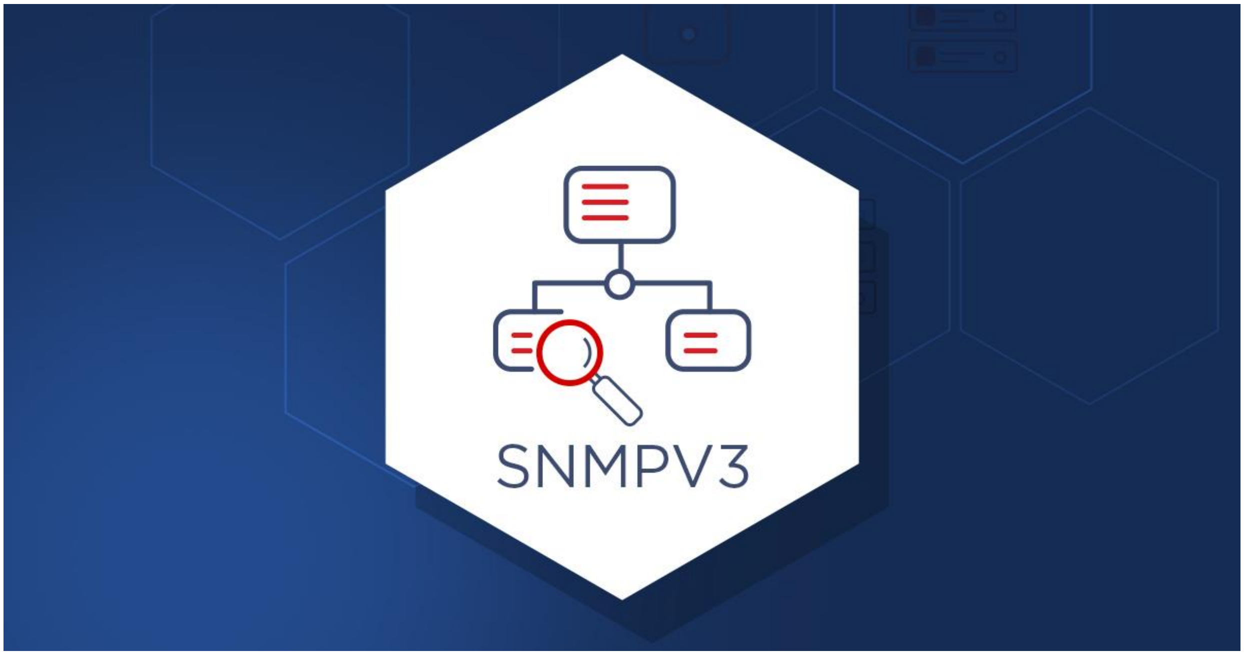


Monitoring network hardware with SNMPv3 in Zabbix

By Alexander Konyukhov April 8, 2020

SNMP is the main protocol for monitoring network hardware which may be used in Zabbix — an all-in-one solution for monitoring a large number of objects in static (changing slowly) networks.

The earlier versions of the protocol—SNMPv1 and SNMPv2—had security vulnerabilities that led to attacks and data breaches. In order to protect sensitive data, SNMPv3 should be enabled.

I'll demonstrate how to configure SNMPv3 in Zabbix to monitor network hardware, how to create proper templates in Zabbix, and what you can achieve by organizing a distributed alert system in a large network.

About SNMPv3

SNMP is the main protocol for monitoring network hardware used to monitor network devices and to manage them by sending simple commands (for example, to reboot a device, to enable or disable network interfaces, etc.).

The main difference between SNMPv3 and the previous versions — the classic security functions [1-3]:

- **authentication**, which allows us to determine if a request came from a trusted source;
- **encryption**, which prevents any third party from reading data if it is intercepted in transit;
- **integrity**, which helps to ensure that a data packet hasn't been tampered with during transit.

SNMPv3 allows using security models where different users and user groups have an authentication strategy assigned to them (while, in a request from a server to a monitored device, the previous versions of SNMP only checked the **community** string, which was transmitted as plain text and served as a password).

SNMPv3 also introduces security levels that define acceptably secure device settings and SNMP agent behavior. The combination of a security model and a specific level determines which security mechanism will be used to process an SNMP data packet [4].

Combinations of security models and levels in SNMPv3

Level	Authentication	Encryption	What Happens
noAuthNoPriv	Username	No	Authentication with a username (strongly not recommended)
authNoPriv	Message Digest Algorithm 5 (MD5) or Secure Hash Algorithm (SHA)	No	Authentication based on Hashed Message Authentication Code (HMAC)-MD5 or HMAC-SHA (not recommended)
authPriv	MD5 or SHA	Data Encryption Standard (DES) or Advanced Encryption Standard (AES)	Authentication based on HMAC-MD5 or HMAC-SHA + encryption based on DES or AES (best practice)

How to

To monitor a network device, we must set up SNMPv3 both on the server and the monitored device.

Setting up network device

- **The basic Cisco network device configuration in the CLI:**

1. Define a group of SNMPv3 users (‘**snmpv3group**‘), the access mode (‘**read**‘), and access privilege for the ‘**snmpv3group**‘ to view certain branches of the device’s MIB tree.

```
snmp-server group snmpv3group v3 priv read snmpv3name
```

2. Define the user — ‘**snmpv3user**‘, the user group — ‘**snmpv3group**‘, and state authentication based on MD5 (with’**md5v3v3v3**‘ as the password) and encryption based on DES (with ‘**des56v3v3v3**‘ as the password).

```
snmp-server  user  snmpv3user  snmpv3group  v3  auth  md5  md5v3v3v3  priv  des
des56v3v3v3
```

NOTE. *It is preferable to use AES. DES here is used as an example only.*

NOTE. *When defining a user,* ***Access Control List*** *can be added to specify IP addresses of servers that can monitor this device.*

3. Define codename (‘**snmpv3name**‘) for specific branches of MIB tree so that ‘**snmpv3group**‘ could access them. ISO, instead of limiting it to a single branch, allows ‘**snmpv3group**‘ to access all MIB objects of the monitored device.

```
snmp-server view snmpv3name iso included
```

