RAPPORT TECHNIQUE

Supervision Zabbix
de l'Active Directory

Rudy COLOMBEL
Vanthary SOK

Février 2025

TABLE DES MATIÈRES

CONTEXTE

Dans une infrastructure IT, il est essentiel de surveiller en temps réel l'état des serveurs critiques, tels que l'Active Directory, afin de garantir la disponibilité des services et la sécurité du réseau.

Le but de ce projet est de mettre en place une supervision avec Zabbix pour surveiller les performances et les événements critiques du serveur Active Directory sous Windows Server.

OBJECTIF

Mettre en place une supervision avec Zabbix pour surveiller les performances et les événements critiques d'un serveur Active Directory sous Windows Server.

ÉLEMENTS SUPERVISES

RESSOURCES SYSTEME

- CPU : (Seuil acceptable <70%, Seuil alerte entre 70 et 80%, Seuil critique >80%)
- RAM : (Seuil acceptable <70%, Seuil alerte entre 70 et 80%, Seuil critique >80%)
- Disque dur : (Seuil acceptable <70%, Seuil alerte entre 70 et 80%, Seuil critique >80%)

ÉVENEMENTS ET LOGS

- Tentatives de connexion échouées
- Événements de sécurité (NTLM)

SUPERVISION D'APACHE (INSTALLE SUR L'ACTIVE DIRECTORY)

- Disponibilité du service Apache
- Nombre de requêtes "GET" et "POST" échouées

PREREQUIS

Installation de l'agent Zabbix sur le serveur Active Directory et le serveur Apache sur le serveur

SUPERVISION DES RESSOURCES SYSTEME

1. Surveillance du CPU, RAM et Disque

Zabbix dispose déjà de modèles Windows intégrant la supervision des performances.
• Appliquer le modèle Template OS Windows by Zabbix agent
• Vérifier les éléments (CPU Utilization, Memory usage, Disk space usage)

2. Configuration des seuils d'alerte

• CPU utilization
• Memory usage
• Free disk space

3. Activer la journalisation Windows

• Ouvrir Observateur d'événements (eventvwr.msc)
• Aller dans Journaux Windows > Sécurité
• Rechercher les ID d'événements :
• Échecs de connexion : ID 4625
• Authentification NTLM : ID 4776

4. Ajouter une règle de supervision sur Zabbix

• Nom : Failed Logins
• Type : Zabbix Agent (active)
• Clé : eventlog[Security,,,,4625]
• Fréquence : 30s
• Créer un déclencheur :
• Expression : {Active_Directory:eventlog[Security,,,,4625].count(300)}>5
• Signification : Si plus de 5 connexions échouées en 5 minutes, générer une alerte.
• Idem pour NTLM avec eventlog[Security,,,,4776].

SUPERVISION D'APACHE

1. Installation d'Apache sur l'Active Directory

2. Surveiller l'état du service Apache

• Dans Configuration > Hôtes > Active Directory, ajouter :
• Nom : Service Apache
• Type : Zabbix Agent
• Clé : service_state[W3SVC]
• Seuil : Si service_state[W3SVC].last() différent de 0, alerte.

3. Suivi des requêtes échouées GET / POST

Configurer Zabbix Agent pour surveiller les logs Apache :
• Modifier httpd.conf (C:\Apache24\conf\httpd.conf)

INSTALLATION DE ZABBIX 7.0 LTS SUR DEBIAN12

Prérequis :

- 8 Go de RAM
- 40 Go d'espace disque de stockage
- Service SSH installé et actif
- Droit « sudo » pour un utilisateur

Source : https://www.zabbix.com/fr/download?zabbix=7.0&os_distribution=debian&os_version=12&components=agent&db=&ws=

Installer le dépôt Zabbix :

```
# wget https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-
release_latest_7.0+debian12_all.deb
# dpkg -i zabbix-release_latest_7.0+debian12_all.deb
# apt update
```

Installer le serveur, l'interface et l'agent Zabbix :

```
# apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts
zabbix-agent mariadb-server mariadb-client
```

Créer une base de données initiale :
Assurez-vous que le serveur de base de données est opérationnel.
Exécutez les opérations suivantes sur votre hôte de base de données.

```
# mysql -uroot -p
password
mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
mysql> create user zabbix@localhost identified by 'password';
mysql> grant all privileges on zabbix.* to zabbix@localhost;
mysql> set global log_bin_trust_function_creators = 1;
mysql> quit;
```

Il convient d'adapter les informations à l'infrastructure.

Sur le serveur hôte Zabbix, importez le schéma initial et les données. Vous serez invité à saisir votre mot de passe nouvellement créé :

```
# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-
set=utf8mb4 -uzabbix -p zabbix
```

Cette commande est généralement utilisée pour initialiser la base de données Zabbix sur un système MySQL. Voici ce qu'elle fait :

1. "zcat" décompresse le fichier SQL compressé contenant le schéma de la base de données Zabbix.
2. Le contenu décompressé est ensuite envoyé via un pipe (|) à la commande mysql.
3. La commande mysql se connecte à la base de données "zabbix" avec l'utilisateur "zabbix".
4. "--default-character-set=utf8mb4" spécifie l'encodage de caractères à utiliser.
5. "-p" demande le mot de passe de l'utilisateur zabbix.

Désactiver l'option log_bin_trust_function_creators après l'importation du schéma de base de données :

```
# mysql -uroot -p
password
mysql> set global log_bin_trust_function_creators = 0;
mysql> quit;
```

Configurer la base de données pour le serveur Zabbix :

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

Et activer la ligne : `DBPassword=password`

Démarrer les processus du serveur et de l'agent Zabbix et le faire démarrer au démarrage du système :

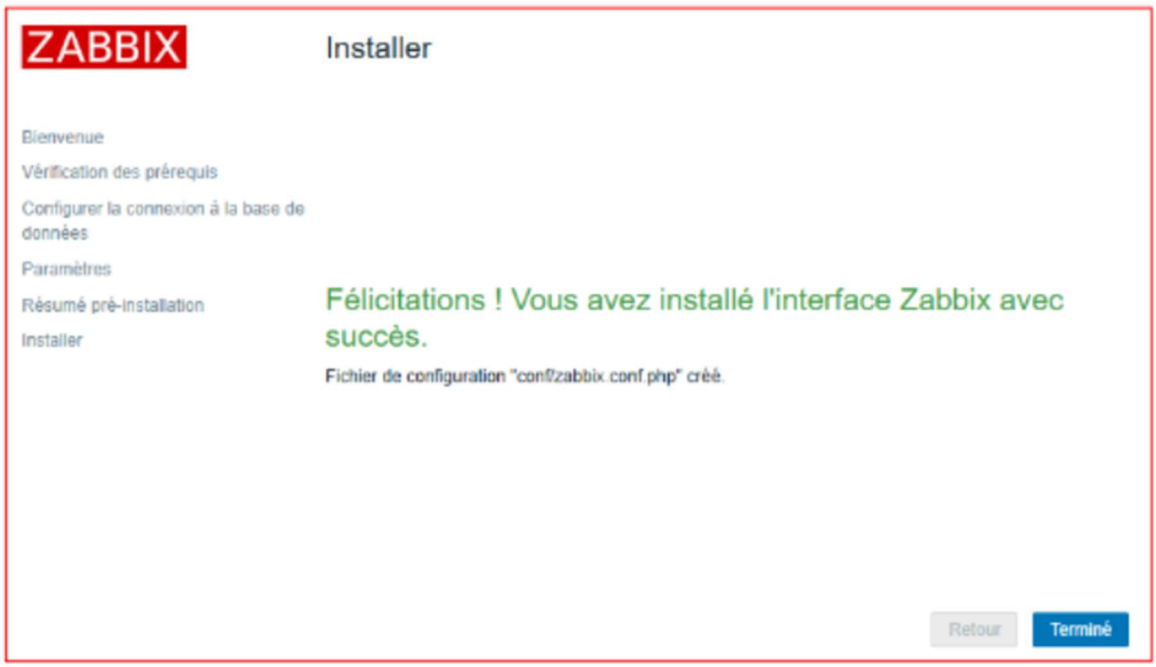
```
# systemctl restart zabbix-server zabbix-agent apache2
# systemctl enable zabbix-server zabbix-agent apache2
```

Ouvrir la page web de l'interface utilisateur de Zabbix

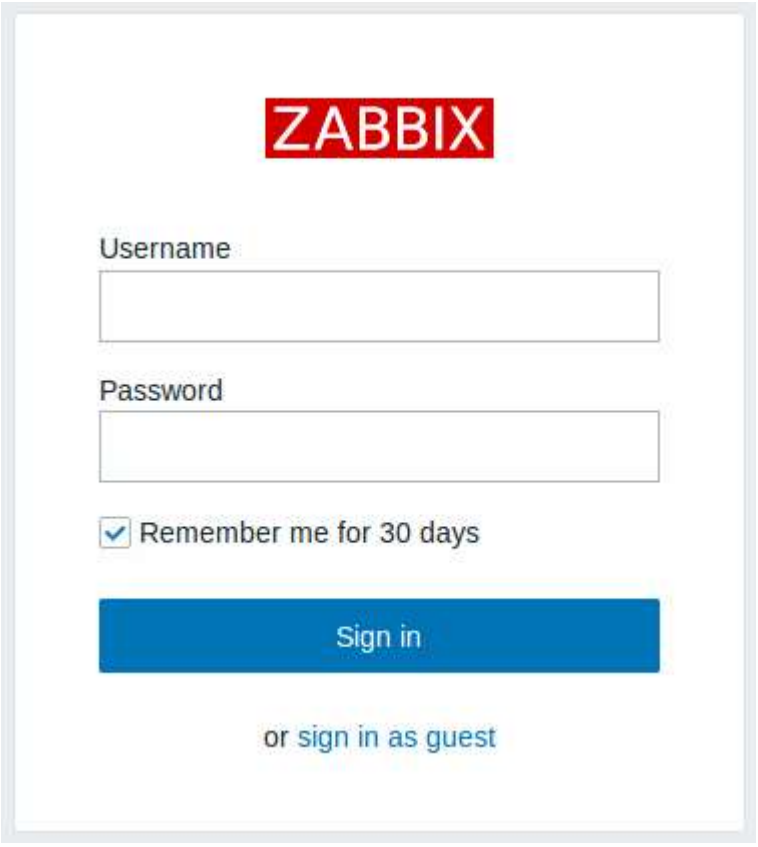
L'URL par défaut pour Zabbix UI lors de l'utilisation du serveur web Apache est http://IP_du_serveur/zabbix

Pour finaliser l'installation, suivre les instructions de l'assistant de configuration :

Une fois que la configuration est terminée :

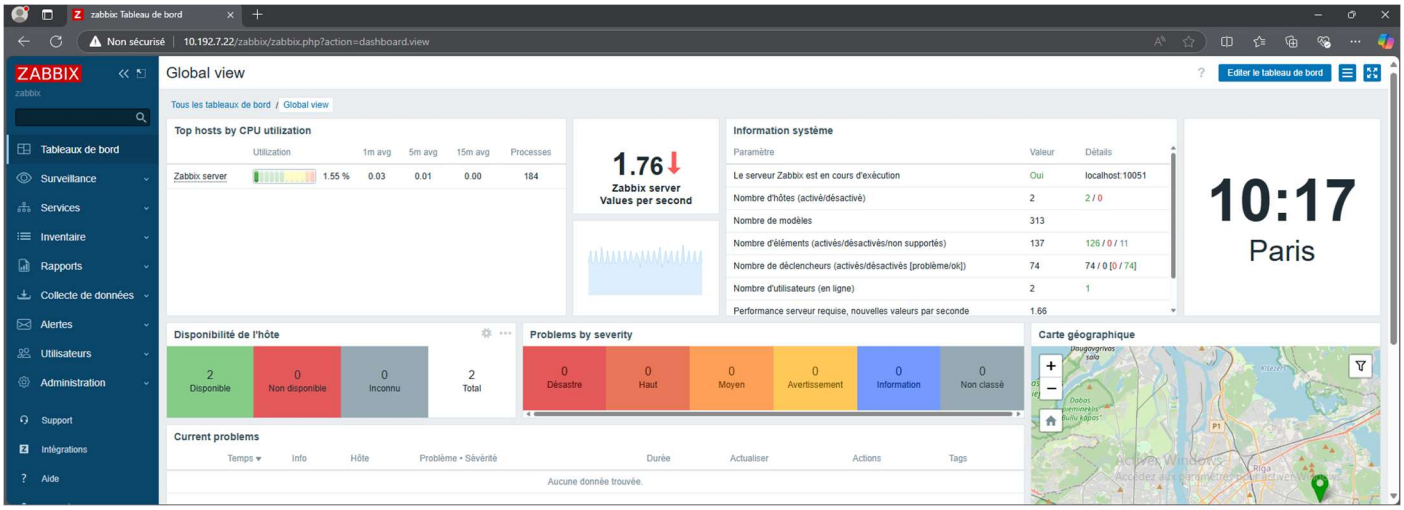


L'accès à l'écran d'authentification est maintenant possible :



Entrez le nom d'utilisateur **Admin** avec le mot de passe **zabbix** pour vous connecter en tant que super-utilisateur de Zabbix. L'accès à toutes les sections du menu sera accordé.

