



ĐẠI HỌC ĐÀ NẴNG

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG VIỆT - HÀN
Vietnam - Korea University of Information and Communication Technology

GIÁM SÁT MẠNG

Giảng viên: Lê Tự Thành

Email : ltthanh@vku.udn.vn

Website : www.vku.udn.vn



CHƯƠNG 6. HỆ THỐNG CẢNH BÁO

6.1. Khái niệm

Hệ thống cảnh báo trong giám sát nhằm tăng cường cảnh báo tức thì theo thời gian thực thông qua các hệ thống như : email, sms, message,...

Mỗi hệ thống cảnh báo đều có ưu điểm và nhược điểm riêng. Các hệ thống phần mềm giám sát thường được tích hợp hệ thống cảnh báo nhằm cung cấp kịp thời nhất các thông tin về hệ thống khi có sự thay đổi, bất thường,...

CHƯƠNG 6. HỆ THỐNG CẢNH BÁO

ZABBIX

Server Zabbix

Monitoring Services Inventory Reports Configuration Administration

- General
- Proxies
- Authentication
- User groups
- User roles
- Users
- Media types
- Scripts
- Queue
- Support
- Integrations
- Help
- User settings
- Sign out

Name	Type	Status	Used in actions	Details
Brevi's one	Webhook	Enabled		
Discord	Webhook	Enabled		
Email	Email	Enabled		SMTP server: "mail.example.com", SMTP helo: "example.com", SMTP email: "zabbix@example.com"
Email (HTML)	Email	Enabled		SMTP server: "mail.example.com", SMTP helo: "example.com", SMTP email: "zabbix@example.com"
Express.ms	Webhook	Enabled		
Github	Webhook	Enabled		
GLPI	Webhook	Enabled		
iLert	Webhook	Enabled		
iTop	Webhook	Enabled		
Jira	Webhook	Enabled		
Jira ServiceDesk	Webhook	Enabled		
Jira with CustomFields	Webhook	Enabled		
ManageEngine ServiceDesk	Webhook	Enabled		
Mattermost	Webhook	Enabled		
MS Teams	Webhook	Enabled		
Opsgenie	Webhook	Enabled		
OTRS	Webhook	Enabled		
PagerDuty	Webhook	Enabled		
Pushover	Webhook	Enabled		
Redmine	Webhook	Enabled		
Rocket Chat	Webhook	Enabled		
ServiceNow	Webhook	Enabled		
SIGNAL4	Webhook	Enabled		
Slack	Webhook	Enabled		
SMS	SMS	Enabled		GSM modem: "/dev/ttyS0"

