

3 Traps SNMP

Aperçu

La réception des traps SNMP est l'opposé de l'interrogation des périphériques compatibles SNMP.

Dans ce cas, les informations sont envoyées depuis un périphérique compatible SNMP et sont "collectées" par Zabbix.

Habituellement, les traps sont envoyées lors de certaines modifications de condition et l'agent se connecte au serveur sur le port 162 (par opposition au port 161 du côté de l'agent utilisé pour les requêtes). L'utilisation des traps peut détecter certains problèmes de courte durée qui surviennent au cours de l'intervalle de requête et peuvent être ignorés par les données de la requête.

La réception des traps SNMP dans Zabbix est conçue pour fonctionner avec `snmptrapd` et l'un des mécanismes intégrés pour transmettre les traps à Zabbix - un script Perl ou `SNMPTT`.

Le flux de travail de la réception d'un trap :

1. `snmptrapd` reçoit un trap
2. `snmptrapd` transfère le trap à `SNMPTT` ou appelle le récepteur de trap Perl
3. Le récepteur de trap `SNMPTT` ou Perl analyse, formate et écrit le trap dans un fichier
4. Le trappeur SNMP Zabbix lit et analyse le fichier de trap
5. Pour chaque trap, Zabbix trouve tous les éléments "trappeur SNMP" avec des interfaces hôtes correspondant à l'adresse du trap reçue. Notez que seuls les "IP" ou "DNS" sélectionnés dans l'interface hôte sont utilisés lors de la mise en correspondance
6. Pour chaque élément trouvé, le trap est comparé à `regex` dans `"snmptrap[regex]"`. Le trap est défini comme la valeur de tous les éléments correspondants. Si aucun élément correspondant n'est trouvé et qu'il existe un élément `"snmptrap.fallback"`, le trap est défini comme valeur de celui-ci
7. Si le trap n'est pas défini comme la valeur d'un élément, Zabbix enregistre par défaut le trap qui ne correspond pas. (Cela est configuré par "Enregistrer les traps SNMP non appariés" dans Administration → Général → Autre.)

1 Configuration des traps SNMP

La configuration des champs suivants dans l'interface web est spécifique pour ce type d'élément :

- Votre hôte doit avoir une interface SNMP

Dans *Configuration* → *Hôtes*, dans le champ *Interface hôte*, définissez une interface SNMP avec l'adresse IP ou DNS correcte. L'adresse de chaque trap reçu est comparé aux adresses IP et DNS de toutes les interfaces SNMP pour trouver les hôtes correspondants.

- Configuration de l'élément

Dans le champs **Clé** utilisez l'une des clés de trap SNMP suivantes :

Clé		
Description	Valeur de retour	Commentaires
snmptrap[regex]		
Reçoit tous les traps SNMP qui correspondent à l' expression régulière spécifiée dans regex . Si regex n'est pas spécifié, reçoit tous les traps	Trap SNMP	Cet élément peut être défini uniquement pour les interfaces SNMP. Cet élément est supporté depuis Zabbix 2.0.0 . <i>Remarque</i> : à partir de Zabbix 2.0.5, les macros utilisateur et les expressions régulières globales sont prises en charge dans le paramètre de cette clé d'élément.
snmptrap.fallback		
Reçoit tous les traps SNMP qui n'ont été reçus par aucun élément snmptrap[] pour cette interface.	Trap SNMP	Cet élément peut être défini uniquement pour les interfaces SNMP. Cet élément est supporté depuis Zabbix 2.0.0 .

La correspondance d'expressions régulières sur plusieurs lignes n'est pas prise en charge pour le moment.

Définissez le **Type d'information** à 'Journal' pour les horodatages à analyser. Notez que d'autres formats tels que 'Numerique' sont également acceptables, mais peuvent nécessiter un gestionnaire de traps personnalisé.

Pour que la supervision des traps SNMP fonctionne, elle doit d'abord être correctement configurée.