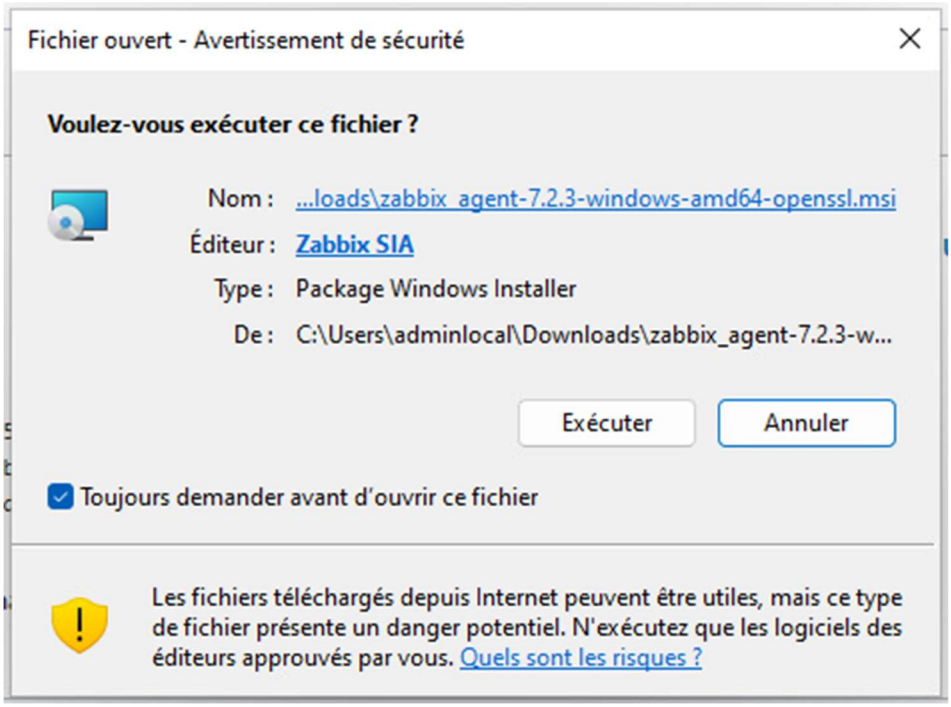
Voici l'écran d'accueil :

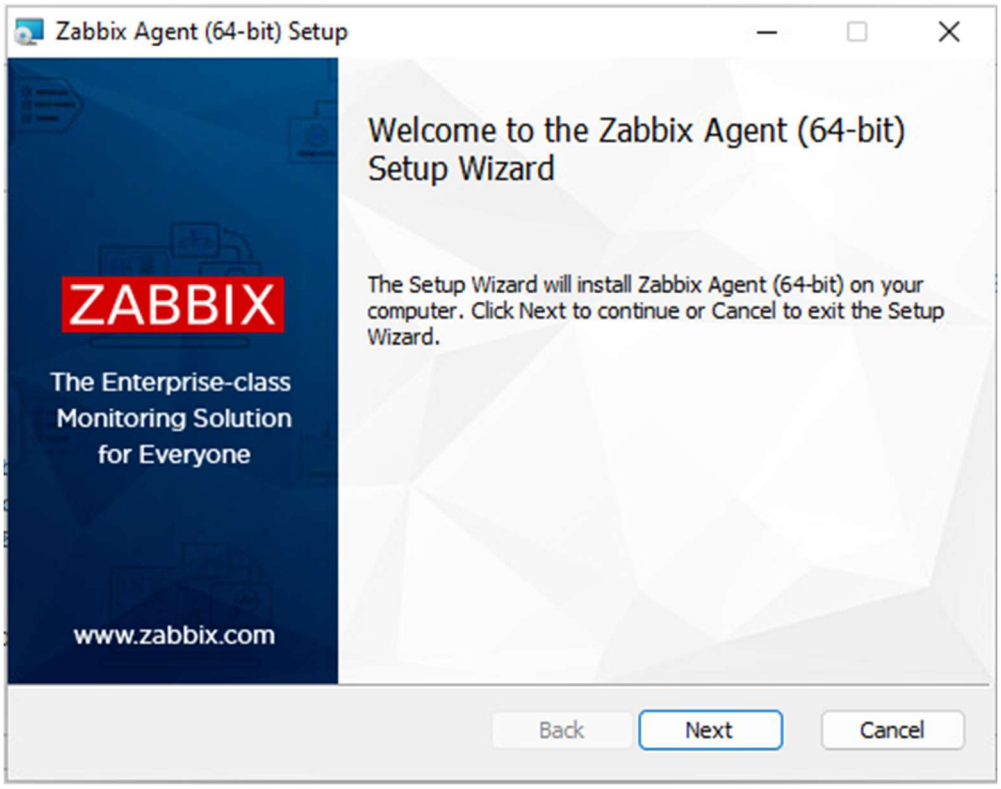


INSTALLATION DE L'AGENT ZABBIX SUR L'AD

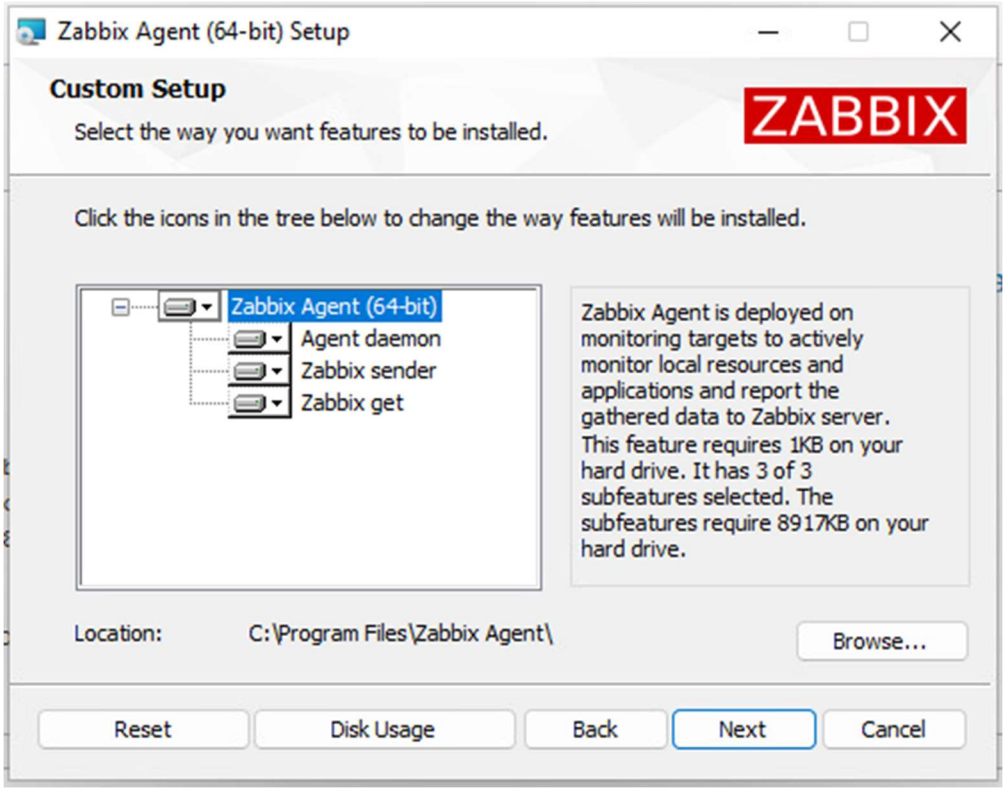
L'AD étant sur Windows Serveur 2022, l'installation de l'agent Zabbix se fait à partir d'un fichier .msi téléchargeable sur le site officiel : https://www.zabbix.com/download_agents

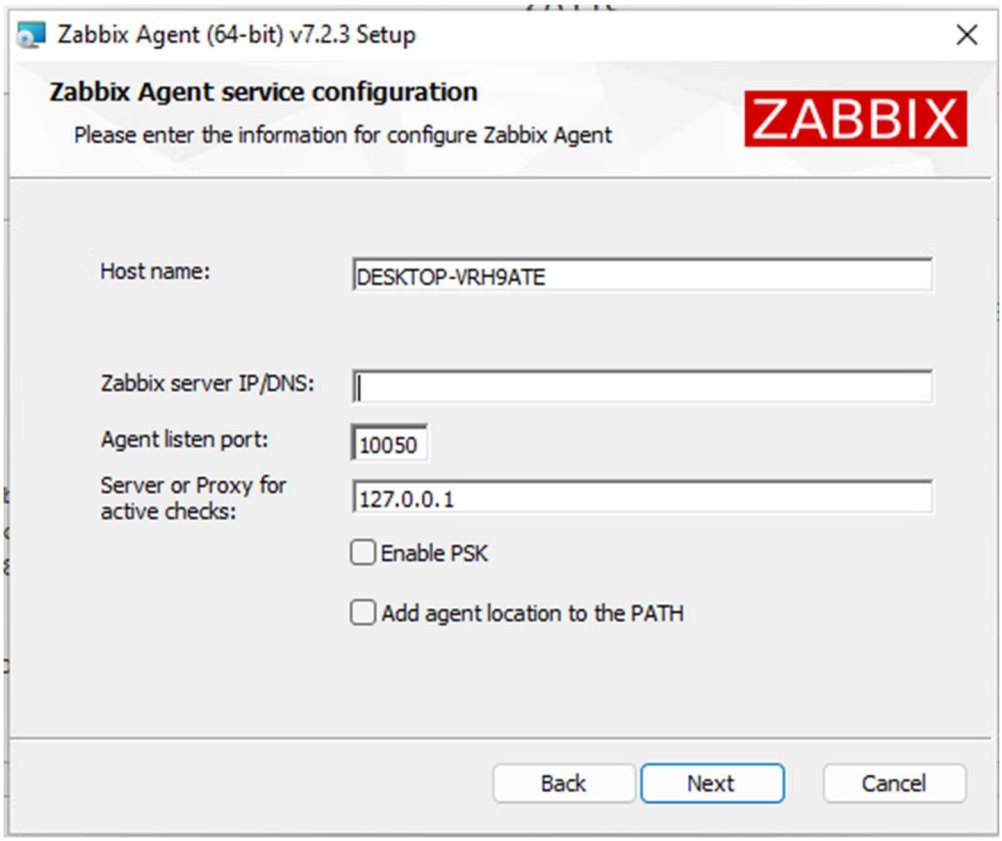
Suivre l'assistant d'installation :



