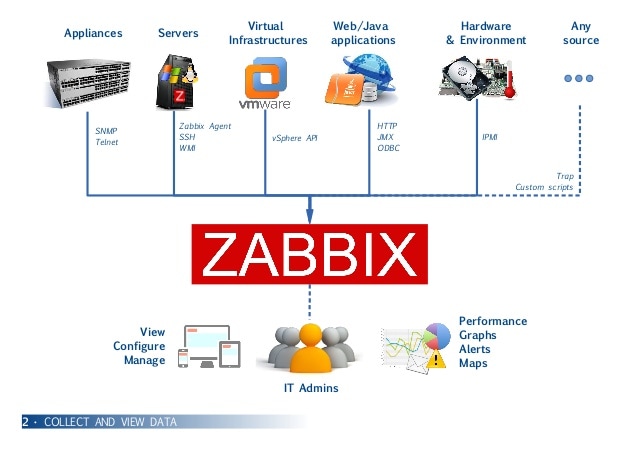
LIBER TECHNOLOGIES

Projet « ANDF – SI Foncier »

*Document d’exploitation Supervision ANDF*

|  |  |
| --- | --- |
| **VOTRE INTERLOCUTEUR COMMERCIAL :**  Abdelkrim EL AKRI  Tél : +33 6 40 15 60 14  abdelkrim.elakri@trustingenierie.com | |
| **VOTRE INTERLOCUTEUR TECHNIQUE :**  Rémi BELLO  Tél : +212 6 54 24 18 24  remi.bello@trustingenierie.com | |
| **Statut :** | Validé |
| **Diffusion :** | Restreinte |
| **Version :** | V1-00 |
| **Référence :** | LT\_BENINTF\_MON |

# Stack technique

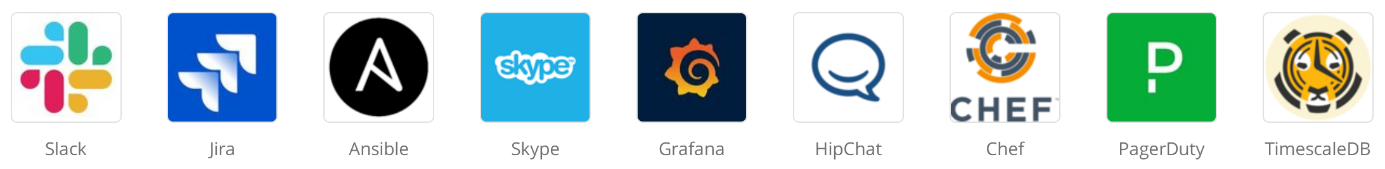
ZABBIX est un logiciel libre (sous licence publique générale GNU version 2) permettant de surveiller l'état de divers services réseau, serveurs et autres matériels réseau et produisant des graphiques dynamiques de consommation des ressources.

Permet de surveiller l’ensemble du réseau, des serveurs et de leurs services :



**Points forts** :

* Solution éprouvée et mature
* Gratuit et open-source
* Packagé avec docker-compose (simplicité de configuration, d’installation et d’exploitation)
* Supporte la supervision en mode pull (le traffic de supervision va de l’ANDF vers le MEF, l’autre sens est impossible)
* Simple à sauvegarder/restaurer (tout contenu dans 1 dossier)
* Intégrable avec de nombreux outils de notification ou de déploiement continu