2 Configuration de la supervision des traps SNMP

Configuration du serveur/proxy Zabbix

Pour lire les traps, le serveur ou le proxy Zabbix doit être configuré pour démarrer le trappeur SNMP et pointer vers le fichier de traps en cours d'écriture par SNMPTT ou un récepteur de traps perl. Pour ce faire, éditez le fichier de configuration ([zabbix_server.conf](#) ou [zabbix_proxy.conf](#)) :

1. StartSNMPTrapper=1
2. SNMPTrapperFile=[TRAP FILE]

Si le paramètre systemd **PrivateTmp** est utilisé, il est peu probable que ce fichier fonctionne dans */tmp*.

Configuration de SNMPTT

Au début, snmptrapd devrait être configuré pour utiliser SNMPTT.

Pour de meilleures performances, SNMPTT doit être configuré en tant que démon en utilisant **snmptthandler-embedded** pour lui transmettre les traps. Voir les instructions pour configurer SNMPTT sur sa page d'accueil :

<http://snmptt.sourceforge.net/docs/snmptt.shtml>

Lorsque SNMPTT est configuré pour recevoir les traps, configurez SNMPTT pour consigner les traps :

1. consignez les traps dans le fichier de trap qui sera lu par Zabbix :
log_enable = 1
fichier_journal = [TRAP FILE]
2. définissez le format date-heure :
date_time_format = %H:%M:%S %Y/%m/%d = [DATE TIME FORMAT]

Maintenant formatez les traps pour que Zabbix les reconnaisse (éditez snmptt.conf) :

1. Chaque instruction FORMAT devrait commencer par "ZBXTRAP [adresse]", où [adresse] sera comparée aux adresses IP et DNS des interfaces SNMP sur Zabbix. Par exemple :
EVENT coldStart .1.3.6.1.6.3.1.1.5.1 "Status Events" Normal
FORMAT ZBXTRAP \$aA Device reinitialized (coldStart)
2. En savoir plus sur le format de trap SNMP ci-dessous.

N'utilisez pas de traps inconnus - Zabbix ne pourra pas les reconnaître. Les traps inconnus peuvent être gérés en définissant un événement général dans snmptt.conf :

```
EVENT general .* "General event" Normal
```

Configuration du récepteur de traps Perl

Prérequis : Perl, Net-SNMP compilé avec -enable-embedded-perl (fait par défaut depuis Net-SNMP 5.4)

Le récepteur de traps Perl (recherchez misc/snmpttrap/zabbix_trap_receiver.pl) peut être utilisé pour transférer les traps au serveur Zabbix directement depuis snmpttrapd. Pour le configurer :

- ajoutez le script perl au fichier de configuration snmpttrapd (snmpttrapd.conf), par exemple :
perl do "[CHEMIN COMPLET DU SCRIPT RECEPTEUR PERL]" ;
- configurez le récepteur, par exemple :
\$SNMPTrapperFile = '[TRAP FILE]' ;
\$DateTimeFormat = '[DATE TIME FORMAT]' ;

Si le nom du script n'est pas entre quote, snmpttrapd refusera de démarrer avec des messages similaires à ceux-ci :

```
Regexp modifiers "/l" and "/a" are mutually exclusive at (eval 2) line 1, at  
end of line  
Regexp modifier "/l" may not appear twice at (eval 2) line 1, at end of line
```

Format de trap SNMP

Tous les récepteurs de traps perl personnalisés et la configuration de SNMPTT doivent formater le trap de la manière suivante : **[timestamp] [trap, partie 1] ZBXTRAP [adresse] [trap, partie 2]**, où

- [timestamp] - horodatage utilisé pour les éléments de journal
- ZBXTRAP - en-tête qui indique qu'un nouveau trap commence dans cette ligne
- [adresse] - adresse IP utilisée pour trouver l'hôte de ce trap

Notez que "ZBXTRAP" et "[adresse]" seront supprimés du message pendant le traitement. Si le trap est formaté autrement, Zabbix peut analyser les traps de façon inattendue.

Exemple de trap :

11:30:15 2011/07/27 .1.3.6.1.6.3.1.1.5.3 Normal "Status Events" localhost - ZBXTRAP 192.168.1.1

Link down on interface 2. Admin state: 1. Operational state: 2

Cela entraînera le trap suivant pour l'interface SNMP avec IP = 192.168.1.1 :

11:30:15 2011/07/27 .1.3.6.1.6.3.1.1.5.3 Normal "Status Events" localhost - Link down on interface 2.
Admin state: 1.

