



## Architecture Système

Procédure techniques  
Supervision Zabbix de l'Active Directory sous  
Windows Server

Version : 1.0  
Date: 10/02/2025  
Page: 1/6

Document technique :

# Supervision Zabbix de l'Active Directory sous Windows Server

	<b>Architecture Système</b>	Version : 1.0 Date: 10/02/2025 Page: 2/6
	Procédure techniques Supervision Zabbix de l'Active Directory sous Windows Server	

## Gestion du Document

### Licence

Copyright © 2024 Ziad MAHDA.

Permission est accordée de copier, distribuer et/ou modifier ce document en respect des termes de la **GNU Free Documentation License**, Version 1.3 ou toute version ultérieure publiée par la Free Software Foundation ;  
avec la section "**Licence**" inaltérable, sans texte de couverture ni texte de dernière page de couverture. Une copie de cette licence est incluse dans la section intitulée "**GNU Free Documentation Licence**" ou peut être obtenue depuis l'adresse suivante : <http://www.gnu.org/copyleft/fdl.html>.

### Historique des Versions

Révisio n	Date	Objet
1.0.0	10/02/2025	Création du document

### Auteurs et Intervenants

Initiales	Nom	Fonction	Organisation - Rôle
ZM	Ziad Mahda	Intégrateur	IIA Laval - Rédaction/Auteur

### Visas

Version	Date	Rédaction	Validation	Approbation
1.0.0	10/02/2025	Ziad Mahda		
1.0.1	10/02/2025	Ziad Mahda		

	<b>Architecture Système</b>	Version : 1.0 Date: 10/02/2025 Page: 3/6
	Procédure techniques Supervision Zabbix de l'Active Directory sous Windows Server	

### Identification du document

<b>Document applicable à compter du</b>	<b>Identification du document</b>		
10/02/2025	Direction:	IIA Saint-Berthevin / BTS SIO 2eme année	
	Objet:	Configuration d'un Relais SMTP vers Office 365	
	Domaine:	Architecture technique	
	Nature:	Procédure technique	
	N° d'ordre:	0001	Version: 1.0
	Durée installation	Environ 1 heure	
	Nb pages:	8	
	Nom fichier:	documentation_installation_zabbix.docx	
	Format document:	ODT réalisé avec LibreOffice	

	<b>Architecture Système</b>	Version : 1.0 Date: 10/02/2025 Page: 4/6
	Procédure techniques Supervision Zabbix de l'Active Directory sous Windows Server	

## **Supervision Zabbix de l'Active Directory sous Windows Server :**

### **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.

### **Sommaire :**

- Éléments supervisés Ressources système
- 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

### **1. Prérequis :**

- Un serveur Zabbix opérationnel (avec le frontend et la base de données installés).
- Un serveur Active Directory sous Windows Server.
- Un accès administrateur au serveur AD.
- Une connexion réseau entre le serveur Zabbix et le serveur AD.

	<b>Architecture Système</b>	Version : 1.0 Date: 10/02/2025 Page: 5/6
	Procédure techniques Supervision Zabbix de l'Active Directory sous Windows Server	

## 1. Installation et configuration de l'Agent Zabbix sur le serveur AD:

L'agent Zabbix permet de collecter des métriques depuis le serveur Windows et de les envoyer à Zabbix Server.

### A-) Télécharger l'agent Zabbix :

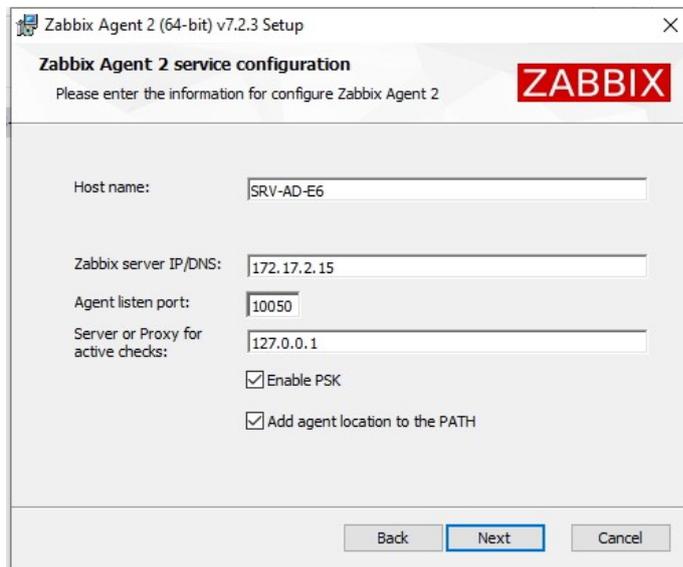
1-) Téléchargez l'agent compatible avec votre version de Windows sur :

