# **RAPPORT TECHNIQUE**

Supervision Zabbix de l'Active Directory

Rudy COLOMBEL Vanthary SOK

Février 2025

Rudy & Vanthary	Supervision Zobbiy de l'Active Directory	Réf:	Zabbix
	Supervision Zabbix de l'Active Directory	Version :	1.0
	Rapport technique - Supervision	Date :	05/02/2025
		Page :	Page <b>1</b> sur <b>25</b>

# **TABLE DES MATIÈRES**

Contexte2
Objectif2
Éléments supervisés2
Ressources système2
Événements et logs2
Supervision d'Apache (installé sur l'Active Directory)2
Prérequis3
Supervision des ressources système3
Supervision d'Apache
Installation de Zabbix 7.0 LTS sur Debian125
Installation de l'agent Zabbix sur l'AD9
Supervision des ressources système de l'AD13
CPU
RAM16
Disque Dur18
Supervision des évènements et logs
Supervision d'Apache

Supervision Zabbix de l'Active Directory Version : 1.0	
Date: 05/02/20	25
Page : Page 2 st	r <b>25</b>

# 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.

# **O**BJECTIF

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

Rudy & Vanthary	Supervision Zobbiy de l'Active Directory	Réf :	Zabbix
	Supervision Zabbix de l'Active Directory	Version :	1.0
	Rapport technique - Supervision	Date :	05/02/2025
		Page:	Page <b>4</b> sur <b>25</b>

- 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) Rapport technique - Supervision

# 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	L-uroot-p
passwor	nd
mysql>	<pre>create database zabbix character set utf8mb4 collate utf8mb4_bin;</pre>
mysql>	<pre>create user zabbix@localhost identified by 'password';</pre>
mysql>	grant all privileges on zabbix.* to zabbix@localhost;
mysql>	<pre>set global log_bin_trust_function_creators = 1;</pre>
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-characterset=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.

Rudy & Vanthary	Supervision Zabbiy de l'Active Divectory	Réf :	Zabbix
	Supervision Zabbix de l'Active Directory	Version :	1.0
	Rapport technique - Supervision	Date :	05/02/2025
		Page :	Page <b>6</b> sur <b>25</b>

Désactiver l'option log\_bin\_trust\_function\_creators après l'importation du schéma de base de données :



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 :

ZABBIX	
Dervenue	
Vérification des prérequis	
Configurer la connexion à la base de données	Bienvenue dans
Paramètres.	
Récurné prè-installation	Zobbiy Z ()
Installer	
	Langage par défaut Français (Ir_FR) 🗸
	Refour Procheine étapa

Rudy & Vanthary	Supervision Zabbix de l'Active Directory	Réf : Version :	Zabbix 1.0
	Rapport technique - Supervision	Date :	05/02/2025
		Page:	

### Une fois que la configuration est terminée :

ZABBIX	Installer
Bienvenue Vérification des prérequis Configurer la connexion à la base de données Paramètres Résumé pré-installation Installer	Félicitations ! Vous avez installé l'interface Zabbix avec succès. Fichier de configuration "confizabbix.conf.php" créé.

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

	ZADDIA	
Usernam	e	
Password	d	
🖌 Reme	mber me for 30 days	
	Sign in	
	or sign in as guest	

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

Rudy & Vanthary	Supervision Zabbix de l'Active Directory	Réf : Version :	Zabbix 1.0
	Rapport technique - Supervision	Date :	05/02/2025
		Page :	Page <b>8</b> sur <b>25</b>

#### Voici l'écran d'accueil :



<b>D</b>	<b>•</b> •		
Rud	٧۵V	vant	harv
	, ~		

Réf: Zabbix Version: 1.0 Date: 05/02/2025 Page: Page 9 sur 25

# 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 : <u>https://www.zabbix.com/download\_agents</u>

MCI		
OpenSSI		
Dynamic		
sha256:	24aedbcb3601f6ca97a32bde779ba5866f9e37974c244ab81fbcdb654b2ec7f4	
sha1:	0dad158df587450015882880d6ecbb2d4d375afa	
md5:	70dff39c06311bb92a4437a146281d2b	
	MSI OpenSSL Dynamic sha256: sha1: md5:	MSI OpenSSL Dynamic sha256: 24aedbcb3601f6ca97a32bde779ba5866f9e37974c244ab81fbcdb654b2ec7f4 sha1: 0dad158df587450015882880d6ecbb2d4d375afa md5: 70dff39c06311bb92a4437a146281d2b

