Installation d’un serveur de supervision Zabbix

Sous Debian 13

1. Contexte et objectif de l'atelier

L'infrastructure de SODECAF a déjà été réorganisée et segmentée lors de l'atelier 1, avec mise en place d'un domaine Active Directory team21.local et d'un adressage structuré par VLAN. Un service de partage de fichiers Nextcloud sécurisé a ensuite été déployé sur un serveur Linux dédié (172.16.21.5) avec HTTPS, intégration LDAP/AD, chiffrement, sauvegardes et mesures de durcissement.

Malgré ces évolutions, l'entreprise ne dispose pas encore d'une vision centralisée de l'état réel de son système d'information. L'objectif de cet atelier est donc de concevoir et déployer une solution de supervision basée sur Zabbix, permettant de surveiller les équipements réseau, les serveurs clés (Windows et Linux) et les services critiques (DNS/AD, Nextcloud, ressources systèmes), avec une interface exploitable et une documentation adaptée à une petite équipe informatique

2. Périmètre de supervision retenu

Conformément au cahier des charges, le périmètre minimal doit couvrir au moins :

- Un équipement d'interconnexion principal et un commutateur principal (ou un commutateur représentatif).
- Le contrôleur de domaine
- Le serveur ayant hébergé le service mis en place lors de l'atelier précédent (Nextcloud).
- Plusieurs services / indicateurs utiles : disponibilité réseau, accès HTTP/HTTPS, espace disque, charge système, mémoire, disponibilité de services applicatifs

2.1. Liste des hôtes et services supervisés

Élément	Rôle	Type	Justification
Routeur (d'interconnexion principale)	Accès vers les autres réseaux / Internet, point critique de connectivité	Équipement réseau	Toute coupure ou saturation affecte l'ensemble des utilisateurs
Switch principal	Commutation cœur de réseau, agrégation des VLAN	Équipement réseau	Point central de la topologie locale, indispensable au trafic interne

Serveur Windows AD/DNS (172.16.21.1)	Contrôleur de domaine + DNS interne	Serveur Windows	Sans AD/DNS, authentification, résolution de noms et services internes sont dégradés
Serveur Linux Nextcloud (172.16.21.3)	Service de partage de fichiers sécurisé	Serveur Linux	Service métier critique pour les échanges de documents, lié aux risques identifiés (intégrité, disponibilité, confidentialité)
Serveur Zabbix (Debian 13)	Plateforme de supervision	Serveur Linux	Surveille les autres et doit lui-même être surveillé (ressources, disponibilité)

Ce périmètre permet de couvrir à la fois la connectivité réseau (routeur + switch), l'infrastructure d'annuaire et de nommage (AD/DNS), le service applicatif critique (Nextcloud) et l'outil de supervision lui-même (Zabbix).

2.2. Indicateurs et services supervisés

Principaux indicateurs configurés :

- **Disponibilité réseau des hôtes** (ping ICMP).
- **Ressources systèmes** (CPU, RAM, espace disque, charge) sur le serveur AD/DNS et sur le serveur Nextcloud.
- Services critiques:
    - **AD/DNS sur le serveur Windows** (ports LDAP/LDAPS, DNS).
    - **Service web Nextcloud** (accès HTTPS via Nginx).
- **Équipements réseau** : état ICMP, et si disponible, SNMP sur le routeur et le switch (état des interfaces, trafic sur les ports principaux).

Ces choix répondent directement aux menaces et risques identifiés autour du service Nextcloud (disques saturés, pannes matérielles, indisponibilité, ransomware, fuite de données, etc.).

3. Solution retenue : Zabbix et intérêt pour SODECAF

La solution Zabbix a été retenu pour la supervision. Zabbix est une plateforme open source de supervision permettant de surveiller serveurs, équipements réseau et services applicatifs via des agents, des sondes ICMP, SNMP et des scénarios web.

Intérêts de Zabbix pour SODECAF :

- Open source et gratuit, adapté à une petite équipe informatique.
- Architecture modulaire :
    - Un serveur central Zabbix.
    - Une base de données PostgreSQL.
    - Un frontend web en PHP hébergé sur Apache.
    - Des agents Zabbix sur les hôtes Windows et Linux.
- Supervision hétérogène : Windows, Linux, routeurs, switches, services HTTP/HTTPS.
- Interface web centralisée avec tableaux de bord, listes de problèmes, graphiques et historiques de performance.
- Évolutivité : possibilité d'ajouter facilement de nouveaux hôtes, templates, scénarios web et mécanismes de notification (e-mail, messagerie, etc.).