[https://www.zabbix.com/download\\_agents](https://www.zabbix.com/download_agents)

2-) Installer l'agent sur le serveur AD avec la commande :

Installation MSI :

Procédez à l'installation et entrez votre nom d'hôte et l'adresse du serveur Zabbix, l'activation de PSK (clé pré-partagée) ne permettra pas de surveiller les données de ce serveur jusqu'à ce que l'agent obtienne une clé pré-partagée du serveur essayant de le faire, nous verrons dans ceci dans d'autres articles. Appuyez sur suivant jusqu'à ce que l'installation soit terminée.



- Puis « **Installer** »



## Architecture Système

Procédure techniques  
Supervision Zabbix de l'Active Directory sous  
Windows Server

Version : 1.0  
Date: 10/02/2025  
Page: 6/6

3-) Modifier le fichier de configuration zabbix\_agent2.conf (situé dans C:\Programmes\Zabbix Agent 2\zabbix\_agent2.conf) : Configurez les paramètres suivants :

- Server=<IP\_ZABBIX\_SERVER>
- ServerActive=<IP\_ZABBIX\_SERVER>
- Hostname=<NOM\_DU\_SERVEUR\_AD>

4-) Redémarrez l'agent pour appliquer les modifications exécuter ces commande en Powershell

```
sc stop ZabbixAgent2
```

```
sc start ZabbixAgent2
```

## 2-) Configurer la supervision des Ressources Système (CPU, RAM,Disque) :

Supervision des Ressources Système (CPU, RAM, Disque)

Zabbix offre un modèle préconfiguré pour Windows qui permet de superviser les performances système.

- Accédez à l'interface Web Zabbix.
- Allez dans Surveillance > Hôtes.
- Cliquez sur Créer un hôte et ajoutez le serveur AD avec :
- Nom d'hôte : <NOM\_DU\_SERVEUR\_AD>
- Groupe : Windows Servers
- Modelés : cliquer sur sélectionner (**Template**> puis **Windows by Zabbix agent**)
- Agent actif : Oui
- Puis Enregistrer.

Hôte

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

\* Nom de l'hôte

Nom visible

Modèles

Nom	Action
<input type="text" value="Windows by Zabbix agent"/>	<a href="#">Supprimer lien</a> <a href="#">Supprimer lien et nettoyer</a>

taper ici pour rechercher

\* Groupes d'hôtes

taper ici pour rechercher

Interfaces

Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent	<input type="text" value="172.17.2.11"/>	<input type="text"/>	<input type="radio"/> IP <input type="radio"/> DNS	<input type="text" value="10050"/>	<input checked="" type="radio"/> Supprimer

[Ajouter](#)

