Documentation d’exploitation de Zabbix

Sous Debian 13

Table des matières

1. Objet et périmètre

Cette documentation a pour but d'expliquer à un technicien comment exploiter la supervision Zabbix mise en place pour SODECAF, sans rentrer dans les détails d'installation ou d'architecture. Elle décrit les actions courantes à réaliser : se connecter à l'interface, comprendre l'organisation générale, identifier les hôtes et les services supervisés, ajouter un nouvel hôte, créer un contrôle simple, consulter les états de supervision et effectuer un premier niveau de diagnostic.

2. Accès à l'interface Zabbix

2.1 URL et connexion

1. Ouvrir un navigateur (Firefox/Chrome).
2. Saisir l'URL :
   https://zabbix.team21.local/
3. Si un avertissement de certificat apparaît (certificat auto-signé ou AC interne), cliquer sur **Avancé** puis **Continuer**.

2.2 Authentification

- Compte administrateur initial :
  - Utilisateur : Admin
  - Mot de passe : zabbix (à modifier après installation).
- Pour l'exploitation, utiliser un compte nominatif créé par l'admin Zabbix

3. Organisation générale de l'interface

Après authentification, Zabbix affiche en général un tableau de bord (Dashboard) avec une synthèse de l'état du système : nombre de problèmes en cours, disponibilité des hôtes, courbes de charge, etc. La barre latérale gauche donne accès aux différents modules :

- La partie **Monitoring** permet de suivre le système en temps réel :

    - le sous-menu **Problems** liste les incidents détectés (triggers en état PROBLEM),
    - **Latest data** affiche les dernières valeurs collectées pour chaque métrique,
    - les dashboards proposent des vues synthétiques adaptées aux administrateurs.
- La partie **Data collection** permet de gérer ce qui est supervisé :
    - **Hosts** recense les hôtes surveillés, organisés par groupes,
    - **Templates** (selon la version) regroupe les modèles de supervision appliqués aux hôtes (Linux, Windows, Cisco, etc.).

Dans notre contexte, les hôtes sont organisés en plusieurs groupes logiques afin de rester lisibles :

- le groupe **Réseau** contient le routeur d'interconnexion et le switch Cisco principal ;
- le groupe **Serveurs Windows** contient le serveur AD/DNS (172.16.21.1) ;
- le groupe **Serveurs Linux** contient le serveur Nextcloud (172.16.21.5) ainsi que le serveur Zabbix lui-même.

Cette structuration permet de filtrer rapidement par type d'équipement (réseau, serveurs Windows, serveurs Linux) et de repérer l'hôte concerné par un incident.

4. Comprendre ce qui est supervisé

Pour savoir quels hôtes sont supervisés, on se rend dans le menu **Data collection → Hosts**. L'écran affiche la liste des hôtes, avec pour chacun son groupe, ses interfaces (Agent, SNMP, ICMP) et une icône de disponibilité. Une icône verte indique que l'agent Zabbix (ou l'interface SNMP) répond correctement, tandis qu'une icône rouge signale un problème de communication (agent à l'arrêt, pare-feu, adresse incorrecte, etc.).

Pour voir le détail de ce qui est effectivement mesuré sur un hôte (CPU, RAM, disque, services, interfaces réseau), on utilise le menu **Monitoring → Latest data**. Il suffit de filtrer sur l'hôte souhaité (par exemple NEXTCLOUD-SRV ou AD-SRV) pour afficher la liste des items collectés : ressources système, volumes de disques, services Windows, scénarios web sur Nextcloud, statistiques SNMP sur le routeur ou le switch, et ainsi de suite. Les

graphiques associés permettent ensuite de visualiser l'évolution de ces indicateurs dans le temps.

5. Paramétrage de la supervision

Cette partie décrit comment les hôtes sont ajoutés, comment les services sont configurés, et comment l'interface a été organisée pour rester lisible, conformément aux attentes de l'atelier.

5.1 Organisation générale des hôtes

Groupes d'hôtes créés dans Zabbix :

- Réseau : routeur, switch Cisco.
- Serveurs Windows : serveur AD/DNS.
- Serveurs Linux : serveur Nextcloud, serveur Zabbix.

Cette organisation permet de filtrer facilement par type d'équipement et d'avoir des vues logiques par domaine de responsabilité (réseau / systèmes).

5.2 Ajout du serveur Windows (exemple avec AD)

1. Installation de l'agent Zabbix Windows à partir du MSI officiel (version la plus récente) sur le contrôleur de domaine.

   https://cdn.zabbix.com/zabbix/binaries/stable/7.4/7.4.8/zabbix_agent-7.4.8-windows-amd64-openssl.msi

2. Paramétrage de l'agent :
   - Server= 172.16.1.2 ou Zabbix.team21.local
   - Hostname=TEAM21-1 (nom utilisé côté Zabbix).

