

# RAPPORT TECHNIQUE

---

Supervision Zabbix  
de l'Active Directory

Rudy COLOMBEL  
Vanthary SOK

Février 2025

## TABLE DES MATIÈRES

Contexte .....	2
Objectif.....	2
Éléments supervisés .....	2
Ressources système .....	2
Événements et logs .....	2
Supervision d'Apache (installé sur l'Active Directory).....	2
Prérequis .....	3
Supervision des ressources système.....	3
Supervision d'Apache.....	3
Installation de Zabbix 7.0 LTS sur Debian12.....	5
Installation de l'agent Zabbix sur l'AD.....	9
Supervision des ressources système de l'AD .....	13
CPU .....	14
RAM.....	16
Disque Dur.....	18
Supervision des évènements et logs.....	20
Supervision d'Apache.....	23

## 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.

## ÉLÉMENTS 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%)

### ÉVÉNEMENTS ET LOGS

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

### SUPERVISION D'APACHE (INSTALLÉ 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=](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
```

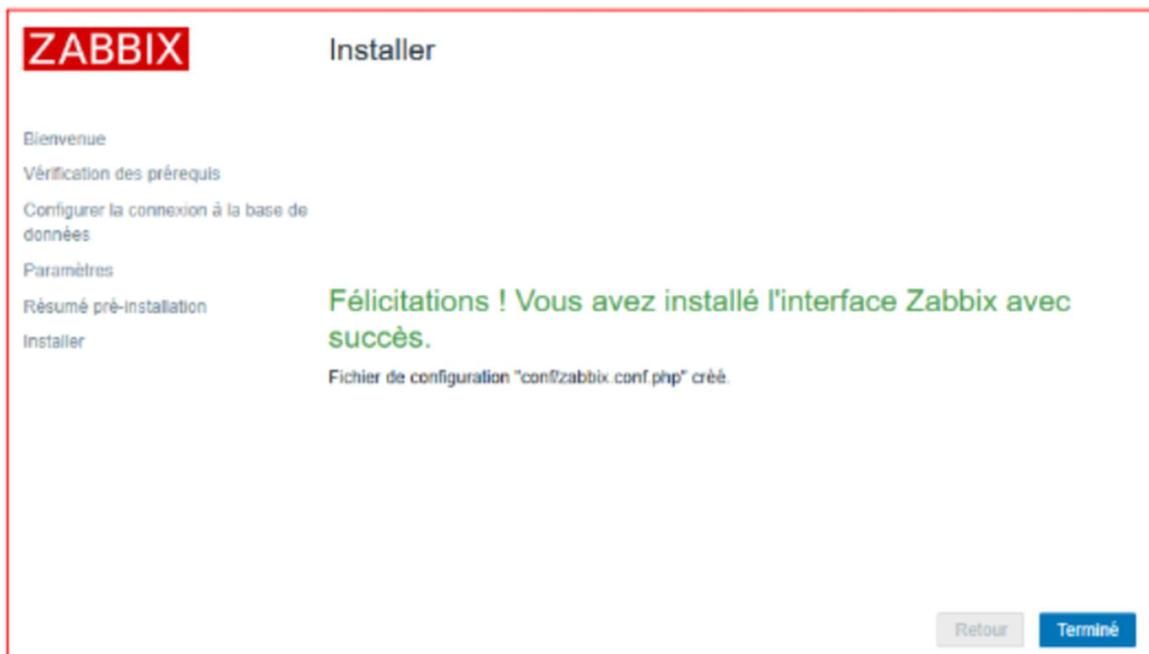
Ouvrir la page web de l'interface utilisateur de Zabbix

L'URL par défaut pour Zabbix UI lors de l'utilisation du serveur web Apache est [http://IP\\_du\\_serveur/zabbix](http://IP_du_serveur/zabbix)

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



Une fois que la configuration est terminée :

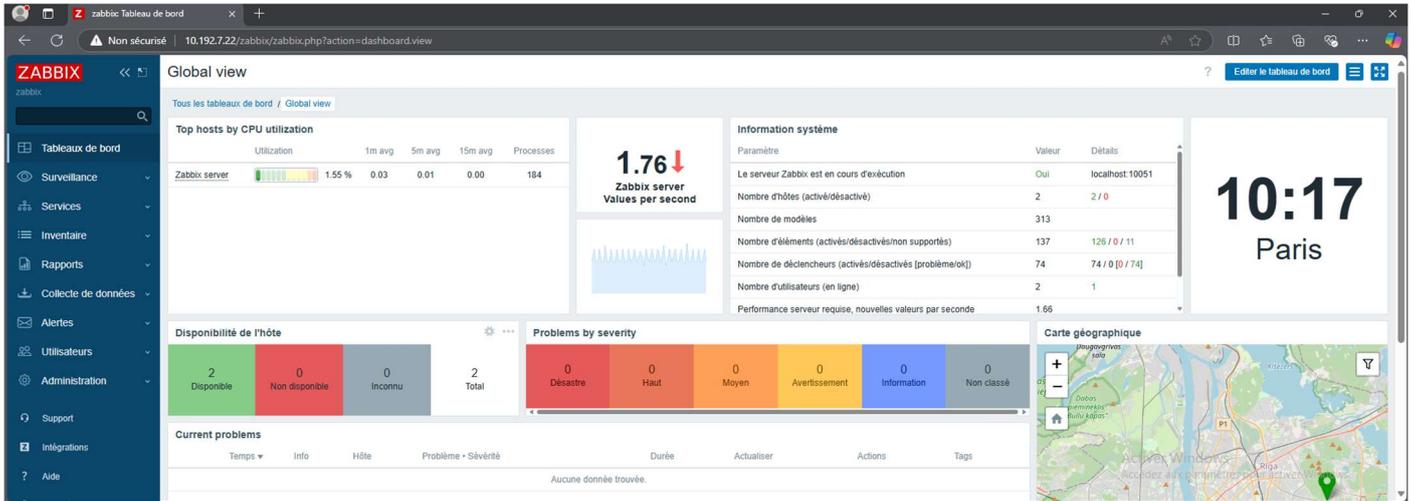


L'accès à l'écran d'authentification est maintenant possible :

The screenshot shows the Zabbix authentication screen. At the top center is the ZABBIX logo. Below it, there are two input fields: "Username" and "Password". Below the password field, there is a checkbox labeled "Remember me for 30 days" which is checked. At the bottom, there is a blue "Sign in" button. Below the button, there is a link that says "or sign in as guest".

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

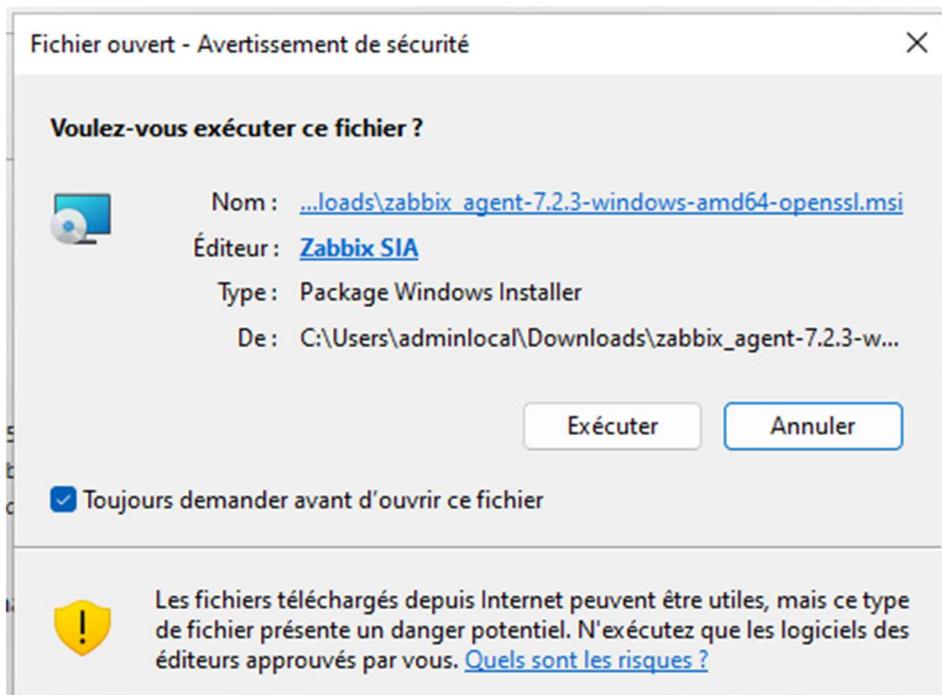
L'AD étant sur Windows Serveur 2022, l'installation de l'agent Zabbix se fait à partir d'un fichier .msi téléchargeable sur le site officiel : [https://www.zabbix.com/download\\_agents](https://www.zabbix.com/download_agents)

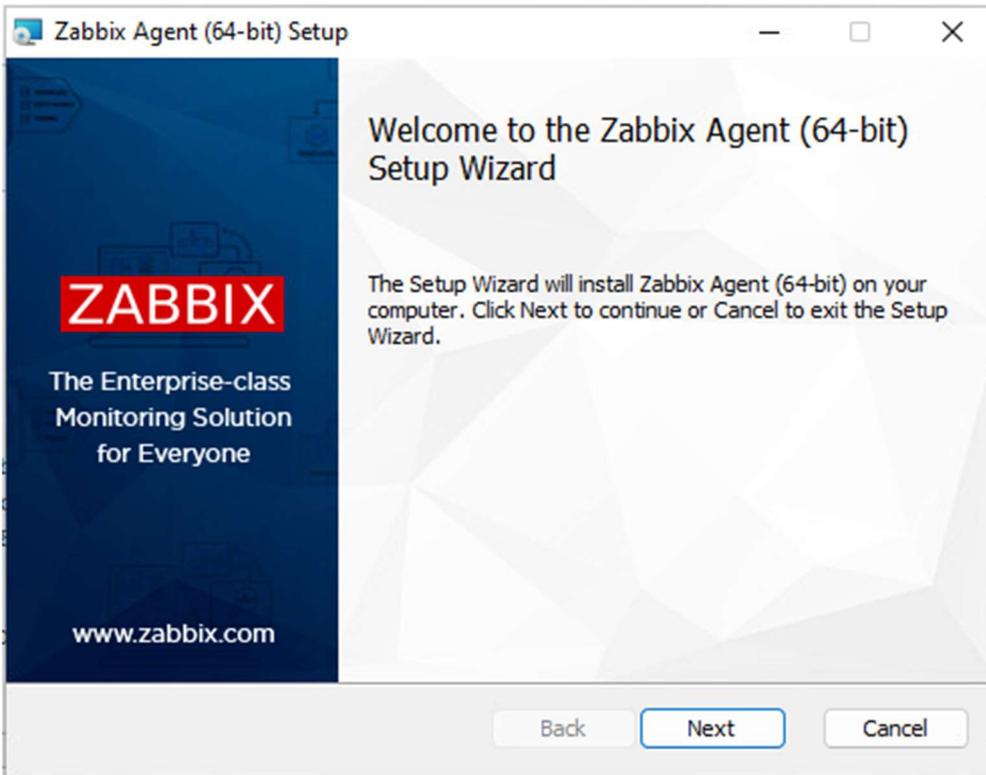
### Zabbix agent v7.2.3 [Read manual](#)

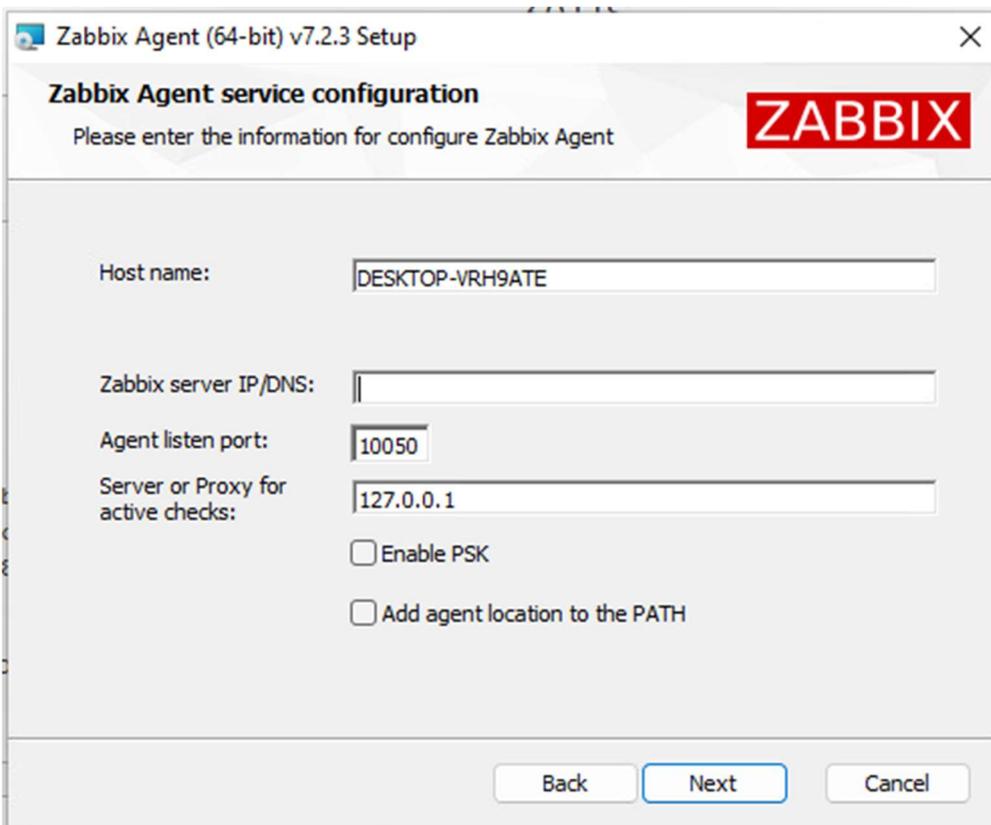
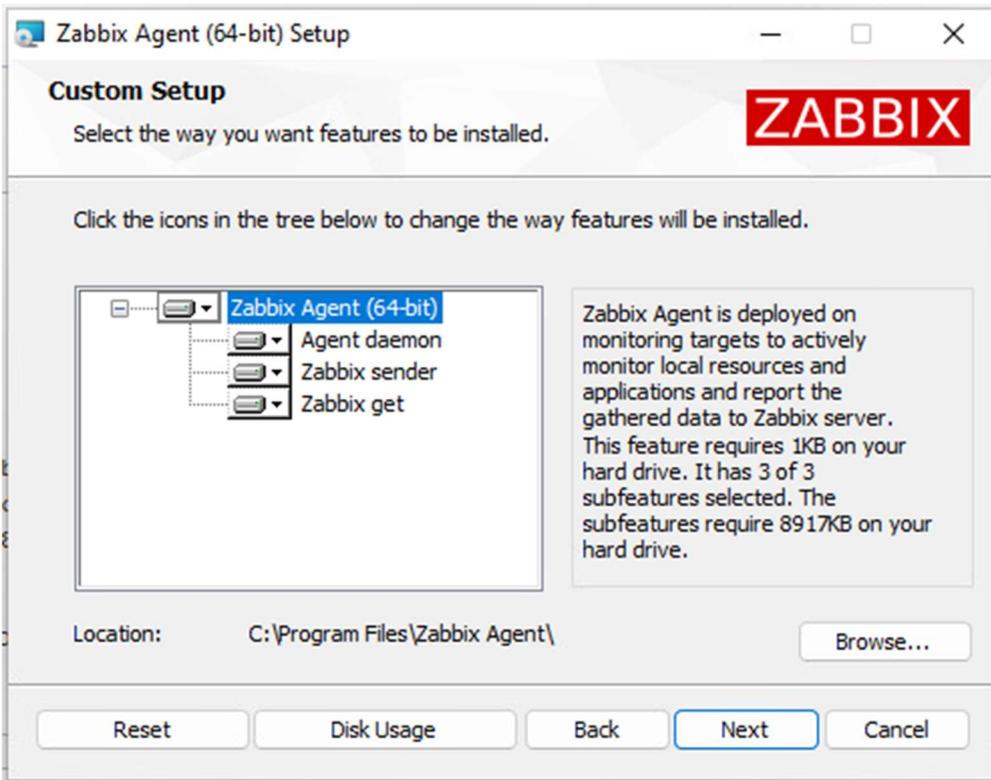
Packaging: MSI  
