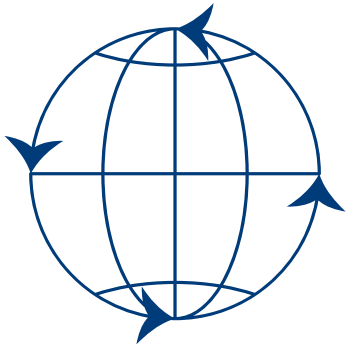
Monitoring a dual homed device with Zabbix

Zabbix BeNeLux conference 2020

whoami

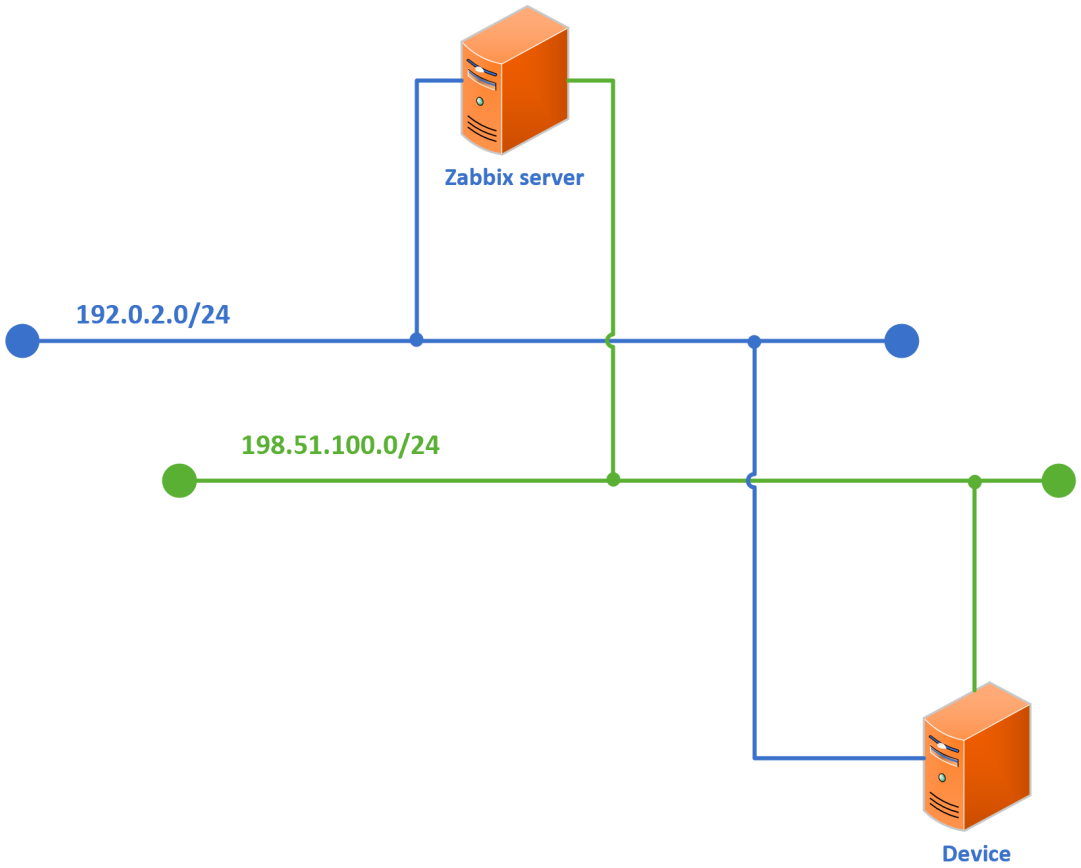
Brian van Baekel

- Zabbix consultant
- Zabbix trainer
- Network engineer



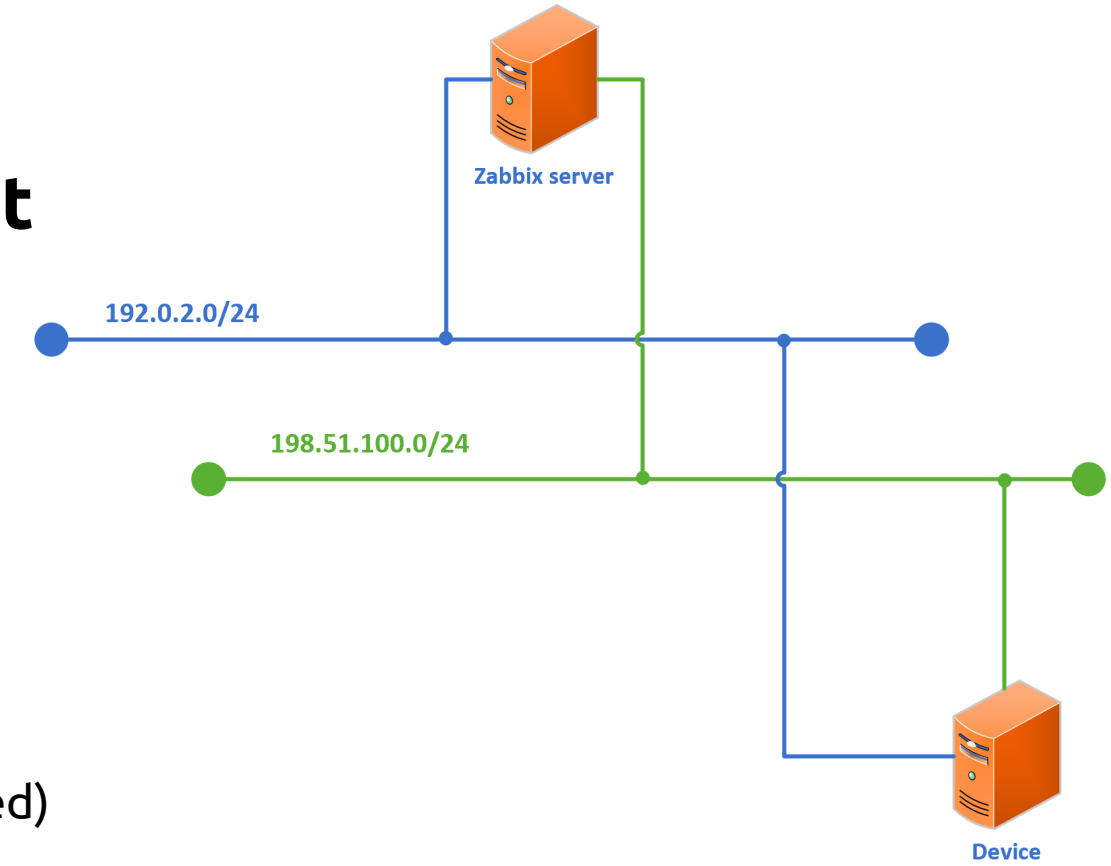
Opensource ICT Solutions

Introduction