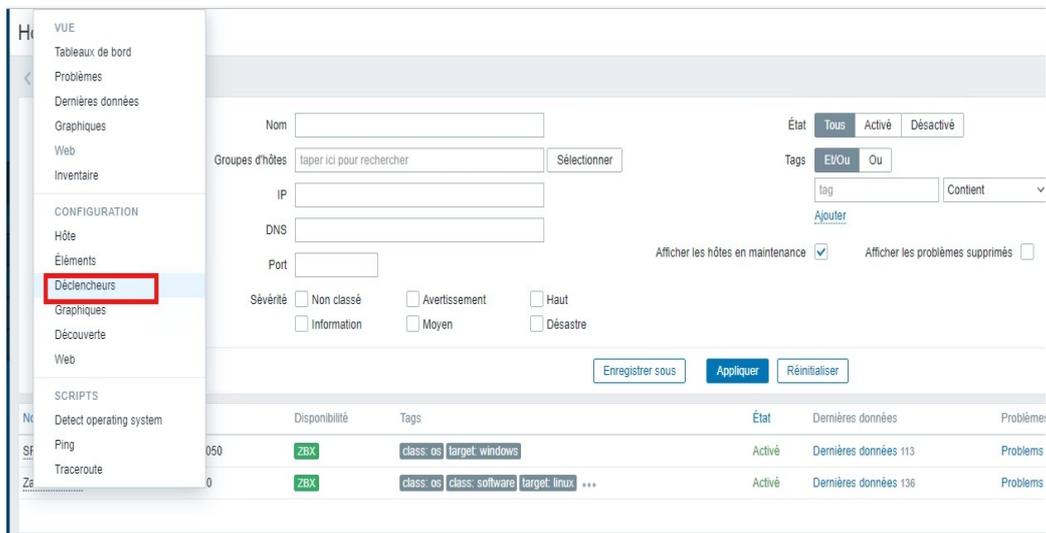
Description

### 3-) Configurer les seuils d'alerte pour (CPU, RAM et Disque) :

Après avoir appliqué le modèle, vous devez configurer des déclencheurs pour générer des alertes lorsque l'utilisation dépasse certains seuils.

a-) Ajouter un déclencheur pour le CPU

- Allez dans "**Surveillance**" > "Hôtes" > sélectionnez votre serveur AD.
- Allez dans l'onglet "Déclencheurs" et cliquez sur "Créer un déclencheur".



- Remplissez les champs comme suit :
- Nom : Utilisation CPU élevée
- Élément : CPU utilisation
- Fonction : last () - Dernière valeur T la plus récente.

**Condition** ✕

\* Élément  Sélectionner

Fonction

Dernier (T)  Compte

Décalage temporel  Temps

\* Résultat

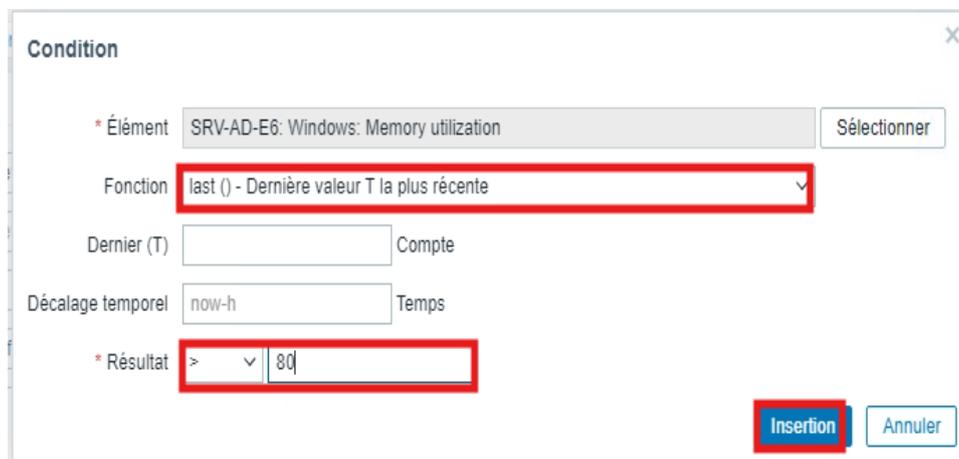
### b-) Ajouter un déclencheur pour la RAM :

Cliquez sur "Créer un déclencheur".

Remplissez les champs comme suit :

Nom : Utilisation RAM élevée

Expression :



Condition

\* Élément SRV-AD-E6: Windows: Memory utilization Sélectionner

Fonction last () - Dernière valeur T la plus récente

Dernier (T) Compte

Décalage temporel now-h Temps

\* Résultat > 80

Insertion Annuler

### c-) Ajouter un déclencheur pour l'espace disque :

- Cliquez sur "Créer un déclencheur".
- Remplissez les champs comme suit :
- Nom : Espace disque faible

## 4-) Configurer la collecte des logs AD :

L'Active Directory stocke ses logs dans l'Observateur d'événements Windows (Event Viewer).

On va configurer Zabbix pour remonter des événements importants.

