

## Configuring a network discovery rule

### Overview

To configure a network discovery rule used by Zabbix to discover hosts and services:

- Go to *Configuration* → *Discovery*
- Click on *Create rule* (or on the rule name to edit an existing one)
- Edit the discovery rule attributes

### Rule attributes

### Discovery rules

Name

Discovery by proxy

IP range

Delay (in sec)

Checks

ICMP ping	<a href="#">Edit</a> <a href="#">Remove</a>
SNMPv2 agent "1.3.6.1.2.1.1.1.0"	<a href="#">Edit</a> <a href="#">Remove</a>
Zabbix agent "system.uname"	<a href="#">Edit</a> <a href="#">Remove</a>
<a href="#">New</a>	

Device uniqueness criteria

IP address

SNMPv2 agent "1.3.6.1.2.1.1.1.0"

Zabbix agent "system.uname"

Enabled

Parameter	Description
<i>Name</i>	Unique name of the rule. For example, "Local network".

Parameter	Description
<i>Discovery by proxy</i>	What performs discovery: <b>no proxy</b> - Zabbix server is doing discovery <b>&lt;proxy name&gt;</b> - this proxy performs discovery
<i>IP range</i>	The range of IP addresses for discovery. It may have the following formats: Single IP: 192.168.1.33 Range of IP addresses: 192.168.1-10.1-255. The range is limited by the total number of covered addresses (less than 64K). IP mask: 192.168.4.0/24 supported IP masks: /16 - /30 for IPv4 addresses /112 - /128 for IPv6 addresses List: 192.168.1.1-255, 192.168.2.1-100, 192.168.2.200, 192.168.4.0/24 Since Zabbix 3.0.0 this field supports spaces, tabulation and multiple lines.
<i>Delay (in sec)</i>	This parameter defines how often Zabbix will execute the rule. Delay is measured after the execution of previous discovery instance ends so there is no overlap.
<i>Checks</i>	Zabbix will use this list of checks for discovery. Supported checks: SSH, LDAP, SMTP, FTP, HTTP, HTTPS, POP, NNTP, IMAP, TCP, Telnet, Zabbix agent, SNMPv1 agent, SNMPv2 agent, SNMPv3 agent, ICMP ping. A protocol-based discovery uses the <b>net.tcp.service[]</b> functionality to test each host, except for SNMP which queries an SNMP OID. Zabbix agent is tested by querying an item in unencrypted mode. Please see <a href="#">agent items</a> for more details. The 'Ports' parameter may be one of following: Single port: 22 Range of ports: 22-45 List: 22-45,55,60-70
<i>Device uniqueness criteria</i>	Uniqueness criteria may be: <b>IP address</b> - no processing of multiple single-IP devices. If a device with the same IP already exists it will be considered already discovered and a new host will not be added. <b>Type of discovery check</b> - either SNMP or Zabbix agent check.
<i>Enabled</i>	With the check-box marked the rule is active and will be executed by Zabbix server. If unmarked, the rule is not active. It won't be executed.

## Changing proxy setting

Since Zabbix 2.2.0 the hosts discovered by different proxies are always treated as different hosts. While this allows to perform discovery on matching IP ranges used by different subnets, changing proxy for an already monitored subnet is complicated because the proxy changes must be also applied to all discovered hosts. For example the steps to replace proxy in a discovery rule:

1. disable discovery rule
2. sync proxy configuration
3. replace the proxy in the discovery rule
4. replace the proxy for all hosts discovered by this rule
5. enable discovery rule

## A real life scenario

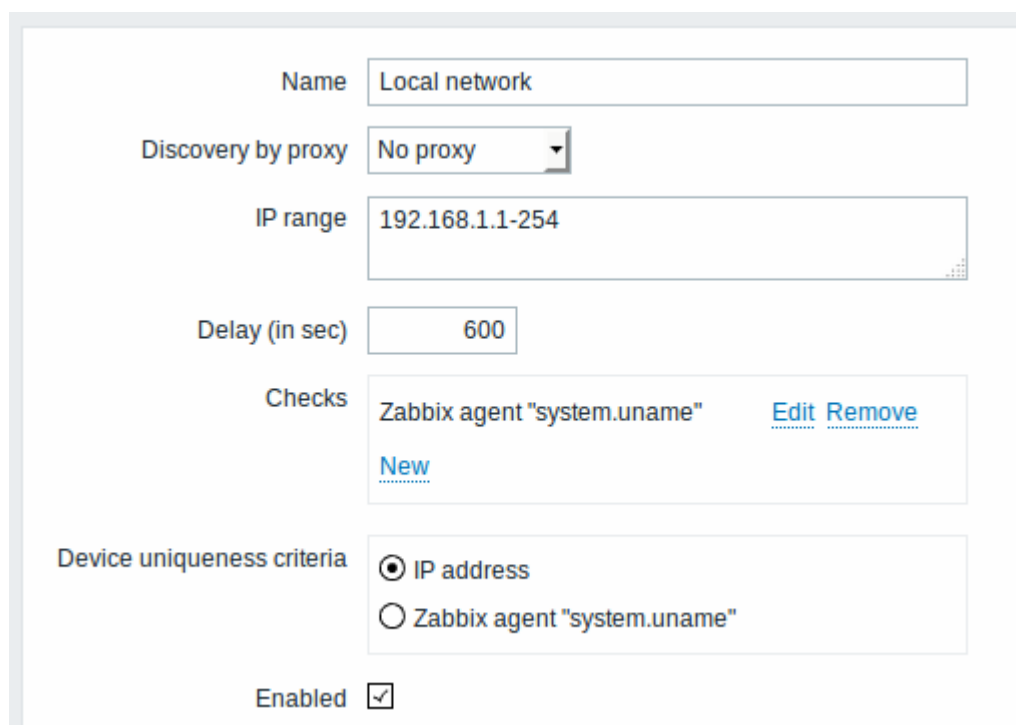
In this example we would like to set up network discovery for the local network having an IP range of 192.168.1.1-192.168.1.254.