# Installation

## Serveur

<https://github.com/zabbix/zabbix-docker/>

<https://www.zabbix.com/documentation/current/manual/installation/containers>

<https://github.com/zabbix/zabbix-docker/blob/5.4/docker-compose_v3_ubuntu_pgsql_latest.yaml>

docker-compose -f docker-compose\_trust.yaml up -d

Connexion en HTTPS sur le port 3000

Login par défaut : Admin/zabbix

Login pour trust : Admin/sVLCUx858DiZmbc

**Configurer SSL côté backend**

Dans le répertoire contenant le dossier **zbx\_env**

sudo cp votre-certificat.crt ./zbx\_env/etc/ssl/nginx/ssl.crt

sudo cp votre-certificat.key ./zbx\_env/etc/ssl/nginx/ssl.key

sudo openssl dhparam -out ./zbx\_env/etc/ssl/nginx/dhparam.pem 4096

# sudo chown zabbix:zabbix ./zbx\_env/etc/ssl/nginx/\*

sudo chmod 744 ./zbx\_env/etc/ssl/nginx/\*

## Agent

Installation d’un agent sur les serveurs à monitorer, qui va ouvrir le port 10050 sur la machine.

### Windows

<https://www.zabbix.com/documentation/4.0/fr/manual/installation/install_from_packages/win_msi>

### Linux

<https://bestmonitoringtools.com/zabbix-agent-linux-install-on-ubuntu-centos-rhel-debian-rasbian/>

sudo apt -y install zabbix-agent

sudo nano /etc/zabbix/zabbix\_agentd.conf

Modifier les propriétés ci-dessous :

Server=vps-30e3917a.vps.ovh.net (dns ou ip du serveur zabbix)

ServerActive=vps-30e3917a.vps.ovh.net (idem)

Hostname=(nom d’hôte)  
 (ou) HostnameItem=system.hostname

HostMetadata=Linux

TLSConnect=psk

TLSAccept=psk

TLSPSKIdentity=ZBX-AGENT-PSK-ID (personnaliser pour chaque hôte)

TLSPSKFile=/etc/zabbix/zabbix\_agent.psk

Générer la clé PSK :