Étape 1 : Identifier les logs importants

Échecs de connexion AD : Security → ID 4625

Compte verrouillé : Security → ID 4740

Changement de mot de passe : Security → ID 4723



## Architecture Système

Procédure techniques  
Supervision Zabbix de l'Active Directory sous  
Windows Server

Version : 1.0  
Date: 10/02/2025  
Page: 9/6

### a-) Allez dans Configuration > Hôtes > AD-Server > Onglet "Éléments".

Cliquez sur "Créer un nouvel élément".

- Pour **Échecs de connexion (ID 4625)** :

Nom : Échecs de connexion AD

Type : Zabbix Agent (active)

Clé : eventlog[Security,,,4625]

Type d'information : Log

Historique : 7 jours

Puis ajouter

- Pour **Compte verrouillé (ID 4740)** :

Nom : Compte verrouillé

Type : Zabbix Agent (active)

Clé : eventlog[Security,,,4740]

Type d'information : Log

- Pour **changement de mot de passe (ID 4723)** :

Nom : Changement de mot de passe

Type : Zabbix Agent (active)

Clé : eventlog[Security,,,4723]

Type d'information : Log

The screenshot shows the Zabbix configuration interface for creating a new item. The interface is in French and includes the following fields and options:

- Nom**: changement de mot de passe
- Type**: agent Zabbix
- Clé**: eventlog[Security,,,4723] (with a "Sélectionner" button)
- Type d'information**: Numérique (non signé)
- Interface hôte**: 172.17.2.11:10050
- Unités**: (empty field)
- Intervalle d'actualisation**: 1m
- Intervalle personnalisé**:

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

(with "Ajouter" and "Supprimer" buttons)
- Période de stockage de l'historique**: Ne pas conserver l'historique (Période de stockage: 90d)
- Période de stockage des tendances**: Ne pas conserver les tendances (Période de stockage: 365d)
- Table de correspondance**: taper ici pour rechercher (with "Sélectionner" button)
- Remplit le champ d'inventaire d'hôte**: -Aucun-
- Description**: (empty text area)

## 5-) Ajouter des déclencheurs pour alertes :

Étape 3 : Ajouter des déclencheurs pour alertes

Allez dans Configuration > Hôtes > AD-Server > Onglet "Déclencheurs".

Cliquez sur "Créer un déclencheur".

- **Pour Alerte pour échecs de connexion répétés :**

Nom : Trop d'échecs de connexion sur AD

Expression: last(/SRV-AD-E6/eventlog[Security,,,4625])>5

Description : Alerte si plus de 5 échecs de connexion en 5 minutes.

- **Pour alerte pour compte verrouillé :**

Nom : Compte utilisateur verrouillé

Expression : last(/SRV-AD-E6/eventlog[Security,,,4740])>0

Description Alerte dès qu'un compte est verrouillé.



# Architecture Système

## Procédure techniques Supervision Zabbix de l'Active Directory sous Windows Server

Version : 1.0  
Date: 10/02/2025  
Page: 11/6

### Déclencheurs

Tous les hôtes / SRV-AD-E6 / Actif / ZBX / Éléments 116 / Déclencheurs 83 / Graphiques 12 / Règles de découverte 4 / Scénarios web

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

Un événement OK ferme  Tous les problèmes  Tous les problèmes si les valeurs de tag correspondent

Autoriser la fermeture manuelle

Nom de l'entrée de menu

URL de l'entrée de menu

Description

- Pour alerte pour changement de mot de passe suspect

Nom : Changement de mot de passe suspect

Expression : `last(/SRV-AD-E6/eventlog[Security,,,4723])>2`

Description : Alerte si un compte change de mot de passe plusieurs fois en peu de

temps.

### Déclencheurs

Tous les hôtes / SRV-AD-E6 / Actif / ZBX / Éléments 116 / Déclencheurs 84 / Graphiques 12 / Règles de découverte 4 / Scénarios web

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

Un événement OK ferme  Tous les problèmes  Tous les problèmes si les valeurs de tag correspondent

Autoriser la fermeture manuelle

Nom de l'entrée de menu

URL de l'entrée de menu

Description

	<b>Architecture Système</b>	Version : 1.0 Date: 10/02/2025 Page: 12/6
	Procédure techniques Supervision Zabbix de l'Active Directory sous Windows Server	

## 6-) Tester la configuration :

Sur Active Directory, essayez : Connexion avec un mauvais mot de passe (Event ID 4625)

Tenter plusieurs fois pour verrouiller un compte (Event ID 4740)

Changer un mot de passe (Event ID 4723)

Dans Zabbix > Surveillance > Dernières données, vérifiez si ces événements remontent.