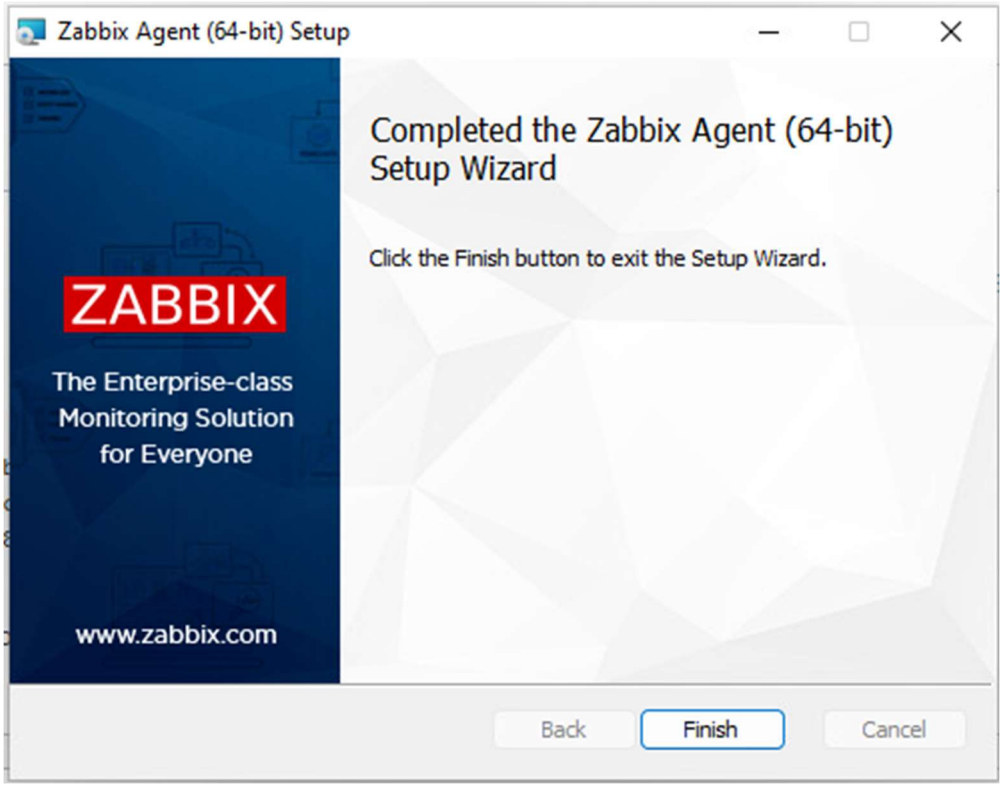

Zabbix Agent (64-bit) Setup
Welcome to the Zabbix Agent (64-bit) Setup Wizard
The Setup Wizard will install Zabbix Agent (64-bit) on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
ZABBIX
The Enterprise-class Monitoring Solution for Everyone
www.zabbix.com
Back
Next
Cancel

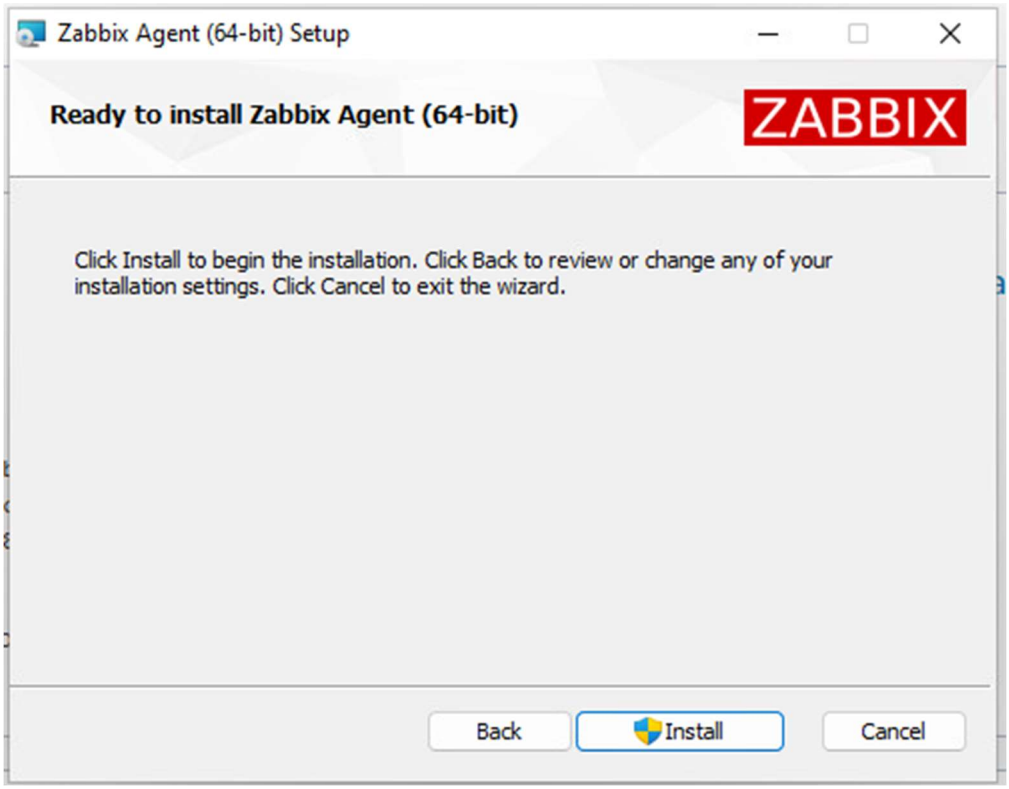

Zabbix Agent (64-bit) Setup
End-User License Agreement
Please read the following license agreement carefully
ZABBIX
GNU AFFERO GENERAL PUBLIC LICENSE
Version 3, 19 November 2007
Copyright (C) 2007 Free Software Foundation, Inc. https://fsf.org/
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.
I accept the terms in the License Agreement
Print
Back
Next
Cancel

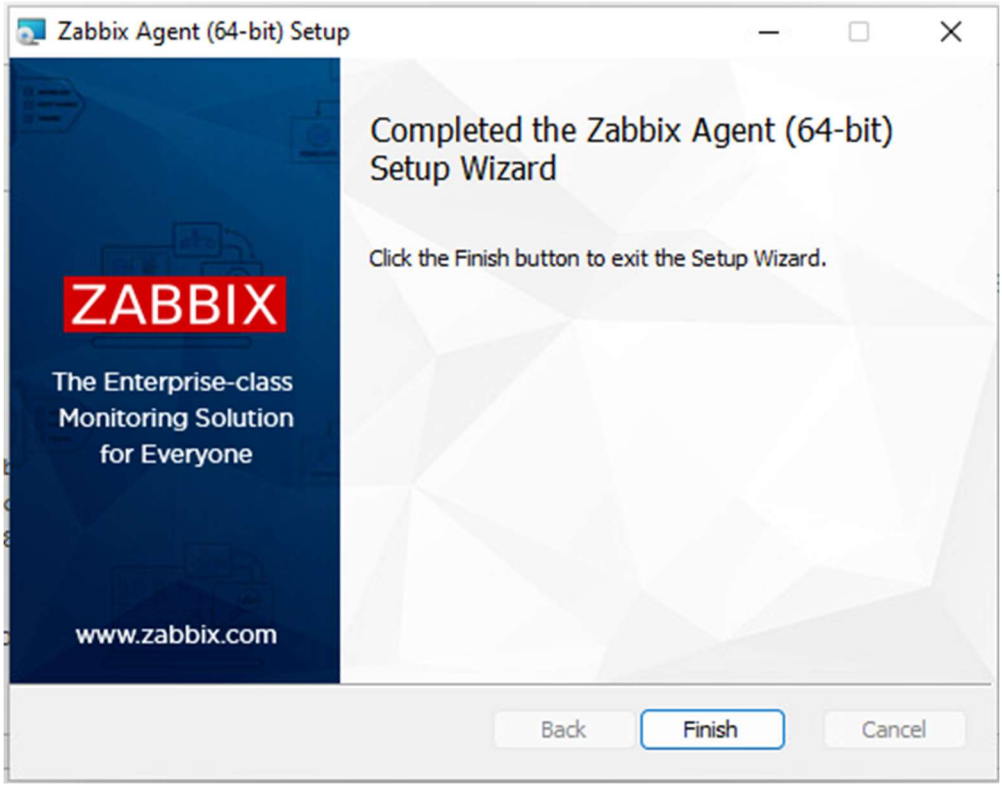




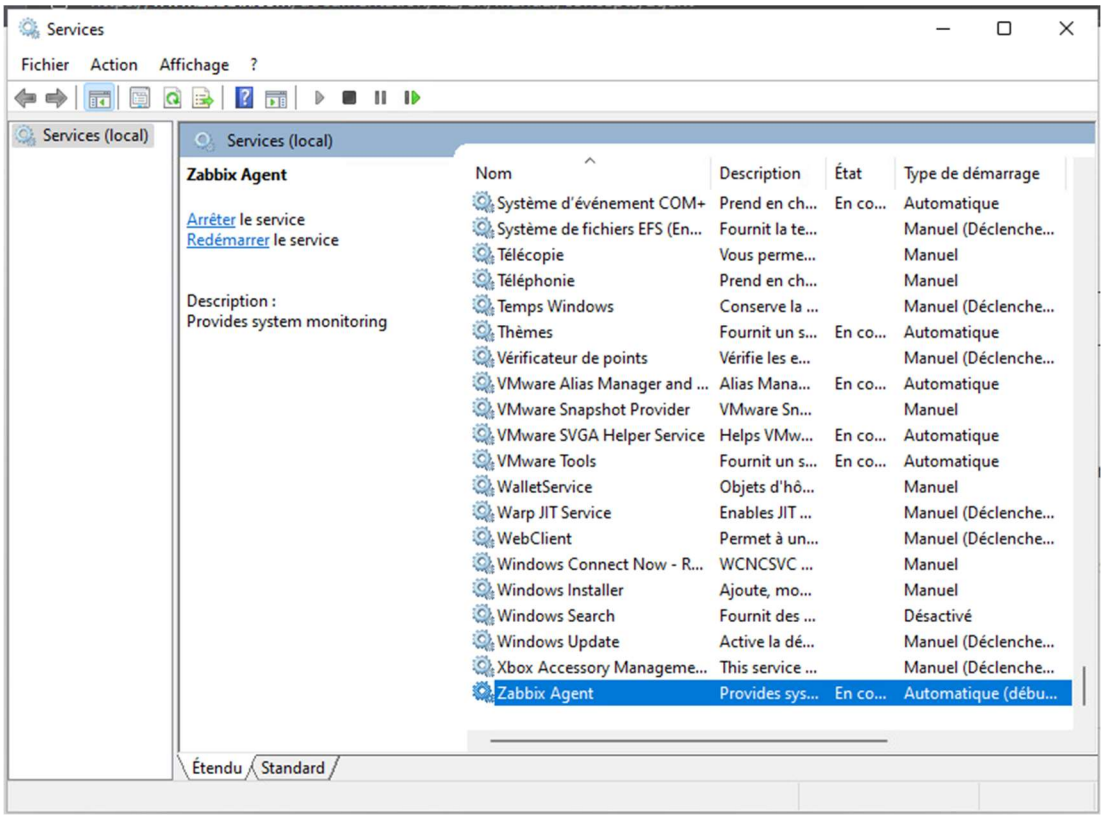
Renseigner l'IP du serveur Zabbix dans la rubrique « Zabbix server IP/DNS »