#### Suivre l'assistant d'installation :

Fichier ouvert - Avertissement de sécurité						
Voulez-	vous exécute	r ce fichier ?				
Nom:loads\zabbix agent-7.2.3-windows-amd64-openssl.msi						
<u></u>	Éditeur: Zabbix SIA					
	Type : Package Windows Installer					
	De : C:\Users\adminlocal\Downloads\zabbix_agent-7.2.3-w					
Exécuter Annuler						
Les fichiers téléchargés depuis Internet peuvent être utiles, mais ce type de fichier présente un danger potentiel. N'exécutez que les logiciels des éditeurs approuvés par vous. <u>Quels sont les risques ?</u>						

	Suponyinian Zahhiy da UAatiya Directory	Réf :	Zabbix
Pudy & Vanthany	Supervision Zabbix de l'Active Directory	Version :	1.0
Ruuy & vanimary	Pannort technique - Supervision	Date :	05/02/2025
	Kappon technique - Supervision	Page :	Page <b>10</b> sur <b>25</b>
🔁 Zabbix Agent (64-bit)	Setup — X		
E	Welcome to the Zabbix Agent (64-bit) Setup Wizard		
-	Jocup milard		
ZABBIX	The Setup Wizard will install Zabbix Agent (64-bit) on your computer. Click Next to continue or Cancel to exit the Setup Wizard.		
The Enterprise class	Wizdi G.		
Monitoring Solution			
for Everyone			
www.zabbix.com			
	Rade Naut Concel		
	Dack Next Cancer		
Zabbix Agent (64-bit)	Setup — 🗆 🗙		
Fred House Linear A			
End-User License Ag			
Please read the follow	ing license agreement carefully		
GNU	J AFFERO GENERAL PUBLIC LICENSE		
	Version 3, 19 November 2007		
Copyright (C) 2007 Fre	ee Software Foundation, Inc. https://fsf.org/		
Everyone is permitted t	to copy and distribute verbatim copies of this license document, but		
changing it is not allow	ed.		
Proomblo			
; i accept the terms in	n me License Agreement		
3	Print Back Next Cancel		

	Supervision 7	Zabbix de l'Active	Directory	Réf : Version :	Zabbix 1.0
Rudy & Vanthary				Date :	05/02/2025
	карро	ort tecnnique - Supervisi	on	Page :	Page <b>11</b> sur <b>25</b>
7-bbis Asset (64 bis) (	• • • • • •				
Zabbix Agent (64-bit) 3	etup				
Custom Setup		7/	BRIX		
Select the way you war	it features to be installed.				
Click the icons in the tre	e below to change the way	features will be installed.	-		
	ie beloit to enonge the noy				
Zabbix	Agent (64-bit)	Zabbix Agent is deploye	d on		
	Agent daemon	monitoring targets to ac monitor local resources	tively		
	Zabbix get	applications and report	the		
		This feature requires 1K	B on your		
		hard drive. It has 3 of 3 subfeatures selected. T	he		
		subfeatures require 891 hard drive.	7KB on your		
Location: C:\Pr	ogram Files\Zabbix Agent\	C	Browse		
Reset	Disk Usage	Back Next	Cancel		
7.11. 4	7220.1				
Zabbix Agent (64-bit) \	17.2.3 Setup		×		
Zabbix Agent service	configuration	7/	BRIX		
Please enter the inform	ation for configure Zabbix A	gent			
Host name:					
nost name:	JDESKTOP-VRH9ATE				
Zabbix server IP/DN	S:				

