

FICHE N°2 — SUPERVISION ET INVENTAIRE

Création d'alertes proactives (Triggers) Zabbix
Surveillance CPU et Mémoire — SRV-AD-01

Champ	Valeur
Candidat	BTS SIO option SISR — 2026
Entreprise	SOS Futur
Serveur supervisé	SRV-AD-01 — 10.11.3.18 (Contrôleur de Domaine Principal)
Serveur Zabbix	10.11.3.19
Date	Mai 2026

1. Objectif

Suite à un incident critique survenu le mois précédent — un crash applicatif silencieux causé par la saturation simultanée du CPU (100 %) et de la RAM de SRV-AD-01, ayant rendu l'authentification des utilisateurs impossible sur l'ensemble du domaine sio.local — le directeur informatique a demandé la mise en place d'une supervision proactive.

Cette procédure décrit la configuration de deux déclencheurs (Triggers) dans Zabbix afin d'émettre automatiquement une alerte critique vers le service IT avant que le serveur n'atteigne un état de panne :

- Trigger 1 : Alerte si le CPU dépasse 90 % pendant plus de 5 minutes consécutives.
- Trigger 2 : Alerte si la mémoire disponible chute en dessous de 10 % de la RAM totale.

2. Prérequis

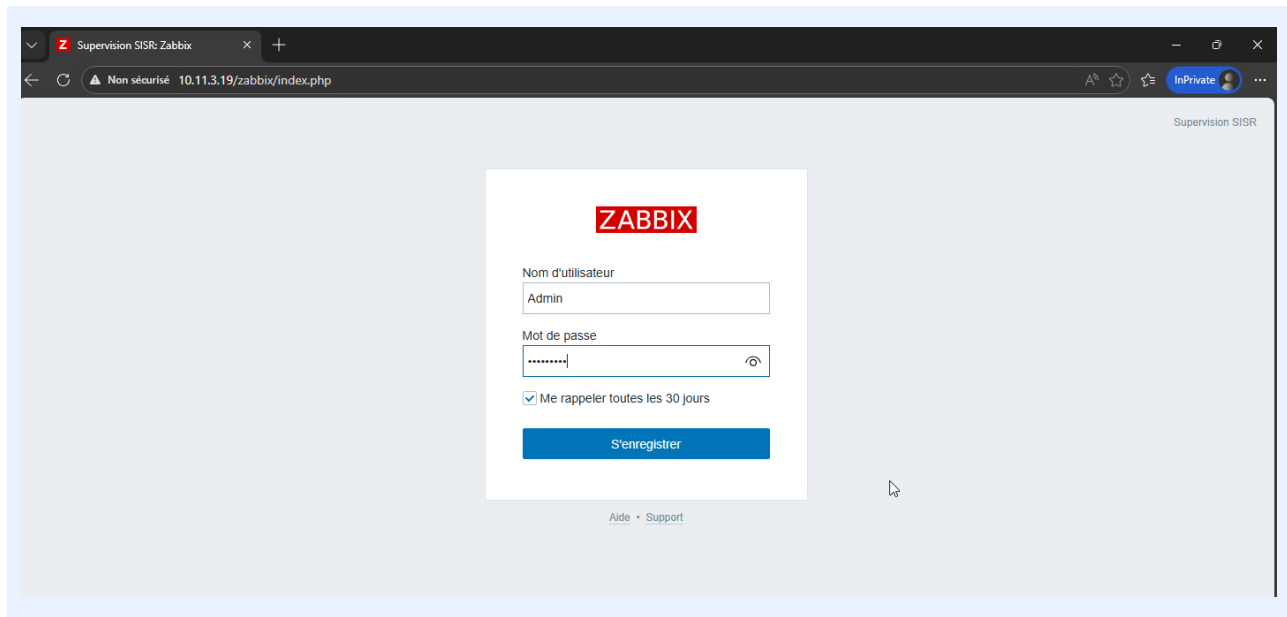
Prérequis	Détail	Statut attendu
Serveur Zabbix	Accessible sur http://10.11.3.19/zabbix	☑ Opérationnel
Agent Zabbix	Installé et actif sur SRV-AD-01 (10.11.3.18)	☑ Service en cours d'exécution
Hôte SRV-AD-01	Déclaré dans Zabbix, statut Monitored	☑ Visible dans Configuration > Hosts
Items de métriques	system.cpu.util et vm.memory.size[available] collectés	☑ Données visibles dans les graphes
Compte Zabbix	Compte administrateur avec droits suffisants	☑ Droits de création de Triggers

⚠ **NOTE** : Si l'agent Zabbix n'est pas encore installé sur SRV-AD-01, se référer à la Fiche n°1 (Installation et configuration de l'agent Zabbix).