Encryption: OpenSSL  
Linkage: Dynamic  
Checksum: sha256: 24aedbc3601f6ca97a32bde779ba5866f9e37974c244ab81fbcdb654b2ec7f4  
sha1: 0dad158df587450015882880d6ecbb2d4d375afa  
md5: 70dff39c06311bb92a4437a146281d2b

[DOWNLOAD](#) [https://cdn.zabbix.com/zabbix/binaries/stable/7.2/7.2.3/zabbix\\_agent-7.2.3-windows-amd64-openssl.msi](https://cdn.zabbix.com/zabbix/binaries/stable/7.2/7.2.3/zabbix_agent-7.2.3-windows-amd64-openssl.msi)

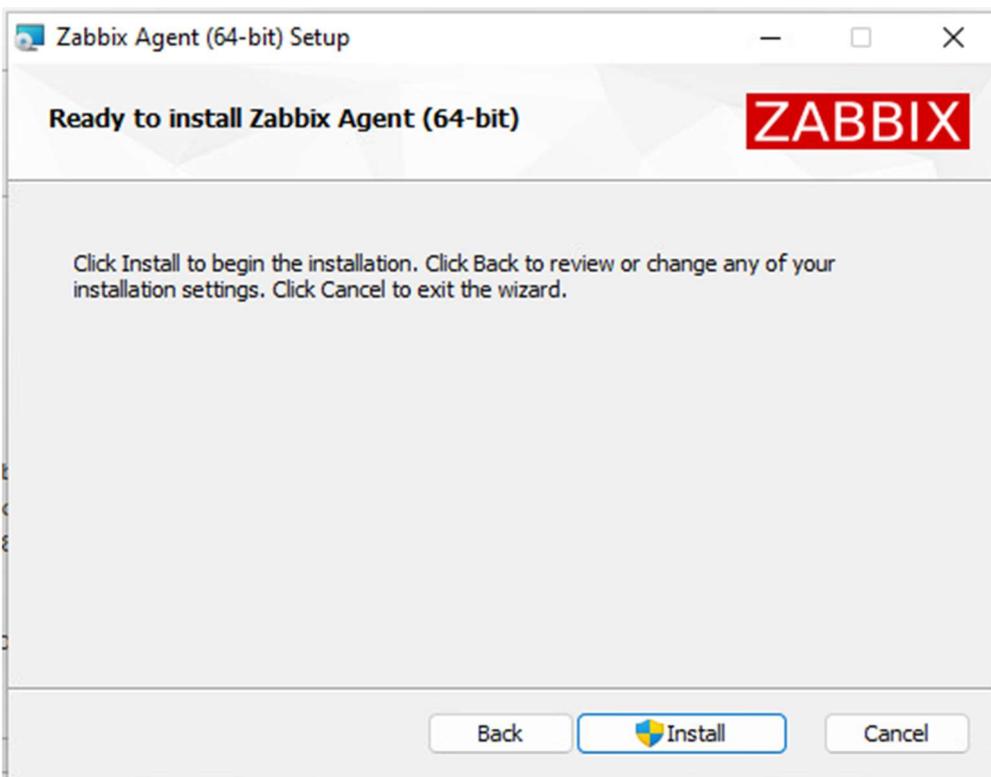
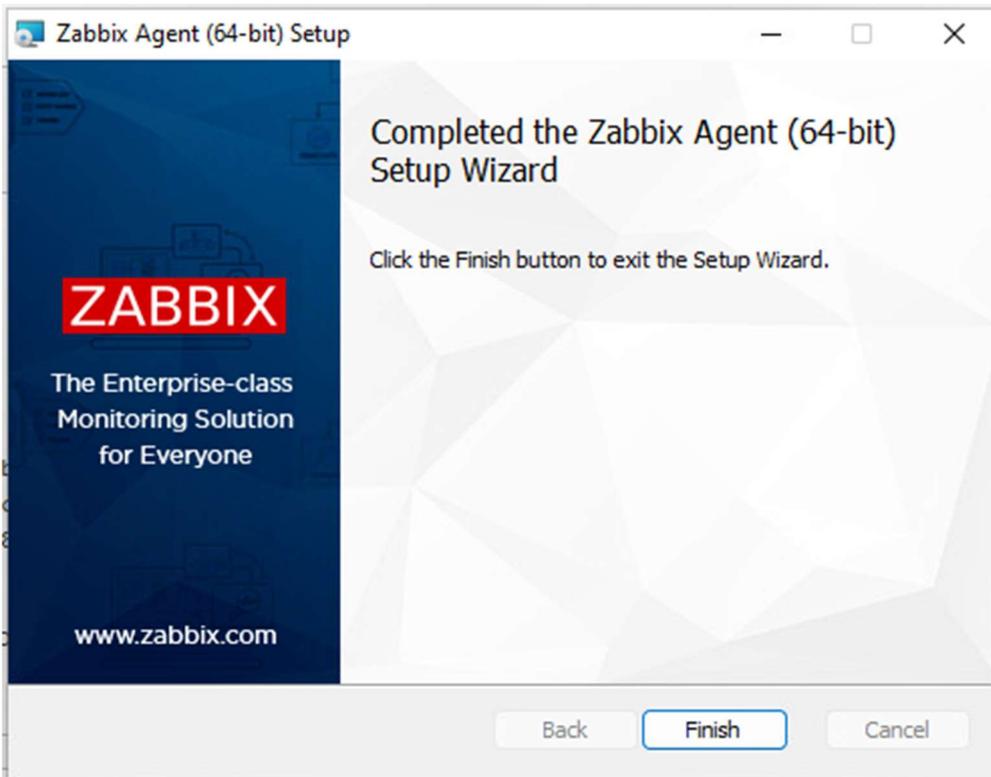
Suivre l'assistant d'installation :

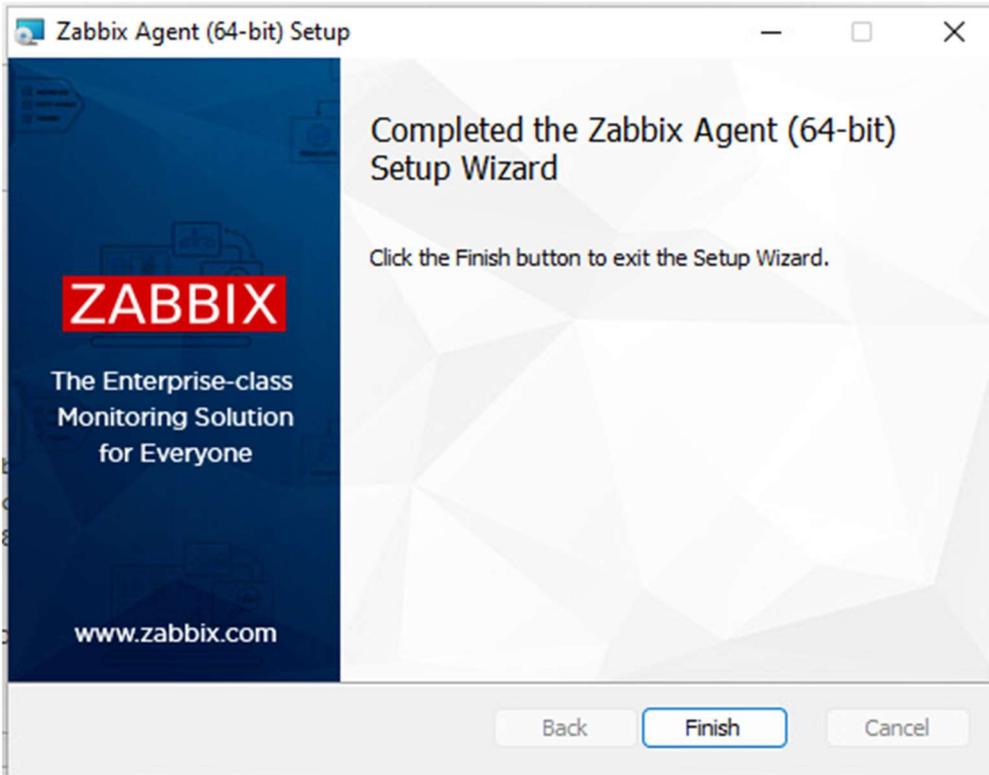




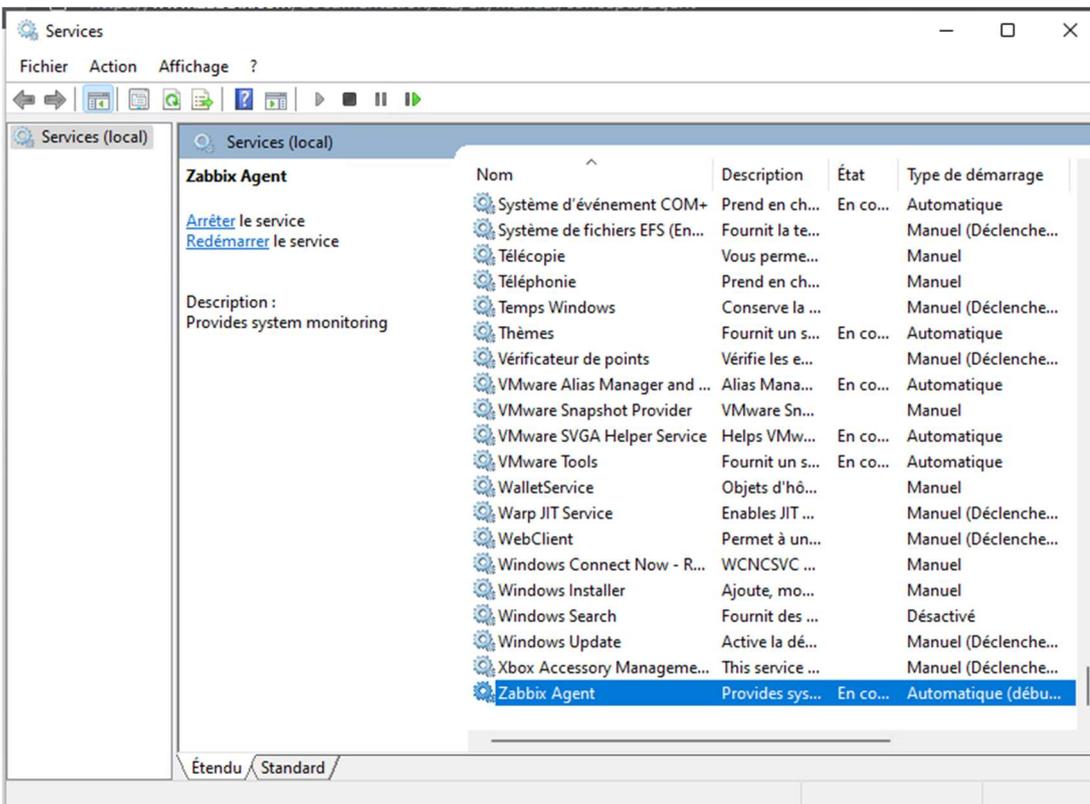


Renseigner l'IP du serveur Zabbix dans la rubrique « Zabbix server IP/DNS »





L'installation de l'agent est terminée 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% :

**Déclencheur** ? ×

Déclencheur [Tags](#) [Dépendances](#)

\* Nom

Nom de l'événement

Données opérationnelles

Sévérité  Non classé  Information  Avertissement  Moyen  Haut  Désastre

\* Expression

[Constructeur d'expression](#)

Génération d'événement OK  Expression  Expression de récupération  Aucun

Mode de génération des événements PROBLÈME  Seul  Multiple

Créer un déclencheur pour une utilisation > à 80% :

Déclencheur

Déclencheur **Tags** Dépendances

\* Nom

Nom de l'événement

Données opérationnelles

Sévérité Non classé Information Avertissement Moyen Haut Désastre

\* Expression

[Constructeur d'expression](#)

Génération d'événement OK Expression Expression de récupération Aucun

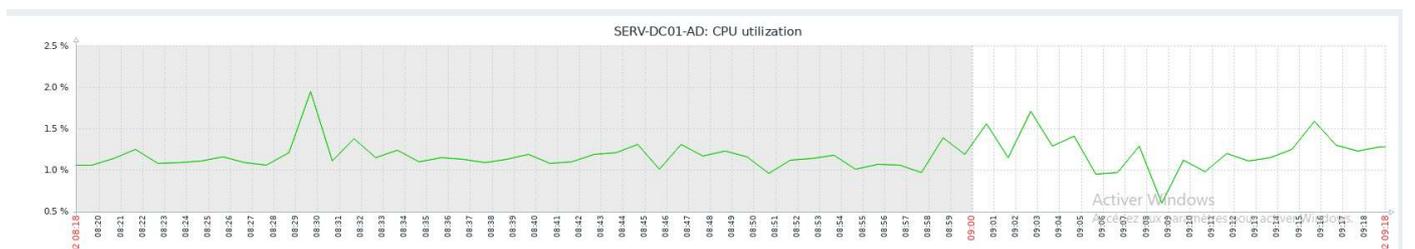
Mode de génération des événements PROBLÈME Seul Multiple

Les métriques sont bien remontées :

<input type="checkbox"/>	Hôte	Nom ▲	Dernière vérification	Dernière valeur	Changer	Tags	Info
<input type="checkbox"/>	SERV-DC01-AD	Context switches per second	29s	322.6057	-22.2554	component.cpu	Graphique
<input type="checkbox"/>	SERV-DC01-AD	CPU DPC time	33s	0 %		component.cpu	Graphique
<input type="checkbox"/>	SERV-DC01-AD	CPU interrupt time	32s	0 %		component.cpu	Graphique
<input type="checkbox"/>	SERV-DC01-AD	CPU privileged time	31s	0 %		component.cpu	Graphique
<input type="checkbox"/>	SERV-DC01-AD	CPU queue length	28s	0		component.cpu	Graphique
<input type="checkbox"/>	SERV-DC01-AD	CPU user time	30s	0 %		component.cpu	Graphique
<input type="checkbox"/>	SERV-DC01-AD	CPU utilization	25s	1.296 %	-0.2904 %	component.cpu	Graphique