	Agent listen port:	10050
ł	Server or Proxy for active checks:	127.0.0.1
v v		Enable PSK
		Add agent location to the PATH
-		Back Next Cancel

×

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

Rudy & Vanthary	Supervision Zabbiy de l'Active Directory	Réf:	Zabbix
	Supervision Zabbix de l'Active Directory	Version :	1.0
	Rapport technique - Supervision	Date :	05/02/2025
		Page :	Page <b>12</b> sur <b>25</b>

Zabbix Agent (64-bit) Setup	c = c		$\times$
ZABBIX The Enterprise-class Monitoring Solution for Everyone	Completed the Zabbix Agent (64 Setup Wizard	-bit)	
www.zabbix.com			
	Back Finish	Cancel	
_			
Zabbix Agent (64-bit) Setup	-		×
Ready to install Zabbix A	gent (64-bit)	BBI.	X
-			
Click Install to begin the insta installation settings. Click Car	llation. Click Back to review or change any of your neel to exit the wizard.		
Click Install to begin the insta installation settings. Click Car	llation. Click Back to review or change any of your ncel to exit the wizard.		

Rudy & Vanthary	Supervision Zabbiy de l'Active Directory	Réf:	Zabbix
	Supervision Zabbix de l'Active Directory	Version :	1.0
	Rapport technique - Supervision	Date :	05/02/2025
		Page :	Page <b>13</b> sur <b>25</b>

		Х
Zabbix Agent (64	-bit)	
to exit the Setup Wizard.		
Finish	Cance	
	Zabbix Agent (64 to exit the Setup Wizard.	Zabbix Agent (64-bit) to exit the Setup Wizard.

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

Services					– 🗆 ×
Fichier Action Af	ffichage ?				
🗢 🄿 🔲 🗔 🖸	ì 📑 🛛 📷 🕨 🔲 II 🕪				
Services (local)	Services (local)				
	Zabbix Agent	Nom	Description	État	Type de démarrage
	Arrêter le service <u>Redémarrer</u> le service Description : Provides system monitoring	Système d'événement COM+ Système de fichiers EFS (En Elécopie Eléphonie Teléphonie Temps Windows	Prend en ch Fournit la te Vous perme Prend en ch Conserve la	En co	Automatique Manuel (Déclenche Manuel Manuel Manuel (Déclenche
	· · · · · · · · · · · · · · · · · · ·	Q: Thèmes Vérificateur de points Ville VMware Alias Manager and VMware Snapshot Provider	Fournit un s Vérifie les e Alias Mana VMware Sn	En co En co	Automatique Manuel (Déclenche Automatique Manuel
		Whware SVGA Helper Service Whware Tools WalletService Warp JIT Service WebClient Windows Connect Now - R Windows Installer Windows Search	Helps VMw Fournit un s Objets d'hô Enables JIT Permet à un WCNCSVC Ajoute, mo Fournit des	En co En co	Automatique Automatique Manuel Manuel (Déclenche Manuel (Déclenche Manuel Manuel Désactivé
	Étendu / Standard /	Windows Update Xbox Accessory Manageme Zabbix Agent	Active la dé This service Provides sys	En co	Manuel (Déclenche Manuel (Déclenche Automatique (débu

#### Rapport technique - Supervision

# 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 Utilisation CPU élevée	
Nom de l'événement Utilisation CPU élevée	
Données opérationnelles	
Sévérité Non classé Information Avertissement Moyen Haut Désastre	
* Expression last(/SERV-AD-DC01/system.cpu.util)>=70 Ajouter	
Constructeur d'expression	
Génération d'événement OK Expression Expression de récupération Aucun	
Mode de génération des événements PROBLÈME Seul Multiple	
Actualiser Cl	one Supprimer Annuler

Rudy & Vanthary	Supervision Zabbix de l'Active Directory	Réf :	Zabbix
			1.0
	Rapport technique - Supervision	Date :	05/02/2025
		Page :	Page <b>15</b> sur <b>25</b>