3. Accès à la configuration des Triggers de SRV-AD-01

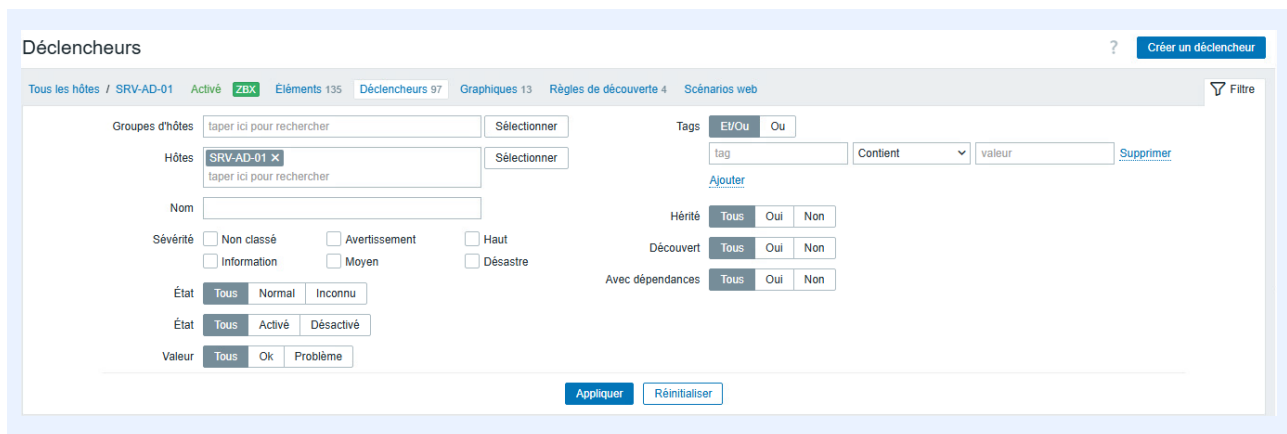
Étape 1 — Connexion à l'interface Zabbix

1. Ouvrir un navigateur et accéder à : `http://10.11.3.19/zabbix`
2. Se connecter avec les identifiants administrateur Zabbix.



Étape 2 — Navigation vers l'hôte SRV-AD-01

3. Dans le menu principal, cliquer sur Configuration.
4. Sélectionner Hosts dans le sous-menu.
5. Localiser SRV-AD-01 (IP : 10.11.3.18) dans la liste des hôtes.
6. Sur la ligne de SRV-AD-01, cliquer sur le lien Triggers dans la colonne des raccourcis.



4. TRIGGER N°1 — ALERTE CPU > 90 %

Étape 3 — Ouverture du formulaire de création

7. Sur la page des Triggers de SRV-AD-01, cliquer sur Create trigger en haut à droite.

Étape 4 — Remplissage du formulaire — Trigger CPU

Champ	Valeur à saisir
Name	Alerte critique : CPU > 90% sur SRV-AD-01
Severity	High
Description	Le CPU de SRV-AD-01 dépasse 90% depuis plus de 5 minutes. Risque de panne applicative imminente.
Enabled	☒ Coché

Construction de l'expression :

8. Cliquer sur le bouton Add à côté du champ Expression.
9. Item : sélectionner CPU utilization (clé : system.cpu.util).
10. Function : sélectionner avg() — calcule la moyenne sur une période.
11. Last (time T) : saisir 5m (5 minutes).
12. Result : sélectionner > puis saisir 90.
13. Cliquer sur Insert.

Expression générée :

```
avg (/SRV-AD-01/system.cpu.util, 5m) > 90
```

⚠ EXPLICATION TECHNIQUE : La fonction avg() sur 5 minutes garantit que l'alerte ne se déclenche pas pour un pic ponctuel, mais uniquement si la charge CPU reste élevée de manière soutenue, réduisant ainsi les faux positifs.

Déclencheur

Déclencheur

Tags

Dépendances

* Nom

Alerte critique : CPU > 90% sur SRV-AD-01

Nom de l'événement

Alerte critique : CPU > 90% sur SRV-AD-01

Données opérationnelles

Sévérité

Non classé

Information

Avertissement

Moyen

Haut

Désastre

* Expression

avg (/SRV-AD-01/system.cpu.util,5m)>90

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

Le CPU de SRV-AD-01 dépasse 90% depuis plus de 5 minutes. Risque de panne applicative imminente.