Zabbix Agent (64-bit) Setup
Completed the Zabbix Agent (64-bit) Setup Wizard
Click the Finish button to exit the Setup Wizard.
ZABBIX
The Enterprise-class Monitoring Solution for Everyone
www.zabbix.com
Back
Finish
Cancel


Zabbix Agent (64-bit) Setup
Ready to install Zabbix Agent (64-bit)
ZABBIX
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel



L'installation de l'agent est terminé et le service est bien actif :



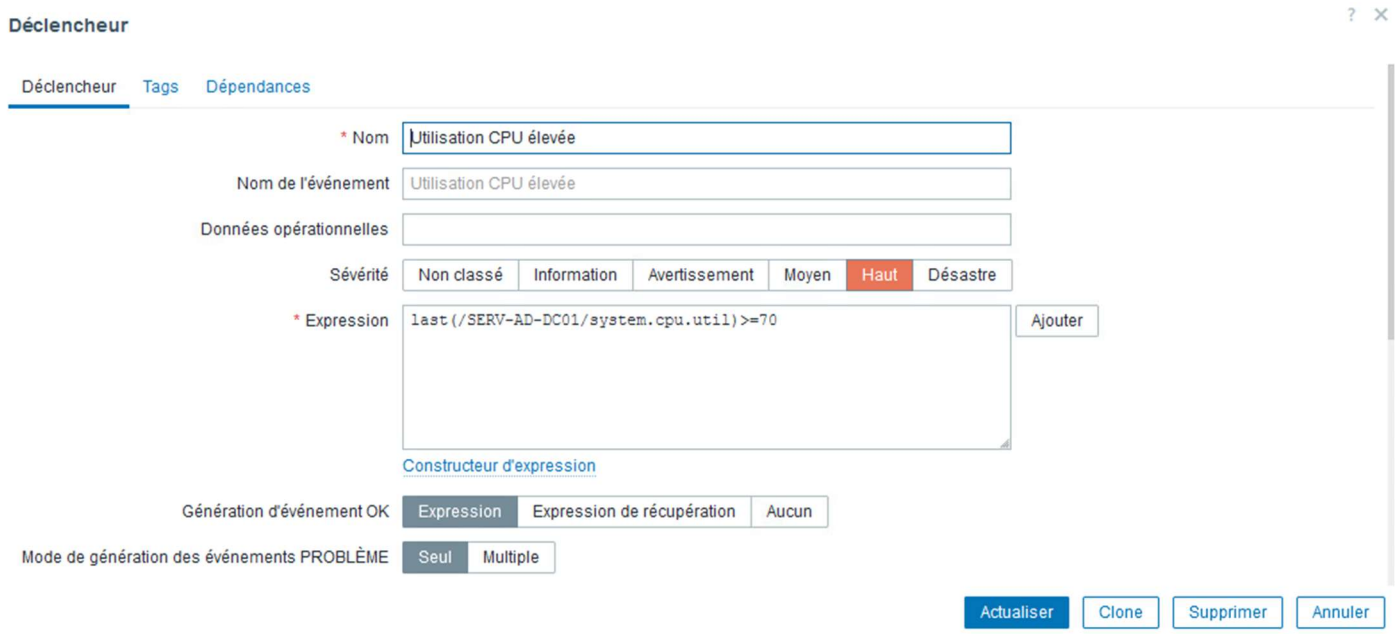
SUPERVISION DES RESSOURCES SYSTEME DE L'AD

Pour rappel, voici les configurations attendues :
• CPU : (Seuil acceptable <70%, Seuil alerte entre 70 et 80%, Seuil critique >80%)
• RAM : (Seuil acceptable <70%, Seuil alerte entre 70 et 80%, Seuil critique >80%)
• Disque dur : (Seuil acceptable <70%, Seuil alerte entre 70 et 80%, Seuil critique >80%)

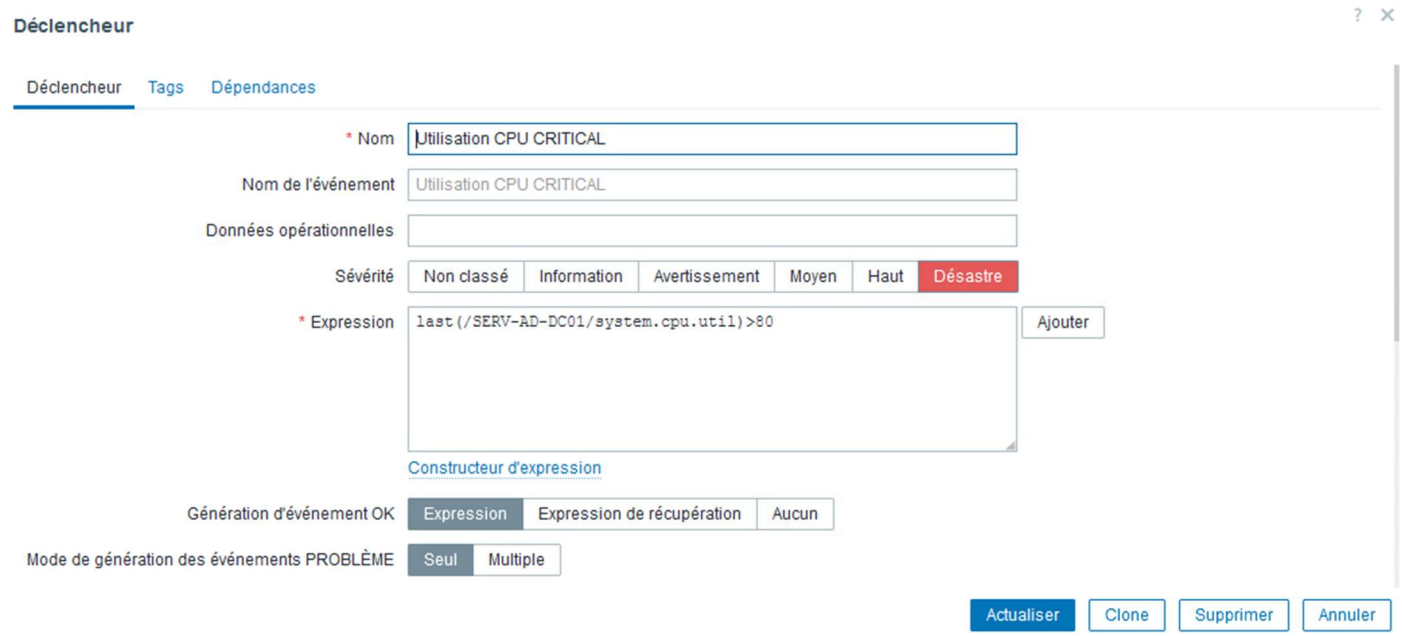
Il faudra donc configurer 2 déclencheurs par ressources :
- Un déclencheur lorsque l'utilisation est supérieure à 70% (sévérité : haute)
- Un autre déclencheur lorsque l'utilisation est supérieure à 80% (sévérité : désastre)

CPU

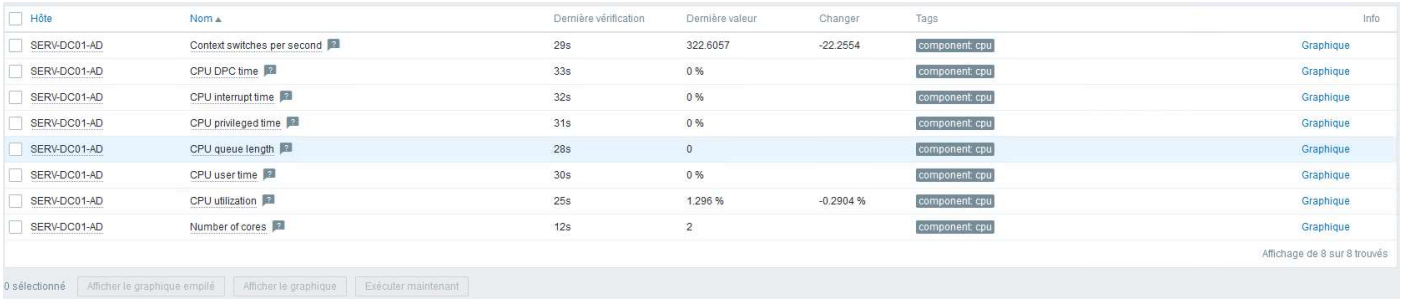
Créer un déclencheur pour une utilisation > à 70% :

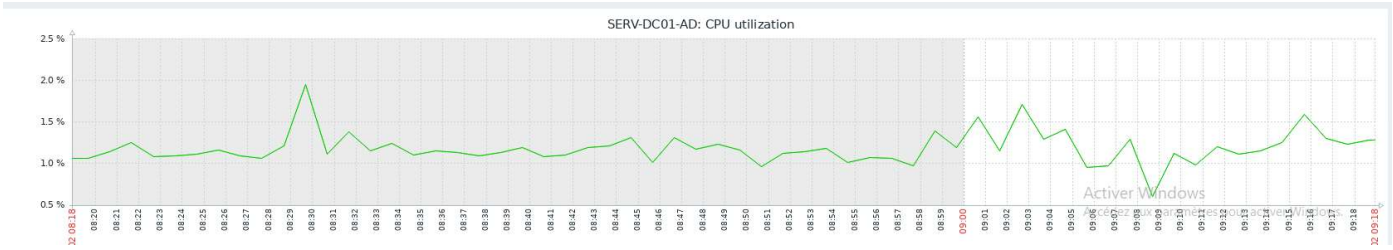


Créer un déclencheur pour une utilisation > à 80% :

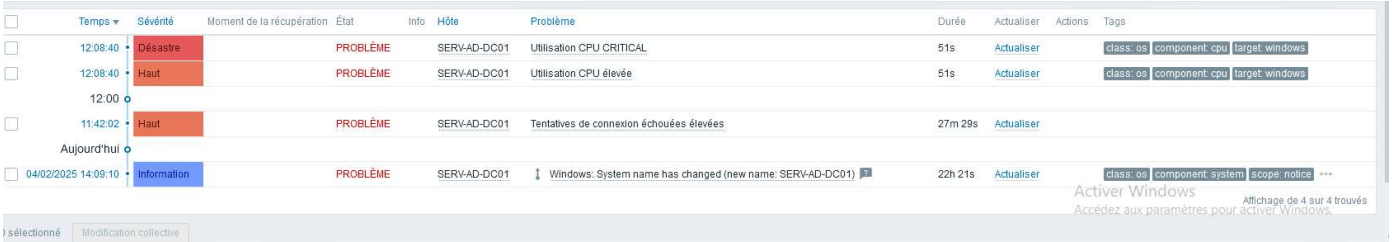


Les métriques sont bien remontées :



