

Contextualisation :

Suite à une recrudescence de cyberattaques, le système d'information de la section SIO doit se renforcer. Deux étapes sont prévues :

1. **Mise en place d'un serveur de supervision**
2. **Mise en œuvre d'une solution de firewalls**

Ce TP se concentre sur la **mise en place de la supervision**.

🎯 Objectif

Tester deux solutions de supervision dans un environnement laboratoire et **justifier le choix de l'outil retenu**, en binôme. **Aucun critère économique n'est imposé.**



Sommaire

Belerge Jérémie

BTS SIO 2

Zabbix c'est quoi ?

Installation de Zabbix

Installation client Windows de Zabbix

Installation client Linux de Zabbix

Ajout d'un hôte

Zabbix pour les switch

Pour windows serveur?

Envoyer une alerte par mail

Conclusion



Consignes:

-Zabbix c'est quoi ?

Zabbix est un logiciel libre de supervision et de monitoring permettant de surveiller l'état d'infrastructures IT, réseaux, serveurs, applications et services en temps réel. Il collecte des données, génère des alertes et propose des tableaux de bord pour analyser la performance des systèmes surveillés.

Source : [Wikipedia](#)

Zabbix surveille en continu les serveurs, équipements réseau (commutateurs, routeurs), bases de données, services cloud et applications. Il fonctionne grâce à une architecture centralisée composée d'un serveur Zabbix, d'agents installés sur les machines à surveiller, d'une interface Web et éventuellement de proxys. Les données collectées permettent de visualiser l'état des ressources, générer des rapports et planifier la capacité

Source : [Zabbix.com](#)



Consignes:

-Installation de Zabbix

On installe le dépôt de Zabbix :

```
root@Jrm:~# wget https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_7.0-2+ubuntu22.04_all.deb
```

Puis on installe Mariadb :

```
root@Jrm:~# apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent -y
```

Puis MariaDB

```
root@Jrm:~# apt install mariadb-server -y
```

Puis MySql :

```
root@Jrm:~# mysql_secure_installation
```

On créer la base de donnée :

```
root@Jrm:~# mysql -u root -p
```



Consignes:

-Installation de Zabbix

A l'intérieur on y ajoute :

```
CREATE DATABASE zabbix character set utf8mb4 collate utf8mb4_bin;  
CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'motdepassefort';  
GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost';  
FLUSH PRIVILEGES;  
EXIT;
```

On importe le schéma de la base de donnée Zabbix :

```
[root@Jrm:~# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -p zabbix
```

```
root@Jrm:~# nano /etc/zabbix/zabbix_server.conf
```

```
DBUser=zabbix  
  
### Option: DBPassword  
# Database password.  
# Comment this line if no password is used.  
#  
# Mandatory: no  
# Default:  
DBPassword=Sio2025
```



Consignes:

-Installation de Zabbix

Puis on redémarre nos services :

```
root@Jrm:~# systemctl restart zabbix-server zabbix-agent apache2  
root@Jrm:~# systemctl enable zabbix-server zabbix-agent apache
```

Depuis une machine client en tapant NOTREIP/zabbix on obtient :



User : Admin
Password : zabbix



Consignes:

-Installation client
Windows de Zabbix

Depuis une machine cliente on installe l'agent Zabbix disponible [ici](#) :