In our scenario we want to:

- discover those hosts that have Zabbix agent running
- run discovery every 10 minutes
- add a host to monitoring if the host uptime is more than 1 hour
- remove hosts if the host downtime is more than 24 hours
- add Linux hosts to the "Linux servers" group
- add Windows hosts to the "Windows servers" group
- use *Template OS Linux* for Linux hosts
- use *Template OS Windows* for Windows hosts

### Step 1

Defining a network discovery rule for our IP range.



The screenshot shows the configuration form for a network discovery rule in Zabbix. The fields are as follows:

- Name:** Local network
- Discovery by proxy:** No proxy
- IP range:** 192.168.1.1-254
- Delay (in sec):** 600
- Checks:** Zabbix agent "system.username" (with [Edit](#) and [Remove](#) links) and [New](#) link.
- Device uniqueness criteria:**  IP address,  Zabbix agent "system.username"
- Enabled:**

Zabbix will try to discover hosts in the IP range of 192.168.1.1-192.168.1.254 by connecting to Zabbix agents and getting the value from **system.username** key. The value received from the agent can be used to apply different actions for different operating systems. For example, link Windows servers to Template OS Windows, Linux servers to Template OS Linux.

The rule will be executed every 10 minutes (600 seconds).

When this rule is added, Zabbix will automatically start the discovery and generating discovery-based events for further processing.

## Step 2

Defining an [action](#) for adding the discovered Linux servers to the respective group/template.

The screenshot shows the 'Action' configuration page in Zabbix, with the 'Operations' tab selected. The configuration is as follows:

- Name:** Add discovered Linux servers
- Type of calculation:** And/Or (A and B and C and D)
- Conditions:**

Label	Name
A	Received value like <i>Linux</i>
B	Discovery status = <i>Up</i>
C	Service type = <i>Zabbix agent</i>
D	Uptime/Downtime >= 3600
- New condition:** Uptime/Downtime >= 3600
- Add:** [Add](#)

The action will be activated if:

- the “Zabbix agent” service is “up”
- the value of system.uname (the Zabbix agent key we used in rule definition) contains “Linux”
- Uptime is 1 hour (3600 seconds) or more

The screenshot shows the 'Action' configuration page in Zabbix, with the 'Operations' tab selected. The configuration is as follows:

- Default subject:** Discovery: {DISCOVERY.DEVICE.STATUS} {DISCOVERY.DEVI
- Default message:** 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}  
Device service name: {DISCOVERY.SERVICE.NAME}
- Operations:**
  - Details**
  - Add to host groups:** Linux servers
  - Link to templates:** Template OS Linux

The action will execute the following operations:

- add the discovered host to the “Linux servers” group (and also add host if it wasn't added previously)

- link host to the “Template OS Linux” template. Zabbix will automatically start monitoring the host using items and triggers from “Template OS Linux”.

### Step 3

Defining an action for adding the discovered Windows servers to the respective group/template.

**Action** **Operations**

Name: Add discovered Windows servers

Type of calculation: And/Or A and B and C and D

Label	Name
A	Received value like <i>Windows</i>
B	Discovery status = <i>Up</i>
C	Service type = <i>Zabbix agent</i>
D	Uptime/Downtime >= 3600

New condition: Uptime/Downtime >= 3600

[Add](#)

**Action** **Operations**

Default subject: Discovery: {DISCOVERY.DEVICE.STATUS} {DISCOVERY.DEVI}

Default message: 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}  
Device service name: {DISCOVERY.SERVICE.NAME}

Operations: Details  
**Add to host groups:** Windows servers  
**Link to templates:** Template OS Windows

### Step 4

Defining an action for removing lost servers.

**Action** **Operations**

Name:

Type of calculation:  A and B and C

Conditions	Label	Name
	A	Uptime/Downtime >= 86400
	B	Discovery status = Down
	C	Service type = Zabbix agent

**Action** **Operations**

Default subject:

Default message:   
Device IP: {DISCOVERY.DEVICE.IPADDRESS}  
Device DNS: {DISCOVERY.DEVICE.DNS}  
Device status: {DISCOVERY.DEVICE.STATUS}  
Device uptime: {DISCOVERY.DEVICE.UPTIME}  
Device service name: {DISCOVERY.SERVICE.NAME}

Operations	Details	Action
	<b>Remove host</b>	<a href="#">Edit</a> <a href="#">Remove</a>

A server will be removed if “Zabbix agent” service is 'down' for more than 24 hours (86400 seconds).

From: <https://www.zabbix.com/documentation/3.2/> - **Zabbix Documentation 3.2**

Permanent link: [https://www.zabbix.com/documentation/3.2/manual/discovery/network\\_discovery/rule](https://www.zabbix.com/documentation/3.2/manual/discovery/network_discovery/rule)

Last update: **2016/04/07 12:22**