## 7-) Surveiller l'état du service Apache avec Zabbix :

### Étape 1 : Installer et configurer Zabbix Agent

Installez Zabbix Agent sur Debian 12 :

```
sudo apt install zabbix-agent -y
```

Éditez le fichier de configuration :

```
nano /etc/zabbix/zabbix_agentd.conf
```

Modifiez ces lignes :

```
Server=192.168.1.100 # Adresse IP du serveur Zabbix
```

```
ServerActive=192.168.1.100 # Adresse IP du serveur Zabbix
```

```
Hostname=Serveur-Apache
```

### Redémarrez Zabbix Agent :

```
sudo systemctl restart zabbix-agent
```

```
sudo systemctl enable zabbix-agent
```

### Étape 2 : Ajouter le serveur Apache dans Zabbix

Dans l'interface Web de Zabbix :

Allez dans Surveillance > Hôtes

Cliquez sur "Créer un hôte"

Nom : Serveur-Apache

Groupe : Linux Servers



## Architecture Système

Procédure techniques  
Supervision Zabbix de l'Active Directory sous  
Windows Server

Version : 1.0  
Date: 10/02/2025  
Page: 13/6

Interface Agent : IP du serveur Debian 12

Dans l'onglet Model "Templates" et ajoutez :

- Template OS Linux by Zabbix agent
- Template App Apache by Zabbix agent

Ensuite faites **"Ajouter"**.

Nouvel hôte

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

\* Nom de l'hôte

Nom visible

Modèles  Sélectionner

\* Groupes d'hôtes  Sélectionner

Interfaces

Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent	172.17.2.14		IP DNS	10050	<input checked="" type="radio"/> Supprimer

Ajouter Annuler

### Étape 3 : Ajouter un élément pour surveiller Apache

Allez dans Surveillance > Hôtes > Serveur-Apache > Éléments.

Cliquez sur **"Créer un élément"**

Nom : État du service Apache

Type : Zabbix Agent

Clé : service\_state[apache2]

Type de données : Entier (integer)

Historique : 7 jours

Cliquez sur **"Ajouter"**



## Architecture Système

### Procédure techniques Supervision Zabbix de l'Active Directory sous Windows Server

Version : 1.0  
Date: 10/02/2025  
Page: 14/6

The screenshot shows the Zabbix configuration interface for a service item. The breadcrumb trail is: Tous les hôtes / Serveur Apache / Actif / ZBX / Éléments 84 / Déclencheurs 22 / Graphiques 15 / Règles de découverte 5 / Scénarios web. The configuration fields are as follows:

- Nom: état du service apache
- Type: agent Zabbix
- Clé: service\_state[apache2] (with a 'Sélectionner' button)
- Type d'information: Numérique (non signé)
- Interface hôte: 172.17.2.14:10050
- Unités: (empty)
- Intervalle d'actualisation: 1m
- Intervalle personnalisé: A table with columns Type, Intervalle, Période, and Action. It contains one row: Flexible, Planification, 50s, 1-7,00:00-24:00, and Supprimer. There is an 'Ajouter' link below.
- Période de stockage de l'historique: Ne pas conserver l'historique (selected), Période de stockage: 90d
- Période de stockage des tendances: Ne pas conserver les tendances (selected), Période de stockage: 365d
- Table de correspondance: taper ici pour rechercher (with a 'Sélectionner' button)
- Remplit le champ d'inventaire d'hôte: -Aucun-
- Description: (empty)

#### Étape 4 : Ajouter un déclencheur pour alerte en cas de panne

Allez dans Surveillance > Hôtes > Serveur-Apache > Déclencheurs.

Cliquez sur "Créer un déclencheur"

Nom : Apache down !

Expression : last(/Serveur

Apache/web.page.get["{\$APACHE.STATUS.SCHEME}://{ \$APACHE.STATUS.HOST }:{ \$APACHE.STATUS.PORT }/{ \$APACHE.STATUS.PATH }"]<>0

Gravité : Haut

Cliquez sur "**Ajouter**".