- **The basic Huawei network device configuration in the CLI:**

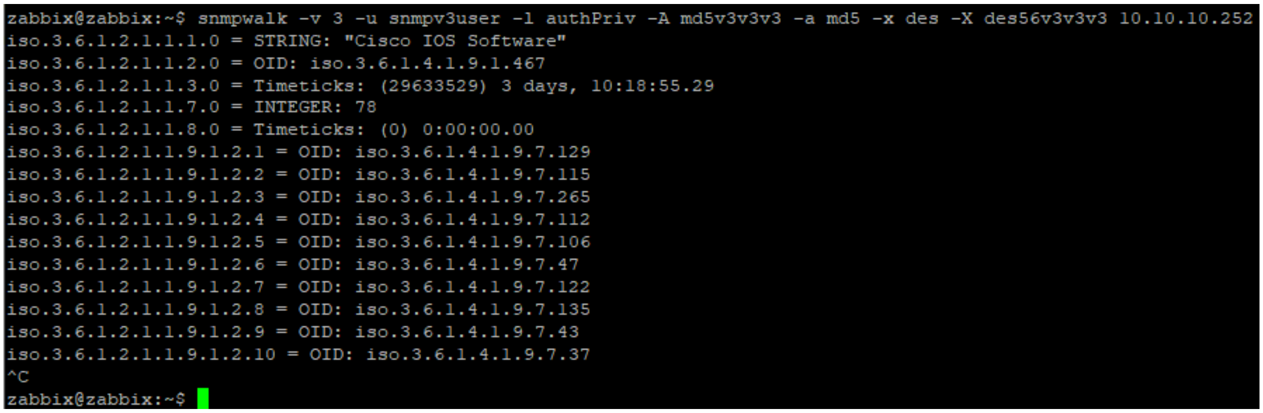
```
snmp-agent mib-view included snmpv3name iso

snmp-agent group v3 snmpv3group privacy read-view snmpv3name

snmp-agent usm-user v3 snmpv3user group snmpv3group

snmp-agent usm-user v3 snmpv3user authentication-mode md5
```

```
md5v3v3v3

snmp-agent usm-user v3 snmpv3user privacy-mode des56

des56v3v3v3
```

Setting up access

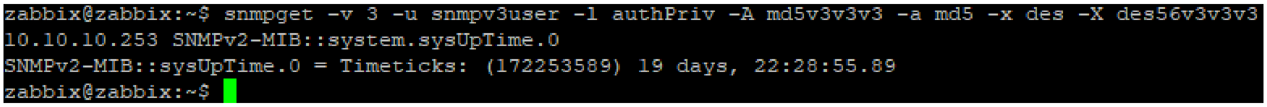
After network devices are configured, to ensure that the monitoring server can access them by SNMPv3, you can run ‘**snmpwalk**‘:

```
snmpwalk -v 3 -u snmpv3user -l authPriv -A md5v3v3v3 -a md5 -x des -X
des56v3v3v3 10.10.10.252
```



```
zabbix@zabbix:~$ snmpwalk -v 3 -u snmpv3user -l authPriv -A md5v3v3v3 -a md5 -x des -X des56v3v3v3 10.10.10.252
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco IOS Software"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.467
iso.3.6.1.2.1.1.3.0 = Timeticks: (29633529) 3 days, 10:18:55.29
iso.3.6.1.2.1.1.7.0 = INTEGER: 78
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.4.1.9.7.129
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.4.1.9.7.115
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.4.1.9.7.265
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.4.1.9.7.112
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.4.1.9.7.106
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.4.1.9.7.47
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.4.1.9.7.122
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.4.1.9.7.135
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.4.1.9.7.43
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.4.1.9.7.37
^C
zabbix@zabbix:~$
```

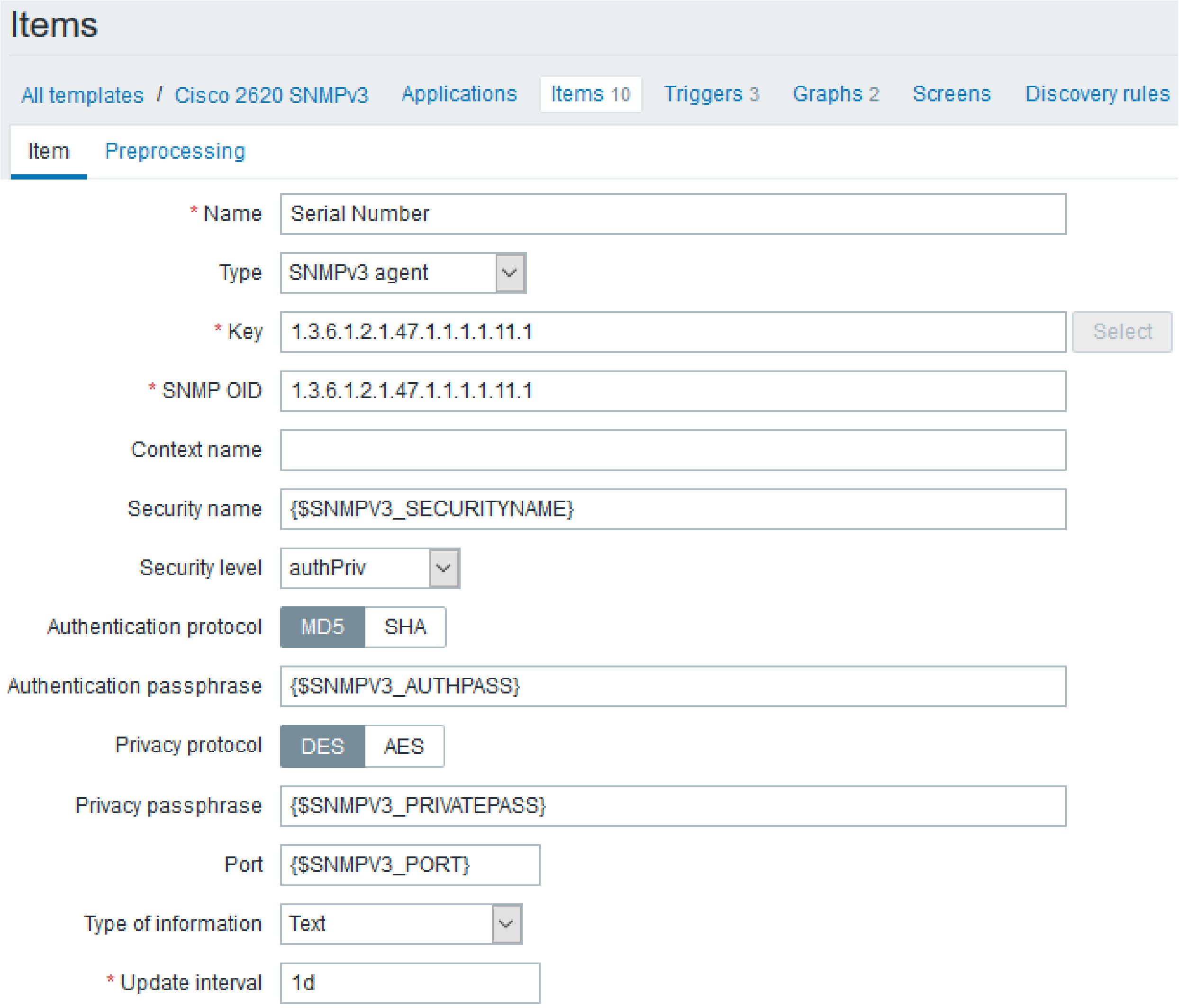
To request specific objects, you can also run ‘**snmpget**‘, which relies on MIB files and gives a more concise output:



```
zabbix@zabbix:~$ snmpget -v 3 -u snmpv3user -l authPriv -A md5v3v3v3 -a md5 -x des -X des56v3v3v3
10.10.10.253 SNMPv2-MIB::system.sysUpTime.0
SNMPv2-MIB::sysUpTime.0 = Timeticks: (172253589) 19 days, 22:28:55.89
zabbix@zabbix:~$
```