Actualiser

Clone

Supprimer

Annuler

Étape 5 — Sauvegarde du Trigger CPU

14. Vérifier l'ensemble des champs renseignés.

15. Cliquer sur le bouton Add en bas du formulaire pour enregistrer le trigger.

5. TRIGGER N°2 — ALERTE RAM DISPONIBLE < 10 %

Étape 6 — Ouverture du second formulaire

16. Sur la page des Triggers de SRV-AD-01, cliquer à nouveau sur Create trigger.

Étape 7 — Remplissage du formulaire — Trigger RAM

Champ	Valeur à saisir
Name	Alerte critique : RAM disponible < 10% sur SRV-AD-01
Severity	High
Description	La mémoire disponible de SRV-AD-01 est inférieure à 10% de la RAM totale. Saturation mémoire imminente.
Enabled	☒ Coché

Construction de l'expression :

17. Cliquer sur Add à côté du champ Expression.
18. Item : sélectionner Available memory in % (clé : vm.memory.size[pavailable]).
19. Function : sélectionner last() — prend la dernière valeur collectée.
20. Result : sélectionner < puis saisir 10.
21. Cliquer sur Insert.

Expression générée :

```
last(/SRV-AD-01/vm.memory.util) > 90
```

△ EXPLICATION TECHNIQUE : La fonction last() est utilisée ici car la saturation mémoire peut être immédiate et ne nécessite pas de moyenne temporelle. Une RAM disponible inférieure à 10 % constitue un seuil critique justifiant une alerte sans délai.

Étape 8 — Sauvegarde du Trigger RAM

22. Vérifier l'ensemble des champs renseignés.
23. Cliquer sur Add pour enregistrer le second trigger.

6. Validation — Vérification des deux Triggers

Étape 9 — Contrôle dans la liste des Triggers

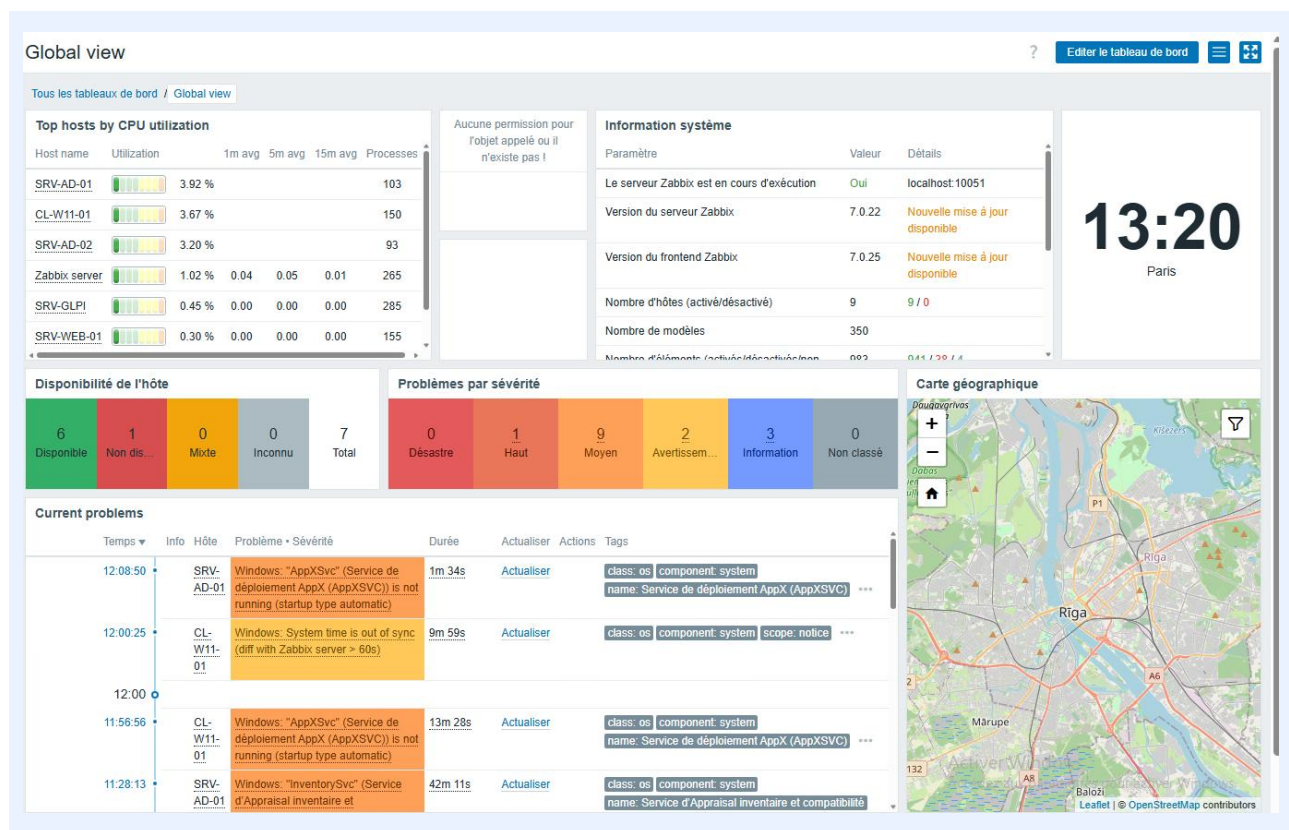
24. Rester sur la page Configuration > Hosts > SRV-AD-01 > Triggers.
25. Vérifier que les deux triggers apparaissent dans la liste avec le statut Enabled.
26. S'assurer que la colonne Status affiche Enabled (fond vert) pour chacun.

