

TP Supervision

Zabbix

1 Introduction

Pour les besoins du TP, installer

- Une machine virtuelle Ubuntu 16.04 pour accueillir Zabbix
- Une ou plusieurs machines virtuelles Ubuntu ayant quelques services de type samba et apache, ayant des capacités de stockage différentes.
- Des machines virtuelles Windows

2 Installation de Zabbix

2.1 Installation via ansible

Prérequis

- Clé SSH copiée sur la machine distante (après création d'une clé sur la machine locale)
- Ubuntu 16.04, avec accès internet pour accès aux dépôts

Lien vers le projet

```
git clone https://github.com/paulbsd/ansible-zabbix.git
```

Fichier inventaire ansible

Créer un fichier d'inventaire ansible nommé hosts

```
<ip_serveur>
```

Lancement du playbook

```
# ansible-playbook -i hosts zabbix-server.yml
```

2.2 Installation manuelle

https://www.zabbix.com/documentation/3.2/manual/installation/install_from_packages

2.3 Gestion du service Zabbix

Les commandes nécessaires sont :

```
# systemctl start zabbix-server  
# systemctl restart zabbix-server  
# systemctl stop zabbix-server
```


3 Analyse de la configuration par défaut

3.1 Fichiers de configuration du serveur

Commande permettant de supprimer les lignes commentées

```
cat /etc/zabbix/zabbix_server.conf | grep -v "#" | grep -v "^$" 
```

Visualisation du fichier de configuration

```
vim /etc/zabbix/zabbix_server.conf
```

3.2 Fichier de configuration de l'agent

Commande permettant de supprimer les lignes commentées

```
cat /etc/zabbix/zabbix_agentd.conf | grep -v "#" | grep -v "^$" 
```

Visualisation du fichier de configuration

```
vim /etc/zabbix/zabbix_agentd.conf
```

4 Analyse de l'interface avec la configuration par défaut

http://<ip_machine>/

Indiquer les logins par défaut : Admin / zabbix

Monitoring

Dashboard : Visualisation par panneau, visualisation des derniers problèmes

Overview : Liste des données collectées sous forme de tableau

Web : État monitoring Web

Latest data : Dernières données collectées

Triggers : Liste des triggers et des problèmes en cours

Events : Liste des événements liés à un hôte

Graphs : Liste des graphiques pour la télémétrie

Screens : Liste des écrans, permettant l'agrégation de plusieurs vues

Maps : Liste des cartes de réseau et topologies

Discovery : Découverte du réseau

IT services : Rapports de disponibilité

Inventory

Overview : Liste des inventaires

Hosts : Liste des hôtes avec leurs inventaires

Reports

Status of Zabbix : Statut global du serveur zabbix

Availability report : Rapport de disponibilité

Triggers top 100 : Triggers les plus fréquemment rencontrés

Audit : Audit des changements effectuées par les différents utilisateurs

Action log : Log des actions (notifications, actions sur les agents)

Notifications : Log des notifications

Configuration

Host groups : Configuration des groupes d'hôtes

Templates : Liste des templates

Hosts : Liste des hôtes

Maintenance : Définition des temps d'arrêt pour maintenance

Actions : Définition des actions à effectuer sur les agents

Discovery : Configuration de la découverte réseau

IT Services : Définition des hôtes sur lesquels la disponibilité est calculée

Administration

General : Configuration générale de zabbix

Proxies : Définition des accès par proxy

Authentication : Définition de l'authentification (locale, LDAP, HTTP basic)

User groups : groupes d'utilisateurs

Users : liste d'utilisateurs locaux ou par import LDAP

Media types : Types de media pour la définition de notifications (Jabber, SMS, Mail, etc.)

Scripts : Définition des scripts côté serveur

Queue : État de la file d'attente des checks

5 Gestion de SNMP et de l'agent Zabbix

5.1 Installation des VM

Installation de machines sur Ubuntu 16.04 server. À installer sur autant de machine à surveiller.

5.2 SNMP

5.2.1 Introduction

SNMP est un protocole applicatif permettant d'extraire des informations par le réseau d'un système d'exploitation.