Configuring an item to use SNMPv3

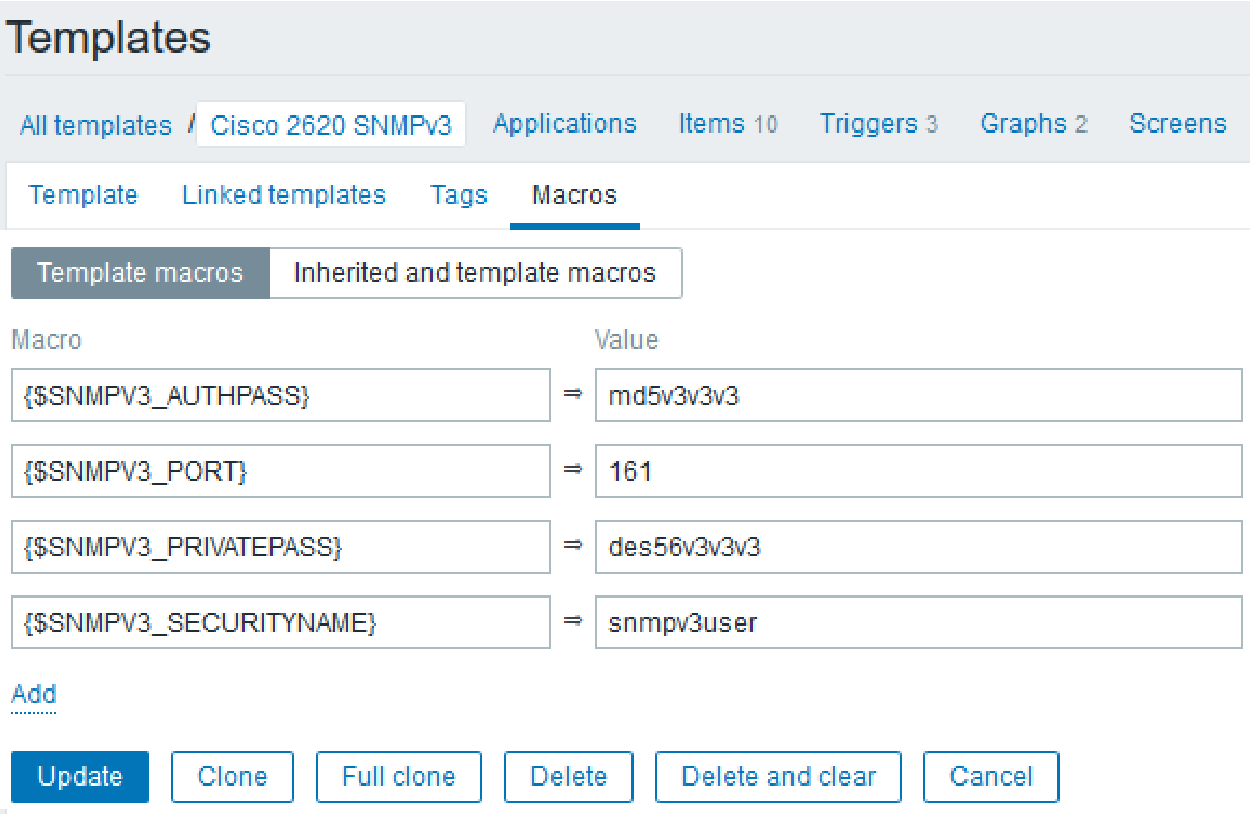
We need to configure a standard item that will use SNMPv3 on the Zabbix template level. The simplest way is to use MIB-independent numerical forms of OIDs.



* Name	Serial Number
Type	SNMPv3 agent
* Key	1.3.6.1.2.1.47.1.1.1.1.11.1
* SNMP OID	1.3.6.1.2.1.47.1.1.1.1.11.1
Context name	
Security name	{$SNMPV3_SECURITYNAME}
Security level	authPriv
Authentication protocol	[✓ MD5] SHA
Authentication passphrase	{$SNMPV3_AUTHPASS}
Privacy protocol	[✓ DES] AES
Privacy passphrase	{$SNMPV3_PRIVATEPASS}
Port	{$SNMPV3_PORT}
Type of information	Text
* Update interval	1d

Data elements

You can use user macros since they will be the same for every template item. If all of your network devices have the same SNMPv3 parameters, macros are defined on a template level, otherwise — on a host level.



