

1 Configuration d'une règle de découverte du réseau

Aperçu

Pour configurer une règle de découverte de réseau utilisée par Zabbix pour découvrir des hôtes et des services :

- Accédez à *Configuration* → *Découverte*
- Cliquez sur *Créer une règle* (ou sur le nom de la règle pour modifier une règle existante).
- Modifiez les attributs de la règle de découverte

Attributs de règle

Règles de découverte

* Nom	Réseau local													
Découverte par le proxy	Aucun proxy													
* Plage d'adresses IP	192.168.0.1-254													
* Intervalle d'actualisation	1h													
* Vérifications	<table><tr><td>HTTP</td><td>Édition Supprimer</td></tr><tr><td>HTTPS</td><td>Édition Supprimer</td></tr><tr><td>Ping ICMP</td><td>Édition Supprimer</td></tr><tr><td>agent Zabbix "system.username"</td><td>Édition Supprimer</td></tr><tr><td>agent SNMPv2 "1.3.6.1.2.1.1.1.0"</td><td>Édition Supprimer</td></tr><tr><td colspan="2">Nouveau</td></tr></table>		HTTP	Édition Supprimer	HTTPS	Édition Supprimer	Ping ICMP	Édition Supprimer	agent Zabbix "system.username"	Édition Supprimer	agent SNMPv2 "1.3.6.1.2.1.1.1.0"	Édition Supprimer	Nouveau	
HTTP	Édition Supprimer													
HTTPS	Édition Supprimer													
Ping ICMP	Édition Supprimer													
agent Zabbix "system.username"	Édition Supprimer													
agent SNMPv2 "1.3.6.1.2.1.1.1.0"	Édition Supprimer													
Nouveau														
Critère d'unicité de l'équipement	<table><tr><td><input checked="" type="radio"/></td><td>adresse IP</td></tr><tr><td><input type="radio"/></td><td>agent Zabbix "system.username"</td></tr><tr><td><input type="radio"/></td><td>agent SNMPv2 "1.3.6.1.2.1.1.1.0"</td></tr></table>		<input checked="" type="radio"/>	adresse IP	<input type="radio"/>	agent Zabbix "system.username"	<input type="radio"/>	agent SNMPv2 "1.3.6.1.2.1.1.1.0"						
<input checked="" type="radio"/>	adresse IP													
<input type="radio"/>	agent Zabbix "system.username"													
<input type="radio"/>	agent SNMPv2 "1.3.6.1.2.1.1.1.0"													
Activé	<input checked="" type="checkbox"/>													
<div>Ajouter Annuler</div>														

Paramètre	Description
Nom	Nom unique de la règle. Par exemple, "Réseau local".
Découverte par le proxy	Qu'est-ce qui effectue la découverte : aucun proxy - le serveur Zabbix effectue la découverte <nom du proxy> - ce proxy effectue la découverte
Plage d'adresses IP	La plage d'adresses IP pour la découverte. Elle peut avoir les formats suivants : Adresse IP unique: 192.168.1.33 Plage d'adresses IP: 192.168.1-10.1-255. La plage est limitée par le nombre total d'adresses couvertes (moins de 64 Ko). Masque IP : 192.168.4.0/24 Masques IP pris en charge : /16 - /30 pour les adresses IPv4 /112 - /128 pour les adresses IPv6 Liste : 192.168.1.1-255, 192.168.2.1-100, 192.168.2.200, 192.168.4.0/24 Depuis Zabbix 3.0.0, ce champ prend en charge les espaces, la tabulation et les lignes multiples.
Intervalle d'actualisation	Ce paramètre définit la fréquence à laquelle Zabbix exécutera la règle. L'intervalle est mesuré après la fin de l'exécution de l'instance de découverte précédente afin d'éviter tout chevauchement. Les suffixes temporels sont supportés ex : 30s, 1m, 2h, 1d, depuis Zabbix 3.4.0. Les macros utilisateurs sont supportées depuis Zabbix 3.4.0. Notez que si une macro utilisateur est utilisée et que sa valeur change (ex : 1w → 1h), la prochaine vérification sera exécutée conformément à la valeur précédente (très loin dans le futur avec les valeurs d'exemple).
Vérifications	Zabbix utilisera cette liste de vérifications pour la découverte. Vérifications supportées : SSH, LDAP, SMTP, FTP, HTTP, HTTPS, POP, NNTP, IMAP, TCP, Telnet, agent Zabbix, agent SNMPv1, agent SNMPv2, agent SNMPv3, ping ICMP. Une découverte basée sur un protocole utilise la fonctionnalité net.tcp.service[] pour tester chaque hôte, à l'exception de SNMP qui interroge un OID SNMP. L'agent Zabbix est testé en interrogeant un élément en mode non crypté. Voir les éléments de l'agent pour plus de détails. Le paramètre 'Ports' peut être l'un des suivants : Port simple : 22 Plage de ports : 22-45 Liste : 22-45,55,60-70
Critère d'unicité de l'équipement	Les critères d'unicité peuvent être : adresse IP - pas de traitement de plusieurs appareils à IP unique. Si un périphérique avec la même adresse IP existe déjà, il sera considéré comme déjà découvert et aucun nouvel hôte ne sera ajouté. Type de vérification - vérification SNMP ou agent Zabbix.
Activé	Avec la case cochée, la règle est active et sera exécutée par le serveur Zabbix. Si non cochée, la règle n'est pas active. Elle ne sera pas exécutée.