Nom du Trigger	Sévérité	Statut
Alerte critique : CPU > 90% sur SRV-AD-01	High	Enabled
Alerte critique : RAM disponible < 10% sur SRV-AD-01	High	Enabled

Sévérité	Valeur	Nom ▲	Données opérationnelles	Expression	État	Info	Tags
Haut	OK	Alerte critique : CPU > 90% sur SRV-AD-01		avg(/SRV-AD-01/system.cpu.util,5m)>90	Activé		
Haut	OK	Alerte critique : RAM disponible < 10% sur SRV-AD-01		last(/SRV-AD-01/vm.memory.util) > 90	Activé		

Étape 10 — Vérification fonctionnelle dans le tableau de bord

27. Se rendre dans Monitoring > Dashboard.
28. En cas de dépassement de seuil, les alertes apparaîtront dans le widget Problems avec la sévérité High.
29. En situation normale, aucune alerte active = configuration correcte.



7. ARGUMENTAIRE POUR L'ORAL — Supervision Proactive

Concept de supervision proactive

La supervision réactive consiste à constater une panne après qu'elle s'est produite. La supervision proactive, mise en place ici, anticipe la défaillance en définissant des seuils d'alerte déclenchés avant l'atteinte du point critique, laissant ainsi au service IT le temps d'intervenir. Zabbix joue le rôle d'un système de surveillance en temps réel : l'agent installé sur SRV-AD-01 collecte les métriques toutes les 30 secondes (par défaut) et les transmet au serveur Zabbix, qui évalue en permanence les expressions des triggers.

Pourquoi coupler la surveillance CPU et RAM ?

L'incident du mois dernier illustre parfaitement l'interdépendance entre ces deux ressources :

- Saturation CPU → consommation mémoire accrue : lorsque le CPU est surchargé, les processus en attente s'accumulent en mémoire. Le kernel Windows augmente l'utilisation du fichier d'échange (paging file), aggravant la lenteur et consommant davantage de RAM.
- Saturation RAM → charge CPU accrue : inversement, lorsque la RAM disponible s'épuise, Windows active intensivement le mécanisme de swap. Les opérations I/O supplémentaires génèrent une charge CPU additionnelle, créant un cercle vicieux.
- Impact sur l'AD : sur un contrôleur de domaine, les services NTDS et Netlogon sont à forte consommation CPU/RAM. Leur dégradation bloque l'authentification Kerberos pour l'ensemble du parc, rendant les postes inaccessibles.

Valeur ajoutée des seuils choisis

Trigger	Seuil	Justification technique
CPU > 90 % pendant 5 min	90 % / 5 min	Élimine les faux positifs (pics courts) tout en détectant une surcharge soutenue avant le crash
RAM disponible < 10 %	< 10 %	Sur 8 Go de RAM : 800 Mo restants — seuil critique avant activation intensive du swap

⚠ CHOIX DE SÉVÉRITÉ : La sévérité High (et non Disaster) est choisie délibérément : elle déclenche une notification immédiate au service IT sans générer une escalade d'urgence maximale, permettant une intervention humaine mesurée avant que la situation ne devienne irrémédiable.