Suivi des requêtes échouées (GET / POST)

Nous allons configurer Zabbix pour surveiller les erreurs Apache (404, 500, etc.).

Étape 1 : Modifier la configuration des logs Apache

Éditez le fichier de configuration :



## Architecture Système

### Procédure techniques Supervision Zabbix de l'Active Directory sous Windows Server

Version : 1.0  
Date: 10/02/2025  
Page: 15/6

The screenshot shows the Zabbix configuration interface for a trigger named "Apache down". The trigger is configured with the following settings:

- Nom:** Apache down
- Nom de l'événement:** Apache down
- Données opérationnelles:** (empty)
- Sévérité:** Non classé, Information, **Avertissement**, Moyen, Haut, Désastre
- Expression:** `last(/Serveur: Apache/web.page.get[{"{APACHE.STATUS.SCHEME}://{APACHE.STATUS.HOST}":{"{APACHE.STATUS.PORT} / {APACHE.STATUS.PATH} *"}]) <> 0`
- Génération d'événement OK:** Expression, Expression de récupération, Aucun
- Mode de génération des événements PROBLÈME:** Seul, Multiple
- Un événement OK ferme:** Tous les problèmes, Tous les problèmes si les valeurs de tag correspondent
- Autoriser la fermeture manuelle:**
- Nom de l'entrée de menu:** URL du déclencheur
- URL de l'entrée de menu:** (empty)
- Description:** (empty)

## 7-) Suivi des requêtes échouées (GET / POST :

Nous allons configurer Zabbix pour surveiller les erreurs Apache (404, 500, etc.).

### Étape 1 : Modifier la configuration des logs Apache

Éditez le fichier de configuration :

```
sudo nano /etc/apache2/apache2.conf
```

Activez le logging des erreurs :

**LogLevel warn (ajouter la ligne suivant) :**

```
ErrorLog ${APACHE_LOG_DIR}/error.log
```

```
LogLevel warn
ErrorLog ${APACHE_LOG_DIR}/error.log
# Include module configuration:
```

Redémarrez Apache :

```
systemctl restart apache2
```

### Étape 2 : Configurer Zabbix Agent pour lire les logs Apache

Ajoutez cette ligne dans /etc/zabbix/zabbix\_agentd.conf :

```
LogFile=/var/log/apache2/error.log
```



## Architecture Système

Procédure techniques  
Supervision Zabbix de l'Active Directory sous  
Windows Server

Version : 1.0  
Date: 10/02/2025  
Page: 16/6

**Étape 3 :** Ensuite allez dans Surveillance > Hôtes > Serveur-Apache > Éléments.

Cliquez sur "Créer un élément"

Nom : Erreurs Apache (404, 500, etc.)

Type : Zabbix Agent (active)

Clé : log[/var/log/apache2/error.log]

Cliquez sur "Ajouter" .

Éléments

Tous les hôtes / Serveur Apache Actif ZBX Éléments 99 Déclencheurs 33 Graphiques 19 Règles de découverte 5 Scénarios web

Élément Tags Prétraitement

\* Nom erreur apache (404, 500, ...)

Type agent Zabbix

\* Clé log[/var/log/apache2/error.log] Sélectionner

Type d'information Numérique (non signé)

\* Interface hôte 172.17.2.14:10050

Unités

\* Intervalle d'actualisation 1m

Intervalle personnalisé

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

Ajouter

\* Période de stockage de l'historique Ne pas conserver l'historique Période de stockage 90d

\* Période de stockage des tendances Ne pas conserver les tendances Période de stockage 365d

Table de correspondance taper ici pour rechercher Sélectionner

Remplit le champ d'inventaire d'hôte -Aucun-

Description

**Étape 4 :** Ajouter un déclencheur pour alerte en cas d'erreurs Apache

Allez dans Surveillance > Hôtes > Serveur-Apache > Déclencheurs.

Cliquez sur "Créer un déclencheur"

Nom : Erreurs Apache détectées

Expression : last(/Serveur Apache/log[/var/log/apache2/error.log])>5

Cliquez sur "Ajouter".