5.2.2 Installation

```
# apt install snmpd
```

5.2.3 Configuration

Adapter la configuration

```
/etc/snmp/snmpd.conf  
agentAddress udp:161  
...  
rocommunity public
```

5.3 Agent Zabbix

5.3.1 Installation

```
# apt install zabbix-agent
```

5.3.2 Configuration

Adapter la ligne suivante

```
/etc/zabbix/zabbix_agentd.conf  
Server=<ip_serveur>
```

6 Ajout d'un hôte et d'un groupe d'hôtes

6.1 Groupe d'hôtes

Dans Configuration -> Hosts groups

Créer un groupe Windows et Switch

6.2 Hôte

Dans Configuration -> Hosts

Définir l'hôte Linux à surveiller

L'ajouter dans le groupe « Linux servers »

The screenshot shows the Zabbix configuration interface for adding a host. The interface is divided into several sections:

- Host name:** A text input field containing "hote_linux".
- Visible name:** An empty text input field.
- Groups:** Two panels are visible. The "In groups" panel contains a list with "Linux servers" selected. The "Other groups" panel contains a list with "Discovered hosts", "Hypervisors", "Templates", "Virtual machines", and "Zabbix servers".
- New group:** An empty text input field with a green border.
- Agent interfaces:** A table with columns for IP address, DNS name, Connect to, Port, and Default. The first row contains: IP address: 172.18.30.25, DNS name: linux.domain.tld, Connect to: IP, DNS, Port: 10050, Default: Remove.
- SNMP interfaces:** A table with columns for IP address, DNS name, Connect to, Port, and Default. The first row contains: IP address: 172.18.30.25, DNS name: (empty), Connect to: IP, DNS, Port: 161, Default: Remove. A checkbox "Use bulk requests" is checked.
- JMX interfaces:** An "Add" button.
- IPMI interfaces:** An "Add" button.
- Description:** A large empty text area.
- Monitored by proxy:** A dropdown menu set to "(no proxy)".
- Enabled:** A checked checkbox.
- Buttons:** "Add" and "Cancel" buttons at the bottom.

Ajouter le template « Template OS Linux ». Celui-ci est lié à l'agent zabbix. Pour utiliser SNMP, il est essentiel d'utiliser le template « Template SNMP OS Linux »

Hosts

[Host](#) [Templates](#) [IPMI](#) [Macros](#) [Host inventory](#) [Encryption](#)

Linked templates	Name	Action
	Template OS Linux	Unlink

Link new templates

[Add](#)

7 Ajout d'une donnée et d'un trigger associé

En plus des checks de base donnés avec les templates par défaut, on peut ajouter des items personnalisés.

7.1 Ajout d'une donnée (item)

<input type="checkbox"/> Name ▲	Applications	Items	Triggers	Graphs	Discovery	Web
<input type="checkbox"/> Zabbix server	Applications 11	Items 74	Triggers 45	Graphs 13	Discovery 2	Web

0 selected

Dans Configuration -> Hosts, cliquer sur « Items » au niveau de l'hôte sur lequel on souhaite ajouter l'item.

Name

Type

Key

Host interface

Type of information

Data type

Units

Use custom multiplier

Update interval (in sec)

Type	Interval	Period	Action
Flexible Scheduling	<input type="text" value="50"/>	<input type="text" value="1-7,00:00-24:00"/>	<input type="button" value="Remove"/>

Ci-dessus un item donnant le nombre de fichier présents dans /tmp. Indiquer un nom, un type de check, une clé, ainsi qu'un type d'information et de donnée. Donner un intervalle d'actualisation et des périodes de contrôles personnalisées, puis cliquer sur Add.

Dans le point 9, nous pourrons voir comment l'intégrer du côté de l'agent Zabbix.

7.2 Ajout d'un trigger

Name

Severity Not classified Information Warning Average High Disaster

Expression

[Expression constructor](#)

OK event generation Expression Recovery expression None

PROBLEM event generation mode Single Multiple

OK event closes All problems All problems if tag values match

Tags

<input type="text" value="tag"/>	<input type="text" value="value"/>	Remove
----------------------------------	------------------------------------	------------------------

[Add](#)

Allow manual close

URL

Description

Enabled

Indiquer un nom au trigger dans le champ « Name ». Définir un niveau de sévérité au trigger en fonction du niveau de criticité. Indiquer une condition basée sur un item. Cliquer sur Add pour l'ajouter.

Ici nous donnons une alerte de type Warning si le nombre d'élément dans /tmp est supérieur à 3.

8 Import d'un template

8.1 Récupération

Un fichier de template zabbix se présente sous la forme d'un fichier XML. Il décrit les items, triggers, règles de découverte, applications nécessaires aux données que l'on souhaite récupérer.

8.2 Insertion

Dans Configuration -> Template, une invite demande l'upload d'un fichier XML de template.