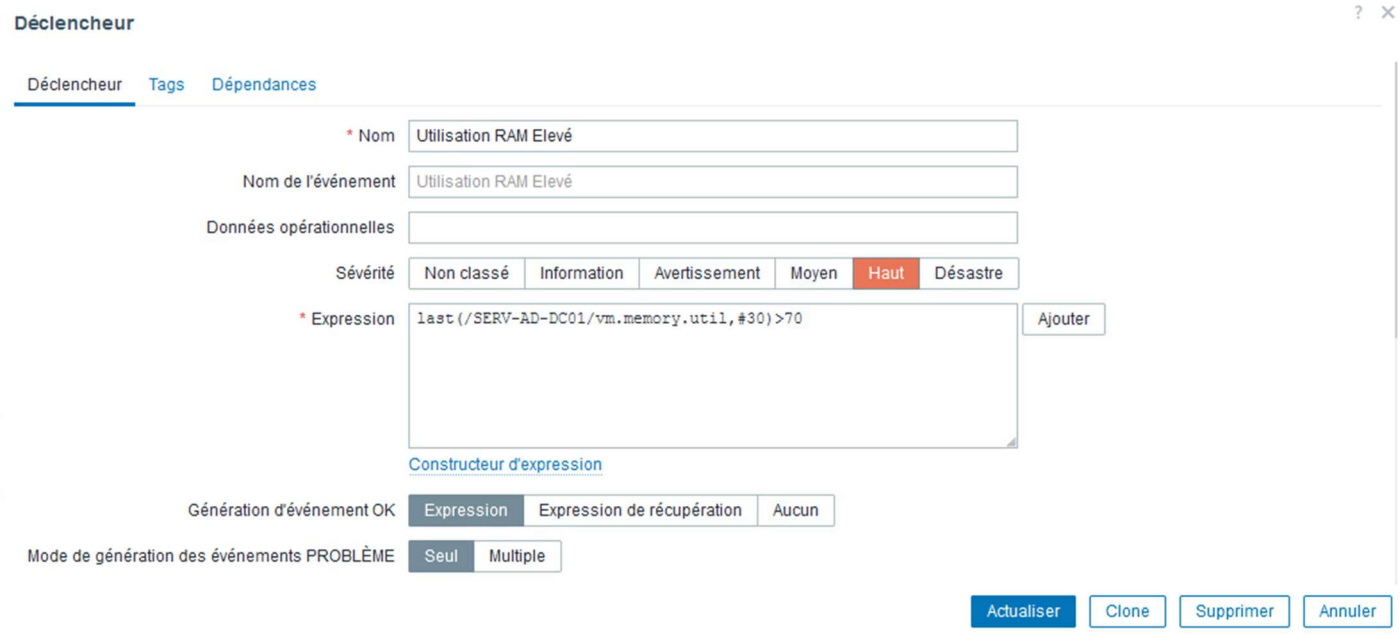


Stress test effectué, voici le résultat :

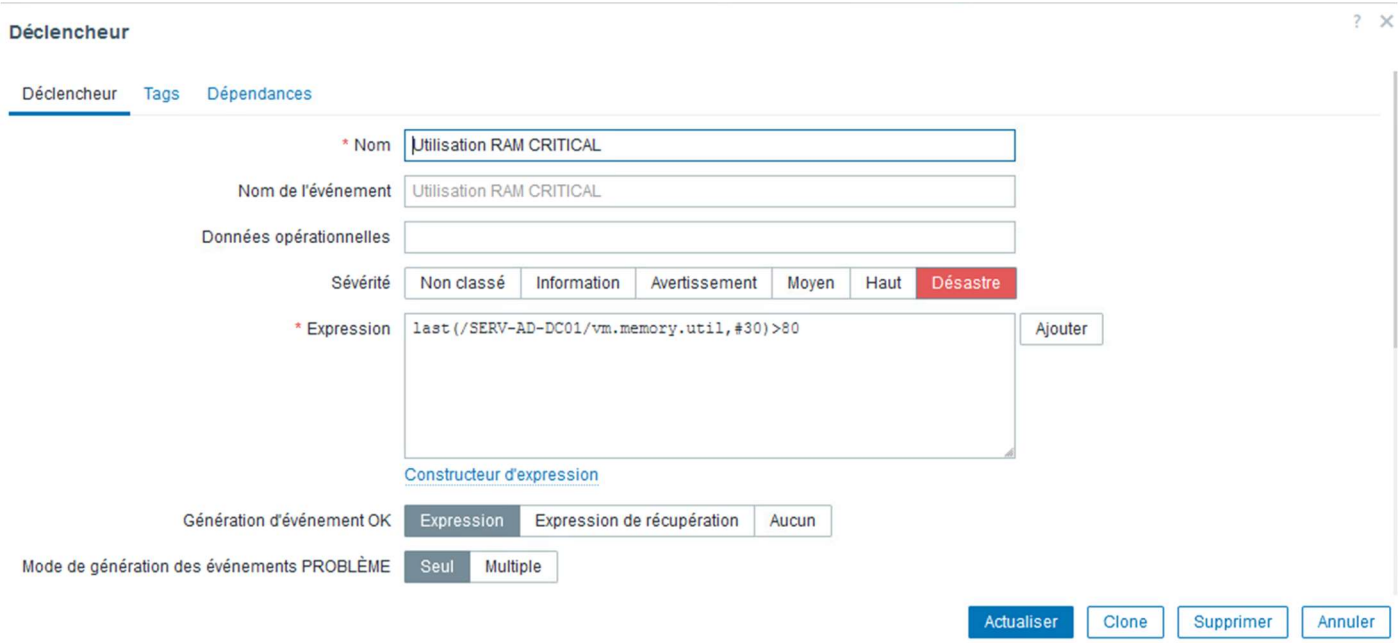


RAM

Créer un déclencheur pour une utilisation > à 70% :



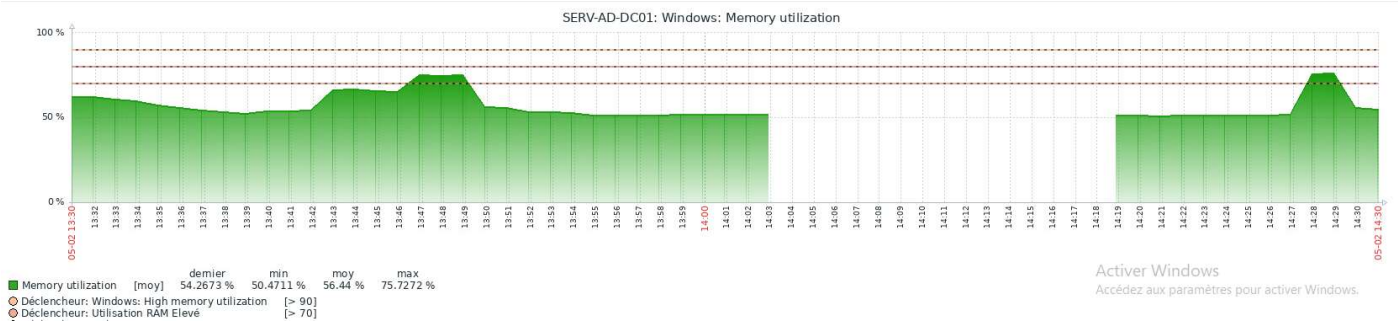
Créer un déclencheur pour une utilisation > à 80% :



Les métriques sont bien remontées :

Hôte	Nom ▲	Dernière vérification	Dernière valeur	Changer	Tags	Info
SERV-DC01-AD	Cache bytes	16s	198.79 MB	+284 KB	component: memory	Graphique
SERV-DC01-AD	Free swap space	57s	920.08 MB		component: memory component: storage	Graphique
SERV-DC01-AD	Free swap space in %	11s	65.347 %	+0.000555 %	component: memory component: storage	Graphique
SERV-DC01-AD	Free system page table entries	15s	16621652	+52	component: memory	Graphique
SERV-DC01-AD	Memory page faults per second	14s	39.6534	-3.6637	component: memory	Graphique
SERV-DC01-AD	Memory pages per second	13s	0		component: memory	Graphique
SERV-DC01-AD	Memory pool non-paged	12s	176.91 MB		component: memory	Graphique
SERV-DC01-AD	Memory utilization	50s	59.8531 %	-0.00248 %	component: memory	Graphique
SERV-DC01-AD	Total memory	52s	4 GB		component: memory	Graphique
SERV-DC01-AD	Total swap space	56s	1.38 GB		component: memory component: storage	Graphique
SERV-DC01-AD	Used memory	51s	2.39 GB	-104 KB	component: memory	Graphique
SERV-DC01-AD	Used swap space in %	11s	34.653 %	-0.000555 %	component: memory component: storage	Graphique

Affichage de 12 sur 12 trouvés



Stress test effectué, voici le résultat :

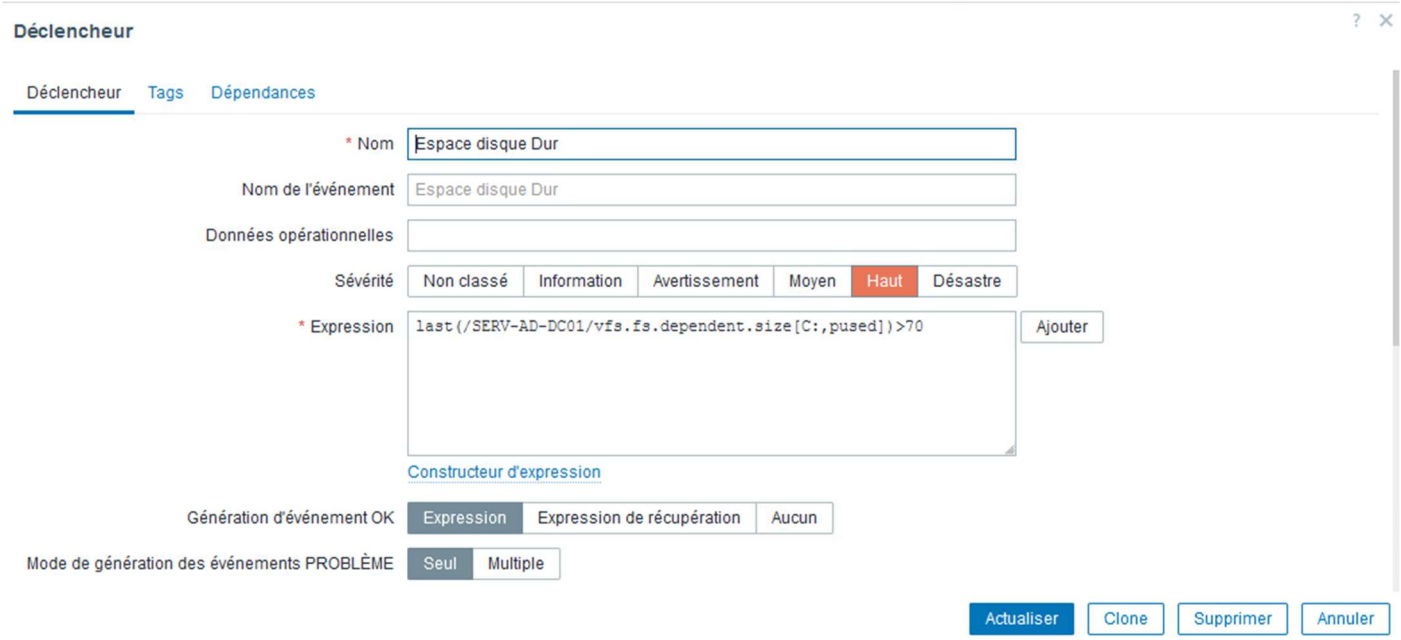
Temps ▼	Sévérité	Moment de la récupération	État	Info	Hôte	Problème	Durée	Actualiser	Actions	Tags
14:30:52	Haut	14:33:52	RÉSOLU		SERV-AD-DC01	Utilisation RAM Elevé	3m	Actualiser		class: os component: memory target: windows
14:28:40	Désastre	14:29:40	RÉSOLU		SERV-AD-DC01	Utilisation CPU CRITICAL	1m	Actualiser		class: os component: cpu target: windows
14:28:40	Haut	14:29:40	RÉSOLU		SERV-AD-DC01	Utilisation CPU élevée	1m	Actualiser		class: os component: cpu target: windows
14:00										
11:42:02	Haut		PROBLÈME		SERV-AD-DC01	Tentatives de connexion échouées élevées	2h 52m	Actualiser		
11:00										
10:43:55	Avertissement		PROBLÈME		Zabbix server	Linux: Number of installed packages has been changed	3h 50m 7s	Actualiser		class: os component: os scope: notice •••