5.2.1 Ajout du nouvel hote

Cliquer sur **Create host** (bouton bleu en haut à droite)

1. **General** tab :
   a. Host name: AD-SRV (DOIT matcher le hostname de l'agent)
   b. Visible name: Controleur de domaine (ce qu'on affiche)

   c. Host groups: Cliquer sur "Select" et ajouter au groupe Windows serveurs)
2. **Interfaces** tab :
   a. Cliquer sur **Add**
   b. Type: Agent
   c. IP address: 172.16.21.1
   d. Port: 10050
   e. Cliquer **Add**
3. Ajout de **template:**
   a. Cliquer sur la machine créée
   b. Dans l'onglet qui s'est ouvert, cliquez sur **Host Wizard**
   c. Cherchez le template **Windows by Zabbix agent**
4. Validez les étapes
5. Attendre 1-2 minutes

Recharger la page Hosts. L'hôte doit devenir **vert** (connecté) dans la colonne "Availability".

Ce template fournit automatiquement des métriques sur CPU, mémoire, disque, services systèmes et disponibilité.

5.3 Ajout du serveur Linux (exemple avec serveur Nextcloud)

1. Sur le serveur Nextcloud (Debian) : installation de l'agent Zabbix 8.0 :

```
# Si 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
dpkg -i zabbix-release_latest_8.0+debian13_all.deb apt update apt install -y zabbix-agent2
apt update
apt install -y zabbix-agent2
```

2. Configurer l'agent

Éditer le fichier de config :

```
nano /etc/zabbix/zabbix_agent2.conf
```

Trouver et modifier/décommenter :

```
# IP du serveur Zabbix (manager)
Server=172.16.21.2

# Hostname (doit être unique et matcher avec Zabbix frontend)
Hostname= Nextcloud

# Port par défaut (ok)
ListenPort=10050
```

Sauvegarder et quitter.

3. Démarrer l'agent

```
systemctl enable zabbix-agent2
systemctl restart zabbix-agent2
systemctl status zabbix-agent2
# Doit afficher "active (running)"
```

5.3.1 Ajout du nouvel hote

Cliquer sur **Create host** (bouton en haut à droite)

1. **General** tab :
    a. Host name: Nextcloud (DOIT matcher le hostname de l'agent)
    b. Visible name: Serveur Nextcloud (ce qu'on affiche)
    c. Host groups: Cliquer sur "Select" et ajouter au groupe Linux serveurs)

2. **Interfaces** tab :
    a. Cliquer sur **Add**
    b. Type: Agent
    c. IP address: 172.16.21.5
    d. Port: 10050
    e. Cliquer **Add**
3. Ajout de **template:**
    a. Cliquer sur la machine créée
    b. Dans l'onglet qui s'est ouvert, cliquez sur **Host Wizard**
    c. Cherchez le template **Linux by Zabbix agent**
4. Validez les étapes
5. Attendre 1-2 minutes

Recharger la page Hosts. L'hôte doit devenir **vert** (connecté) dans la colonne "Availability".

Si c'est rouge, vérifier :

```
# Sur le serveur
zabbix_get -s <IP_CLIENT> -p 10050 -k "agent.version"


# Sur le client
sudo systemctl status zabbix-agent2
sudo tail -20 /var/log/zabbix/zabbix_agent2.log
```

Zabbix remonte alors les informations sur la charge système, la mémoire, l'espace disque (en particulier sur les volumes utilisés par Nextcloud), ce qui permet de traiter les risques de débordement disque identifiés.

5.4 Ajout du routeur ou switch (SNMP)

L'objectif est de superviser le routeur d'interconnexion et le switch Cisco principal en SNMP v2c et ICMP (ping), afin de remonter l'état des équipements et de leurs interfaces de manière régulière.

5.4.1 Activation de SNMP v2c sur les équipements réseau

Sur le routeur et sur le switch Cisco, la configuration de base en CLI est la suivante :

```
configure terminal

# Définir une communauté SNMP en lecture seule
snmp-server community TEAM21-RO RO

#(Optionnel) Renseigner des infos de contact / localisation
snmp-server contact it@team21.local
snmp-server location Brive

end
write memory
```

- TEAM21-RO est la communauté SNMP utilisée par Zabbix pour collecter les informations.
- On reste en **lecture seule (RO)**, ce qui est suffisant pour la supervision.

5.4.2 Ajout du routeur dans Zabbix

Dans l'interface Zabbix :

1. Aller dans **Data collection → Hosts → Create host**.
2. Renseigner :
    - **Host name** : ROUTER-21.
    - **Visible name** : Routeur Interconnexion.
    - **Host groups** : Réseau.
3. Dans la section **Interfaces** :
    - Cliquer sur **Add**.
    - Type : **SNMP**.
    - IP address : IP de gestion du routeur (ici 10.200.200.21).
    - Port : 161.