<input type="checkbox"/>	SERV-DC01-AD	Number of cores	12s	2		component.cpu	Graphique

Affichage de 8 sur 8 trouvés

0 sélectionné



Stress test effectué, voici le résultat :

<input type="checkbox"/>	Temps ▼	Sévérité	Moment de la récupération	État	Info	Hôte	Problème	Durée	Actualiser	Actions	Tags
<input type="checkbox"/>	12:08:40	Désastre		PROBLÈME		SERV-AD-DC01	Utilisation CPU CRITICAL	51s	Actualiser		class:os component.cpu target:windows
<input type="checkbox"/>	12:08:40	Haut		PROBLÈME		SERV-AD-DC01	Utilisation CPU élevée	51s	Actualiser		class:os component.cpu target:windows
<input type="checkbox"/>	12:00										
<input type="checkbox"/>	11:42:02	Haut		PROBLÈME		SERV-AD-DC01	Tentatives de connexion échouées élevées	27m 29s	Actualiser		
<input type="checkbox"/>	Aujourd'hui										
<input type="checkbox"/>	04/02/2025 14:09:10	Information		PROBLÈME		SERV-AD-DC01	Windows: System name has changed (new name: SERV-AD-DC01)	22h 21s	Actualiser		class:os component:system scope:notice ***

Activer Windows  
Accédez aux paramètres pour activer Windows.

Affichage de 4 sur 4 trouvés

1 sélectionné

## RAM

Créer un déclencheur pour une utilisation &gt; à 70% :

## Déclencheur

? X

Déclencheur Tags Dépendances

\* Nom Utilisation RAM Elevé

Nom de l'événement Utilisation RAM Elevé

Données opérationnelles

Sévérité Non classé Information Avertissement Moyen Haut Désastre

\* Expression last(/SERV-AD-DC01/vm.memory.util,#30)&gt;70 Ajouter

[Constructeur d'expression](#)

Génération d'événement OK Expression Expression de récupération Aucun

Mode de génération des événements PROBLÈME Seul Multiple

Actualiser

Clone

Supprimer

Annuler

Créer un déclencheur pour une utilisation &gt; à 80% :

## Déclencheur

? X

Déclencheur Tags Dépendances

\* Nom Utilisation RAM CRITICAL

Nom de l'événement Utilisation RAM CRITICAL

Données opérationnelles

Sévérité Non classé Information Avertissement Moyen Haut Désastre

\* Expression last(/SERV-AD-DC01/vm.memory.util,#30)&gt;80 Ajouter

[Constructeur d'expression](#)

Génération d'événement OK Expression Expression de récupération Aucun

Mode de génération des événements PROBLÈME Seul Multiple

Actualiser

Clone

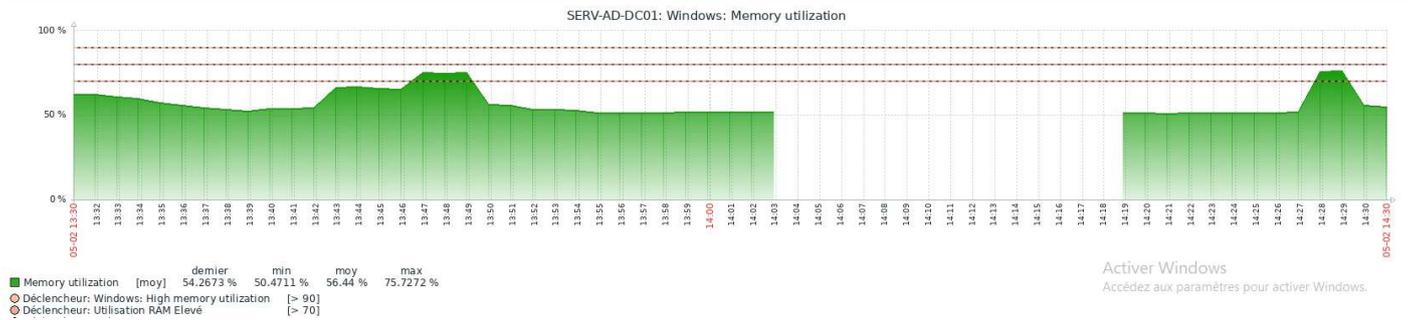
Supprimer

Annuler

Les métriques sont bien remontées :

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