The problem

“Monitor the device in such a way that the monitoring is redundant”



Zabbix server: fully redundant. 2 interfaces per LAN (bonded)

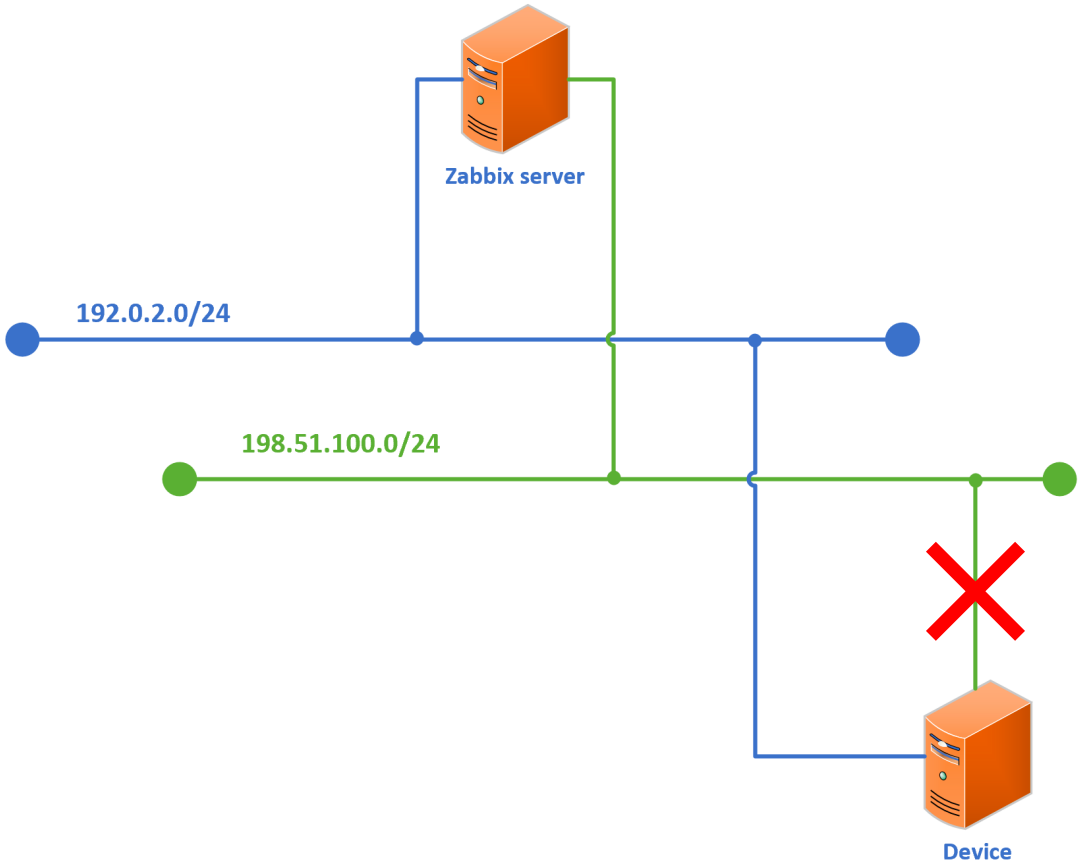
Device: Single interfaces per lan

Network: Separated; no connections, no routers.

The problem

We are monitoring over the blue network.