Modification du paramètre proxy

Depuis Zabbix 2.2.0, les hôtes découverts par différents proxys sont toujours traités comme des hôtes différents. Bien que cela permette d'effectuer une découverte sur les plages IP correspondantes

utilisées par différents sous-réseaux, la modification du proxy pour un sous-réseau déjà surveillé est compliquée, car les modifications du proxy doivent également être appliquées à tous les hôtes découverts. Par exemple, les étapes pour remplacer le proxy dans une règle de découverte :

1. désactiver la règle de découverte
2. configuration de la synchronisation du proxy
3. remplacer le proxy dans la règle de découverte
4. remplacer le proxy pour tous les hôtes découverts par cette règle
5. activer la règle de découverte

Scénario concret

Dans cet exemple, nous souhaiterions configurer la détection de réseau pour le réseau local ayant une plage d'adresses IP : 192.168.1.1-192.168.1.254.

Dans notre scénario, nous voulons :

- découvrir les hôtes sur lesquels l'agent Zabbix est en cours d'exécution
- lancer la découverte toutes les 10 minutes
- ajouter un hôte à la surveillance si le temps de disponibilité de l'hôte est supérieur à 1 heure
- supprimer des hôtes si le temps d'inactivité de l'hôte est supérieur à 24 heures
- ajouter des hôtes Linux au groupe "serveurs Linux"
- ajouter des hôtes Windows au groupe "serveurs Windows"
- utiliser *Template OS Linux* pour les hôtes Linux
- utiliser *Template OS Windows* pour les hôtes Windows

Étape 1

Définir une règle de découverte de réseau pour notre plage IP.

* Nom	<input type="text" value="Réseau local"/>	
Découverte par le proxy	<input type="text" value="Aucun proxy"/>	
* Plage d'adresses IP	<input type="text" value="192.168.0.1-254"/>	
* Intervalle d'actualisation	<input type="text" value="10m"/>	
* Vérifications	<div>agent Zabbix "system.uname" Édition Supprimer</div> <div>Nouveau</div>	
Critère d'unicité de l'équipement	<div><input checked="" type="radio"/> adresse IP</div> <div><input type="radio"/> agent Zabbix "system.uname"</div>	
Activé	<input checked="" type="checkbox"/>	

Zabbix essaiera de découvrir les hôtes de la plage IP 192.168.1.1-192.168.1.254 en se connectant aux agents Zabbix et en obtenant la valeur de la clé **system.uname**. La valeur reçue de l'agent peut être utilisée pour appliquer différentes actions pour différents systèmes d'exploitation. Par exemple, liez les serveurs Windows au Template OS Windows, les serveurs Linux au Template OS Linux.

La règle sera exécutée toutes les 10 minutes (600 secondes).

Lorsque cette règle est ajoutée, Zabbix lance automatiquement la découverte et génère des événements basés sur la découverte pour un traitement ultérieur.

Étape 2

Définir une [action](#) pour ajouter les serveurs Linux découverts au groupe/modèle correspondant.

Action

Opérations

* Nom

Auto discovery. Linux servers.