sudo openssl rand -hex 32

(coller le contenu dans -->) sudo nano /etc/zabbix/zabbix\_agent.psk

sudo chown zabbix:zabbix /etc/zabbix/zabbix\_agent.psk

sudo chmod 700 /etc/zabbix/zabbix\_agent.psk

sudo systemctl restart zabbix-agent

sudo systemctl enable zabbix-agent

# CONFIGURATION

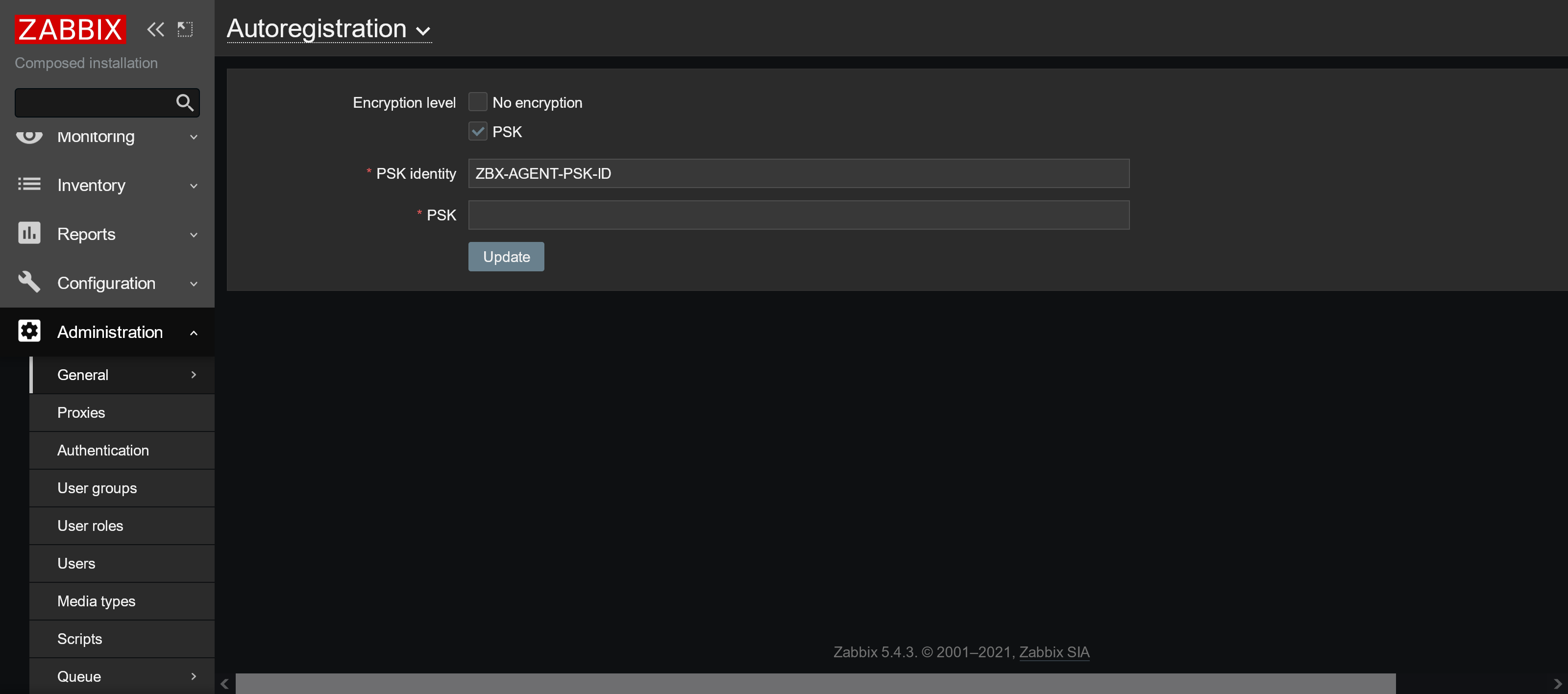
## Comptes utilisateurs

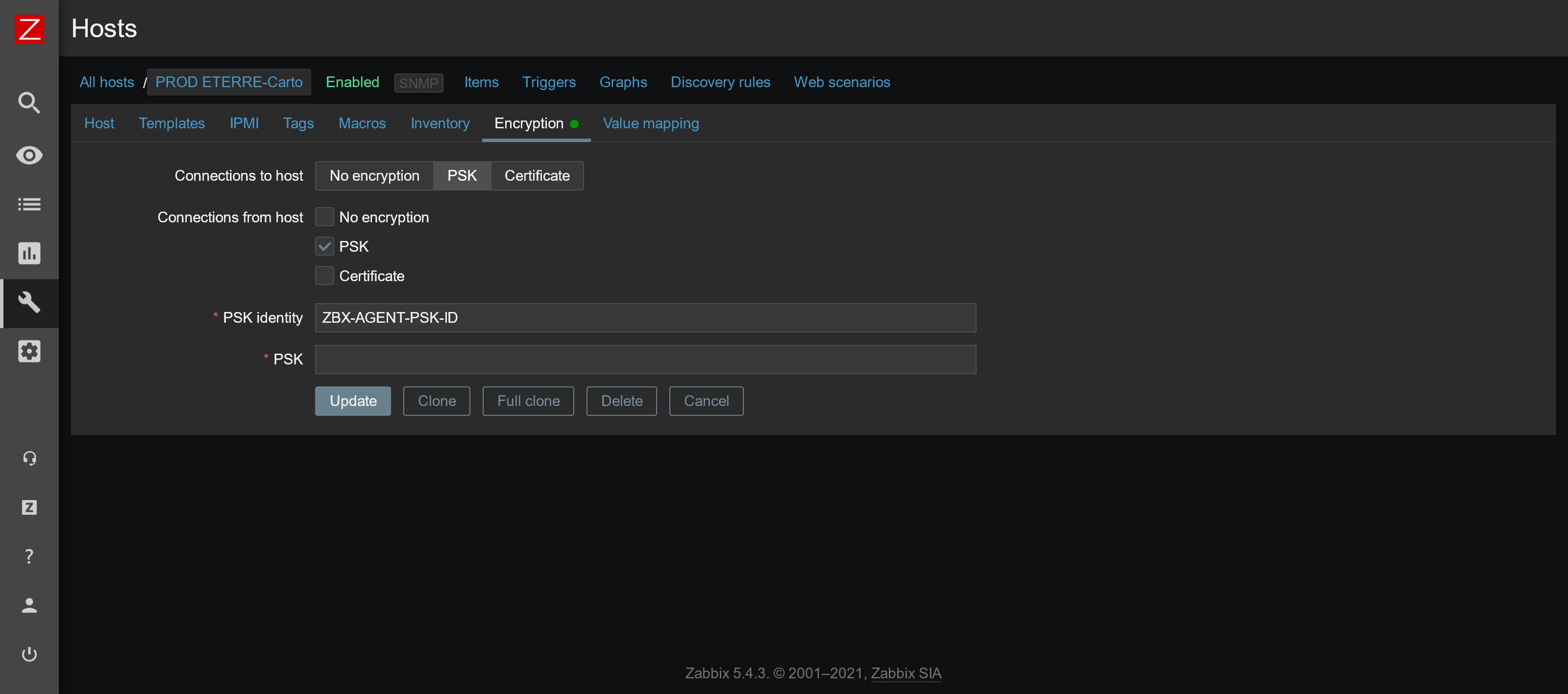
Consultation, administration

## Hosts

Créer hôte, hostname doit matcher avec la config du client zabbix

Voir : <https://www.zabbix.com/documentation/current/manual/discovery/auto_registration>





Vérifier connexion depuis un hôte en consultant les logs côté serveur : docker logs zabbix-docker\_zabbix-server\_1 -f

## Monitorer un service Web

Dans : Configuration > Hosts > (Choisir un hôte) > Web scenarios

Créer un scénario, indiquer l’URL et le code attendu en retour.

Il est possible d’associer chaque scénario à un déclencheur.

Dans : Configuration > Hosts > (Choisir un hôte) > Triggers

Créer un trigger en utilisant l’expression suivante :

* Item : le web scenario (dans la liste des items)
* Fonction : change()
* Valeur : 1

Ce trigger peut ensuite être associé à un service, pour signaler qu’une application est indisponible.

Dans : Configuration > Services > (Choisir un service)

Le trigger se configure dans l’écran de configuration du service.