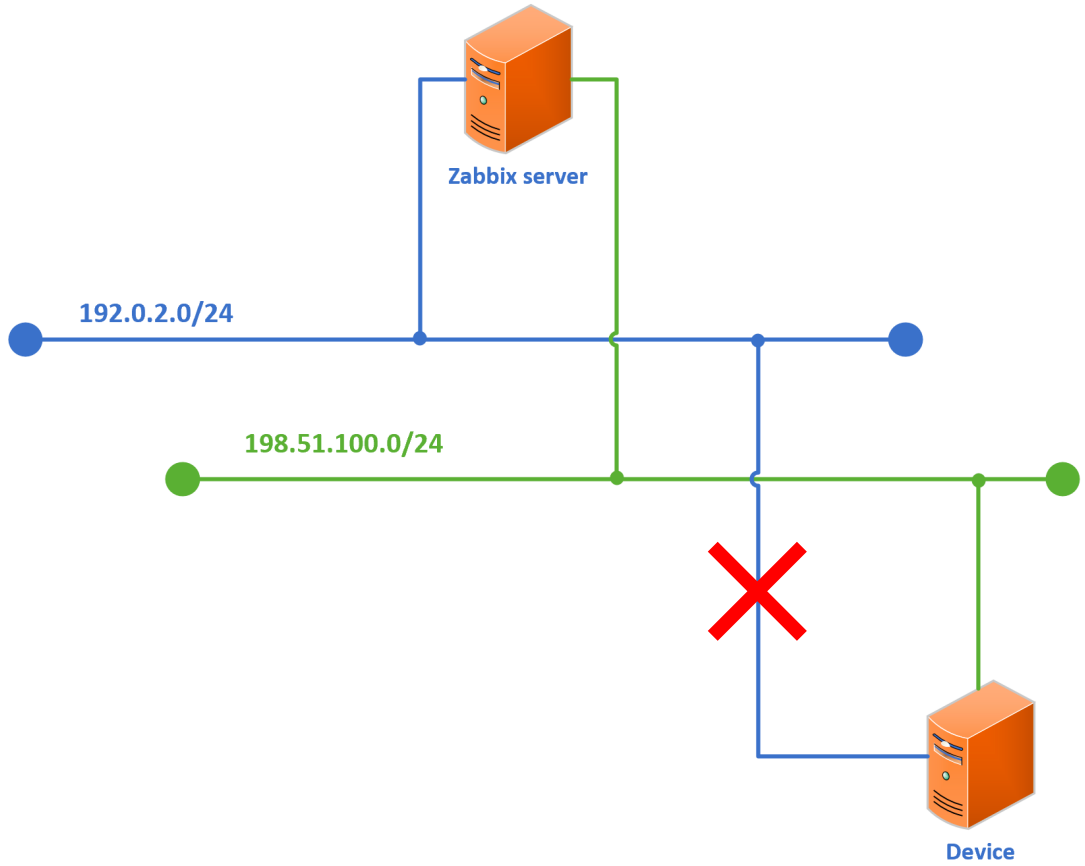
-> Green network goes down, no problem.



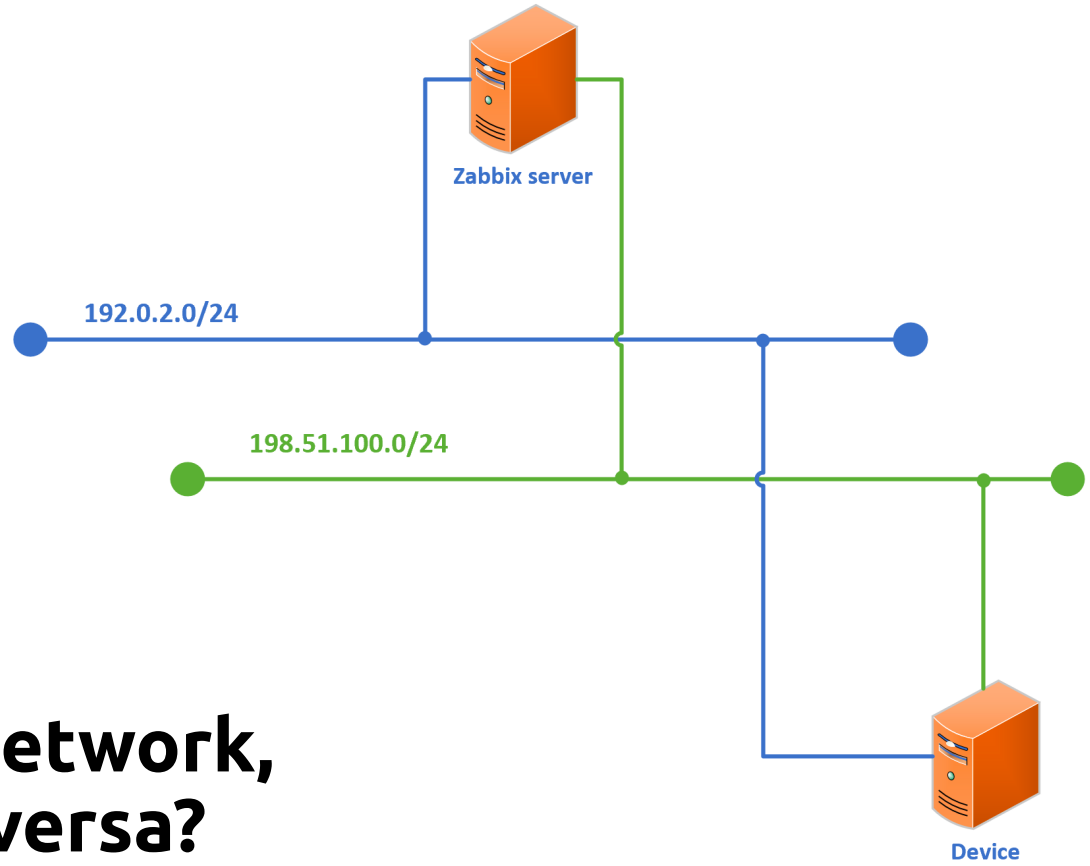
The problem

We are monitoring over the blue network.

-> Blue network goes down, monitoring is gone.