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

Activer Windows  
Accédez aux paramètres pour activer Windows.

Affichage de 5 sur 5 trouvés

## DISQUE DUR

Créer un déclencheur pour une utilisation > à 70% :

**Déclencheur** ? x

Déclencheur Tags Dépendances

\* Nom

Nom de l'événement

Données opérationnelles

Sévérité  Non classé  Information  Avertissement  Moyen  Haut  Désastre

\* Expression

[Constructeur d'expression](#)

Génération d'événement OK  Expression  Expression de récupération  Aucun

Mode de génération des événements PROBLÈME  Seul  Multiple

Créer un déclencheur pour une utilisation > à 80% :

**Nouveau déclencheur** ? x

Déclencheur Tags Dépendances

\* Nom

Nom de l'événement

Données opérationnelles

Sévérité  Non classé  Information  Avertissement  Moyen  Haut  Désastre

\* Expression

[Constructeur d'expression](#)

Génération d'événement OK  Expression  Expression de récupération  Aucun

Mode de génération des événements PROBLÈME  Seul  Multiple

Les métriques sont bien remontées :

<input type="checkbox"/>	Hôte	Nom	Dernière vérification	Dernière valeur	Changer	Tags	Info
<input type="checkbox"/>	SERV-DC01-AD	0 C:: Average disk read queue length	56s	0.000135	-0.000065	component: storage; disk: 0 C:	Graphique
<input type="checkbox"/>	SERV-DC01-AD	0 C:: Average disk write queue length	55s	0.01405	+0.005795	component: storage; disk: 0 C:	Graphique
<input type="checkbox"/>	SERV-DC01-AD	0 C:: Disk average queue size (avgqu-sz)	52s	0		component: storage; disk: 0 C:	Graphique
<input type="checkbox"/>	SERV-DC01-AD	0 C:: Disk read rate	51s	0.06586 r/s	+0.0327 r/s	component: storage; disk: 0 C:	Graphique
<input type="checkbox"/>	SERV-DC01-AD	0 C:: Disk read request avg waiting time	54s	0.15ms	+0.053ms	component: storage; disk: 0 C:	Graphique
<input type="checkbox"/>	SERV-DC01-AD	0 C:: Disk utilization by idle time	57s	0.8349 %	+0.2019 %	component: storage; disk: 0 C:	Graphique
<input type="checkbox"/>	SERV-DC01-AD	0 C:: Disk write rate	50s	1.9299 w/s	+0.8042 w/s	component: storage; disk: 0 C:	Graphique
<input type="checkbox"/>	SERV-DC01-AD	0 C:: Disk write request avg waiting time	53s	2.89ms	+0.72ms	component: storage; disk: 0 C:	Graphique
<input type="checkbox"/>	SERV-DC01-AD	Free swap space	50s	920.09 MB	+8 KB	component: memory; component: storage	Graphique