## Architecture Système

Procédure techniques  
Supervision Zabbix de l'Active Directory sous  
Windows Server

Version : 1.0  
Date: 10/02/2025  
Page: 17/6

Déclencheurs

Tous les hôtes / Serveur Apache Activé ZBX Éléments 100 Déclencheurs 33 Graphiques 19 Règles de découverte 5 Scénarios web

Déclencheur Tags Dépendances

\* Nom erreur apache détectée

Nom de l'événement erreur apache détectée

Données opérationnelles

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

\* Expression `last(/Serveur Apache/log[/var/log/apache2/error.log])>5` Ajouter

Constructeur d'expression

Génération d'événement OK Expression Expression de récupération Aucun

Mode de génération des événements PROBLÈME Seul Multiple

Un événement OK ferme Tous les problèmes Tous les problèmes si les valeurs de tag correspondent

Autoriser la fermeture manuelle

Nom de l'entrée de menu URL du déclencheur

URL de l'entrée de menu

Description

## 8-) Tester la remontée d'information d'Apache :

### 1. Vérifier si l'agent envoie des données à Zabbix :

Sur le serveur Zabbix, allez dans Monitoring > Latest Data et sélectionnez Serveur-Apache.

Cherchez l'élément `service_state[apache2]`.

Si vous voyez des valeurs mises à jour, Zabbix reçoit bien les données.

### 2. Simuler une panne d'Apache :

Arrêtez Apache pour voir si Zabbix détecte la panne :



## Architecture Système

### Procédure techniques Supervision Zabbix de l'Active Directory sous Windows Server

Version : 1.0  
Date: 10/02/2025  
Page: 18/6

<input type="checkbox"/>	Serveur Apache	Apache: Bytes per second	3m 55s	17.2891 Bps	+0.4631 Bps	component: network	Graphique
<input type="checkbox"/>	Serveur Apache	Apache: Get processes summary				component: raw	
<input type="checkbox"/>	Serveur Apache	Apache: Get status	3m 55s	("Date": "Thu, 06 Feb 202...		component: raw	Historique
<input type="checkbox"/>	Serveur Apache	Apache: Requests per second	3m 55s	0.01888	+0.0004522	component: network	Graphique
<input type="checkbox"/>	Serveur Apache	Apache: Service ping	2m 54s	Down (0)	-1	component: application component: health	Graphique
<input type="checkbox"/>	Serveur Apache	Apache: Service response time	53s	0		component: application component: health	Graphique
<input type="checkbox"/>	Serveur Apache	Apache: Total bytes	3m 55s	34 KB	+1 KB	component: network	Graphique
<input type="checkbox"/>	Serveur Apache	Apache: Total requests	3m 55s	48	+1	component: network	Graphique
<input type="checkbox"/>	Serveur Apache	Apache: Total workers busy	3m 55s	1		component: system	Graphique
<input type="checkbox"/>	Serveur Apache	Apache: Total workers idle	3m 55s	4		component: system	Graphique
<input type="checkbox"/>	Serveur Apache	Apache: Uptime	3m 55s	00:48:45	+00:00:59	component: system	Graphique
<input type="checkbox"/>	Serveur Apache	Apache: Version	1h 32m 55s	Apache/2.4.62 (Debian)		component: system	Historique
<input type="checkbox"/>	Serveur Apache	Apache: Workers closing connection	3m 55s	0		component: system	Graphique
<input type="checkbox"/>	Serveur Apache	Apache: Workers DNS lookup	3m 55s	0		component: system	Graphique
<input type="checkbox"/>	Serveur Apache	Apache: Workers finishing	3m 55s	0		component: system	Graphique

Activer Windows  
Accédez aux paramètres pour activer Windows

### 3. Tester la surveillance des logs Apache :

#### 1. Générer une erreur 404 pour tester les logs

Accédez à une page inexistante : <http://172.17.2.14/page-introuvable>

<input type="checkbox"/>	Serveur Apache	erreur apache (404, 500, ...)					Graphique
<input type="checkbox"/>	Serveur Apache	FS [/boot]: Get data	30s	("fname": "/boot", "bytes": ...		component: raw component: storage filesystem: /boot	Historique
<input type="checkbox"/>	Serveur Apache	FS [/boot]: Inodes: Free: In %	30s	99.7107 %		component: storage filesystem: /boot fstype: ext4	Graphique

Cela fonctionne bien Zabbix nous alerte bien que la page est inexistante.