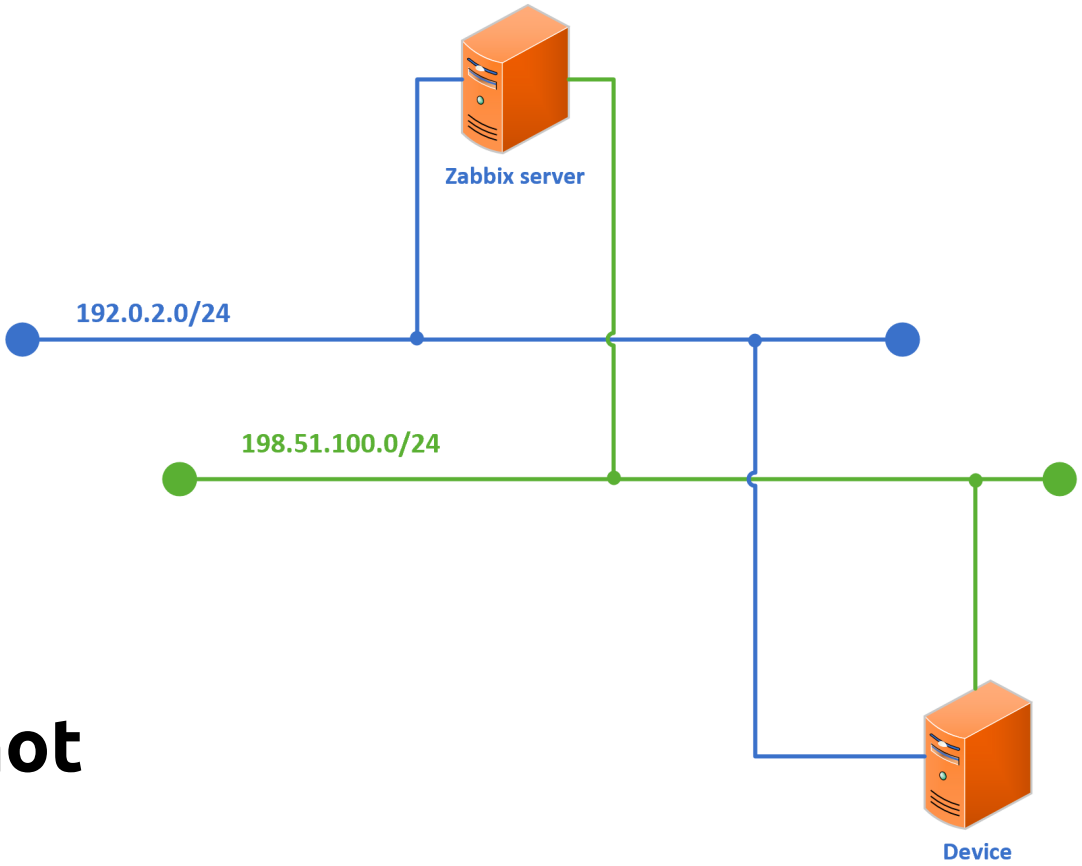


The question



How to tell Zabbix to use the green network, if the blue network is down and vice versa?

The Challenge



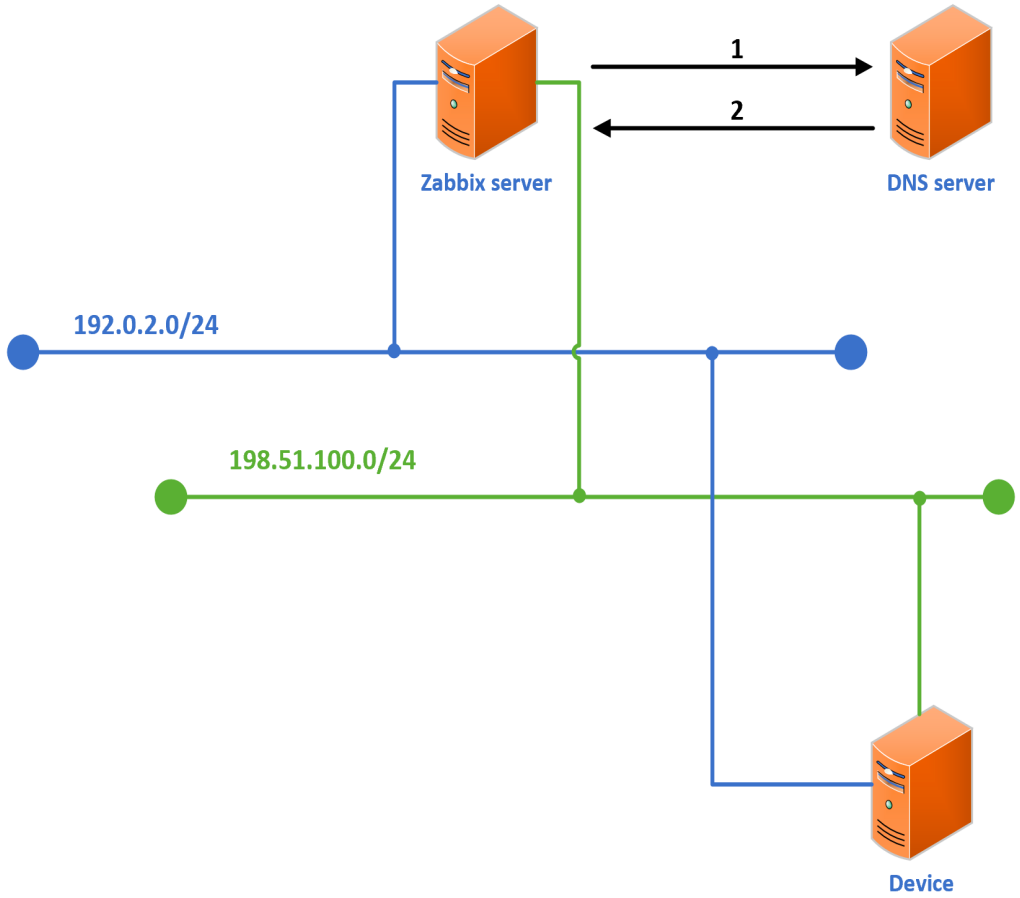
Monitoring based on IP address will not work

The fix

DNS + some custom scripts.

