	Jamais connecté	✍

Reverse proxy avec apache et ajout d'un certificat SSL



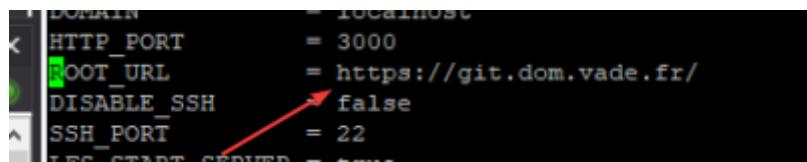
Modification configuration root_url (pour passer en https)

- Avant de lancer l'installation :



- Après avoir lancé l'installation :

```
nano /etc/gitea/app.ini
```



Création de la config apache2

- Activer l'option reverse_proxy :

```
a2enmod proxy proxy_http
service apache2 restart
```

- Créer la configuration dans les *sites-available* :

```
nano /etc/apache2/sites-available/git.dom.vade.fr.conf
```

[snippet.sh](#)

```
<VirtualHost *:80>
    ServerName git.dom.vade.fr
    Redirect permanent / https://git.dom.vade.fr/
</VirtualHost>
<VirtualHost *:443>
    ServerName git.dom.vade.fr
    ServerAdmin valentin@moimeme.fr

    ProxyPass / http://127.0.0.1:3000/
    ProxyPassReverse / http://127.0.0.1:3000/
    ProxyRequests Off
</VirtualHost>
```

- Activer la configuration :

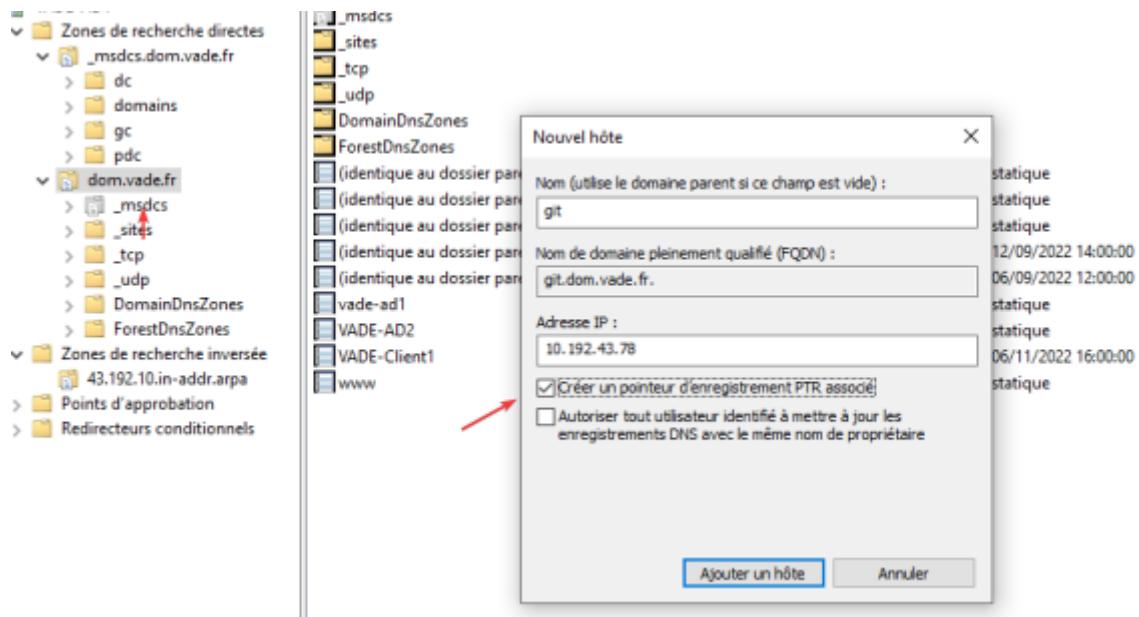
```
a2ensite git.dom.vade.fr.conf
systemctl apache2 reload
```

- Puis vérifier :

```
systemctl status apache2
```

Ajout de la règle CNAME dans le DNS

- Créer la règle DNS en recherche directe dans le serveur DNS :



Création certificat auto-signé sur git.dom.vade.fr

```
apt-get install openssl
```

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -sha256 -out /etc/apache2/server.crt -keyout /etc/apache2/server.key
```

Suivre la procédure pour générer le certificat, mettre en FQDN : git.dom.vade.fr.

- Ajout dans le virtual-host:443 le certificat :

```
nano /etc/apache2/sites-available/git.dom.vade.fr.conf
```

```
SSLEngine on
SSLCertificateFile /etc/apache2/server.crt
SSLCertificateKeyFile /etc/apache2/server.key
```

- Activer le SSL :

