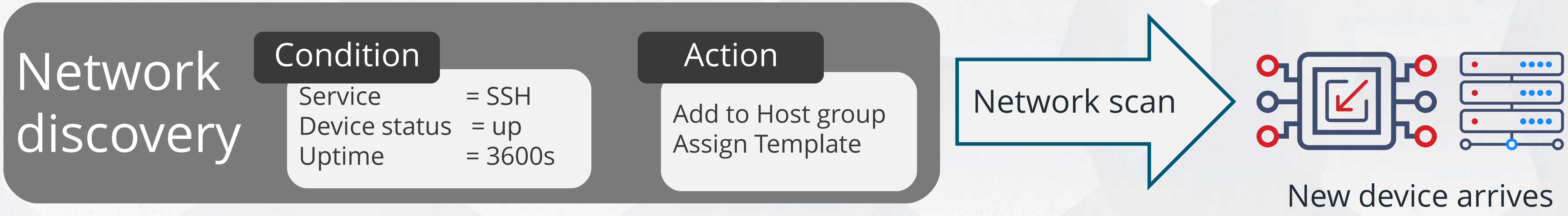
Network Discovery

30 minutes

NETWORK DISCOVERY

Zabbix offers network discovery functionality that is effective and very flexible.

- Speeds up deployment:
  - ✓ Scans the network segments to detect monitored services
  - ✓ Gets the templates assigned based on discovery results
- Makes administration easier:
  - ✓ Discovery actions will be performed automatically
- Supports dynamic environments:
  - ✓ Hosts are created or removed automatically based on discovery results



Network discovery

Condition

Service = SSH
Device status = up
Uptime = 3600s

Action

Add to Host group
Assign Template

Network scan

New device arrives

https://www.zabbix.com/documentation/6.0/manual/discovery/network_discovery

NETWORK DISCOVERY - HOW IT WORKS

- Zabbix periodically scans IP ranges defined in the network discovery rule:
  - ✓ Scanning frequency is configurable for each rule individually
  - ✓ For each rule, one or multiple checks can be defined
    - Zabbix agent ,SNMP, TCP port etc.

- Once a host or a service is discovered, a discovery event (or several events) are generated:
  - ✓ Discovered Service/host is discovered for the first time or is up after a downtime
  - ✓ Lost Service/host is down after being up
  - ✓ Up Every time service/host is detected
  - ✓ Down Every time the service host cannot be detected

- Based on events, one or multiple discovery actions are executed:
  - ✓ Create / Remove host
  - ✓ Add / Remove from a host group
  - ✓ Link / Unlink Template
  - ✓ Send message