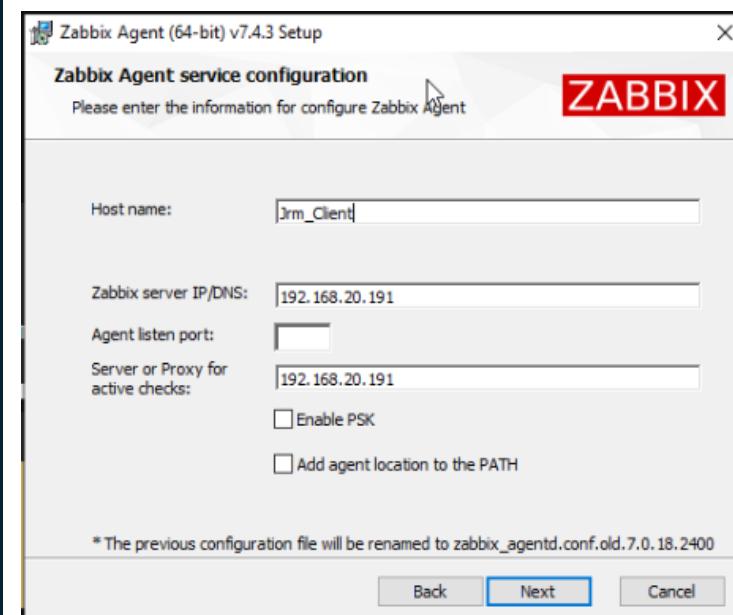
Zabbix agent v7.4.3

Packaging: MSI
Encryption: OpenSSL
Linkage: Dynamic
Checksum:
sha256: 5843101226bfff4e76dd8d60595a2a297ae5c8e69186c061f554e80a690c039c
shal: 9cdf94513e0af2de3a2331127a07c7fc23f89e32
md5: bdb6d4ce0e4bb4724da5058df0d44f54

[Read manual](#)

[DOWNLOAD](#) https://cdn.zabbix.com/zabbix/binaries/stable/7.4/7.4.3/zabbix_agent-7.4.3-windows-amd64-openssl.msi

Puis on lance le .exe



Puis on y rentre notre IP : 192.168.20.191



Consignes:

-Installation client
Linux de Zabbix

Pour installer le client Zabbix sous linux il suffit de suivre les étapes ci-dessous :

On installe le dépôt Zabbix sur le client :

-wget

https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-release_7.0-2+debian12_all.deb

-sudo dpkg -i zabbix-release_7.0-2+debian12_all.deb

-sudo apt update -y

Ensuite on installe l'agent Zabbix

sudo apt install zabbix-agent -y

Puis on rentre et modifie le fichier de configuration de l'agent

sudo nano /etc/zabbix/zabbix_agentd.conf

Server=192.168.20.191

ServerActive=192.168.20.191

Hostname=nom_de_ta_machine



Consignes:

-Ajout d'un hôte

Depuis une Zabbix on ajoute notre client :

The screenshot shows the Zabbix host creation process. Step 1 highlights the 'Services' menu item. Step 2 highlights the 'Créer un hôte' button. Step 3 highlights the 'Agent' IP address field containing '192.168.20.96'. A callout points from the text 'On rentre l'IP du client' to this field.

1

2

3

Créer un hôte

On rentre l'IP du client

Actualiser

Clone

Supprimer

Hôte

Nom de l'hôte: jrm-hote

Nom visible: jrm-hote

Modèles: taper ici pour rechercher

Sélectionner

Groupe d'hôtes: Virtual machines X

Sélectionner

Interfaces

Type: Agent

adresse IP: 192.168.20.96

Nom DNS:

Connexion à: IP

Port: 10050

Défaut

Supprimer

Surveillé par: Serveur, Proxy, Groupe de proxy

Activé: checked



Consignes:

-Zabbix pour les switch

```
|SW-APGR7(config)#snmp-server community groupe7 R0|
```

snmp-server → active ou configure le service **SNMP** sur le switch (outil de gestion à distance).

community → crée une **communauté SNMP**, c'est comme un mot de passe partagé.
groupe7 → nom de la communauté (choisi par l'administrateur).

RO → signifie **Read Only** : accès en **lecture seule**, donc on peut lire les infos mais pas changer la configuration

```
root@APGR7LAMP:~# apt install snmp
```

Puis on installe le service snmp sur notre serveur Zabbix.