<input type="checkbox"/>	SERV-DC01-AD	Free swap space in %	4s	65.347 %		component: memory; component: storage	Graphique
<input type="checkbox"/>	SERV-DC01-AD	FS [Système(C:)]: Get data	46s	{!\$name":"C:",!\$label"...		component: raw; component: storage; filesystem: C:; ...	Historique
<input type="checkbox"/>	SERV-DC01-AD	FS [Système(C:)]: Space: Available	46s	60.52 GB		component: storage; filesystem: C:; fstype: NTFS	Graphique
<input type="checkbox"/>	SERV-DC01-AD	FS [Système(C:)]: Space: Total	46s	79.33 GB		component: storage; filesystem: C:; fstype: NTFS	Graphique
<input type="checkbox"/>	SERV-DC01-AD	FS [Système(C:)]: Space: Used	46s	18.81 GB		component: storage; filesystem: C:; fstype: NTFS	Graphique
<input type="checkbox"/>	SERV-DC01-AD	FS [Système(C:)]: Space: Used, in %	46s	23.7145 %		component: storage; filesystem: C:; fstype: NTFS	Graphique
<input type="checkbox"/>	SERV-DC01-AD	Total swap space	49s	1.38 GB		component: memory; component: storage	Graphique
<input type="checkbox"/>	SERV-DC01-AD	Used swap space in %	4s	34.653 %		component: memory; component: storage	Graphique

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

<input type="checkbox"/>	Temps	Sévérité	Moment de la récupération	État	Info	Hôte	Problème
<input type="checkbox"/>	13:36:49	Haut		PROBLÈME		SERV-AD-DC01	Espace disque Dur

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

<input type="checkbox"/>	Temps	Sévérité	Moment de la récupération	État	Info	Hôte	Problème	Durée
<input type="checkbox"/>	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 :

Mots clés	Date et heure	Source	ID de l'évènement	Catégorie de la tâche
Succès de l'audit	05/02/2025 11:11:56	Microsoft Windows securit...	4648	Logon
Succès de l'audit	05/02/2025 11:11:56	Microsoft Windows securit...	4769	Kerberos Service Ticket Oper...
Succès de l'audit	05/02/2025 11:11:56	Microsoft Windows securit...	4768	Kerberos Authentication Ser...
Échec de l'audit	05/02/2025 11:11:47	Microsoft Windows securit...	4625	Logon
Succès de l'audit	05/02/2025 11:11:34	Microsoft Windows securit...	4634	Logoff
Succès de l'audit	05/02/2025 11:11:31	Microsoft Windows securit...	4634	Logoff

Créer un élément :

### Élément

Élément    Tags    Prétraitement

\* Nom

Type

\* Clé

Type d'information

\* Intervalle d'actualisation

Intervalle personnalisé

Type	Intervalle	Période	Action
Flexible	Planification	50s	1-7,00:00-24:00

[Ajouter](#) [Supprimer](#)