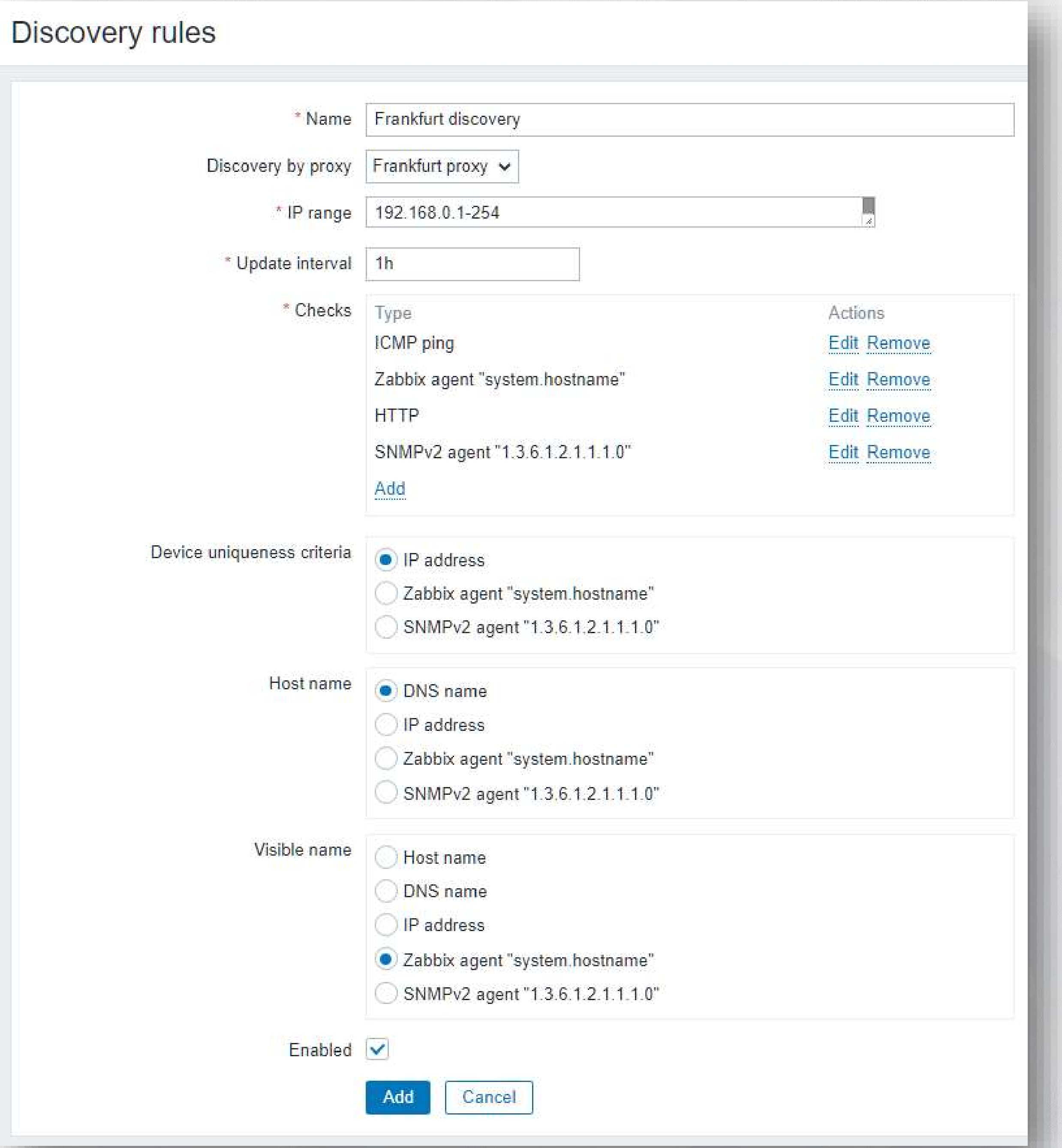
DISCOVERY CONFIGURATION

Creation of New Discovery rule:

- Name
- Proxy
- IP ranges
  - ✓ Comma separated list
  - ✓ CIDR notation supported
- Update interval
- Device uniqueness criteria
- Hostname
- Visible name

Checks:

- Information from Zabbix agent
- Information from SNMP
- Availability of external services
  - ✓ FTP, SSH, WEB, POP3, IMAP, TCP, etc.



Discovery rules

* Name	Frankfurt discovery
Discovery by proxy	Frankfurt proxy
* IP range	192.168.0.1-254
* Update interval	1h

* Checks

Type	Actions
ICMP ping	Edit Remove
Zabbix agent "system.hostname"	Edit Remove
HTTP	Edit Remove
SNMPv2 agent "1.3.6.1.2.1.1.1.0"	Edit Remove

Add

Device uniqueness criteria
- ● IP address
- ○ Zabbix agent "system.hostname"
- ○ SNMPv2 agent "1.3.6.1.2.1.1.1.0"

Host name
- ● DNS name
- ○ IP address
- ○ Zabbix agent "system.hostname"
- ○ SNMPv2 agent "1.3.6.1.2.1.1.1.0"

Visible name
- ○ Host name
- ○ DNS name
- ○ IP address
- ● Zabbix agent "system.hostname"
- ○ SNMPv2 agent "1.3.6.1.2.1.1.1.0"

Enabled ☑

HOW NETWORK DISCOVERY WORKS

- Each time a service is detected as Up or Down, new events are generated:
  - ✓ Events are generated for a host and additionally for each service
  - ✓ Normally only "Up" or "Down" events are generated
  - ✓ "Discovered" + "Up" and "Lost" + "Down" events are generated when discovery status changes

- Discovery rule looks for both HTTP and SSH services in the example below:

	Host events			Service events					
		WEB server			HTTP service events			SSH service events	
At least one service up	1	Discovered	Up	1	Discovered	Up	1	Discovered	Up
	1		Up	0	Lost	Down	1		Up
	1		Up	1	Discovered	Up	1		Up
All services down	0	Lost	Down	0	Lost	Down	0	Lost	Down
	0		Down	0		Down	0		Down
At least one service up	1	Discovered	Up	0		Down	1	Discovered	Up
	1		Up	1	Discovered	Up	1		Up