Consignes:

-Zabbix pour les switch

Depuis : "Configuration" > "Hôtes"

The screenshot shows the 'Hosts' configuration page in Zabbix. The host is named 'Switch gp7'. Under the 'Interfaces' section, there is an SNMP interface with the IP '192.168.20.17'. The 'Version SNMP' is set to 'SNMPv2' and the 'Communauté SNMP' is set to '{\$SNMP_COMMUNITY}'. The 'Nombre maximal de répétitions' is set to '10'. A blue arrow points from the text 'On ajoute l'IP de notre switch et un nom d'hôtes , cela générera une communauté SNMP à mettre dans l'option "macros" puis il faudra entrée le nom de la communauté "groupe 7"' to the '192.168.20.17' field.

On ajoute l'IP de notre switch et un nom d'hôtes , cela générera une communauté SNMP à mettre dans l'option "macros" puis il faudra entrée le nom de la communauté "groupe 7"

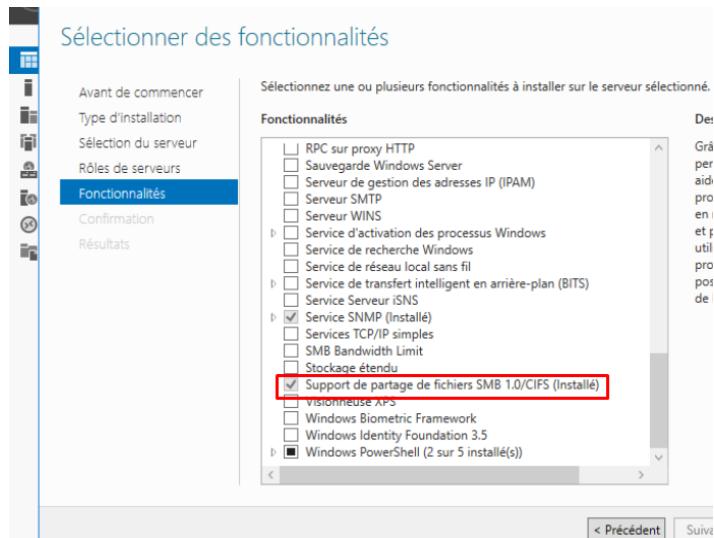
The screenshot shows the 'Macros' configuration page in Zabbix. A macro named '{\$SNMP_COMMUNITY}' is defined with a value of 'Groupe 7'. A blue arrow points from the same text in the previous slide to the 'Value' field of this macro entry.



Consignes:

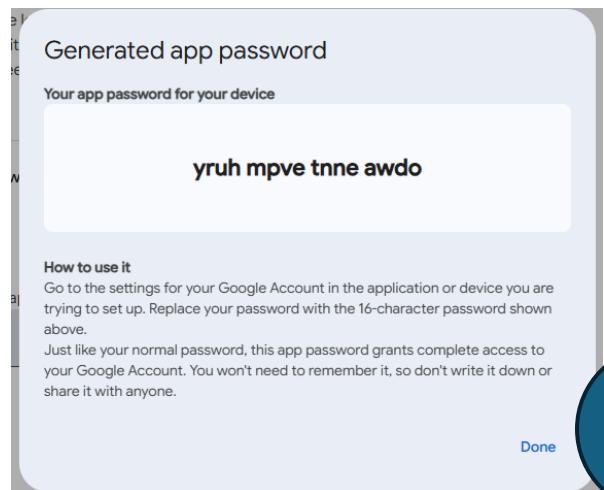
-Pour windows serveur?

-Envoyer une alerte par mail



1

Zabbix utilise le protocole **SMB** pour accéder à des fichiers partagés sur Windows



3

← App passwords

App passwords help you sign into your Google Account on older apps and services that don't support modern security standards.

App passwords are less secure than using up-to-date apps and services that use modern security standards. Before you create an app password, you should check to see if your app needs this in order to sign in.

[Learn more](#)

You don't have any app passwords.

To create a new app specific password, type a name for it below...