\* Expiration    [Délais d'attente](#)

\* Historique

Format de l'horodatage du journal

Description

Créer un déclencheur :

## Déclencheur

? X

Déclencheur Tags Dépendances

\* Nom Tentatives de connexion échouées élevées

Nom de l'événement Tentatives de connexion échouées élevées

Données opérationnelles

Sévérité Non classé Information Avertissement Moyen **Haut** Désastre

\* Expression `count(/SERV-AD-DC01/eventlog[Security,,,4625,,skip],300)>5`

Ajouter

Constructeur d'expression

Génération d'événement OK Expression Expression de récupération Aucun

Mode de génération des événements PROBLÈME Seul Multiple

Actualiser

Clone

Supprimer

Annuler

Groupes d'hôtes taper ici pour rechercher Sélectionner

Hôtes **SERV-AD-DC01** Sélectionner

taper ici pour rechercher

Nom echec de connexion

Tags ETOU Ou

tag Contient valeur Supprimer

Ajouter

Voir les tags Aucun 1 2 3 Nom de tag Tout Raccourci Aucun

Priorité d'affichage des tags liste séparée par des virgules

Échec d'ouverture de session d'un compte.

Affiche

Sujet:  
 ID de sécurité : AUTORITE NT\Système  
 Nom du compte : SERV-AD-DC01\$  
 Domaine du compte : RUCO  
 ID d'ouverture de session : 0x3E7

Type d'ouverture de session : 2

Compte pour lequel l'ouverture de session a échoué:  
 ID de sécurité : NULL SID  
 Nom du compte : Administrateur  
 Domaine du compte : RUCO

Enregistrer sous

Appl

Sous-filtre affecte uniquement les données filtrées

HÔTES

SERV-AD-DC01

DONNÉES

Avec données Sans données

<input type="checkbox"/>	Hôte	Nom	Dernière vérification	Dernière
<input type="checkbox"/>	SERV-AD-DC01	echec de connexion	39s	Échec d'ouverture de se...

Activer Windows

Historique

Accédez aux paramètres pour activer Windows.

Affichage de 1 sur 1 trouvés

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

<input type="checkbox"/>	Temps	Sévérité	Moment de la récupération	État	Info	Hôte	Problème	Durée	Actualiser	Actions	Tags
<input type="checkbox"/>	11:24:02	<b>Haut</b>		PROBLÈME		SERV-AD-DC01	Tentatives de connexion échouées élevées	3m 11s	Actualiser		

Aujourd'hui

## Création de l'élément : Authentification NTLM

Élément ? x

Élément [Tags](#) [Prétraitement](#)

\* Nom

Type

\* Clé

Type d'information

\* Intervalle d'actualisation

Intervalle personnalisé

Type	Intervalle	Période	Action
Flexible	Planification	50s	1-7,00:00-24:00

[Ajouter](#)