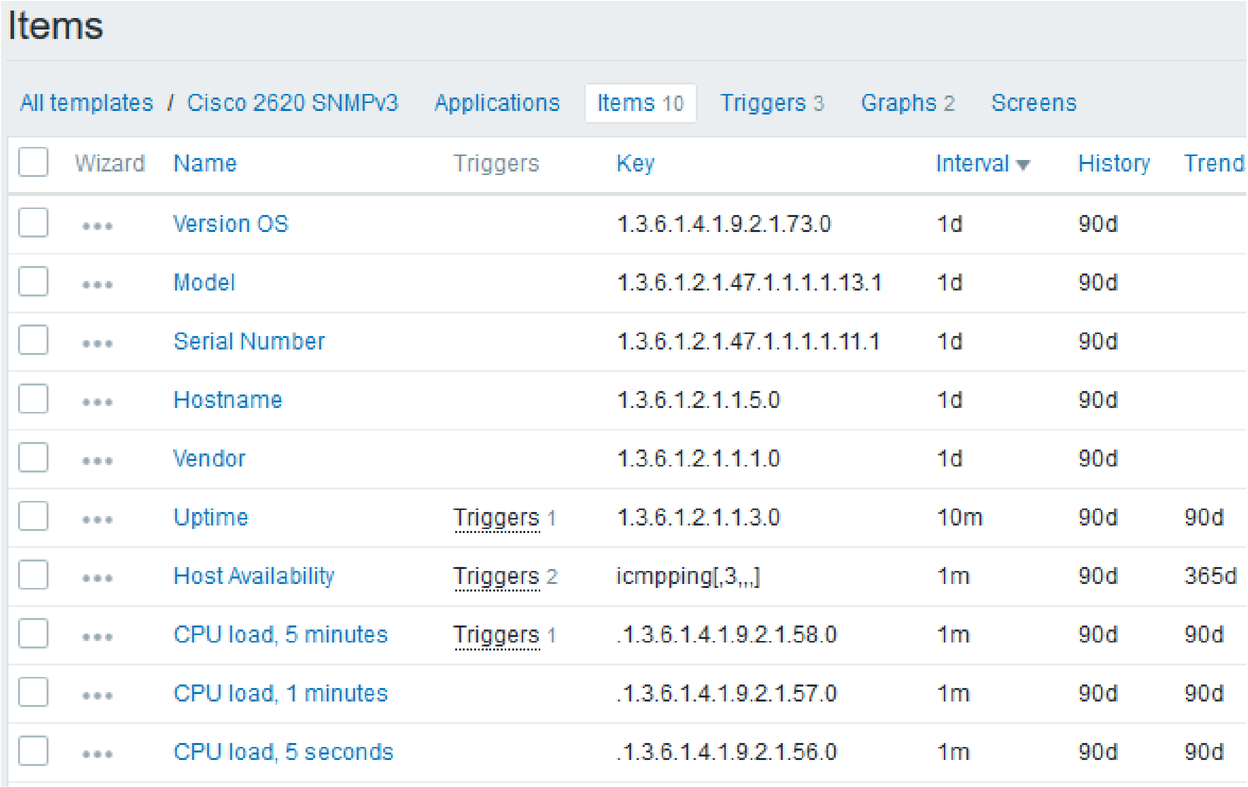
Macro		Value
{$SNMPV3_AUTHPASS}	⇒	md5v3v3v3
{$SNMPV3_PORT}	⇒	161
{$SNMPV3_PRIVATEPASS}	⇒	des56v3v3v3
{$SNMPV3_SECURITYNAME}	⇒	snmpv3user

Templates

NOTE. *Keep in mind that the monitoring system has usernames and passwords for authentication and encryption only. The user group and access to MIB objects are defined on each monitored device.*

Zabbix Polling template

It is recommended to make any polling templates as detailed as possible:



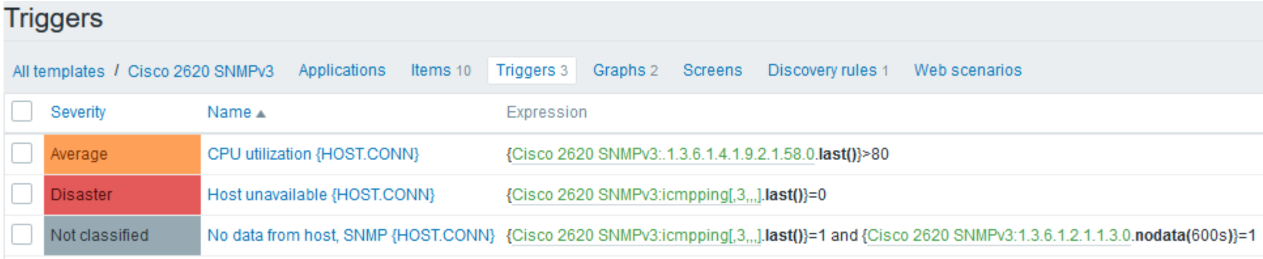
Items

All templates / Cisco 2620 SNMPv3 | Applications | Items 10 | Triggers 3 | Graphs 2 | Screens

□	Wizard	Name	Triggers	Key	Interval ▼	History	Trend
□	•••	Version OS		1.3.6.1.4.1.9.2.1.73.0	1d	90d	
□	•••	Model		1.3.6.1.2.1.47.1.1.1.1.13.1	1d	90d	
□	•••	Serial Number		1.3.6.1.2.1.47.1.1.1.1.11.1	1d	90d	
□	•••	Hostname		1.3.6.1.2.1.1.5.0	1d	90d	
□	•••	Vendor		1.3.6.1.2.1.1.1.0	1d	90d	
□	•••	Uptime	Triggers 1	1.3.6.1.2.1.1.3.0	10m	90d	90d
□	•••	Host Availability	Triggers 2	icmpping[,3,,,]	1m	90d	365d
□	•••	CPU load, 5 minutes	Triggers 1	.1.3.6.1.4.1.9.2.1.58.0	1m	90d	90d
□	•••	CPU load, 1 minutes		.1.3.6.1.4.1.9.2.1.57.0	1m	90d	90d
□	•••	CPU load, 5 seconds		.1.3.6.1.4.1.9.2.1.56.0	1m	90d	90d