## Monitorer l’ouverture/fermeture d’un port

Créer un item qui correspond au test sur l’ouverture ou non du port.

Dans : Configuration > Hosts > (Choisir un hôte) > Items

Créer un item avec les paramètres suivants (ici pour tester le port 443) :

* Name : Test TCP Port 443
* Key : net.tcp.service[http,,443]
* Type of information : Numeric (Unsigned)

Créer ensuite un déclencheur (trigger) qui correspond au changement d’état oui/non de l’item.

Dans : Configuration > Hosts > (Choisir un hôte) > Triggers

Créer un trigger en utilisant l’expression suivante :

* Item : celui créé précédemment
* Fonction : change()
* Valeur : 1

Ce trigger peut ensuite être associé à un service, pour signaler qu’une application est indisponible.

Dans : Configuration > Services > (Choisir un service)

Le trigger se configure dans l’écran de configuration du service.

## Monitorer la connexion à internet d’un hôte

Créer un Web Scenario (voir §3.3) qui pointe vers Google ou autre site internet à réponse rapide.

Une solution plus optimale est de tester la connexion avec le protocole DNS moins coûteux, voir : <https://www.zabbix.com/forum/zabbix-help/43679-what-is-a-good-way-to-set-a-trigger-that-checks-for-internet-connectivity>

## Détecter des ouvertures de ports

Piste : <https://share.zabbix.com/cat-app/misc/template-listening-port-discovery>

## Configurer les notifications

*Fin du document*