### Créer un déclencheur pour une utilisation > à 80% :

Déclencheur									? X
Déclencheur Tags Dépendances									
* Nom	Utilisation CPU CRITICAL								
Nom de l'événement	Utilisation CPU CRITICAL								
Données opérationnelles									
Sévérité	Non classé Informati	on Avertissement	Moyen	Haut	Désastre				
* Expression	last(/SERV-AD-DC01/s	ystem.cpu.util)>80	)			Ajouter			
	Constructeur d'expression				Å				
Génération d'événement OK	Expression Expressi	on de récupération	Aucun						
Mode de génération des événements PROBLÈME	Seul Multiple								
					Actu	aliser	Clone	Supprimer	Annuler

#### Les métriques sont bien remontées :

Hôte	Nom 🔺	Demière vérification	Derniêre valeur	Changer	Tags	Info
SERV-DC01-AD	Context switches per second 🔎	29s	322.6057	-22.2554	component: cpu	Graphique
SERV-DC01-AD	CPU DPC time M	33s	0 %		component: cpu	Graphique
SERV-DC01-AD	CPU interrupt time 🔎	32s	0 %		component: cpu	Graphique
SERV-DC01-AD	CPU privileged time 🔎	31s	0 %		component: cpu	Graphique
SERV-DC01-AD	CPU queue length 🔎	28s	0		component: cpu	Graphique
SERV-DC01-AD	CPU user time 🗾	30s	0 %		component: cpu	Graphique
SERV-DC01-AD	CPU utilization	25s	1.296 %	-0.2904 %	component: cpu	Graphique
SERV-DC01-AD	Number of cores 🔽	12s	2		component: cpu	Graphique
						the second se

0 sélectionné Afficher le graphique empilé Afficher le graphique Exécuter maintenan



#### Stress test effectué, voici le résultat :

	Temps 🔻	Sévérité	Moment de la récupération	État	Info	Hôte	Problème	Durée	Actualiser	Actions	Tags
	12:08:40	Désastre		PROBLÈME		SERV-AD-DC01	Utilisation CPU CRITICAL	51s	Actualiser		class: os component: cpu target windows
	12:08:40	Haut		PROBLÈME		SERV-AD-DC01	Utilisation CPU élevée	51s	Actualiser		class: os component: cpu target: windows
	12:00 c										
	11:42:02	Haut		PROBLÊME		SERV-AD-DC01	Tentatives de connexion échouées élevées	27m 29s	Actualiser		
	Aujourd'hui c										
04/0	2/2025 14:09:10	Information		PROBLÈME		SERV-AD-DC01	1 Windows: System name has changed (new name: SERV-AD-DC01) 🕅	22h 21s	Actualiser		class: os component system scope: notice
	and the second									Act	Affichage de 4 sur 4 trouvés édez aux paramètres pour activer Windows.

Rudy & Vanthary	Supervision Zabbix de l'Active Directory	Réf:	Zabbix
	Supervision Zabbix de l'Active Directory	Version :	1.0
	Bannart taghniqua Supervision	Date :	05/02/2025
	Rapport technique - Supervision	Page :	Page <b>16</b> sur <b>25</b>

? ×

### RAM

# Créer un déclencheur pour une utilisation > à 70% :

#### Déclencheur

Déclencheur Tags Dépendances											
* Nom	Utilisation RAM Ele	illisation RAM Elevé									
Nom de l'événement	Utilisation RAM Ele	evé									
Données opérationnelles											
Sévérité	Non classé In	formation	Avertissement	Moyen	Haut	Désastre	]				
* Expression	* Expression last(/SERV-AD-DC01/vm.memory.util,#30)>70										
	Constructeur d'expre	ession				,h					
Génération d'événement OK	Expression E	xpression de r	récupération A	ucun							
Mode de génération des événements PROBLÈME	Seul Multiple										
						Actu	aliser	Clone	Supprimer	Ann	uler

### Créer un déclencheur pour une utilisation > à 80% :

Déclencheur		? ×
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)>80 Ajouter	
	Constructeur d'expression	
Génération d'événement OK	Expression de récupération Aucun	
Mode de génération des événements PROBLÈME	Seul Multiple	
	Actualiser Clone Supprimer	Annuler