Polling template

Configuring triggers



Triggers

All templates / Cisco 2620 SNMPv3 | Applications | Items 10 | Triggers 3 | Graphs 2 | Screens | Discovery rules 1 | Web scenarios

□	Severity	Name ▲	Expression
□	Average	CPU utilization {HOST.CONN}	{Cisco 2620 SNMPv3:.1.3.6.1.4.1.9.2.1.58.0.**last()**}>80
□	Disaster	Host unavailable {HOST.CONN}	{Cisco 2620 SNMPv3:icmpping[,3,,,].**last()**}=0
□	Not classified	No data from host, SNMP {HOST.CONN}	{Cisco 2620 SNMPv3:icmpping[,3,,,].**last()**}=1 and {Cisco 2620 SNMPv3:1.3.6.1.2.1.1.3.0.**nodata(600s)**}=1

Triggers

If trigger names include a system macro **{HOST.CONN}**, alerts on the dashboard would display not only device names but also their IP addresses.

SNMP may be used to determine whether a device is not available, besides a regular echo request.

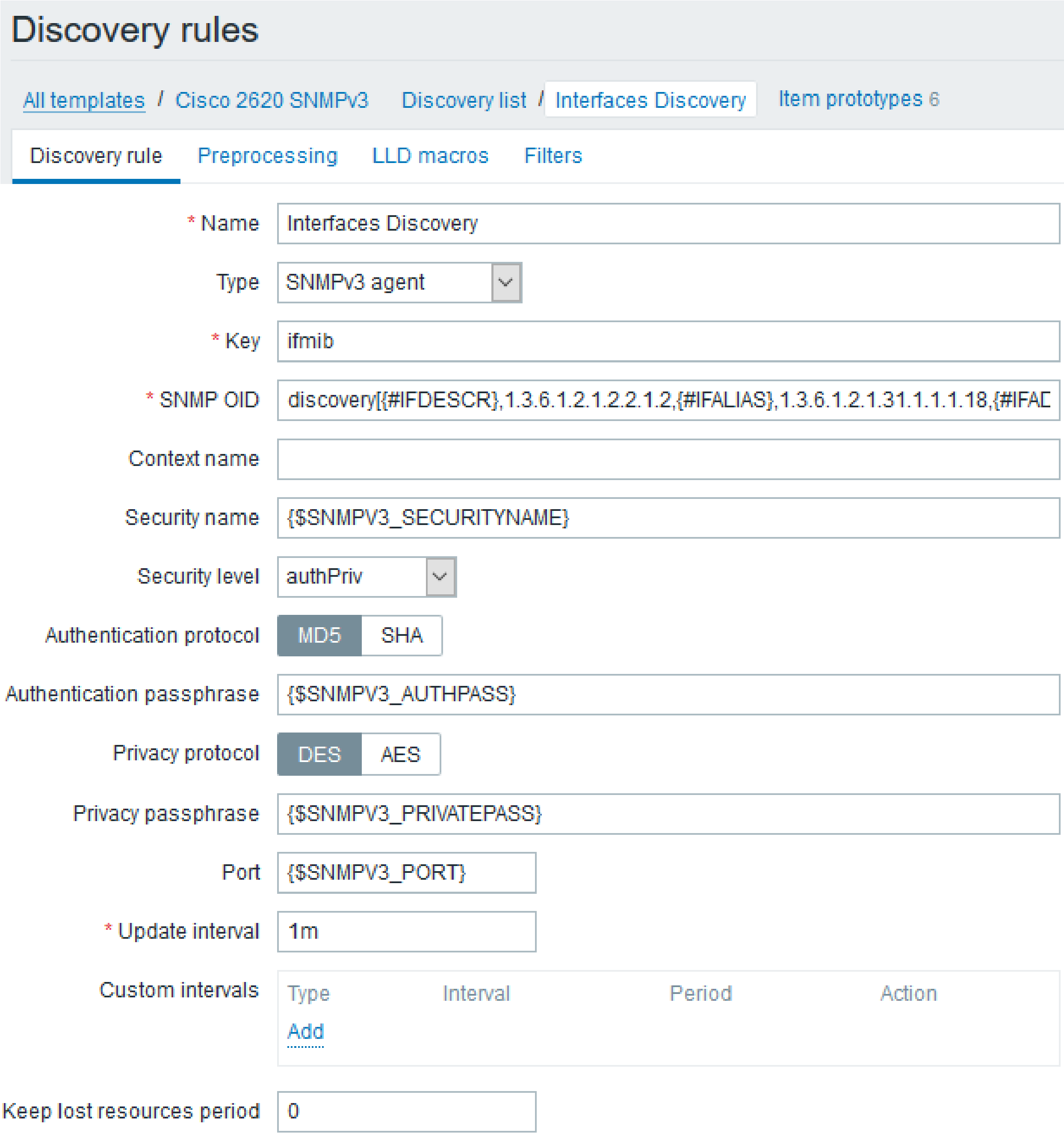
Sometimes a device responds only to ICMP requests, which may mean that different devices have the same IP address because of firewall or SNMP settings. Still, you might not get all monitoring data to investigate a network incident if you use only ICMP to check host availability.

Network interface discovery

Network interface discovery is the most important monitoring function for networking hardware. Since a single network device can have hundreds of interfaces, we must filter unneeded interfaces out, so that they don’t clutter up the database and data visualization.