Import file Aucun fichier choisi

Rules	Update existing	Create new	Delete missing
Groups		<input checked="" type="checkbox"/>	
Hosts	<input type="checkbox"/>	<input type="checkbox"/>	
Templates	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Template screens	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Template linkage		<input checked="" type="checkbox"/>	
Applications		<input checked="" type="checkbox"/>	<input type="checkbox"/>
Items	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Discovery rules	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Triggers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Graphs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Web scenarios	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Screens	<input type="checkbox"/>	<input type="checkbox"/>	
Maps	<input type="checkbox"/>	<input type="checkbox"/>	
Images	<input type="checkbox"/>	<input type="checkbox"/>	
Value mappings	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

9 Écriture d'un script lancé par l'agent zabbix

Créer un script contrôlant sur la machine surveillée un contrôle bien spécifique, tel que :

- Contrôle de l'état d'un service
- Contrôle du nombre de fichiers ayant des droits d'écriture à tout le monde (World writeable) dans le répertoire /var

Faire ce script en python ou en Shell UNIX

Exemple de contrôle du nombre de fichiers dans un répertoire :

```
#!/usr/bin/python

import os
import sys

if len(sys.argv) >= 2:
    folder = sys.argv[1]

    d_list = os.listdir(folder)
    d_list_len = len(d_list)

    print(str(d_list_len))
else:
    print(-1)
    sys.exit(1)
```

10 Notifications

Dans Configuration -> Actions cliquer sur « Report problems to Zabbix administrators »

Action | **Operations** | **Recovery operations**

Name:

Conditions:

Label	Name	Action
-------	------	--------

New condition:

[Add](#)

Enabled

Action | **Operations** | **Recovery operations**

Default operation step duration: (minimum 60 seconds)

Default subject:

Default message:

Trigger: {TRIGGER.NAME}
Trigger status: {TRIGGER.STATUS}
Trigger severity: {TRIGGER.SEVERITY}
Trigger URL: {TRIGGER.URL}

Item values:

Pause operations while in maintenance

Operations

Steps	Details	Start in	Duration (sec)	Action
1	Send message to user groups: Zabbix administrators via all media	Immediately	Default	Edit Remove

[New](#)

Il est possible de personnaliser les messages de notification sur Zabbix via ce menu. Il est aussi possible de définir des actions à effectuer lorsqu'un événement survient.

11 Template

11.1 Liens

<https://share.zabbix.com>

<https://github.com>

https://zabbix.org/wiki/Zabbix_Templates

11.2 Installation et mise en marche d'un template

Installation au choix d'un template parmi ceux disponibles sur les pages web indiquées ci-dessus et accompagnement de son intégration dans Zabbix.

12 Exercices

12.1 Monitoring serveur Web

Installer nginx ou apache sur une machine existante. Créer un service qui va contrôler l'état d'un serveur web. Effectuer une configuration permettant de contrôler cet état tous les jours ouvrables de 8h à 19h.

12.2 Monitoring serveur SMTP

Installer postfix sur une des machines. Via l'utilitaire telnet, contrôler que le service écoute bien sur le réseau.

Créer un service permettant de diagnostiquer le bon fonctionnement du service. Indiquer un contrôle toutes les 10 minutes.

12.3 Monitoring espace disque

Créer un service permettant d'analyser l'espace disque occupé sur la partition principale de l'hôte. Définir un warning lorsque le niveau est supérieur à 80% et critique à 90%.

12.4 Monitoring par agent Zabbix 1

Utiliser un plugin permettant d'analyser le nombre de mise à jour possibles sur un système Debian / Ubuntu. Faire la même chose sur un système Windows.

12.5 Monitoring par agent Zabbix 2

Utiliser un plugin permettant de contrôler le nombre d'utilisateur connectés sur le service. Définissez une alerte lorsqu'au moins 2 utilisateurs sont connectés en même temps.

12.6 Monitoring par agent Zabbix 3

Créer un plugin permettant de contrôler le nombre de processus d'apache (httpd) sur le serveur web à surveiller.

Faire en sorte qu'une alerte soit donnée si le nombre est plus important que 5. Rendre le contrôle opérationnel.

Indiquer ensuite un nombre plus important (plus que 5) de sous-processus Apache dans sa configuration et redémarrer Apache. Vérifier que l'alerte a bien été donnée.

12.7 Monitoring par agent Zabbix 4

Sur le serveur de Mail, configurer un plugin permettant de donner le nombre de mails en file d'attente sur postfix.

12.8 Monitoring passif 1

Créer les même services, en chargeant l'agent d'envoyer ses propres données. Ici, le serveur Zabbix pourra éviter de solliciter du temps CPU en effectuant les requêtes de supervision lui-même.

13 Autres liens Utiles

- <https://www.zabbix.com/documentation/3.2/manual/appendix/items/activepassive>
- <https://wiki.monitoring-fr.org/zabbix/zabbix-work>

14 Notes

Gestion des contrôles par Windows des cartes RAID

<https://github.com/ArtemK007/Zabbix-LSI-RAID-Monitoring>

- Effectuer le value mapping (voir fichier value_mappings.txt), dans Administration -> General
- Ajouter le template LSI_RAID_template.xml
- Ajouter les commandes Megacli nécessaires sur le serveur Windows
- Ajouter les fichiers powershell sur le serveur, ajouter le fichier windows/lsi_raid.conf dans la configuration de l'agent zabbix
- Importer le template LSI_RAID_template.xml