\* Expiration    [Délais d'attente](#)

\* Historique

Format de l'horodatage du journal

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

Déclencheur ? x

Déclencheur [Tags](#) [Dépendances](#)

\* Nom

Nom de l'événement

Données opérationnelles

Sévérité

\* Expression

[Constructeur d'expression](#)

Génération d'événement OK

Mode de génération des événements PROBLÈME

## Test effectué, voici le résultat :

Temps	Sévérité	Moment de la récupération	État	Info	Hôte	Problème	Durée	Actualiser	Actions	Tags
05/02/2025 22:00:34	Haut		PROBLÈME		SERV-AD-DC01	Activité NTLM élevée	13h 31m 14s	Actualiser		

# SUPERVISION DU SERVICE APACHE

Création de l'hôte :

Hôte ? ×

Hôte IPMI Tags Macros 1 Inventaire Chiffrement Table de correspondance

\* Nom de l'hôte

Nom visible

Modèles

Nom	Action
Apache by HTTP	<a href="#">Supprimer lien</a> <a href="#">Supprimer lien et nettoyer</a>

\* Groupes d'hôtes

Interfaces

Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent	<input type="text" value="192.168.1.3"/>	<input type="text"/>	<input checked="" type="radio"/> IP <input type="radio"/> DNS	<input type="text" value="10050"/>	<input checked="" type="radio"/> Supprimer

[Ajouter](#)

Description

Hôte ? ×

Hôte IPMI Tags Macros 1 Inventaire Chiffrement Table de correspondance

Macros d'hôte Macros héritées et de l'hôte

Macro

Macro	Valeur	Description
<input type="text" value="{\$APACHE.STATUS.HOST}"/>	<input type="text" value="192.168.1.3"/> <input type="button" value="T"/>	<input type="text" value="The hostname or IP address of the Apache status page host"/> <a href="#">Supprimer</a>

[Ajouter](#)

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
```

```
GNU nano 7.2 /etc/apache2/sites-available/000-default.conf  
<VirtualHost *:80>  
  ServerName 192.168.1.3  
  
  DocumentRoot /var/www/html/glpi/public  
  <Directory /var/www/html/glpi/public>  
    Require all granted  
    RewriteEngine On  
    # Exclusion de /server-status  
    RewriteCond %{REQUEST_URI} !~/server-status  
    RewriteCond %{REQUEST_FILENAME} !-f  
    RewriteRule ^(.*)$ index.php [QSA,L]  
  </Directory>  
  
  <Location /server-status>  
    SetHandler server-status  
    Require ip 127.0.0.1  
    Require ip 192.168.1.8  
  </Location>  
  
  ErrorLog ${APACHE_LOG_DIR}/error-glpi.log  
  CustomLog ${APACHE_LOG_DIR}/access-glpi.log combined  
</VirtualHost>
```