Standard discovery function for SNMP with many detectable parameters allows for more flexible filtration:

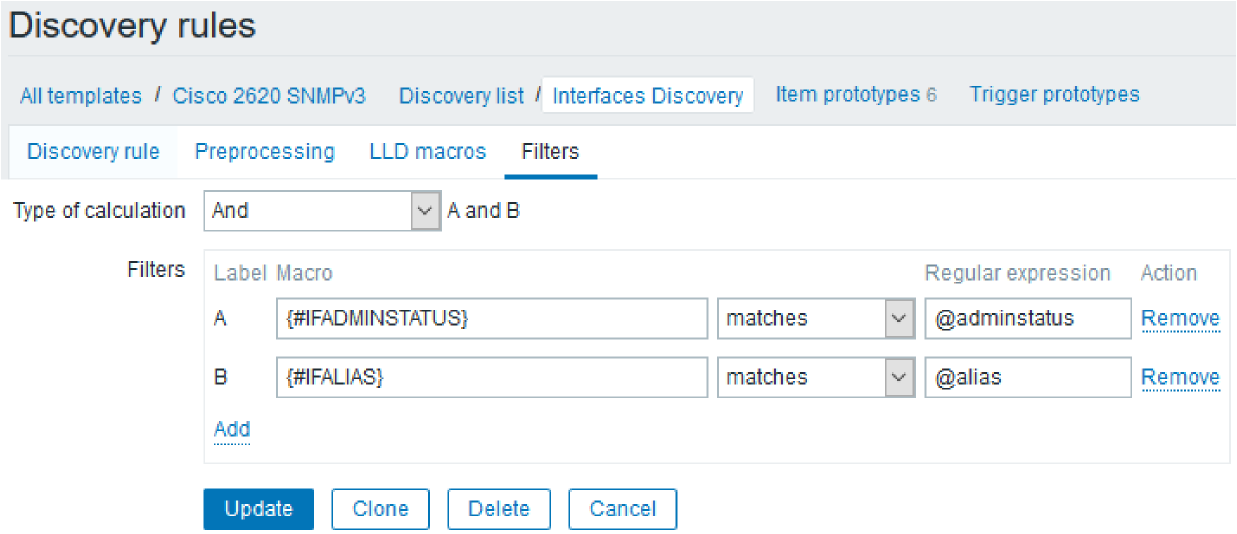
```
discovery[{#IFDESCR},1.3.6.1.2.1.2.2.1.2,{#IFALIAS},1.3.6.1.2.1.31.1.1.1.18,{
#IFADMINSTATUS},1.3.6.1.2.1.2.2.1.7]
```


Discovery rules
All templates / Cisco 2620 SNMPv3 Discovery list / Interfaces Discovery Item prototypes 6
Discovery rule
Preprocessing
LLD macros
Filters

* Name	Interfaces Discovery
Type	SNMPv3 agent
* Key	ifmib
* SNMP OID	discovery[{#IFDESCR},1.3.6.1.2.1.2.2.1.2,{#IFALIAS},1.3.6.1.2.1.31.1.1.1.18,{#IFAD
Context name	
Security name	{$SNMPV3_SECURITYNAME}
Security level	authPriv
Authentication protocol	[✓ MD5] SHA
Authentication passphrase	{$SNMPV3_AUTHPASS}
Privacy protocol	[✓ DES] AES
Privacy passphrase	{$SNMPV3_PRIVATEPASS}
Port	{$SNMPV3_PORT}
* Update interval	1m
Custom intervals	
Keep lost resources period	0

Discovery rules

Network interfaces can be discovered and filtered by their type, user description, and the administrative state of their ports.


Discovery rules
All templates / Cisco 2620 SNMPv3 Discovery list / Interfaces Discovery Item prototypes 6 Trigger prototypes
Discovery rule
Preprocessing
LLD macros
Filters
Update
Clone
Delete
Cancel

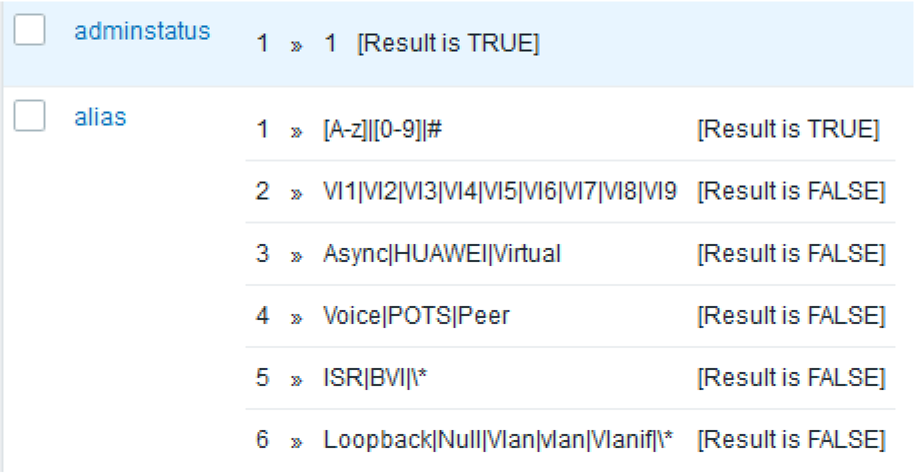
Type of calculation: And — A and B

Filters

Label	Macro		Regular expression	Action
A	{#IFADMINSTATUS}	matches	@adminstatus	Remove
B	{#IFALIAS}	matches	@alias	Remove

Add

Filters



□	adminstatus	1	»	1	[Result is TRUE]
□	alias	1	»	[A-z]|[0-9]|#	[Result is TRUE]
		2	»	Vl1|Vl2|Vl3|Vl4|Vl5|Vl6|Vl7|Vl8|Vl9	[Result is FALSE]
		3	»	Async|HUAWEI|Virtual	[Result is FALSE]
		4	»	Voice|POTS|Peer	[Result is FALSE]
		5	»	ISR|BVI|*	[Result is FALSE]
		6	»	Loopback|Null|Vlan|vlan|Vlanif|*	[Result is FALSE]