Rudy & Vanthary	Supervision Zabbiy de l'Active Directory	Réf:	Zabbix
	Supervision Zabbix de l'Active Directory	Version :	1.0
	Depart technique Supervision	Date :	05/02/2025
	Rappon technique - Supervision	Page :	Page <b>17</b> sur <b>25</b>

#### Les métriques sont bien remontées :

Hôte	Nom 🛦	Dernière vérification	Demière 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 🔎	148	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 阔	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 :

-			61.7	1.20	V PACE			1000	1000	-
Temps 🔻	Severite	Moment de la recuperation	Etat	Info	Hote	Probleme	Duree	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 <b>c</b>	<b>,</b>									
11:42:02	Haut		PROBLÈME		SERV-AD-DC01	Tentatives de connexion échouées élevées	2h 52m	Actualiser		
11:00	<b>,</b>									
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 ····
										Activer Windows Affichage de 5 sur 5 trouvés
) sélectionné	Modification collect	tive								Accédez aux paramètres pour activer Windows.

Rudy & Vanthary	Supervision Zabbix de l'Active Directory	Réf:	Zabbix
	Supervision Zabbix de l'Active Directory	Version :	1.0
	Pennert technique Supervision	Date :	05/02/2025
	Rapport technique - Supervision	Page :	Page <b>18</b> sur <b>25</b>

# **DISQUE DUR**

### Créer un déclencheur pour une utilisation > à 70% :

Déclencheur	?	×
Déclencheur Tags Dépendances		
* Nom	Espace disque Dur	
Nom de l'événement	Espace disque Dur	
Données opérationnelles		
Sévérité	Non classé Information Avertissement Moyen Haut Désastre	
* Expression	last(/SERV-AD-DC01/vfs.fs.dependent.size[C:,pused])>70 Ajouter	
	Constructeur d'expression	
Génération d'événement OK	Expression de récupération Aucun	
Mode de génération des événements PROBLÈME	Seul Multiple	
	Actualiser Clone Supprimer Annul	ər

# Créer un déclencheur pour une utilisation > à 80% :

Nouveau déclencheur		? ×
Déclencheur Tags Dépendances		
* Nor	Utilisation disque dur critique	
Nom de l'événemer	t Utilisation disque dur critique	
Données opérationnelle	3	
Sévérit	Non classé Information Avertissement Moyen Haut Désastre	
* Expression	last(/SERV-AD-DC01/vfs.fs.dependent.size[C:,pused])>80 Ajouter	
	Constructeur d'expression	
Génération d'événement Ol	Expression de récupération Aucun	
Mode de génération des événements PROBLÈM	Seul Multiple	
	Ajouter	Annuler

Rudy & Vanthary	Supervision Zabbix de l'Active Directory	Réf : Version :	Zabbix 1.0
	Pennert technique Supervision	Date :	05/02/2025
	Kappon technique - Supervision	Page :	Page <b>19</b> sur <b>25</b>

### Les métriques sont bien remontées :

Hôte	Nom 🔺	Dernière vérification	Demière 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: stype: 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 liver Windows	Graphique
					Accedez aux paramètres pour activ Affichag	er windows. je 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
A 1 10 1						

# 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

Rudy & Vanthary
-----------------

? X

#### Rapport technique - Supervision

# **SUPERVISION DES EVENEMENTS ET LOGS**

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

Sécurité Nombre d'événements : 45 378								
Mots clés	Date et heure	Source	ID de l'événement	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	echec de connexion						
Туре	agent Zabbix (actif)	~					
* Clé	eventlog[Security,,,,4625,,sk	ip]		Sélectionner			
Type d'information	Journal	·					
* Intervalle d'actualisation	30s						
Intervalle personnalisé	Туре	Intervalle	Période	Action			
	Flexible Planification	50s	1-7,00:00-24:00	Supprimer			
	Ajouter						
* Expiration	Global Surcharge 3s	Délais d'attente					
* Historique	Ne pas stocker Stockez	z jusqu'à 31d					
Format de l'horodatage du journal							
Description							
	Actualiser	Clone Exécuter ma	aintenant Test Ef	facer l'historiqu	e et les tendances	Supprimer	Annuler