UPTIME AND DOWNTIME

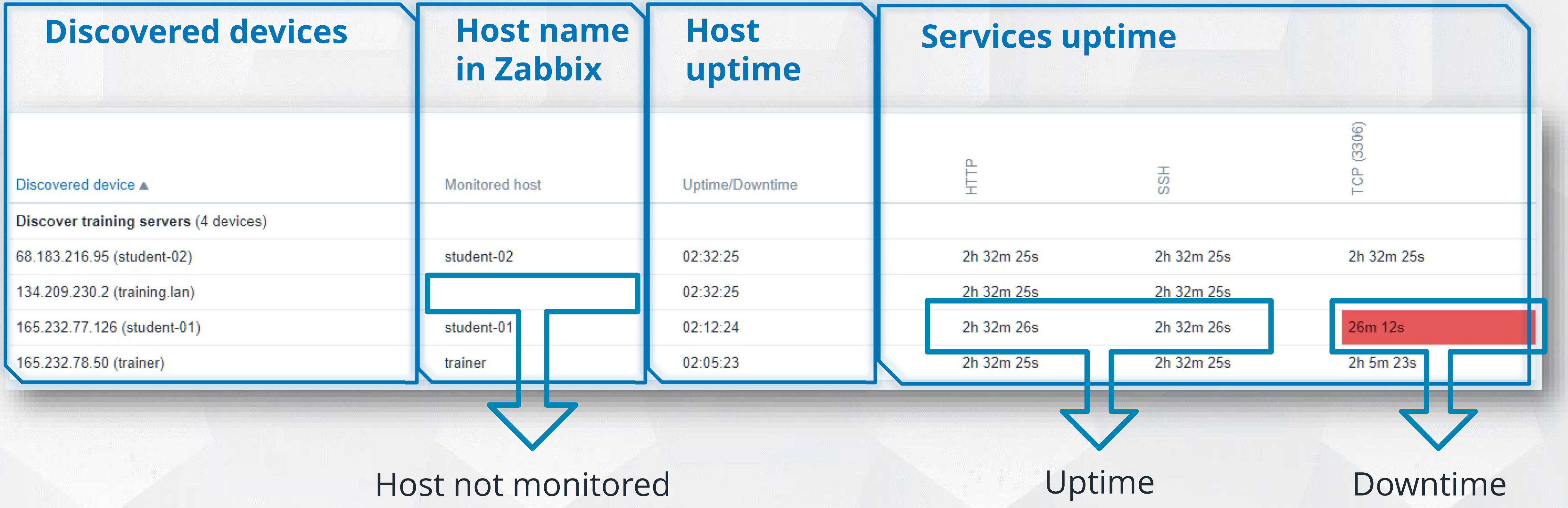
- Uptime/Downtime column shows the time when the device was:
  - Discovered for uptime
  - Lost for downtime
- Every time the discovery status changes, the time is reset to 00:00:00
  - The same counter is used for Uptime and Downtime

- Example - discovery rule is running every 15 minute

	WEB server		Time	Type
1	Discovered	Up	00:00:00	Uptime
1		Up	00:15:00	Uptime
1		Up	00:30:00	Uptime
0	Lost	Down	00:00:00	Downtime
0		Down	00:15:00	Downtime
1	Discovered	Up	00:00:00	Uptime
1		Up	00:15:00	Uptime