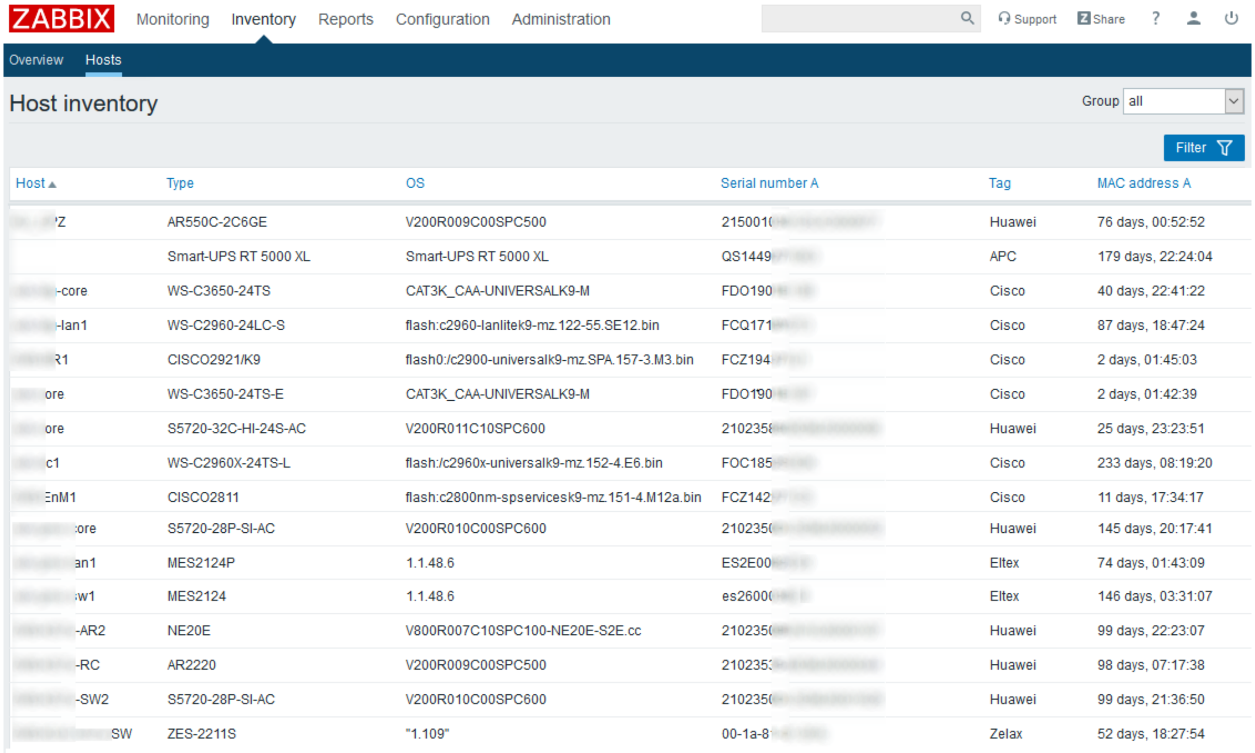
Regular expression

So, excluded interfaces will be those that:

- have been manually disabled (‘**adminstatus<>1**‘), because of ‘**IFADMINSTATUS**‘;
- don’t have a text description, because of ‘**IFALIAS**‘;
- have an asterisk (*) in their text description, because of ‘**IFALIAS**‘;
- are service/technical interfaces, because of ‘**IFDESCR**‘ (when regular expressions are applied in discovery, one regular expression, alias, will check on both ‘**IFALIAS**‘ and ‘**IFDESCR**‘).

Monitoring results

So, we’ve got a list of network devices:



Host inventory

Group: all

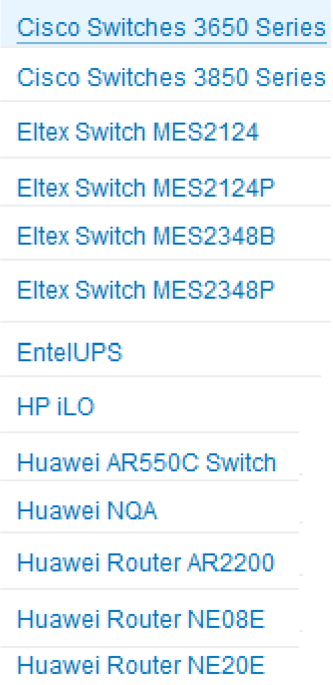
Host ▲	Type	OS	Serial number A	Tag	MAC address A
[redacted]'Z	AR550C-2C6GE	V200R009C00SPC500	215001[redacted]	Huawei	76 days, 00:52:52
[redacted]	Smart-UPS RT 5000 XL	Smart-UPS RT 5000 XL	QS1449[redacted]	APC	179 days, 22:24:04
[redacted]-core	WS-C3650-24TS	CAT3K_CAA-UNIVERSALK9-M	FDO190[redacted]	Cisco	40 days, 22:41:22
[redacted]-lan1	WS-C2960-24LC-S	flash:c2960-lanlitek9-mz.122-55.SE12.bin	FCQ171[redacted]	Cisco	87 days, 18:47:24
[redacted]R1	CISCO2921/K9	flash0:/c2900-universalk9-mz.SPA.157-3.M3.bin	FCZ194[redacted]	Cisco	2 days, 01:45:03
[redacted]ore	WS-C3650-24TS-E	CAT3K_CAA-UNIVERSALK9-M	FDO190[redacted]	Cisco	2 days, 01:42:39
[redacted]ore	S5720-32C-HI-24S-AC	V200R011C10SPC600	210235[redacted]	Huawei	25 days, 23:23:51
[redacted]c1	WS-C2960X-24TS-L	flash:/c2960x-universalk9-mz.152-4.E6.bin	FOC185[redacted]	Cisco	233 days, 08:19:20
[redacted]EnM1	CISCO2811	flash:c2800nm-spservicesk9-mz.151-4.M12a.bin	FCZ142[redacted]	Cisco	11 days, 17:34:17
[redacted]ore	S5720-28P-SI-AC	V200R010C00SPC600	210235[redacted]	Huawei	145 days, 20:17:41
[redacted]an1	MES2124P	1.1.48.6	ES2E00[redacted]	Eltex	74 days, 01:43:09
[redacted]w1	MES2124	1.1.48.6	es2600[redacted]	Eltex	146 days, 03:31:07
[redacted]-AR2	NE20E	V800R007C10SPC100-NE20E-S2E.cc	210235[redacted]	Huawei	99 days, 22:23:07
[redacted]-RC	AR2220	V200R009C00SPC500	210235[redacted]	Huawei	98 days, 07:17:38
[redacted]-SW2	S5720-28P-SI-AC	V200R010C00SPC600	210235[redacted]	Huawei	99 days, 21:36:50
[redacted]SW	ZES-2211S	"1.109"	00-1a-8[redacted]	Zelax	52 days, 18:27:54