Affichage de 5 sur 5 trouvés

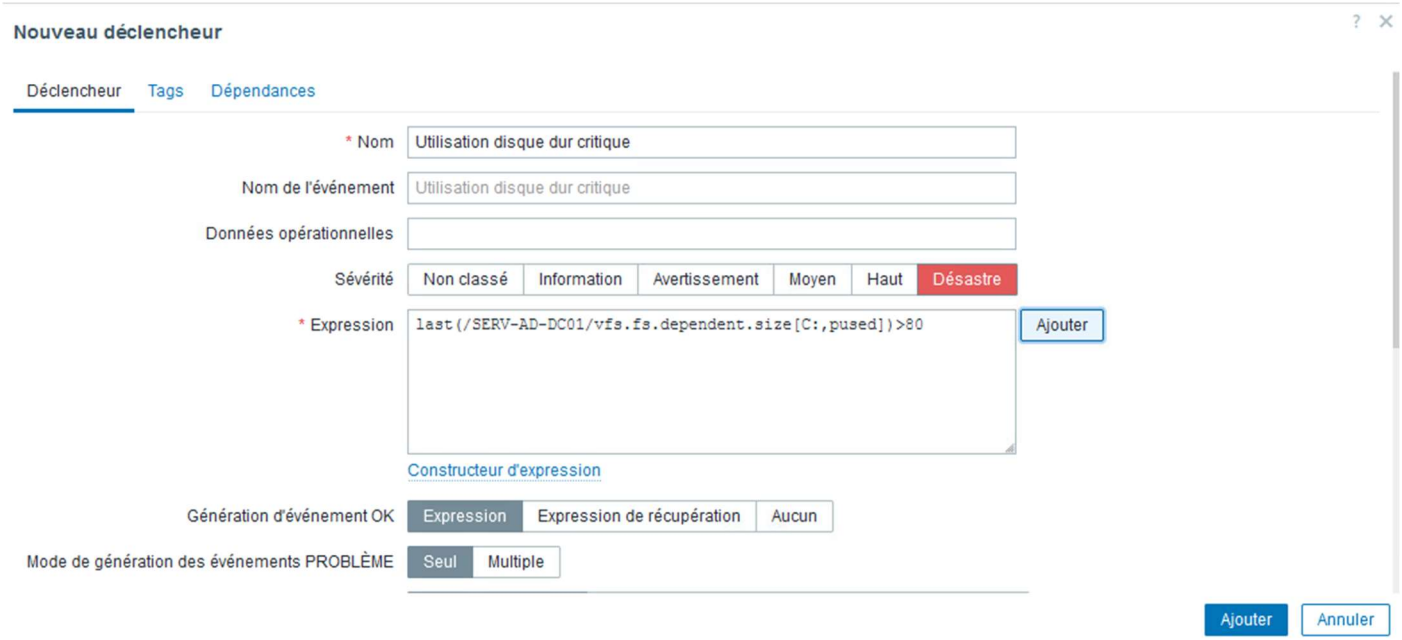
0 sélectionné | Modification collective

DISQUE DUR

Créer un déclencheur pour une utilisation > à 70% :



Créer un déclencheur pour une utilisation > à 80% :



Les métriques sont bien remontées :

Hôte	Nom ▲	Dernière vérification	Dernière valeur	Changer	Tags	Info
SERV-DC01-AD	0 C:: Average disk read queue length	56s	0.000135	-0.000065	component: storage disk: 0 C:	Graphique
SERV-DC01-AD	0 C:: Average disk write queue length	55s	0.01405	+0.005795	component: storage disk: 0 C:	Graphique
SERV-DC01-AD	0 C:: Disk average queue size (avgqu-sz)	52s	0		component: storage disk: 0 C:	Graphique
SERV-DC01-AD	0 C:: Disk read rate	51s	0.06586 r/s	+0.0327 r/s	component: storage disk: 0 C:	Graphique
SERV-DC01-AD	0 C:: Disk read request avg waiting time	54s	0.15ms	+0.053ms	component: storage disk: 0 C:	Graphique
SERV-DC01-AD	0 C:: Disk utilization by idle time	57s	0.8349 %	+0.2019 %	component: storage disk: 0 C:	Graphique
SERV-DC01-AD	0 C:: Disk write rate	50s	1.9299 w/s	+0.8042 w/s	component: storage disk: 0 C:	Graphique
SERV-DC01-AD	0 C:: Disk write request avg waiting time	53s	2.69ms	+0.72ms	component: storage disk: 0 C:	Graphique
SERV-DC01-AD	Free swap space	50s	920.09 MB	+8 KB	component: memory component: storage	Graphique
SERV-DC01-AD	Free swap space in %	4s	65.347 %		component: memory component: storage	Graphique
SERV-DC01-AD	FS [Système(C:)]: Get data	46s	{"fsname":"C:","fslabel":"...		component: raw component: storage filesystem: C: •••	Historique
SERV-DC01-AD	FS [Système(C:)]: Space: Available	46s	60.52 GB		component: storage filesystem: C: fstype: NTFS	Graphique
SERV-DC01-AD	FS [Système(C:)]: Space: Total	46s	79.33 GB		component: storage filesystem: C: fstype: NTFS	Graphique
SERV-DC01-AD	FS [Système(C:)]: Space: Used	46s	18.81 GB		component: storage filesystem: C: fstype: NTFS	Graphique
SERV-DC01-AD	FS [Système(C:)]: Space: Used, in %	46s	23.7145 %		component: storage filesystem: C: fstype: NTFS	Graphique
SERV-DC01-AD	Total swap space	49s	1.38 GB		component: memory component: storage	Graphique
SERV-DC01-AD	Used swap space in %	4s	34.653 %		component: memory component: storage	Graphique

Affichage de 17 sur 17 trouvés

Test effectué en créant un fichier de 40 Go ce qui occupe plus de 70% du disque dur, voici le résultat :

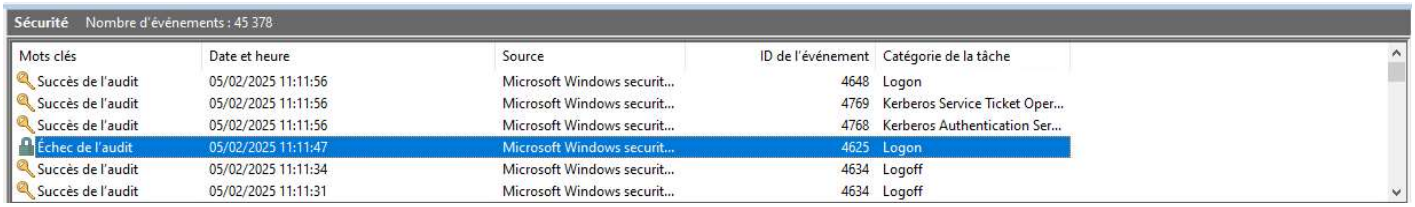
Temps ▾	Sévérité	Moment de la récupération	État	Info	Hôte	Problème
13:36:49	Haut		PROBLÈME		SERV-AD-DC01	Espace disque Dur

Tes effectué en créant un fichier de 55 go ce qui occupe plus de 80 % du disque dur, voici le résultat :

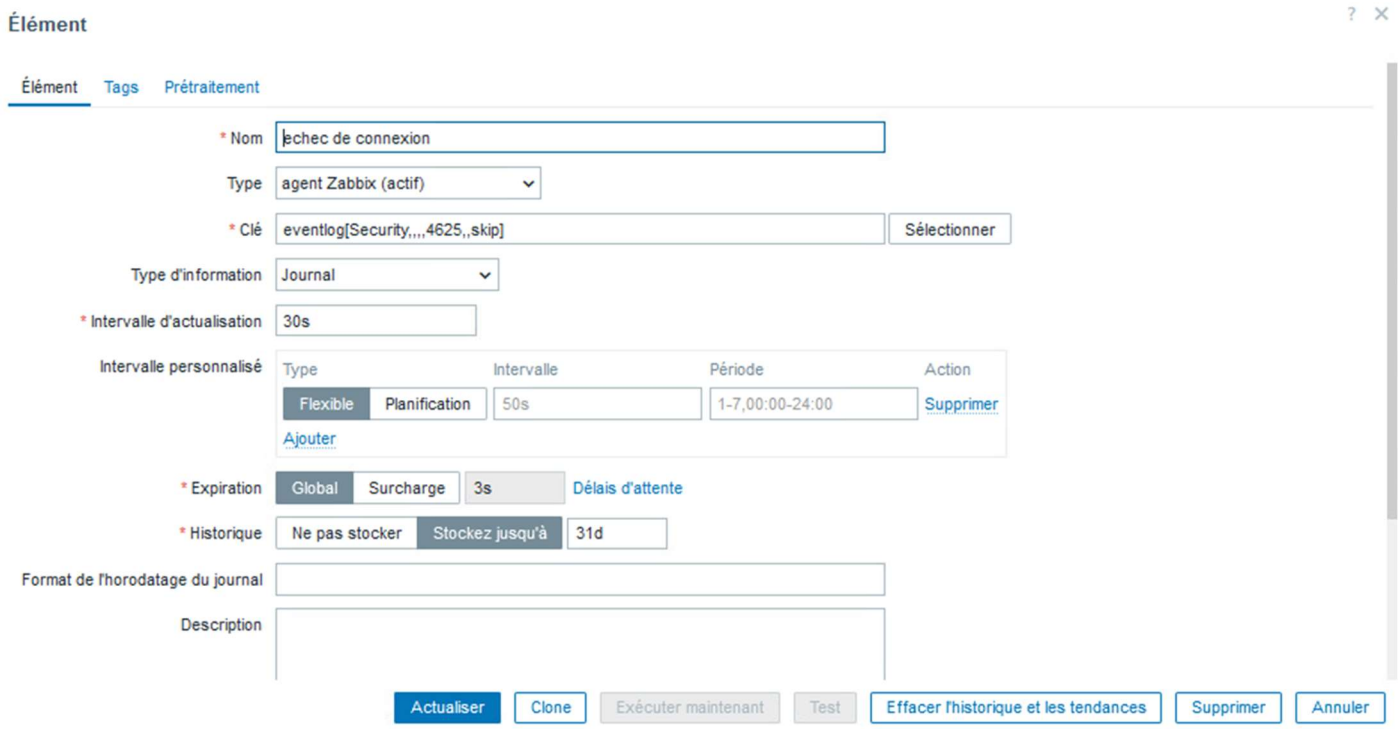
Temps ▾	Sévérité	Moment de la récupération	État	Info	Hôte	Problème	Durée
13:40:49	Désastre		PROBLÈME		SERV-AD-DC01	Utilisation disque dur critique	6s