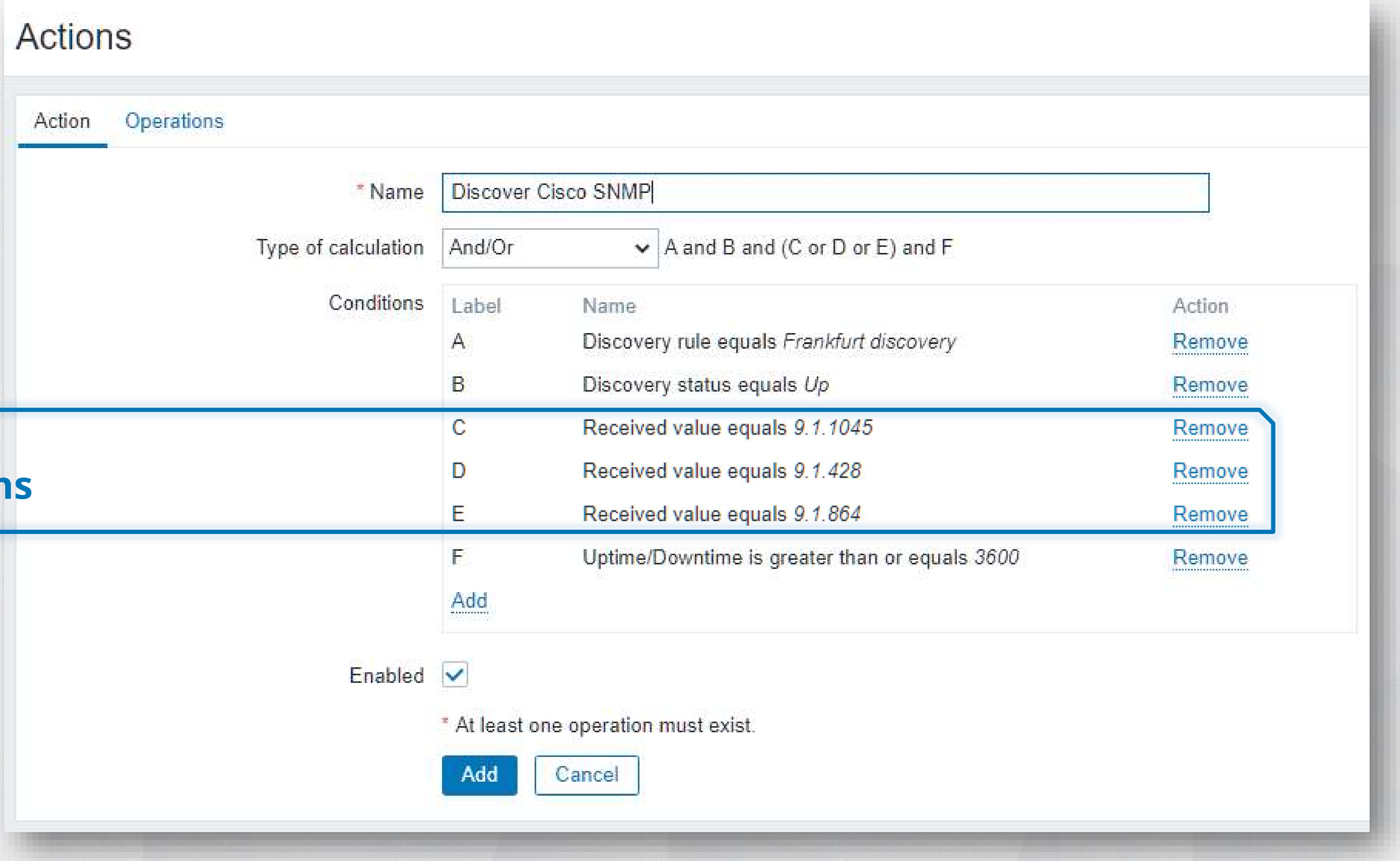
VIEW DISCOVERY STATE

- Monitoring > Discovery section displays discovery results:
  - ✓ Discovered devices
  - ✓ IP address
  - ✓ Whether it is already monitored
  - ✓ Uptime/Downtime
  - ✓ Individual service states



Discovered device ▲	Monitored host	Uptime/Downtime	HTTP	SSH	TCP (3306)
Discover training servers (4 devices)					
68.183.216.95 (student-02)	student-02	02:32:25	2h 32m 25s	2h 32m 25s	2h 32m 25s
134.209.230.2 (training.lan)		02:32:25	2h 32m 25s	2h 32m 25s	
165.232.77.126 (student-01)	student-01	02:12:24	2h 32m 26s	2h 32m 26s	26m 12s
165.232.78.50 (trainer)	trainer	02:05:23	2h 32m 25s	2h 32m 25s	2h 5m 23s

Discovery actions react to the events with the source "Discovery"



* Name: Discover Cisco SNMP

Type of calculation: And/Or A and B and (C or D or E) and F

Conditions

Label	Name	Action
A	Discovery rule equals *Frankfurt discovery*	Remove
B	Discovery status equals *Up*	Remove
C	Received value equals *9.1.1045*	Remove
D	Received value equals *9.1.428*	Remove
E	Received value equals *9.1.864*	Remove
F	Uptime/Downtime is greater than or equals *3600*	Remove
Add		