List of network devices

Creating templates for each series of hardware makes analysis of monitoring results more convenient as it allows to see information grouped by series on:

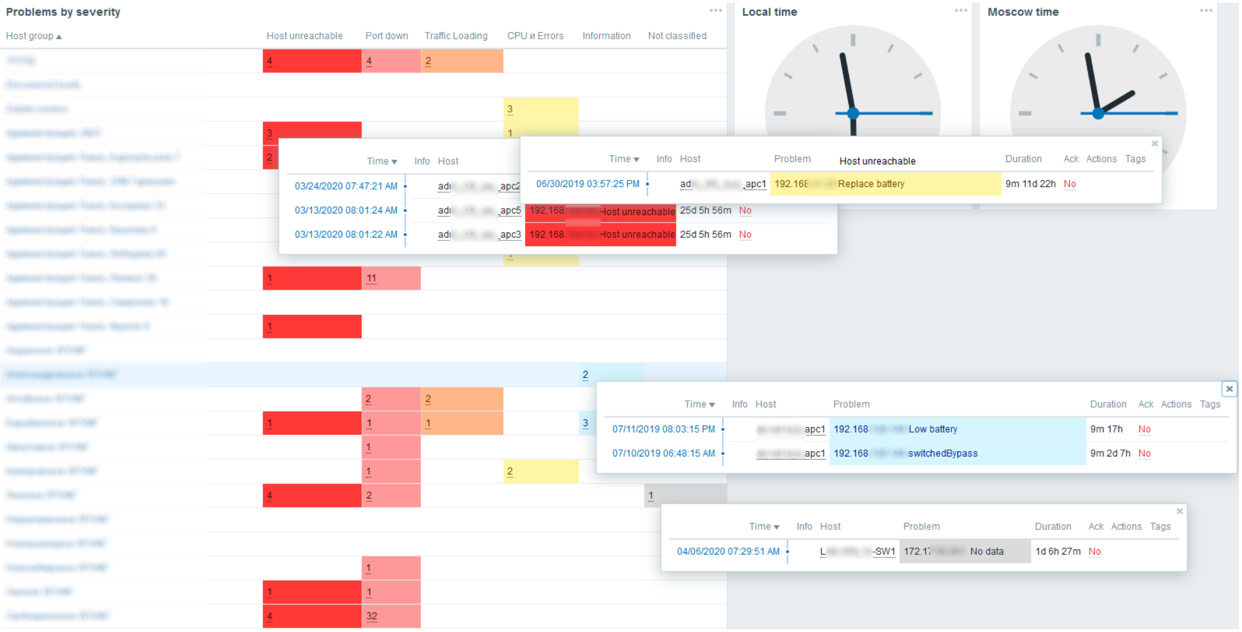
- up-to-date software,
- serial numbers, and
- presence of a janitor in the server room (indicated by low uptime percentage).

Various templates may give different views on your network, for example:



- Cisco Switches 3650 Series
- Cisco Switches 3850 Series
- Eltex Switch MES2124
- Eltex Switch MES2124P
- Eltex Switch MES2348B
- Eltex Switch MES2348P
- EntelUPS
- HP iLO
- Huawei AR550C Switch
- Huawei NQA
- Huawei Router AR2200
- Huawei Router NE08E
- Huawei Router NE20E

Hardware series templates



Problems by severity

Host group ▲	Host unreachable	Port down	Traffic Loading	CPU и Errors	Information	Not classified
[redacted]	4	4	2			
[redacted]						
[redacted]				3		
[redacted]	3			1		
[redacted]	2					
[redacted]						
[redacted]						
[redacted]						
[redacted]				1		
[redacted]	1	11				
[redacted]						
[redacted]	1					
[redacted]						
[redacted]					2	
[redacted]		2	2			
[redacted]	1	1	1		3	
[redacted]		1				
[redacted]		1		2		
[redacted]	4	2				1
[redacted]						
[redacted]						
[redacted]		1				
[redacted]	1	1				
[redacted]	4	32				

Local time

Moscow time

Time ▾	Info	Host	Problem	Duration	Ack	Actions	Tags
03/24/2020 07:47:21 AM		ad[redacted]_apc2					
03/13/2020 08:01:24 AM		ad[redacted]_apc5	192.168.[redacted] Host unreachable	25d 5h 56m	No		
03/13/2020 08:01:22 AM		ad[redacted]_apc3	192.168.[redacted] Host unreachable	25d 5h 56m	No		

Time ▾	Info	Host	Problem	Duration	Ack	Actions	Tags
06/30/2019 03:57:25 PM		ad[redacted]_apc1	192.168[redacted] Replace battery	9m 11d 22h	No		

Host unreachable

Time ▾	Info	Host	Problem	Duration	Ack	Actions	Tags
07/11/2019 08:03:15 PM		[redacted]apc1	192.168[redacted] Low battery	9m 17h	No		
07/10/2019 06:48:15 AM		[redacted]apc1	192.168[redacted] switchedBypass	9m 2d 7h	No		

Time ▾	Info	Host	Problem	Duration	Ack	Actions	Tags
04/06/2020 07:29:51 AM		L[redacted]-SW1	172.17[redacted] No data	1d 6h 27m	No		

Main monitoring dashboard with triggers divided by level of importance

If you create templates for each device model in your network, your monitoring system can become a tool for forecasting malfunctions and failures (if you have necessary sensors and metrics). Zabbix is a good solution for monitoring network, server, and service infrastructures, and leveraging Zabbix for maintaining network hardware demonstrates the system's capabilities.

References

1. Hucaby D. CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. Cisco Press, 2014. pp. 325-329.
2. RFC 3410. https://tools.ietf.org/html/rfc3410
3. RFC 3415. https://tools.ietf.org/html/rfc3415
4. SNMP Configuration Guide, Cisco IOS XE Release 3SE.
   Chapter: SNMP Version 3.
   https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/3850/snmp-xe-3se-3850-book/nm-snmp-snmpv3.html

LNC 22082020