App name
zabbix

Create

2 Afin de pouvoir recevoir des alertes par email il nous faut accéder à [cette page](#), y rentrer le nom de l'alerte

"Puis, un code apparaîtra. Cela permettra à Zabbix de se connecter au mail



Consignes:

-Envoyer une alerte par mail

Type de média Modèles de messages Options

* Nom: mail
Type: Courriel
Fournisseur de messagerie: Generic SMTP
* serveur SMTP: smtp@gmail.com
Port du serveur SMTP: 25
* Courriel: jrm.gray07@gmail.com
SMTP helo:
Sécurité de la connexion: Aucun STARTTLS SSL/TLS
Authentification: Aucun Nom d'utilisateur et mot de passe
Nom d'utilisateur: jrm.gray07@gmail.com
Mot de passe:

Depuis: Administration > Utilisateurs > crée un nouvel utilisateur > Média

Ce paramétrage permet à Zabbix d'envoyer automatiquement des notifications d'alerte à une personne par email (machine , switch , serveur)

Média

Type: Email
* Envoyer à: jrm.gray07@gmail.com
* Lorsque actif: 1-7,00:00-24:00
Utiliser si严重性: Non classé Information Avertissement Moyen Haut Désastre
Activé:

Il faudra créer un type de média pour y entrer notre mail qui recevra les alertes, dans la catégorie courriel, puis dans nom d'utilisateur, et y insérer le mot de passe qui apparaît dans la diapo précédente.



Consignes:

-Envoyer une alerte par mail

Il faut bien constater que ton e-mail est enregistré dans Zabbix pour vérifier que tu recevras les alertes par mail

Depuis : Administration > Utilisateurs> Média

Cela signifie que Zabbix enverra automatiquement des alertes à cette adresse lors d'un événement critique

Type	Envoyer à	Lorsque arrivé	Utiliser si severité	Etat	Action
Email	jrm.gray07@gmail.com	1-7,00:00-24:00	N I A M H D	Activé	Édition Supprimer
	Ajouter				

Ensuite il faudra créer une action (Alertes > Actions > Action de déclencheur > Créer une action)

On rentre le nom de l'action :

Nouvelle action

Action Opérations

* Nom : appareil déconnecté

Conditions Étiquette Nom

Ajouter



Consignes:

-Envoyer une alerte par mail

Dans la section Opérations, spécifie le ou les groupes d'utilisateurs à qui les alertes doivent être envoyées

Détails de l'opération

Opération Envoi message

Étapes 1 - 1 (0 - indéfiniment)

Durée de l'étape 0 (0 - utiliser les paramètres par défaut de l'action)

* Au moins un utilisateur ou un groupe d'utilisateurs doit être sélectionné.

Envoyer aux groupes d'utilisateurs

Envoyer aux utilisateurs

Envoyer au type de média

Message personnalisé

Conditions	Étiquette	Nom	Action
	Ajouter		

Action Opérations 1

* Durée de l'étape d'opération par défaut 5 min

Opérations	Détails	Démarrer dans	Durée	Action
1 Envoyer le message aux groupes d'utilisateurs: Zabbix administrators via tous les médias		Immédiatement	Défaut	Édition Supprimer

Opérations de récupération

Opérations de mise à jour

Interrompre les opérations en cas de problèmes symptomatiques

Suspendre les opérations des problèmes supprimés

Notifier les escalades annulées

* Au moins une opération doit exister.

C'est le temps en minutes (ici 5 min) pendant lequel une alerte est considérée active. Cela évite d'envoyer des notifications trop fréquemment si le problème persiste



Consignes:

-Conclusion

En conclusion, avec la configuration réalisée dans Zabbix, tu recevras bien un e-mail dès qu'une alerte est déclenchée : le système enverra automatiquement un message aux adresses e-mail ou groupes définis pour prévenir immédiatement d'un incident.

Zabbix est un outil de supervision centralisé pour les réseaux, serveurs, équipements et applications. Il permet :

- De surveiller en temps réel la disponibilité, la performance et l'état de tous tes équipements informatiques (via SNMP, agents, etc.).
- De générer des alertes automatiques dès qu'un problème ou une anomalie est détecté sans avoir besoin de surveiller en continu l'interface
- D'automatiser l'envoi de notifications (e-mail, SMS, messagerie, etc.) aux bonnes personnes pour une réaction rapide en cas d'incident.