The fix

We start monitoring a device using it's DNS name instead of IP address

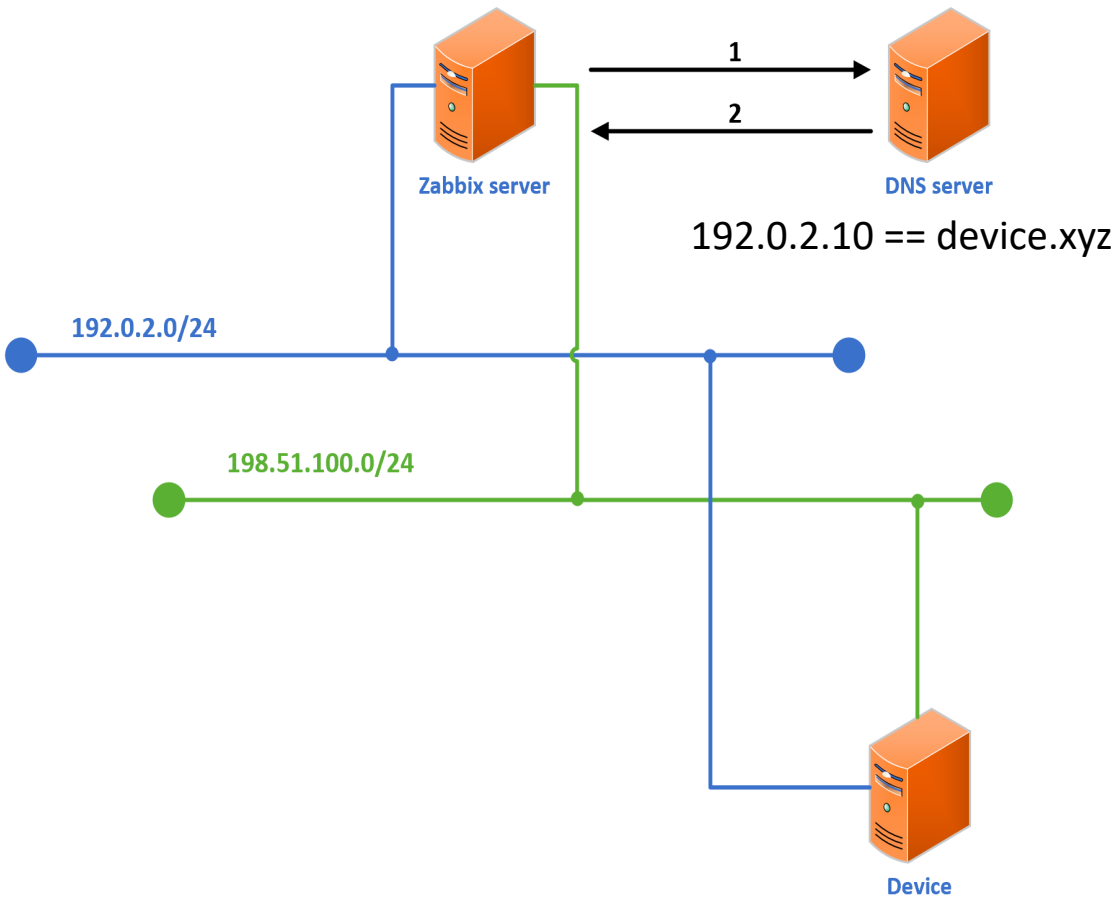


The fix

Item must be polled:

1: Request ip of device.xyz

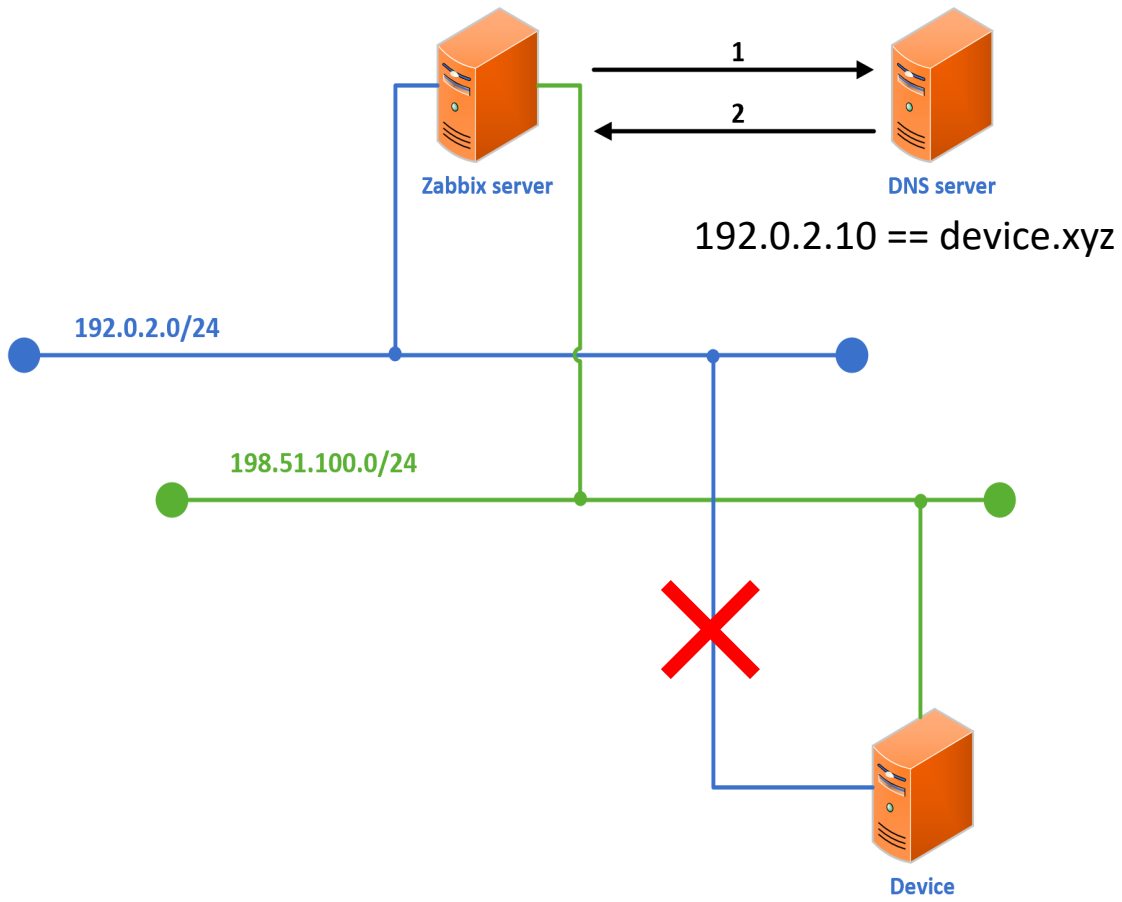
2: device.xyz = 192.0.2.10



Monitoring happens over the blue network.

The fix

What if the blue network is down?



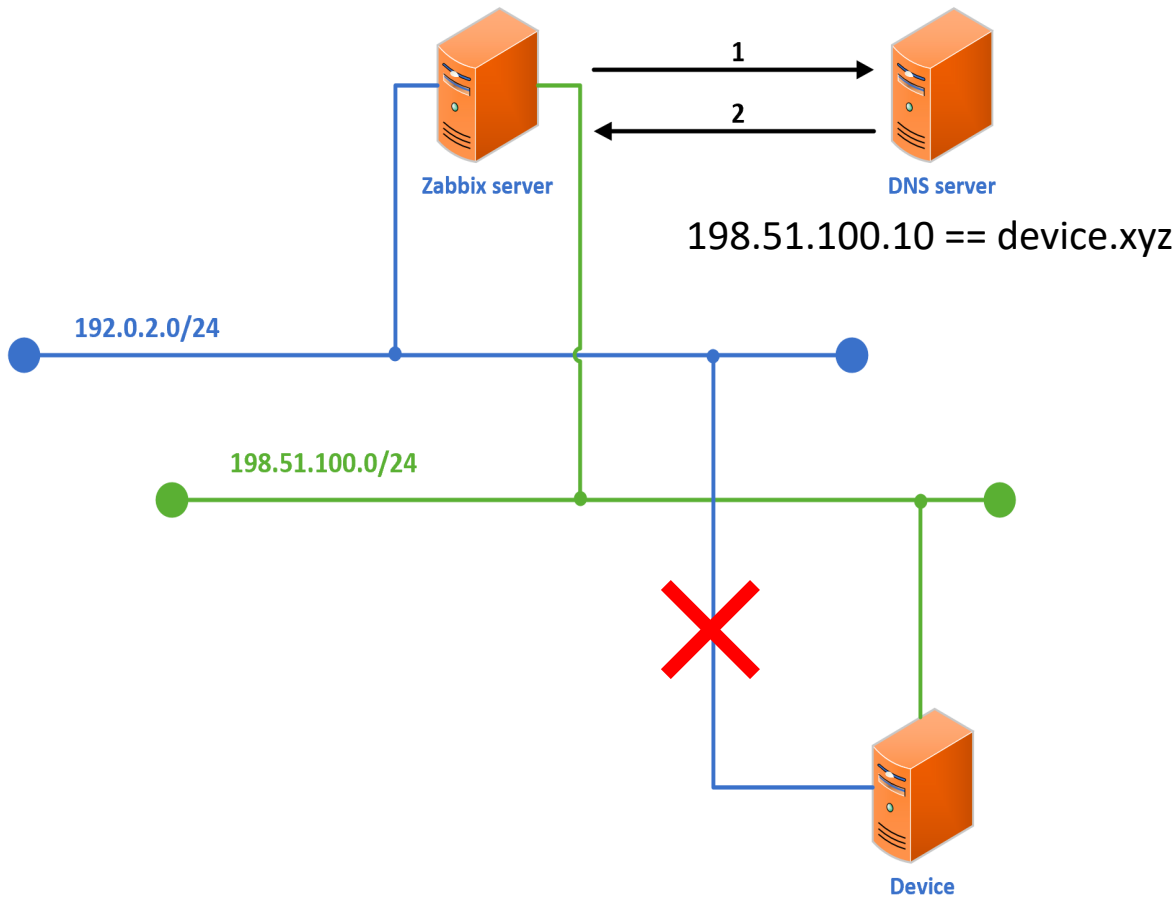
- Create a ‘keepalive’ item on the host with a trigger on it.
- If that trigger goes into problem state, fire an action: change DNS record

The fix

If trigger ‘device keepalive is in problem state, execute remote command:

python dnschange.py {blue ip} {green ip}

- API call to dns server to edit entry



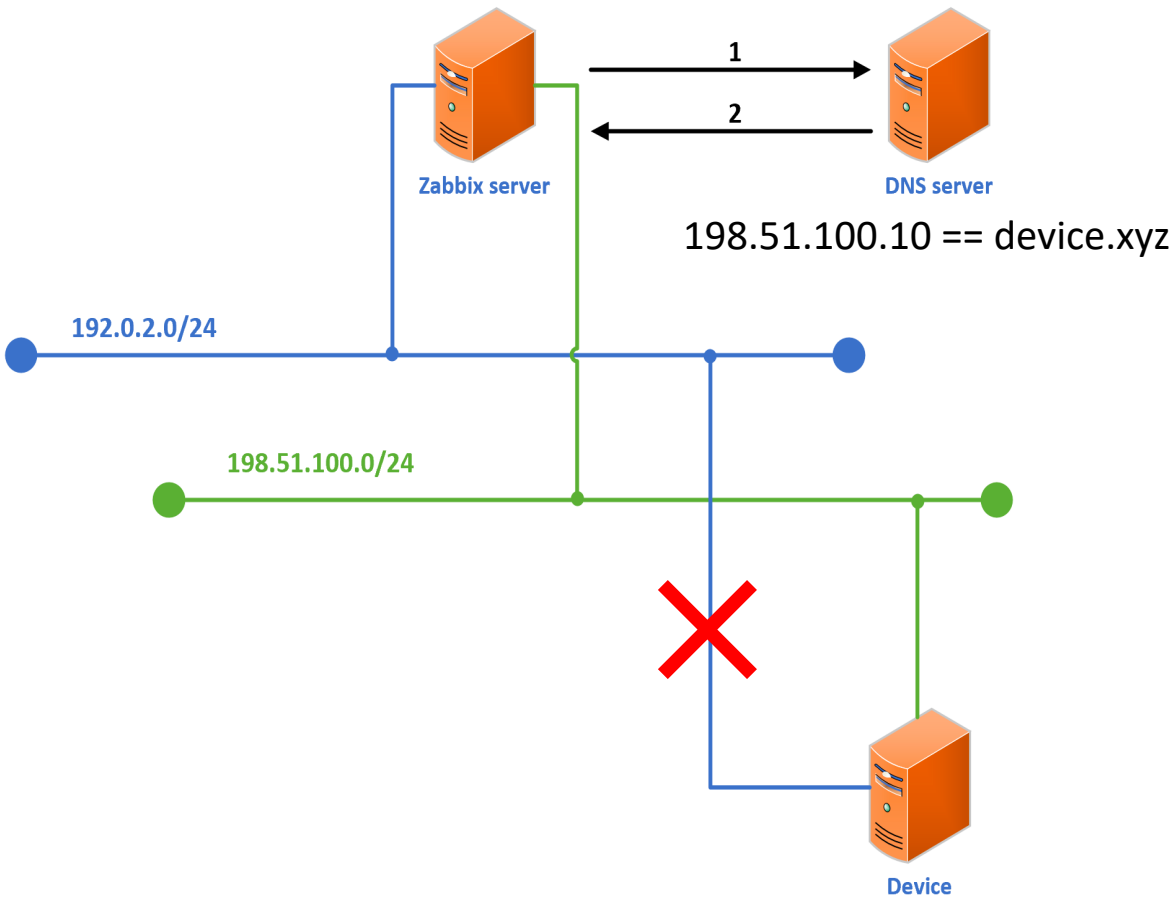
The fix

Item must be polled:

1: Request ip of device.xyz

2: device.xyz = 198.51.100.10

Monitoring happens over the green network.



Type of DNS records

A record: device.xyz = IP

Edit zone "xyz"

	Id	Name	Type	Content	Priority	TTL
	32	xyz	SOA	2020021801 28800 7200 604800 86400		86400
	33	device.xyz	A	192.0.2.10	0	8640

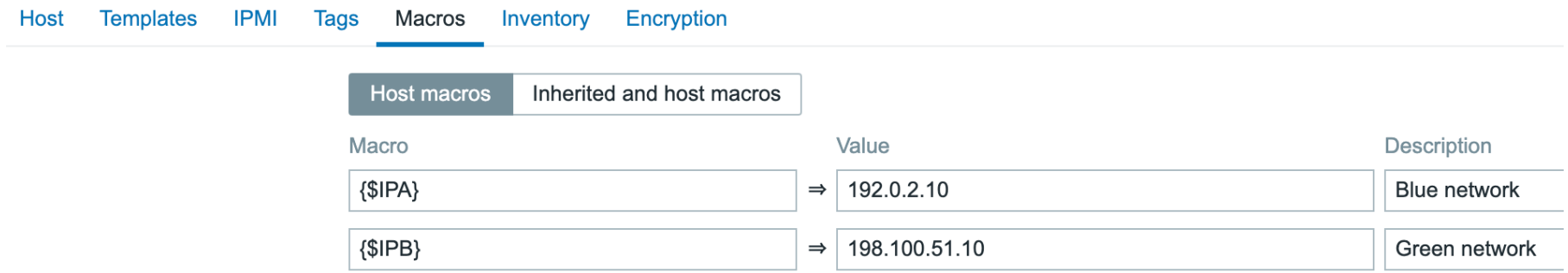
CNAME record: device.xyz = device1.xyz

Edit zone "xyz"

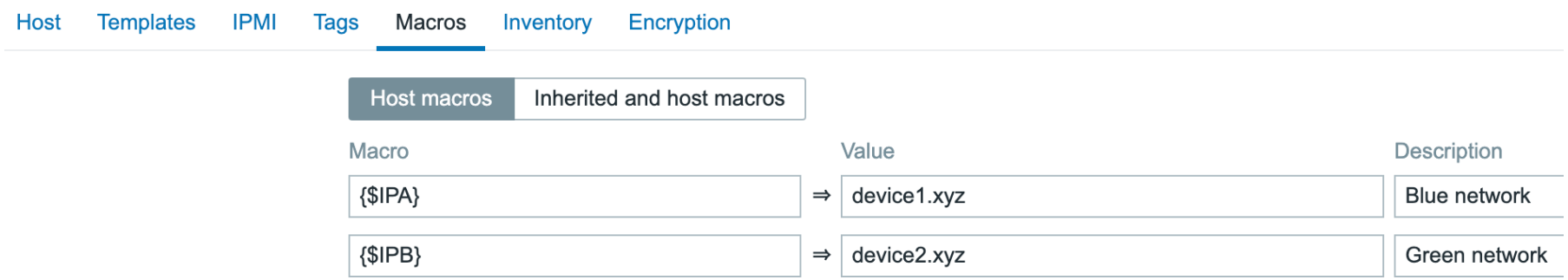
	Id	Name	Type	Content	Priority	TTL
	32	xyz	SOA	2020021804 28800 7200 604800 86400		86400
	33	device.xyz	CNAME	device1.xyz	0	8640
	34	device1.xyz	A	192.0.2.10	0	8640
	35	device2.xyz	A	198.51.100.10	0	8640

Zabbix Host config

A record: device.xyz = IP



CNAME record: device.xyz = device1.xyz



Why the different approaches?