SUPERVISION DES EVENEMENTS ET LOGS

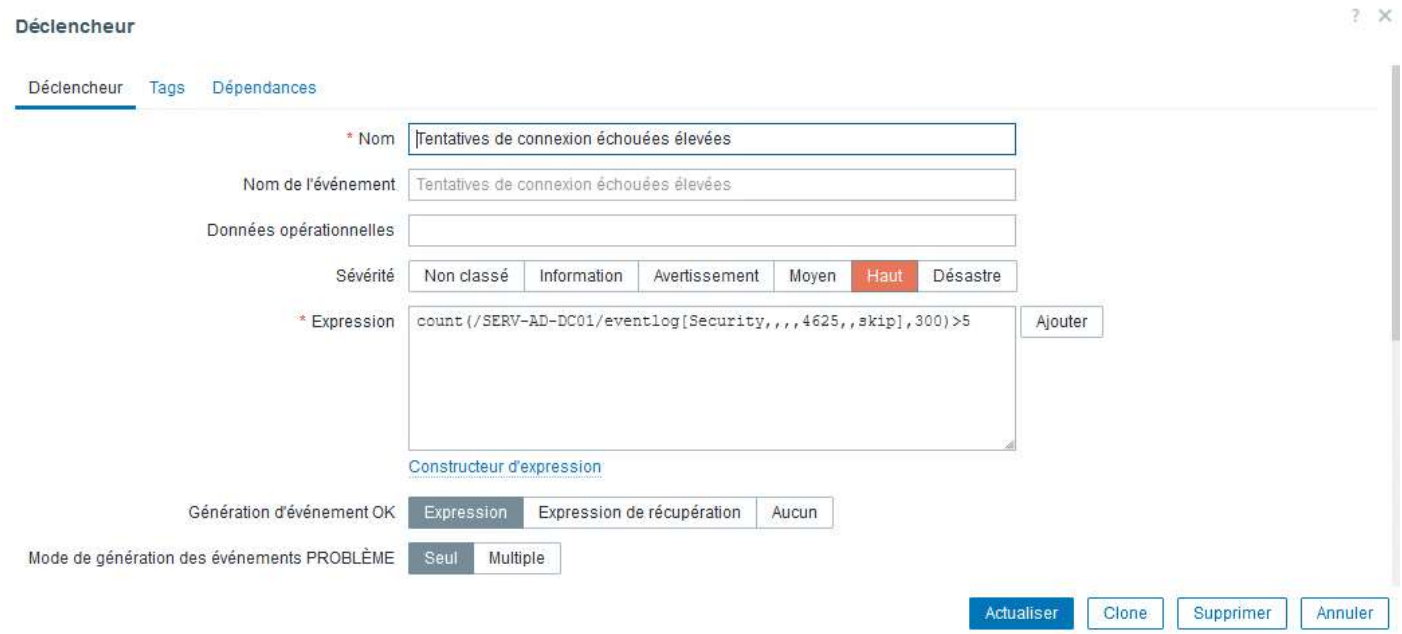
Sur l'observateur d'évènements Windows, nous souhaitons superviser les ID de l'évènement 4625 et 4776 :

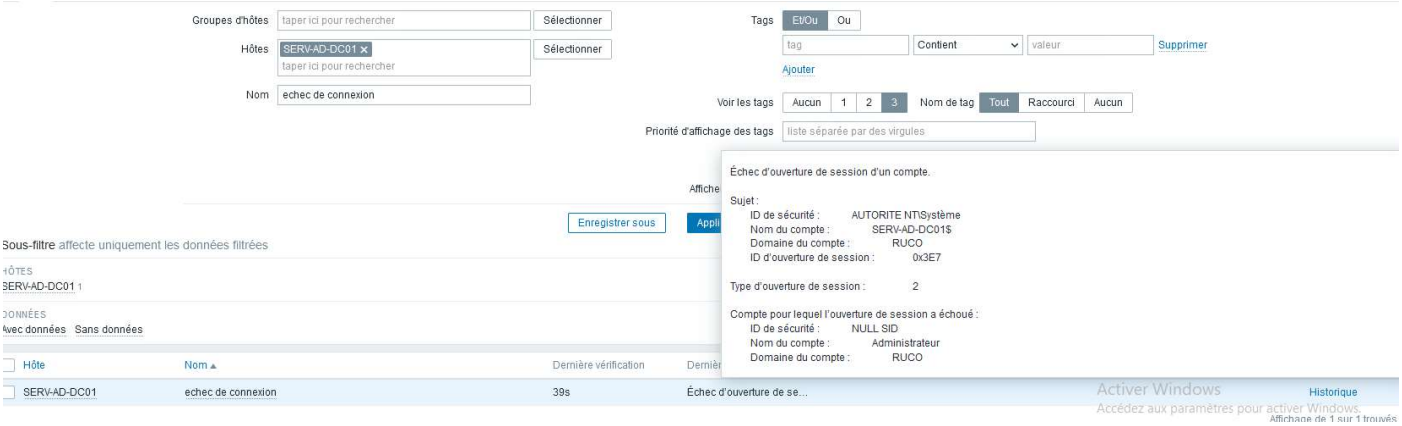


Créer un élément :



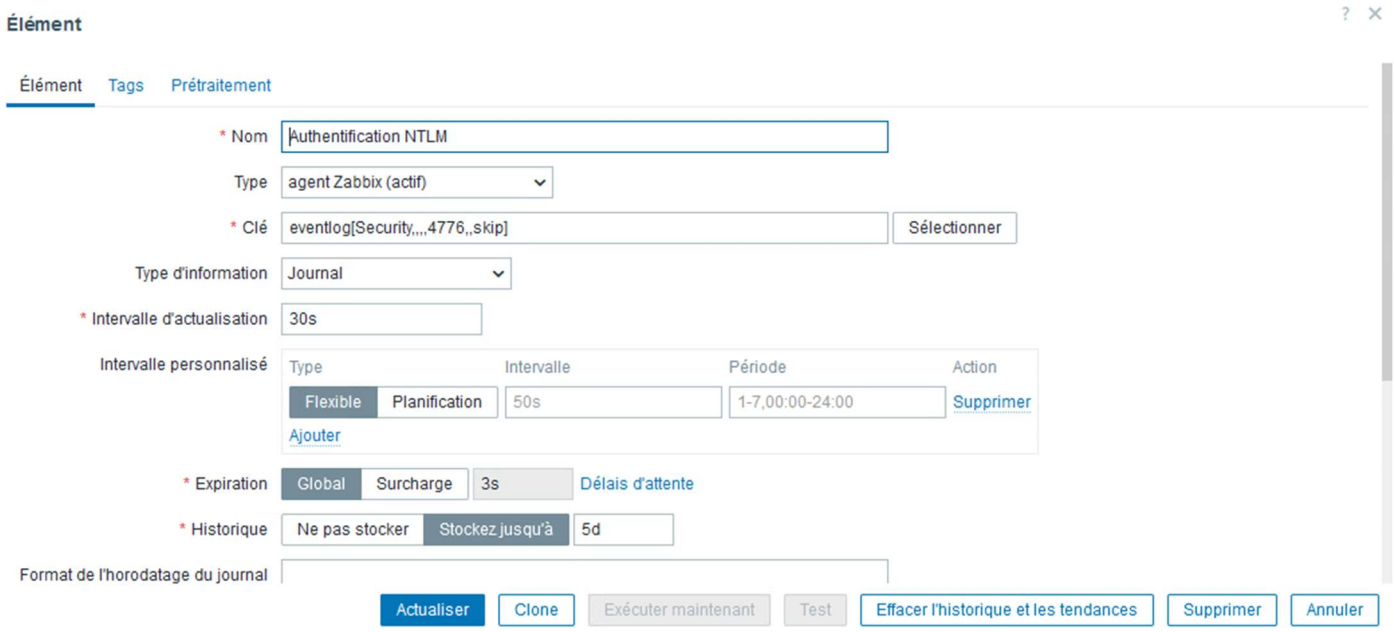
Créer un déclencheur :



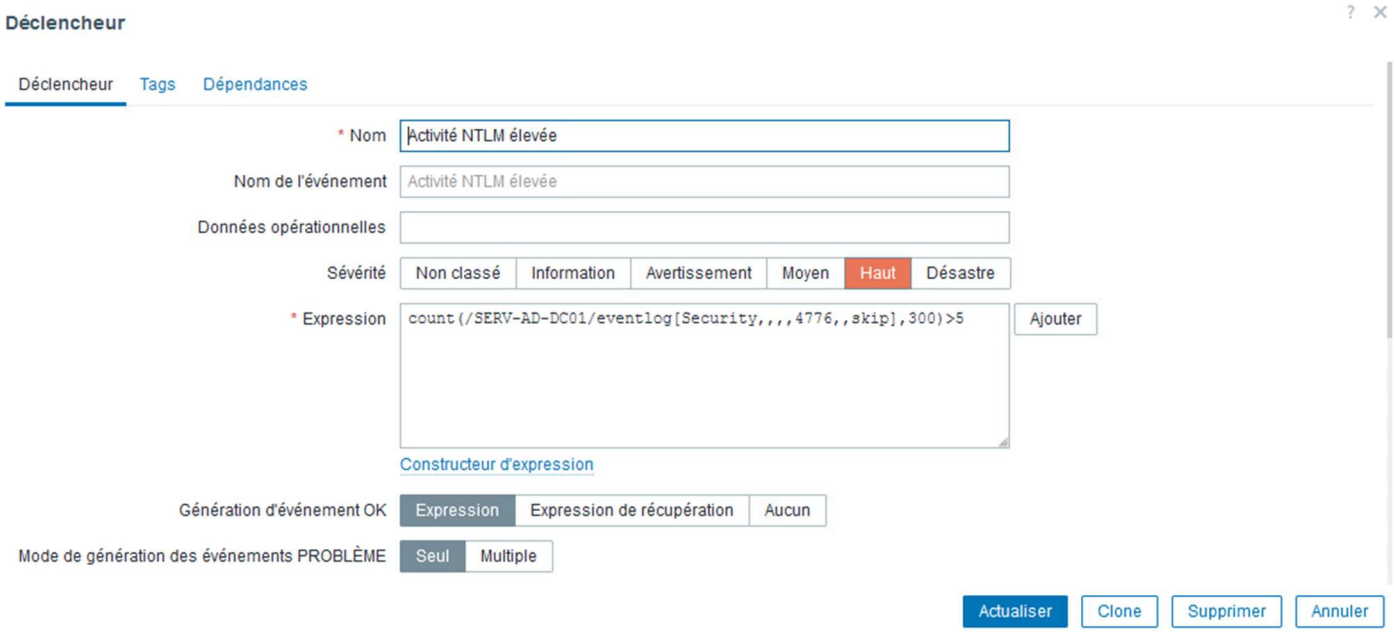


Test de connexion avec une session et mot de passe erronés sur l'AD, voici le résultat :

Création de l'élément : Authentification NTLM



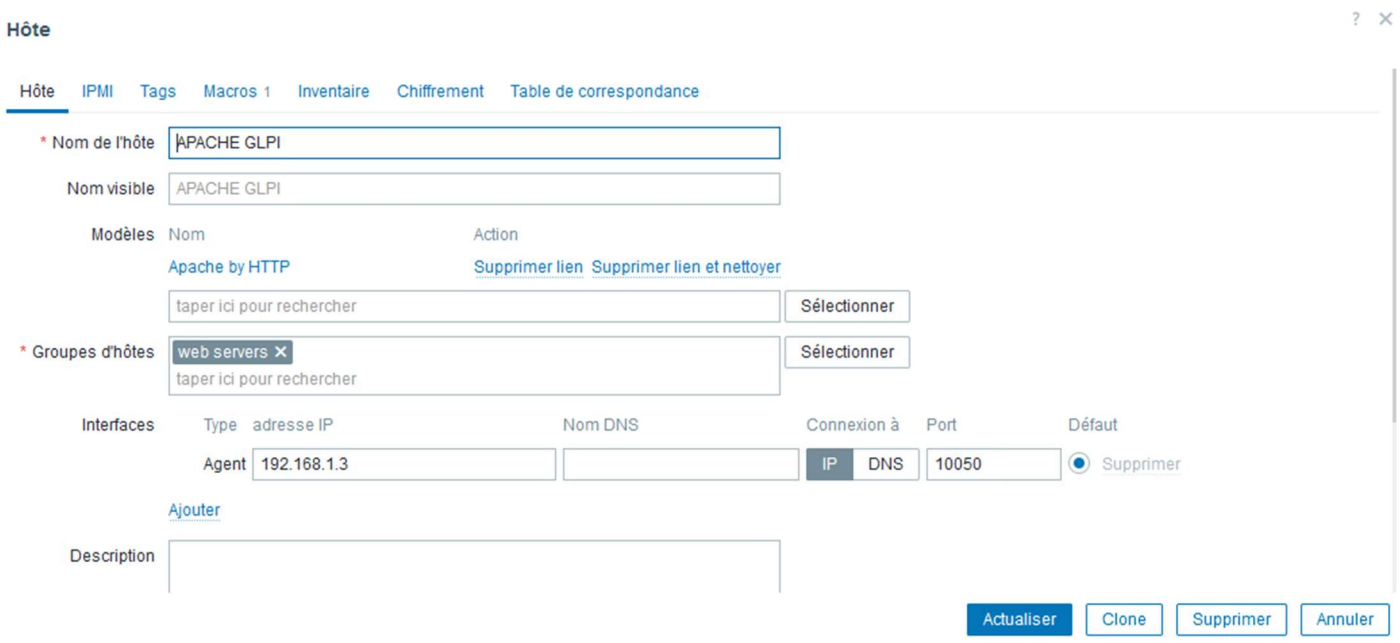
Création d'un déclencheur pour alerter d'une activité NTLM élevée, soit plus de 5 tentatives de connexion :