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.

<input type="checkbox"/>	APACHE GLPI	Bytes per second	28s	17,0666 Bps	+17,0666 Bps	component: network	Graphique
<input type="checkbox"/>	APACHE GLPI	Get status	28s	["Date": "Thu, 06 Feb 2025 10:3...		component: raw	Historique
<input type="checkbox"/>	APACHE GLPI	Requests per second	28s	0.01667	-0.0000001286	component: network	Graphique
<input type="checkbox"/>	APACHE GLPI	Service ping	2m 26s	Up (1)		component: application component: health	Graphique
<input type="checkbox"/>	APACHE GLPI	Service response time	27s	0.36ms	-0.015ms	component: application component: health	Graphique
<input type="checkbox"/>	APACHE GLPI	Total bytes	28s	60 KB	+1 KB	component: network	Graphique
<input type="checkbox"/>	APACHE GLPI	Total requests	28s	108	+1	component: network	Graphique
<input type="checkbox"/>	APACHE GLPI	Total workers busy	28s	1		component: system	Graphique
<input type="checkbox"/>	APACHE GLPI	Total workers idle	28s	5		component: system	Graphique
<input type="checkbox"/>	APACHE GLPI	Uptime	28s	01:48:04	+00:01:00	component: system	Graphique
<input type="checkbox"/>	APACHE GLPI	Version	1h 16m 26s	Apache/2.4.62 (Debian)		component: system	Historique
<input type="checkbox"/>	APACHE GLPI	Workers closing connection	28s	0		component: system	Graphique
<input type="checkbox"/>	APACHE GLPI	Workers DNS lookup	28s	0		component: system	Graphique
<input type="checkbox"/>	APACHE GLPI	Workers finishing	28s	0		component: system	Graphique
<input type="checkbox"/>	APACHE GLPI	Workers idle cleanup	28s	0		component: system	Graphique
<input type="checkbox"/>	APACHE GLPI	Workers keepalive (read)	28s	0		component: system	Graphique
<input type="checkbox"/>	APACHE GLPI	Workers logging	28s	0		component: system	Graphique
<input type="checkbox"/>	APACHE GLPI	Workers reading request	28s	0		component: system	Graphique
<input type="checkbox"/>	APACHE GLPI	Workers sending reply	28s	1		component: system	Graphique
<input type="checkbox"/>	APACHE GLPI	Workers slot with no current process	28s	144		component: system	Graphique
<input type="checkbox"/>	APACHE GLPI	Workers starting up	28s	0		component: system	Graphique

 Activer Windows  
 Accédez aux paramètres pour activer Windows.

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).