A record: device.xyz = IP

- ✓ Easier to see the Ipaddresses
- ✓ Easier to understand
- ✕ Nightmare with DTAP and different subnets

CNAME record: device.xyz = device1.xyz

- ✓ Bit harder to configure
- ✓ Bit harder to understand
- ✕ No problem with DTAP and different subnets

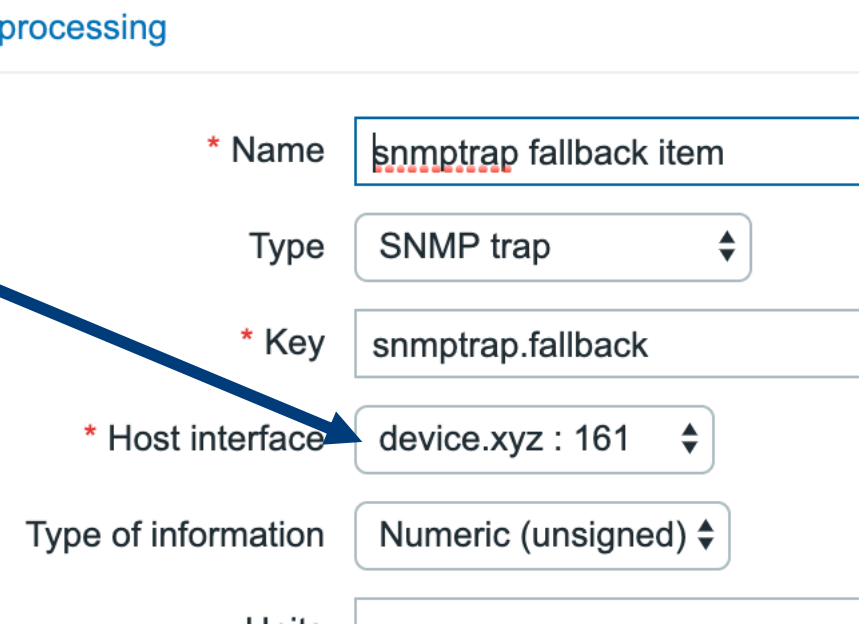
Did we cover everything?

- How about SNMPtraps?

Mismatch!

Received trap:

09:40:49 2020/02/18 ZBXTRAP 192.0.2.10
truncated
receivedfrom UDP: [192.0.2.10]:43205->[192.0.2.1]:162
*truncated



Did we cover everything?

- How about SNMPtraps?

Fix? -> Adjust the default perl script, or build your own
If trap is received, extract the from ip, do a reverse DNS lookup and parse the dns name

Received trap:

09:40:49 2020/02/18 ZBXTRAP device.xyz
truncated
receivedfrom UDP: [192.0.2.10]:43205->[192.0.2.1]:162
*truncated

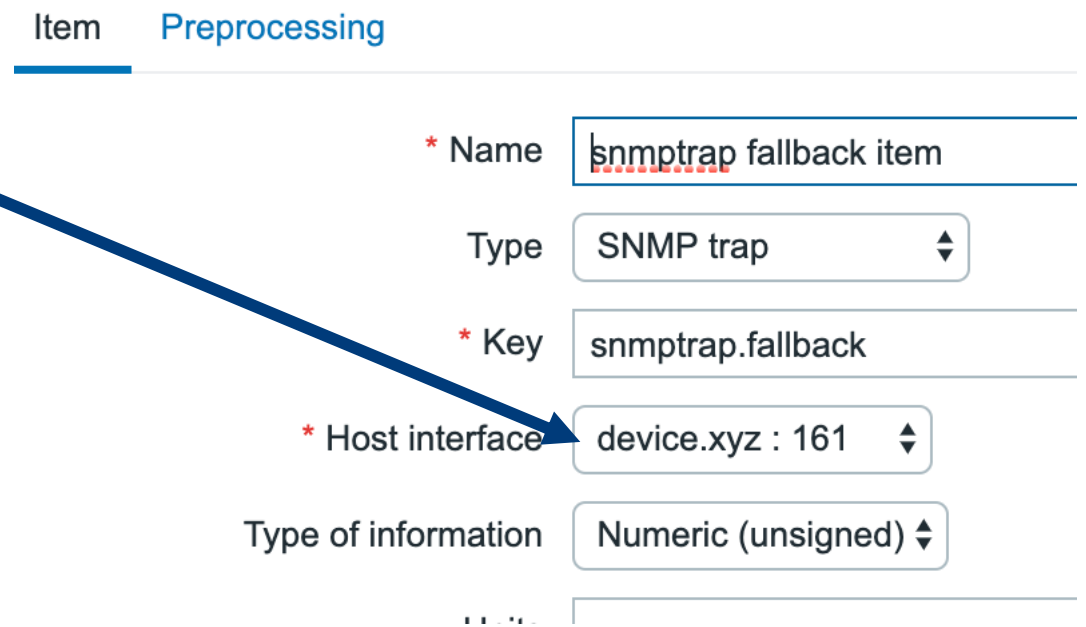
Did we cover everything?

- How about SNMPtraps?

Match!

Received trap:

09:40:49 2020/02/18 ZBXTRAP device.xyz
truncated
receivedfrom UDP: [192.0.2.10]:43205->[192.0.2.1]:162
*truncated



Thank you