Enabled ☑

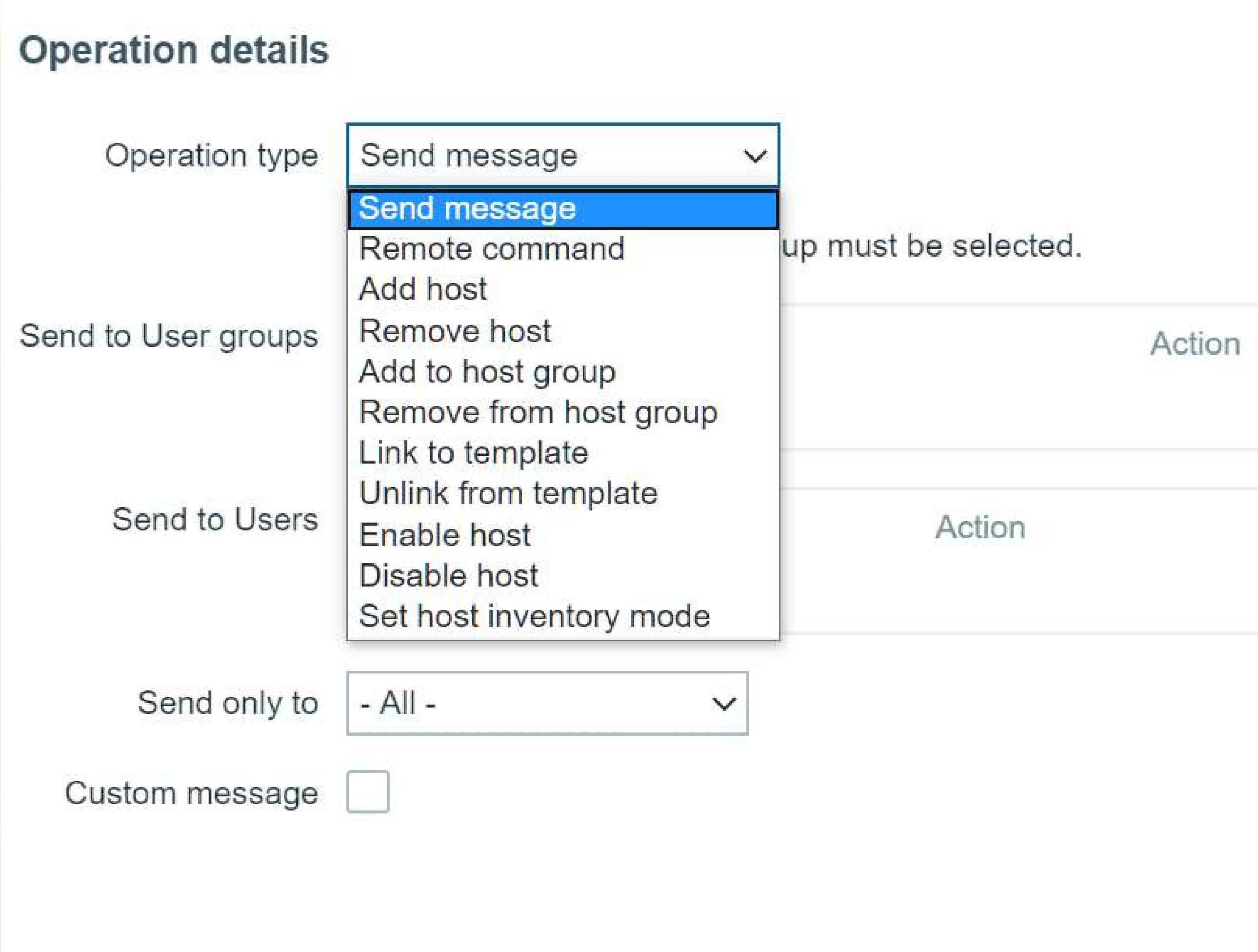
* At least one operation must exist.

Device matches
one of the specified patterns

ACTION OPERATIONS - DISCOVERY

Configuration > Actions > Discovery

- Add/Remove host
- Assign/Unassign host group
- Link/Unlink templates
- Send message:
  - ✓ To user
  - ✓ To user group
- Remote command:
  - ✓ On Zabbix server, agent or proxy
  - ✓ On a current or another host
- Enable/Disable host
- Set host inventory mode:
  - ✓ Automatic, manual or disabled
  - ✓ This overrides global inventory mode



Operation details

Operation type: Send message

up must be selected.