Type de calcul

Et/Ou

A and B and C and D

Conditions

Étiquette	Nom
A	Valeur reçue contient <i>Linux</i>
B	État de la découverte égal <i>Fonctionne</i>
C	Type de service égal <i>agent Zabbix</i>
D	Fonctionnement/Arrêt est supérieur ou égal à <i>3600</i>

Nouvelle condition

Fonctionnement/Arrêt

est supérieur ou égal à

600

Ajouter

L'action sera activée si :

- le service “agent Zabbix” est “démarré”
- la valeur de system.uname (la clé de l'agent Zabbix que nous avons utilisée dans la définition de la règle) contient “Linux”
- La disponibilité est de 1 heure (3600 secondes) ou plus

Action

Opérations

Sujet par défaut

Discovery: {DISCOVERY.DEVICE.STATUS} {DISCOVERY.DEVICE.IP}

Message par défaut

Discovery rule: {DISCOVERY.RULE.NAME}
Device IP: {DISCOVERY.DEVICE.IPADDRESS}
Device DNS: {DISCOVERY.DEVICE.DNS}
Device status: {DISCOVERY.DEVICE.STATUS}
Device uptime: {DISCOVERY.DEVICE.uptime}

Opérations

Détails

Ajouter aux groupes d'hôtes: Linux servers

Lier aux modèles: Template OS Linux

Nouveau

L'action exécutera les opérations suivantes :

- ajoute l'hôte découvert au groupe “serveurs Linux” (et ajoute également l'hôte s'il n'a pas été ajouté précédemment)
- lie l'hôte au “Template OS Linux”. Zabbix commencera automatiquement à surveiller l'hôte à l'aide d'éléments et de déclencheurs de “Template OS Linux”.

Étape 3

Définir une action pour ajouter les serveurs Windows découverts au groupe/modèle correspondant.

Action

Opérations

* Nom

Ajout de serveurs Windows découverts

Type de calcul

Et/Ou

A and B and C and D

Conditions

Étiquette	Nom
A	Valeur reçue contient <i>Windows</i>
B	État de la découverte égal <i>Fonctionne</i>
C	Type de service égal <i>agent Zabbix</i>
D	Fonctionnement/Arrêt est supérieur ou égal à 3600

Nouvelle condition

Fonctionnement/Arrêt

est supérieur ou égal à

600

[Ajouter](#)

Action

Opérations

Sujet par défaut

Discovery: {DISCOVERY.DEVICE.STATUS} {DISCOVERY.DEVICE.IPADDRESS}

Message par défaut

Discovery rule: {DISCOVERY.RULE.NAME}
Device IP: {DISCOVERY.DEVICE.IPADDRESS}
Device DNS: {DISCOVERY.DEVICE.DNS}
Device status: {DISCOVERY.DEVICE.STATUS}
Device uptime: {DISCOVERY.DEVICE.uptime}

Opérations

Détails

Ajouter aux groupes d'hôtes: Serveurs Windows

Lier aux modèles: Template OS Windows

[Nouveau](#)

Étape 4

Définir une action pour supprimer les serveurs perdus.

Action

Opérations

* Nom

Suppression des serveurs obsolètes

Type de calcul

Et/Ou (A or B) and C and D

Conditions

Étiquette	Nom
A	Fonctionnement/Arrêt est supérieur ou égal à 86400
B	Fonctionnement/Arrêt est supérieur ou égal à 600
C	État de la découverte égal Arrêté
D	Type de service égal agent Zabbix

Nouvelle condition

Type de service

égal

FTP

[Ajouter](#)

Action

Opérations

Sujet par défaut

Discovery: {DISCOVERY.DEVICE.STATUS} {DISCOVERY.DEVICE.IPADDRE

Message par défaut

Discovery rule: {DISCOVERY.RULE.NAME}
Device IP: {DISCOVERY.DEVICE.IPADDRESS}
Device DNS: {DISCOVERY.DEVICE.DNS}
Device status: {DISCOVERY.DEVICE.STATUS}
Device uptime: {DISCOVERY.DEVICE.uptime}

Opérations

Détails	Action
Supprimer l'hôte	Édition Supprimer
Nouveau	

* Au moins une opération doit exister.

Actualiser

Clone

Supprimer

Annuler

Un serveur sera supprimé si le service "Agent Zabbix" est 'arrêté' pendant plus de 24 heures (86400 secondes).

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

Permanent link:
https://www.zabbix.com/documentation/4.0/fr/manual/discovery/network_discovery/rule

Last update: 2019/03/26 12:41