Rudy & Vanthary	Supervision Zabbix de l'Active Directory	Réf:	Zabbix
	Supervision Zabbix de l'Active Directory	Version :	1.0
	Dennert te chairme. Currenticien	Date :	05/02/2025
	Rapport technique - Supervision	Page :	Page <b>21</b> sur <b>25</b>

#### Créer un déclencheur :

Déclencheur												? >
Déclencheur Tag	is Dépend	ances										
		* Nom	Tentatives de o	connexion écho	uées élevée	s			]			
	Non	n de l'événement	Tentatives de o	connexion écho	uées élevée	)S						
	Données	opérationnelles										
		Sévérité	Non classé	Information	Avertisse	ment Moyer	n Haut	Désastre	]			
		* Expression	count (/SERV	-AD-DC01/eve	ntlog[Sec	urity,,,,462	5,,skip],	300)>5	Ajoute	r		
			Constructeur d'	expression				3	<u>a</u> ]			
	Génération	d'événement OK	Expression	Expression d	le récupérat	ion Aucun	1					
Mode de génération	des événeme	ents PROBLÈME	Seul Multi	iple								
								Art	tolioor	Clone	Cupptimer	Annular
								Act	Janser	Cione	Supplimen	Annuler
	Groupes d'hôtes	taper ici pour rechercher		Sélectionner		Tags Et/Ou	Ou					
	Hôtes	SERV-AD-DC01 × taper ici pour rechercher		Sélectionner		tag Ajouter		Contient	<ul> <li>✓ valeur</li> </ul>	Su	pprimer	
	Nom	echec de connexion			3	Voir les tags Aucun	1 2 3	Nom de tag Tout	Raccourci	Aucun		
					Priorité d'afficha	ge des tags liste sépa	arée par des virgule	BS				
					Affiche	Échec d'ouverture de	session d'un comp	pte.				
				Enregistrer	sous Appl	Sujet : ID de sécurité : Nom du compte :	AUTORITE NT SERV-AD	∩Système -DC01\$				
ous-filtre affecte uniquement le	s données filtrées					Domaine du com ID d'ouverture de	pte : RUC session : (	O Dx3E7				
ERV-AD-DC01 1						Type d'ouverture de se	ession: 2	2				
ONNÉES vec données Sans données						Compte pour lequel l' ID de sécurité : Nom du compte :	ouverture de sessi NULL SID Administr	on a échoué : ateur				
Hôte	Nom 🔺			Dernière vérificati	on Derniè	Domaine du com	pte : RUC	0				
SERV-AD-DC01	echec de connexior	1		39s	Échec	d'ouverture de se				Activer Wi Accédez aux	ndows paramètres pour act	Historique Iver Windows.

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

Temps 🔻	Sévérité	Moment de la récupération	État	info Hôte	Problème	Durée	Actualiser Actions Tags
11:24:02	Haut		PROBLÈME	SERV-AD-DC0	Tentatives de connexion échouées élevées	3m 11s	Actualiser
Aujourd'hui o							

Rudy & Vanthary	Supervision Zobbiy de l'Active Directory	Réf:	Zabbix
	Supervision Zabbix de l'Active Directory	Version :	1.0
	Dennert technique Supervision	Date :	05/02/2025
	Rapport technique - Supervision	Page:	Page <b>22</b> sur <b>25</b>

#### Création de l'élément : Authentification NTLM

Élément				? ×
Élément Tags Prétraitement				
* Nom	Authentification NTLM			
Туре	agent Zabbix (actif)			
* Clé	eventlog[Security,,4776,,skip]		Sélectionner	
Type d'information	Journal			
* Intervalle d'actualisation	30s			
Intervalle personnalisé	Type Intervalle	Période	Action	
	Flexible Planification 50s	1-7,00:00-24:00	Supprimer	
	Ajouter			
* Expiration	Global Surcharge 3s Délais d'attente			
* Historique	Ne pas stocker Stockez jusqu'à 5d			
Format de l'horodatage du journal				
	Actualiser Clone Exécuter mainte	nant Test Effa	acer l'historique et les tendance	s Supprimer Annuler