Prérequis techniques retenus :

- **OS** : Debian 13 sur le serveur Zabbix (machine virtuelle déjà installée).
- **Base de données** : PostgreSQL (au lieu de MariaDB).
- **Serveur web** : Apache.
- **Accès web** : Zabbix accessible en **HTTPS** via Apache.
- **Réseau** : serveur placé dans le VLAN des serveurs, avec un nom DNS interne du type zabbix.team21.local.

4. Installation de la solution Zabbix

L'objectif de cette partie est de présenter l'environnement utilisé, les prérequis, les étapes principales d'installation, ainsi que les difficultés et ajustements réalisés, sans détailler chaque capture d'écran de l'assistant web.

4.1 Environnement et prérequis

- Machine virtuelle Debian 13, à jour (apt update && apt upgrade -y).
- Accès root ou sudo pour installer paquets et services.

- Résolution DNS fonctionnelle pour zabbix.team21.local.
- Ports ouverts entre Zabbix et les hôtes :
    - 10051/TCP pour le serveur Zabbix.
    - 10050/TCP pour les agents Zabbix.
    - 161/UDP pour SNMP (routeur, switch, si utilisé).
    - ICMP autorisé pour les tests de ping.

4.2 Ajout du dépôt Zabbix et installation des paquets

1. Mise à jour du système :

```
apt update
apt upgrade –y
apt autoremove –y
```

2. Ajout du dépôt Zabbix :

```
# Télécharger le dépôt Zabbix 8.0 pour Debian 13
wget https://repo.zabbix.com/zabbix/8.0/release/debian/pool/main/z/zabbix-release/zabbix-release_latest_8.0+debian13_all.deb
# Installer le dépôt
dpkg -i zabbix-release_latest_8.0+debian13_all.deb
# Mettre à jour les repos
apt update
```

3. Installation de Zabbix Server + Frontend + Agent + apache2 + PHP-FPM :

```
# Télécharger le dépôt Zabbix 8.0 pour Debian 13
wget https://repo.zabbix.com/zabbix/8.0/release/debian/pool/main/z/zabbix-release/zabbix-release_latest_8.0+debian13_all.deb
```

```
apt install -y zabbix-server-pgsql zabbix-frontend-php php-pgsql php-gd php-simplexml php-xmlrpc php-xsl php-curl zabbix-sql-scripts zabbix-agent2 php-fpm zabbix-get
```

4. Installation de PostgreSQL (base de données)

Zabbix supporte MySQL et PostgreSQL. On utilise PostgreSQL ici (plus léger et performant).

```
apt install -y postgresql postgresql-contrib
```

Vérifier que PostgreSQL tourne :

```
systemctl status postgresql
# Doit afficher "active (running)"
```

4.3. Création de la base PostgreSQL et import du schéma

1. Création de l'utilisateur et de la base Zabbix

```
sudo -u postgres psql
CREATE USER zabbix WITH ENCRYPTED PASSWORD '1234';
CREATE DATABASE zabbix
   WITH ENCODING 'UTF8'
   TEMPLATE template0
   OWNER zabbix;
/q
```

2. Import du schéma de base Zabbix pour PostgreSQL

```
# Importer la base de données
zcat /usr/share/zabbix/sql-scripts/postgresql/server.sql.gz | sudo -u zabbix psql zabbix
```

(Cette opération peut prendre quelques minutes en fonction des performances du serveur.)

4.4 Configuration du serveur Zabbix

Éditer le fichier de configuration :

```
nano /etc/zabbix/zabbix_server.conf
```

Chercher et modifier/décommenter les lignes suivantes :

```
# Database
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=1234

# Cache et performance (pour petit réseau, par défaut c'est ok)
CacheSize=32M
HistoryCacheSize=16M
TrendCacheSize=4M

# Logs
LogFile=/var/log/zabbix/zabbix_server.log
LogFileSize=100
```

Sauvegarder et quitter (Ctrl+S,Crtl+X).