3 Pré-requis système

Prise en charge des fichiers volumineux

Zabbix "prend en charge les fichiers volumineux" pour les fichiers de trapper SNMP. La taille limite maximum que Zabbix peut lire est 2^{63} (8 EiB). Notez que le système de fichier peut imposer une limite inférieure sur la taille du fichier.

Rotation des logs

Zabbix ne fournit aucun système de rotation des logs - cela devrait être géré par l'utilisateur. La rotation des logs doit d'abord renommer l'ancien fichier et seulement le supprimer plus tard afin qu'aucun trap ne soit perdu :

1. Zabbix ouvre le fichier de traps au dernier emplacement connu et passe à l'étape 3
2. Zabbix vérifie si le fichier actuellement ouvert a été pivoté en comparant le numéro d'inode au numéro d'inode du fichier de traps défini. S'il n'y a pas de fichier ouvert, Zabbix réinitialise le dernier emplacement et passe à l'étape 1.
3. Zabbix lit les données du fichier actuellement ouvert et définit le nouvel emplacement.
4. Les nouvelles données sont analysées. S'il s'agissait du fichier pivoté, le fichier est fermé et retourne à l'étape 2.
5. S'il n'y avait pas de nouvelles données, Zabbix attend 1 seconde et retourne à l'étape 2.

Système de fichiers

En raison de l'implémentation du fichier de trap, Zabbix a besoin du système de fichiers pour prendre en charge les inodes afin de différencier les différents fichiers (les informations sont acquises par un appel stat()).

4 Exemple d'implémentation

Cet exemple utilise snmptrapd + SNMPTT pour transmettre les traps au serveur Zabbix :

1. **zabbix_server.conf** - configurez Zabbix pour démarrer le trappeur SNMP et définir le fichier de traps :
StartSNMPTrapper=1

- SNMPTrapperFile=/tmp/my_zabbix_traps.tmp
2. **snmptrapd.conf** - ajoutez SNMPTT en tant que gestionnaire de traps :
traphandle default snmptt
 3. **snmptt.ini** - configurez le fichier de sortie et le format de l'heure :
log_file = /tmp/my_zabbix_traps.tmp
date_time_format = %H:%M:%S %Y/%m/%d
 4. **snmptt.conf** - définissez un format de trap par défaut :
EVENT general .* "General event" Normal
FORMAT ZBXTRAP \$aA \$ar
 5. Créer un élément SNMP de test :
IP de l'interface SNMP de l'hôte : 127.0.0.1
Clé : snmptrap["General"]
Format de l'heure du journal : hh:mm:ss yyyy/MM/dd

Cela a pour résultat :

1. Commande utilisée pour envoyer un trap :
snmptrap -v 1 -c public 127.0.0.1 '.1.3.6.1.6.3.1.1.5.3' '0.0.0.0' 6 33 '55' .1.3.6.1.6.3.1.1.5.3 s
"teststring000"
2. Le trap reçu :
15:48:18 2011/07/26 .1.3.6.1.6.3.1.1.5.3.0.33 Normal "General event" localhost - ZBXTRAP
127.0.0.1 127.0.0.1
3. Valeur pour l'élément TEST :
15:48:18 2011/07/26 .1.3.6.1.6.3.1.1.5.3.0.33 Normal "General event" localhost - 127.0.0.1

Cet exemple simple utilise SNMPTT comme **traphandle**. Pour de meilleures performances sur les systèmes de production, utilisez le Perl intégré pour transmettre les traps de snmptrapd à SNMPTT ou directement à Zabbix.

5 Voir aussi

- [Tutoriel sur les traps SNMP basé sur CentOS sur zabbix.org](#)

From:

<https://www.zabbix.com/documentation/4.0/> - **Zabbix Documentation 4.0**

Permanent link:

<https://www.zabbix.com/documentation/4.0/fr/manual/config/items/itemtypes/snmptrap>

Last update: **2019/02/26 10:46**