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

Déclencheur					? ×
Déclencheur Tags Dépendances					
* Nom	Activité NTLM élevée				
Nom de l'événement	Activité NTLM élevée				
Données opérationnelles					
Sévérité	Non classé Information	Avertissement Moyen	Haut Désastre	]	
* Expression	count (/SERV-AD-DC01/ever	ntlog[Security,,,,4776,	,skip],300)>5	Ajouter	
	Constructeur d'expression		Å		
Génération d'événement OK	Expression Expression de	e récupération Aucun			
Mode de génération des événements PROBLÈME	Seul Multiple				
			Actu	aliser Clone	Supprimer Annuler
Test effectué, voici le résultat :					
,					
Temps - Sévérité Moment de la récupération État	Info Hôte Problème		Durée Actualise	er Actions Tags	
05/02/2025 22:00:34 Haut PROBLÈ	ACTIVITÉ NTLM élevé	ée	13h 31m 14s Actualise	er	

Rudy & Vanthary	Supervision Zobbix de l'Active Directory	Réf:	Zabbix
	Supervision Zabbix de l'Active Directory	Version :	1.0
	Deprest technique Supervision	Date :	05/02/2025
	Rapport technique - Supervision	Page :	Page <b>23</b> sur <b>25</b>

# **SUPERVISION DU SERVICE APACHE**

#### Création de l'hôte :

Hôte								? ×
Hôte IPMI Tag	gs Macros 1 Inventaire	Chiffrement Table de co	rrespondance					
* Nom de l'hôte	APACHE GLPI							
Nom visible	APACHE GLPI							
Modèles	Nom	Action						
	Apache by HTTP	Supprimer lien	Supprimer lien et nettoyer					
	taper ici pour rechercher			Sélectionner				
* Groupes d'hôtes	web servers × taper ici pour rechercher			Sélectionner				
Interfaces	Type adresse IP	Nom	DNS	Connexion à	Port	Défaut		
	Agent 192.168.1.3			IP DNS	10050	Supprimer	ŗ.	
	Ajouter							
Description								
					_			
					Actualiser	Clone	Supprimer	Annuler
Hôte								? ×
Hote IPMI Ta	gs Macros 1 Inventaire	Chiffrement Table de co	rrespondance					
Macros d'hôte	Macros héritées et de l'hôte	]						
Macro	Va	leur		Description				
{\$APACHE.STAT	US.HOST}	92.168.1.3	Τ~	The hostname of	or IP address of the	Apache status	Supprimer	
Aiouter				,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,				
Ajouter								
					Actualizati		Quantimat	Annular
					Actualiser	Cione	Supplimer	Annuler
Sur le serveu	r 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

Rudy & Vanthary	Supervision Zobbiy de l'Active Directory	Réf:	Zabbix
	Supervision Zabbix de l'Active Directory		1.0
	Depart technique Supervision	Date :	05/02/2025
	Rapport technique - Supervision	Page :	Page <b>24</b> sur <b>25</b>

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
//etcory//www/htm1/glpi/public
//etcory//www/htm1/glpi/public
//oinectory/
//oinector
```

**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.

Rudy & Vanthary	Supervision Zabbix de l'Active Directory	Réf:	Zabbix
	Supervision Zabbix de l'Active Directory	Version :	1.0
	Pennert technique Supervision	Date :	05/02/2025
	Rapport technique - Supervision	Page :	Page <b>25</b> sur <b>25</b>

ARACHE CL PL	Bidae per eacond	296	17 0666 Bor	+17 0666 Boe	component network		Graphique
		200					Chapter of the second sec
AMACHE GLM	Get status pui	285	{"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 comp	onent: health	Graphique
APACHE GLPI	Service response time	27s	0.36ms	-0.015ms	component: application comp	onent: 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	Activer Windows	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).