4.5 Configuration de Apache et HTTPS pour Zabbix

1. Générer un certificat HTTPS pour zabbix.team21.local (auto-signé ou via l'AC interne, sur le même modèle que pour Nextcloud) :

```
mkdir -p /etc/ssl/private/zabbix.team21.local
cd /etc/ssl/private/zabbix.team21.local

openssl req -x509 -nodes -days 825 -newkey rsa:4096 –keyout
zabbix.team21.local.key -out zabbix.team21.local.crt -subj "/C=FR/L=Brive-la-
Gaillarde/O=SODECAF/CN=zabbix.team21.local"
```

2. Contenu du fichier /etc/apache2/sites-available/zabbix.conf :

```
<VirtualHost *:80>
   ServerName zabbix.team21.local
   ServerAdmin admin@team21.local

   DocumentRoot /usr/share/zabbix/ui

   # Redirection de tout le HTTP vers le HTTPS
   Redirect / https://zabbix.team21.local/

   <Directory /usr/share/zabbix/ui>
      Require all granted
      AllowOverride All
      Options FollowSymLinks MultiViews
   </Directory>

   ErrorLog ${APACHE_LOG_DIR}/zabbix_error.log
   CustomLog ${APACHE_LOG_DIR}/zabbix_access.log combined
</VirtualHost>

<VirtualHost *:443>
   ServerName zabbix.team21.local
   ServerAdmin admin@team21.local
```

```
    DocumentRoot /usr/share/zabbix/ui

    SSLEngine on
    SSLCertificateFile /etc/ssl/private/zabbix.team21.local/zabbix.team21.local.crt
    SSLCertificateKeyFile
/etc/ssl/private/zabbix.team21.local/zabbix.team21.local.key

    SSLProtocol -all +TLSv1.3 +TLSv1.2
    SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-
AES256-GCM-SHA384
    SSLHonorCipherOrder on
    SSLCompression off

    Header always set Strict-Transport-Security "max-age=31536000;
includeSubDomains"
    Header always set X-Content-Type-Options "nosniff"
    Header always set X-Frame-Options "SAMEORIGIN"
    Header always set X-XSS-Protection "1; mode=block"

    <Directory /usr/share/zabbix/ui>
        Require all granted
        AllowOverride All
        Options FollowSymLinks MultiViews
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/zabbix_ssl_error.log
    CustomLog ${APACHE_LOG_DIR}/zabbix_ssl_access.log combined
</VirtualHost>
```

3. Activer le site et vérifier la configuration :

```
a2ensite zabbix.conf
a2dissite 000-default.conf # si ce n'est pas déjà fait
systemctl reload apache2
apache2ctl configtest # doit afficher "Syntax OK"
```

4. Démarrer les services au boot et les relancer

```
systemctl enable zabbix-server zabbix-agent2 apache2 php8.4-fpm postgresql
systemctl restart zabbix-server zabbix-agent2 apache2 php8.4-fpm postgresql
```

5. Vérifier que tout tourne :

```
systemctl status zabbix-server
systemctl status zabbix-agent2
systemctl status apache2
systemctl status php8.4-fpm
systemctl status postgresql
```

Tous doivent afficher "active (running)".

En cas de problème vérifer les logs :

```
tail -50 /var/log/zabbix/zabbix_server.log
```

4.6 Assistant web d'installation Zabbix

L'accès à l'interface se fait désormais via :

https://zabbix.team21.local/zabbix

Vous devriez voir l'assistant d'installation Zabbix. Cliquer sur **Next step**.

1. **Check of pre-requisites** : Tout doit être en vert. Cliquer **Next step**.
2. **Configure DB connection** :
    a. Host: localhost

   b. Port: 0 (Utilisera le port par défaut)
   c. Database: zabbix
   d. User: zabbix
   e. Password: 1234
   f. Cliquer **Next step**
3. **Zabbix server details** :
   a. Host: localhost (ou IP du serveur)
   b. Port: 10051
   c. Cliquer **Next step**
4. **Pre-Installation summary** : Vérifier les infos, cliquer **Next step**.
5. **Installation complete** :
   a. Message "Congratulations! You have successfully installed the Zabbix frontend."
   b. Cliquer **Finish**

Identifiants par défaut :

- Username: Admin
- Password: zabbix (à modifier immédiatement pour des raisons de sécurité)

Cliquer **Sign in**.