Send to User groups

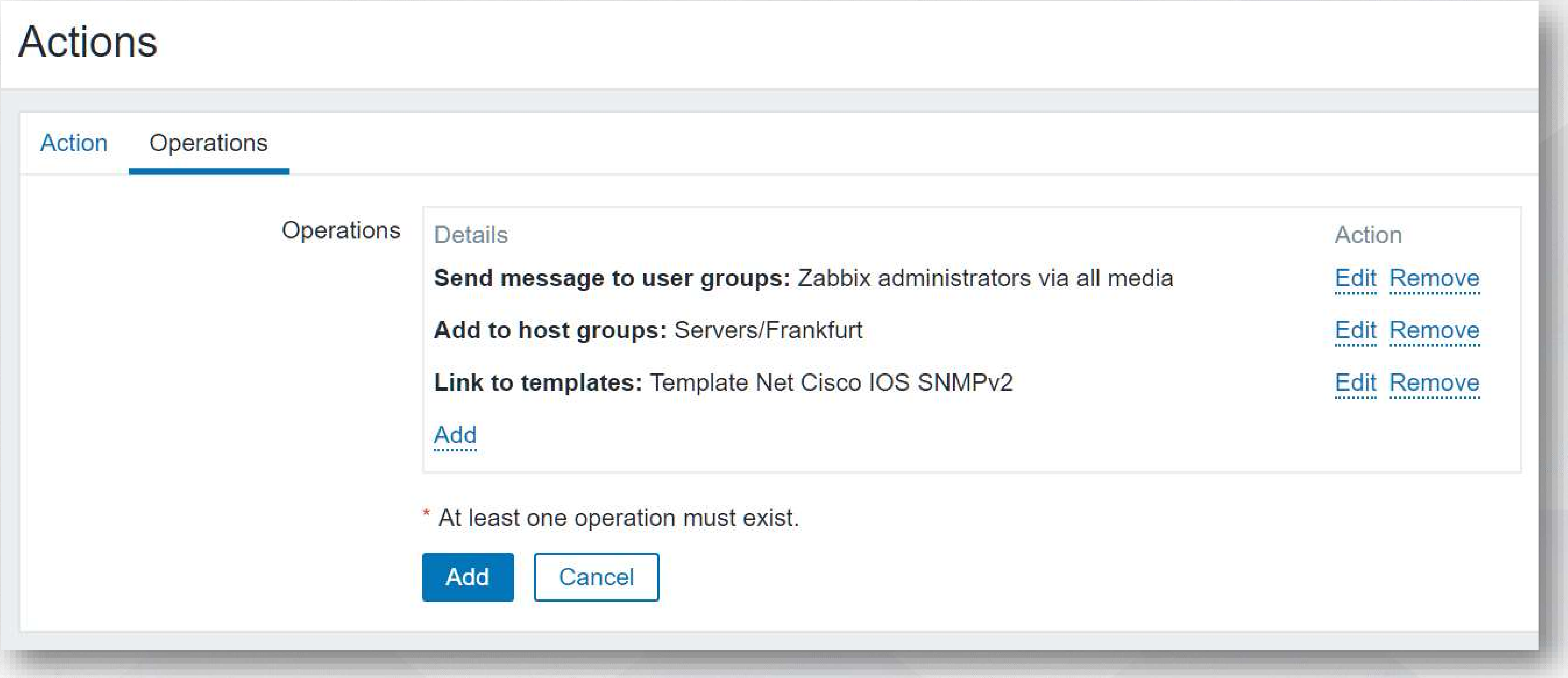
Send to Users

Send only to: - All -

Custom message □

Multiple operation steps:

- All the steps are executed at the same time



Actions

Operations

Details	Action
Send message to user groups: Zabbix administrators via all media	Edit Remove
Add to host groups: Servers/Frankfurt	Edit Remove
Link to templates: Template Net Cisco IOS SNMPv2	Edit Remove
Add	

* At least one operation must exist.

```
There is no option to control step execution order!
```

BEST PRACTICES & LIMITATIONS

Suggested:

- Do not add/remove hosts immediately - use Uptime/Downtime
- Use data received from Zabbix agent/SNMP to link to different templates
- Use reasonable update interval
- Smaller network segments are more reliable than the big ones - they are scanned faster
- Set number of discoverer processes equal to the amount of discovery rules
  - ✓ Number of processes is defined in configuration files with StartDiscoverers= option
  - ✓ If discovery is performed by proxy, the discoverer processes must be started on proxy
- Timeout setting of a server/proxy affects the speed of discovery
  - ✓ With long timeouts Zabbix will wait longer for nonresponsive checks

Limitations:

- No discovery of a network topology
- Encryption is not supported by a network discovery