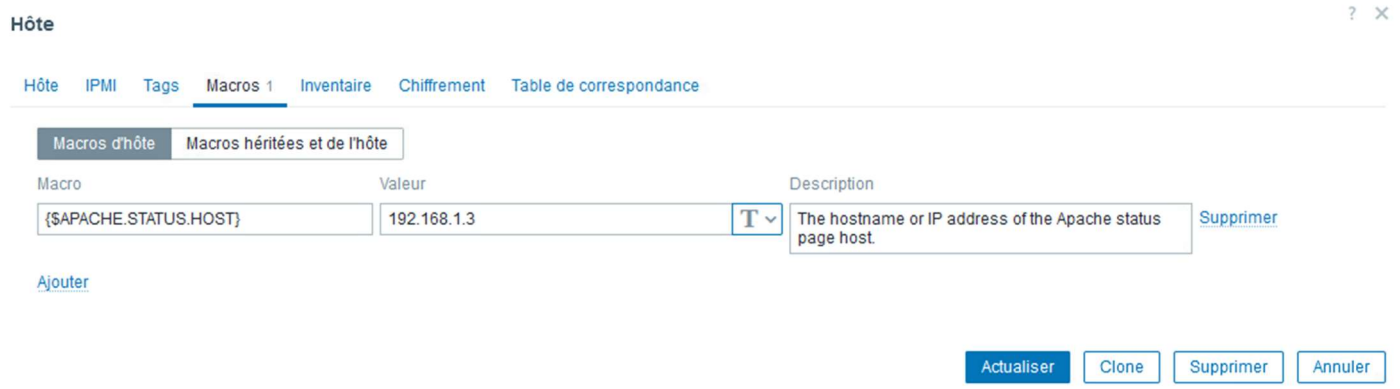


Test effectué, voici le résultat :

SUPERVISION DU SERVICE APACHE

Création de l'hôte :





Sur le serveur GLPI :

Activer le module « mod_status »

```
sudo a2enmod status
sudo systemctl reload apache2
```

Configuration du mode server-status dans Apache : Modifier le fichier de configuration :

```
sudo nano /etc/apache2/mods-available/status.conf
```

```
<IfModule mod_status.c>
ExtendedStatus On
<Location /server-status>
SetHandler server-status
Require local
```

```
Require ip 192.168.1.8
</Location>
</IfModule>
```

Recharger la configuration :

```
sudo systemctl reload apache2
```

Vérifier l'accès à /server-status :

Tester en local :

```
curl -I http://127.0.0.1/server-status
```

Tester depuis une autre machine autorisée :

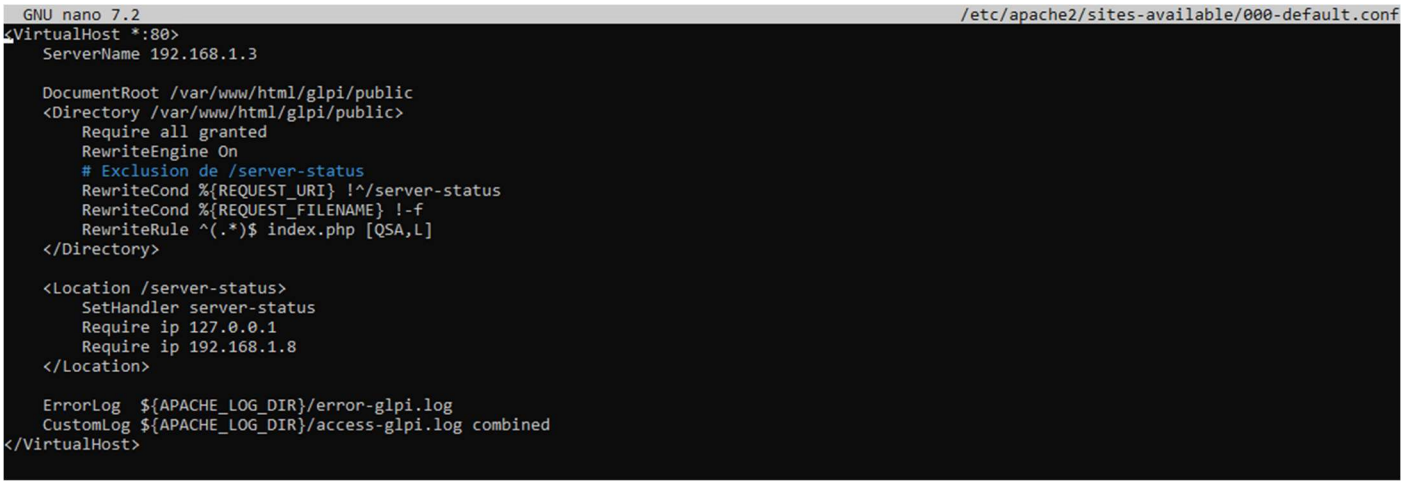
```
curl -I http://192.168.1.3/server-status
```

Recharger Apache :

```
sudo systemctl reload apache2
```

Corriger le conflit avec le VirtualHost GLPI :

```
sudo nano /etc/apache2/sites-available/000-default.conf
```



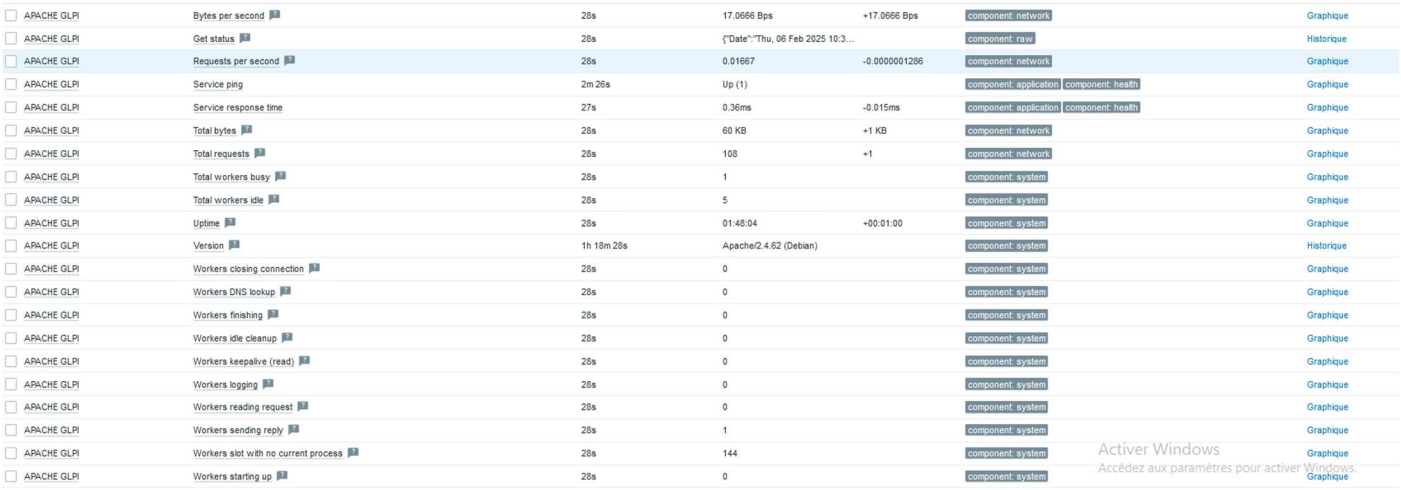
Recharger Apache :

```
sudo systemctl reload apache2
```

Vérifier que server-status fonctionne :

```
curl -I http://192.168.1.3/server-status
```

Les métriques sont bien remontés : On voit effectivement un ensemble de métriques récupérées depuis mod_status (via l'URL /server-status?auto) et affichées dans Zabbix.



APACHE GLPI	Bytes per second	28s	17.0666 Bps	+17.0666 Bps	component: network	Graphique
APACHE GLPI	Get status	28s	{"Date":"Thu, 06 Feb 2025 10:3...		component: raw	Historique
APACHE GLPI	Requests per second	28s	0.01667	-0.0000001286	component: network	Graphique
APACHE GLPI	Service ping	2m 26s	Up (1)		component: application component: health	Graphique
APACHE GLPI	Service response time	27s	0.36ms	-0.015ms	component: application component: health	Graphique
APACHE GLPI	Total bytes	28s	60 KB	+1 KB	component: network	Graphique
APACHE GLPI	Total requests	28s	108	+1	component: network	Graphique
APACHE GLPI	Total workers busy	28s	1		component: system	Graphique
APACHE GLPI	Total workers idle	28s	5		component: system	Graphique
APACHE GLPI	Uptime	28s	01:48:04	+00:01:00	component: system	Graphique
APACHE GLPI	Version	1h 18m 28s	Apache/2.4.62 (Debian)		component: system	Historique
APACHE GLPI	Workers closing connection	28s	0		component: system	Graphique
APACHE GLPI	Workers DNS lookup	28s	0		component: system	Graphique
APACHE GLPI	Workers finishing	28s	0		component: system	Graphique
APACHE GLPI	Workers idle cleanup	28s	0		component: system	Graphique
APACHE GLPI	Workers keepalive (read)	28s	0		component: system	Graphique
APACHE GLPI	Workers logging	28s	0		component: system	Graphique
APACHE GLPI	Workers reading request	28s	0		component: system	Graphique
APACHE GLPI	Workers sending reply	28s	1		component: system	Graphique
APACHE GLPI	Workers slot with no current process	28s	144		component: system	Graphique
APACHE GLPI	Workers starting up	28s	0		component: system	Graphique

Voici une brève explication des principales :

- **Bytes per second / Requests per second :** Donnent une idée du débit d'informations envoyé par Apache et du nombre de requêtes traitées en continu. Sur un serveur peu chargé, ces valeurs peuvent être faibles (ex. 0,016 requêtes/s).

- **Service ping / Service response time :** Souvent liés à un scénario Zabbix "Simple check" ou "Web scenario" qui mesure la disponibilité et le temps de réponse du service. "Up (1)" et un temps de ~0,36 ms indiquent que le service est disponible et répond très rapidement.

- **Total bytes / Total requests :** Compteurs cumulatifs du trafic et des requêtes depuis le démarrage d'Apache. Total workers busy / idle : Indique combien de workers sont actuellement occupés (1) et combien sont en attente (5) pour traiter de nouvelles requêtes.

- **Uptime :** Durée écoulée depuis le dernier démarrage ou redémarrage d'Apache. Ici, ~1h48.

- **Version :** La version d'Apache (2.4.62 sur Debian).

- **Workers closing connection, DNS lookup, finishing, etc. :** Correspondent aux différents états dans lesquels peuvent se trouver les threads/processus Apache. Des valeurs à 0 signifient qu'aucun worker n'est dans cet état au moment de la mesure.

- **Workers sending reply :** Le nombre de workers actuellement en train d'envoyer une réponse au client. Ici, on en voit 1.

- **Workers slot with no current process :** Indique les "slots" disponibles (ou non utilisés) pour lancer des nouveaux workers si besoin (144 ici).