

1 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

* Name

Discovery by proxy

* IP range

* Update interval

* Checks

SNMPv2 agent "iso.3.6.1.2.1.1.1.0" [Edit](#) [Remove](#)

[New](#)

Check type

* Port range

* SNMP community

* SNMP OID

[Update](#) [Cancel](#)

Device uniqueness criteria

IP address

SNMPv2 agent "iso.3.6.1.2.1.1.1.0"

Host name

DNS name

IP address

SNMPv2 agent "iso.3.6.1.2.1.1.1.0"

Visible name

Host name

DNS name

IP address

SNMPv2 agent "iso.3.6.1.2.1.1.1.0"

Enabled

Parameter	Description
Name	Unique name of the rule. For example, "Local network".

Parameter	Description
<i>Discovery by proxy</i>	What performs discovery: no proxy - Zabbix server is doing discovery <proxy name> - 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>Update interval</i>	This parameter defines how often Zabbix will execute the rule. The interval is measured after the execution of previous discovery instance ends so there is no overlap. Time suffixes are supported, e.g. 30s, 1m, 2h, 1d, since Zabbix 3.4.0. User macros are supported, since Zabbix 3.4.0. Note that if a user macro is used and its value is changed (e.g. 1w → 1h), the next check will be executed according to the previous value (far in the future with the example values).
<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 net.tcp.service[] 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 agent items 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: IP address - 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. <discovery check> - either Zabbix agent or SNMP agent check.
<i>Host name</i>	Set the technical host name of a created host using: DNS name - DNS name (default) IP address - IP address <discovery check> - received string value of the discovery check (e.g. Zabbix agent, SNMP agent check) See also: Host naming . This option is supported since 4.2.0.
<i>Visible name</i>	Set the visible host name of a created host using: Host name - technical host name (default) DNS name - DNS name IP address - IP address <discovery check> - received string value of the discovery check (e.g. Zabbix agent, SNMP agent check) See also: Host naming . This option is supported since 4.2.0.

Parameter	Description
<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.

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 interface for a network discovery rule in Zabbix. The form includes the following fields and options:

- Name:** Local network
- Discovery by proxy:** No proxy
- IP range:** 192.168.1.1-254
- Update interval:** 10m
- Checks:** Zabbix agent "system.uname" (with [Edit](#) and [Remove](#) links) and [New](#) link.
- Device uniqueness criteria:** IP address, Zabbix agent "system.uname"
- Host name:** DNS name, IP address, Zabbix agent "system.uname"
- Visible name:** Host name, DNS name, IP address, Zabbix agent "system.uname"
- 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 the **system.uname** key. The value received from the agent can be used to name the hosts and also 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.

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.

* 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 >= 600 [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

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

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
[New](#)

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

Type of calculation 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

[Add](#)

Action **Operations**

Default subject

Default message

Operations
Add to host groups: Windows servers
Link to templates: Template OS Windows
[New](#)

Step 4

Defining an action for removing lost servers.

Action **Operations**

* Name

Type of calculation A and B and C

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

New condition =

[Add](#)

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
Remove host		Edit Remove
New		

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

From: <https://www.zabbix.com/documentation/4.2/> - **Zabbix Documentation 4.2**

Permanent link: https://www.zabbix.com/documentation/4.2/manual/discovery/network_discovery/rule

Last update: **2019/03/11 12:35**