- SNMP version : SNMPv2.
- Community : TEAM21-RO.

4. Dans la section **Templates** :
    - Cliquer sur **Add** et rechercher un template adapté (par ex. Cisco IOS by SNMP ou un template réseau.
5. Enregistrer l'hôte.

Après quelques minutes, Zabbix commence à interroger le routeur en SNMP et à alimenter les items du template (interfaces, trafic, état up/down, etc.).

5.4.3 Ajout du switch Cisco principal dans Zabbix

Procédure similaire pour le **switch** :

1. **Data collection → Hosts → Create host**.
2. Renseigner :
    - **Host name** : SWITCH-21.
    - **Visible name** : Switch Cisco Principal.
    - **Host groups** : Réseau.
3. **Interfaces** :
    - Ajouter une interface **SNMP** avec :
        - IP address : IP de gestion du switch (ici 172.21.50.1).
        - Port : 161.
        - SNMPv2, communauté SODECAF-RO.
4. **Templates** :
    - Appliquer un template Cisco (SNMP) ou un template réseau générique.
5. Enregistrer l'hôte.

Les interfaces du switch sont alors découvertes automatiquement (LLD, low-level discovery) et Zabbix commence à grapher le trafic et l'état des ports.

5.4.4 Vérifications et exploitation

Pour vérifier que la supervision des équipements réseau fonctionne correctement :

- **Monitoring → Hosts** :
    - ROUTEUR-SRV et SWITCH-CORE doivent apparaître avec l'icône SNMP en **vert** (SNMP disponible).
- **Monitoring → Latest data** :

    - En filtrant sur ROUTEUR-SRV ou SWITCH-CORE, on voit les principaux items SNMP (interfaces, trafic entrant/sortant, statut des ports, etc.).
- **Monitoring → Problems** :
    - Les triggers fournis par les templates (interface down, hôte injoignable, etc.) génèrent des problèmes visibles en cas d'anomalie.

Cette configuration répond pleinement aux exigences pour la supervision des deux équipements d'interconnexion.

5.5 Supervision applicative d'un URL (exemple avec Nextcloud)

Pour vérifier que le service Nextcloud est réellement accessible côté utilisateur, un scénario web HTTPS est créé :

- Host Nextcloud clic
- Web → Create web scenario.
- Nom : nextcloud - HTTPS.
- Hôte associé : NEXTCLOUD-SRV.
- Étape :
    - URL : https://nextcloud.team21.local/ (ou /status.php si activé).
    - Timeout : 10s.
    - Code HTTP attendu : 200.

Un trigger est configuré pour remonter un problème si le scénario échoue plusieurs fois consécutives, ce qui permet de détecter l'arrêt de Nginx, un problème de certificat ou une indisponibilité applicative.

6. Tests, scénarios et résultats

Conformément à la demande, plusieurs scénarios de test ont été définis pour vérifier que la supervision fonctionne effectivement et que les anomalies simples sont bien détectées.

6.1 Scénario 1 – Arrêt du service web Nextcloud

- Action :

```
systemctl stop nginx
```

Sur le serveur NEXTCLOUD-SRV.

- Résultat attendu :
  - Le ping ICMP vers 172.16.21.3 reste OK (VM en ligne).
  - Le scénario web Nextcloud - HTTPS échoue.
  - Un problème de type Web scenario failed apparaît dans Zabbix pour NEXTCLOUD-SRV.

Ce test permet de valider la détection d'une panne applicative sans extinction complète de la machine.

6.2 Scénario 2 – Perte de communication avec le serveur AD/DNS

- Action : arrêt temporaire de l'agent Zabbix sur le serveur AD/DNS :

```
systemctl stop Zabbix-agent2
```

- Résultat attendu :
  - Zabbix remonte un problème de type Zabbix agent on AD-SRV is unreachable.
  - La disponibilité de l'hôte passe en rouge dans la liste des Hosts.

Ce test valide la capacité de Zabbix à détecter la perte de supervision sur un serveur critique, même si la machine elle-même est encore en ligne.

6.3 Scénario 3 – Incident réseau simulé sur le switch

- Action : désactiver temporairement un port du switch Cisco relié à un des serveurs (par exemple Nextcloud).
- Résultat attendu :
    - L'hôte concerné devient injoignable (ping KO).
    - Les triggers SNMP liés à l'interface passent en état PROBLEM (si template SNMP en place).

Ce test valide la remontée d'un incident réseau au niveau des équipements d'interconnexion.

6.4 Scénario 4 – Seuil d'espace disque sur Nextcloud

- Action : provoquer un dépassement de seuil sur la partition de données (ou abaisser temporairement le seuil dans le template).
- Résultat attendu :
    - Un problème du type Free disk space is less than X% apparaît pour NEXTCLOUD-SRV.