```
a2enmod ssl
```

Puis redémarrer le service :

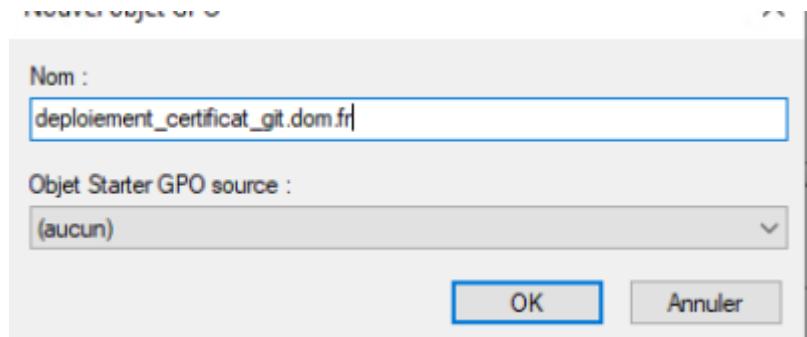
```
systemctl restart apache2
```

Déploiement GPO du certificat

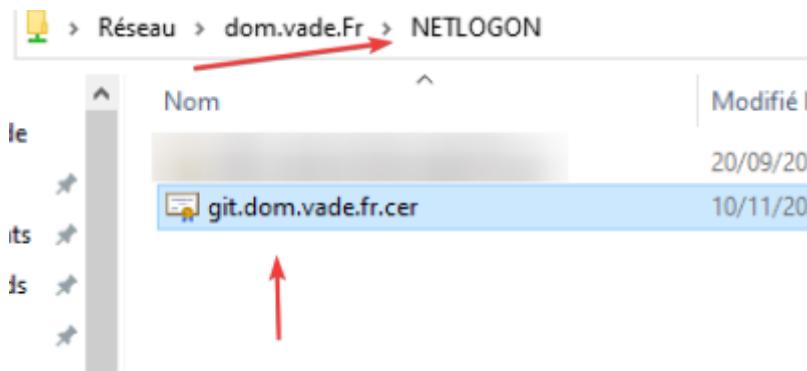


Rappel, utilitaire de certificat sur windows : certmgr.msc

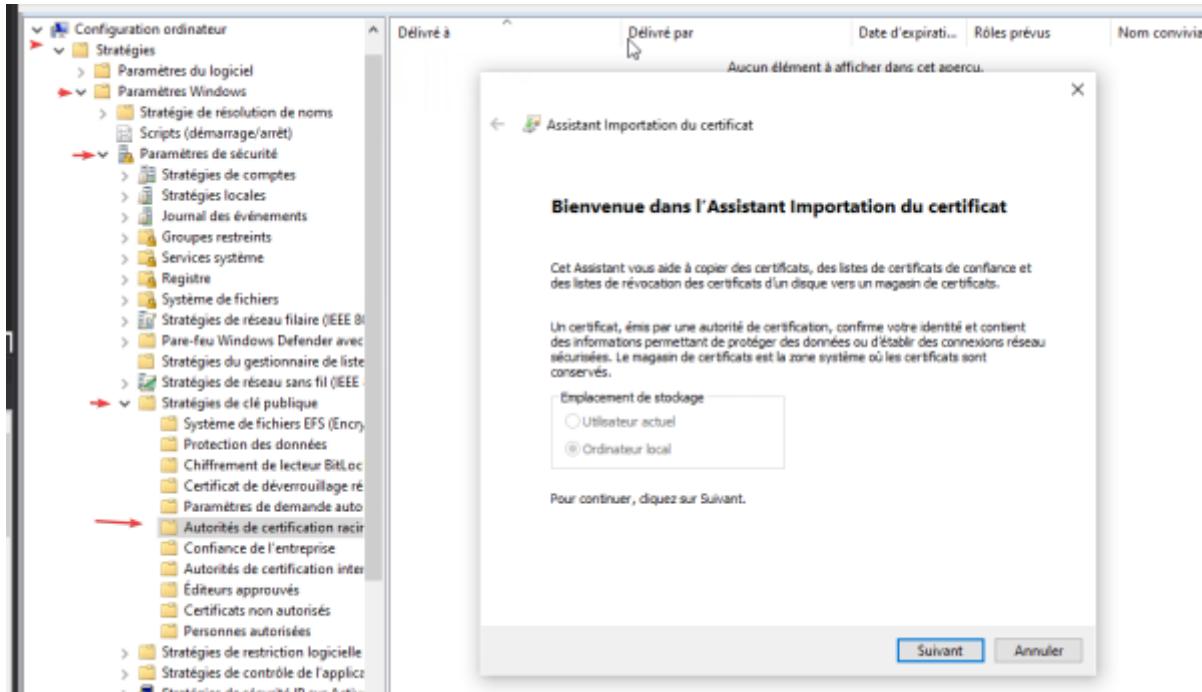
- Création de la GPO :



- Mettre le certificat dans le NETLOGON du serveur :



- Ajout du certificat dans l'importation :



- Test du déploiement du certificat

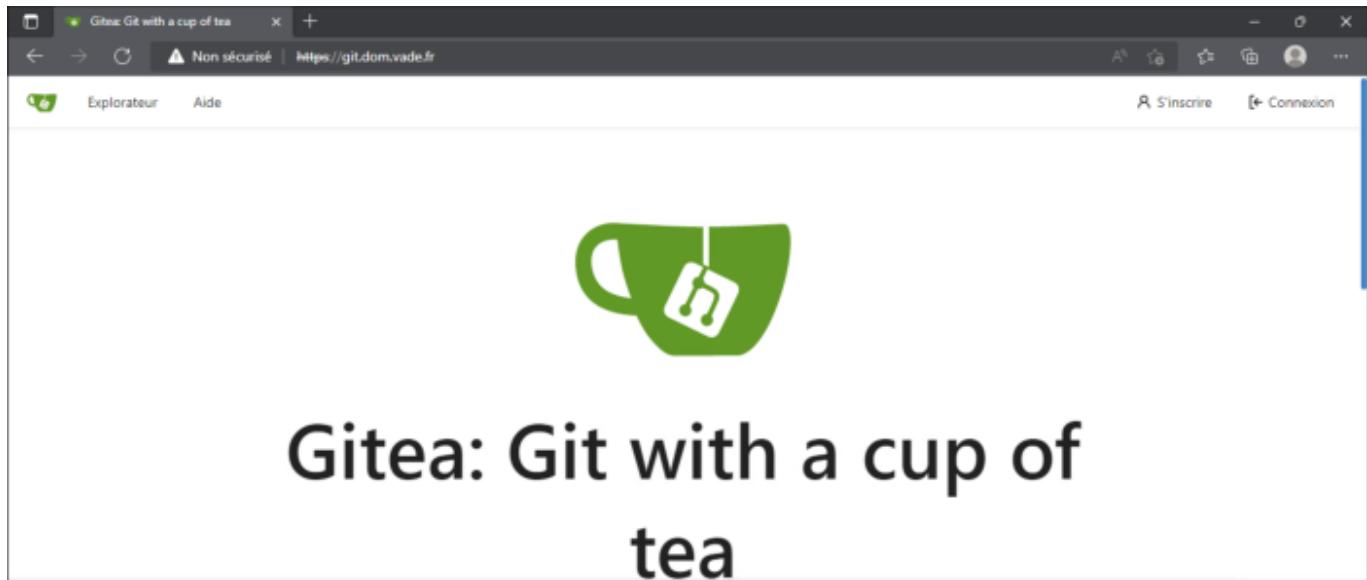
- Redémarrer le poste
- Ouvrir la console MMC de gestion de certificat sur l'ordinateur local et aller sur Autorité de certification racines de confiance et vérifier la présence du certificat.

certmgr - [Certificats - Utilisateur actuel\Autorités de certification racines de confiance\Certificats]							
	Délivré à	Délivré par	Date d'expirati...	Rôles prévus	Nom convivial	Statut	Modèle de cert...
> Personnel					Sectigo (AAA)		
✓ Autorités de certification racines de confiance					DigiCert Baltimore ...		
Certificates					VenSign Class 3 Pu...		
> Confiance de l'entreprise					Microsoft Timesca...		
> Autorités de certification intermédiaires					DigiCert		
> Objet utilisateur Active Directory					DigiCert Global Root...		
> Éditeurs approuvés					DigiCert Global Root G2		
> Certificats non autorisés					DigiCert High Assurance EV Ro...		
> Autorités de certification racine tierce partie					DigiCert Trusted Root G4		
> Personnes autorisées					git.dom.vade.fr		
> Émetteurs d'authentification de client					GlobalSign Root CA		
> Local NonRenouvelable Certificates							

Le certificat est présent sur le client.

Essai HTTPS client windows

Les navigateurs moderne notifie l'utilisateur en cas d'utilisation d'un certificat auto-signé.



Mes sources

1. <https://docs.gitea.io/en-us/install-from-binary/>
2. <https://rdr-it.com/gpo-deployer-un-certificat/>

From:

<https://wiki.stoneset.fr/> - **StoneSet - Documentations**

Permanent link:

<https://wiki.stoneset.fr/doku.php?id=wiki:linux:icinga2&rev=1669049624>

Last update: **2022/11/21 17:53**