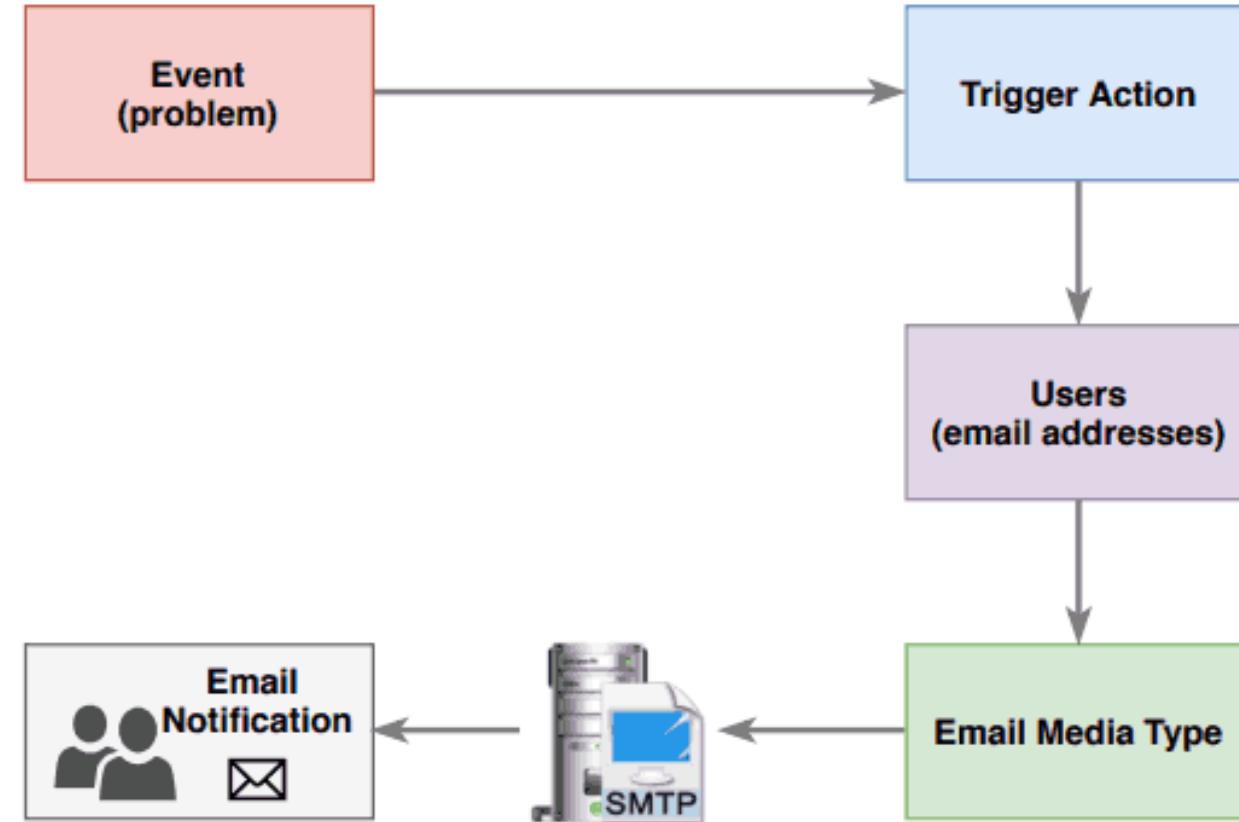


CHƯƠNG 6. HỆ THỐNG CẢNH BÁO

6.2. Cảnh báo qua email

Thông tin cảnh báo của hệ thống được gửi qua email cho người chịu trách nhiệm giám sát hệ thống hoặc do phân cấp, phân quyền. Người quản trị hệ thống có thể thiết lập cảnh báo qua email nội bộ hoặc gmail,....

CHƯƠNG 6. HỆ THỐNG CẢNH BÁO



CHƯƠNG 6. HỆ THỐNG CẢNH BÁO

Ví dụ: Cảnh báo qua email

Media type Message templates 5 Options

* Name: Email

Type: Email

* SMTP server: mail.example.com

SMTP server port: 25

* SMTP helo: example.com

* SMTP email: Zabbix_info <zabbix@example.com>

Connection security: None STARTTLS SSL/TLS

Authentication: None Username and password

Message format: HTML Plain text

Description:

Enabled:

CHƯƠNG 6. HỆ THỐNG CẢNH BÁO

Ví dụ: Cảnh báo qua email

ZABBIX

Monitoring
Inventory
Reports
Configuration
1 Administration
General
Proxies
Authentication
User groups
2 Media types
Users
Scripts
Queue
Support
Share
Help
User settings
Sign out

Media types

3 Click on existing media type called "Email"

4

* Name: Email
Type: Email
* SMTP server: smtp.office365.com
SMTP server port: 587
* SMTP helo: smtp.office365.com
* SMTP email: aldin.osmanagic@bestmonitoringtools.com
Connection security: None STARTTLS SSL/TLS
SSL verify peer:
SSL verify host:
Authentication: None Username and password
Username: aosmana@bestmonitorin
Password: [Change password](#)
Message format: HTML Plain text
Description:
Enabled: **5**
6 Update Clone Delete Cancel

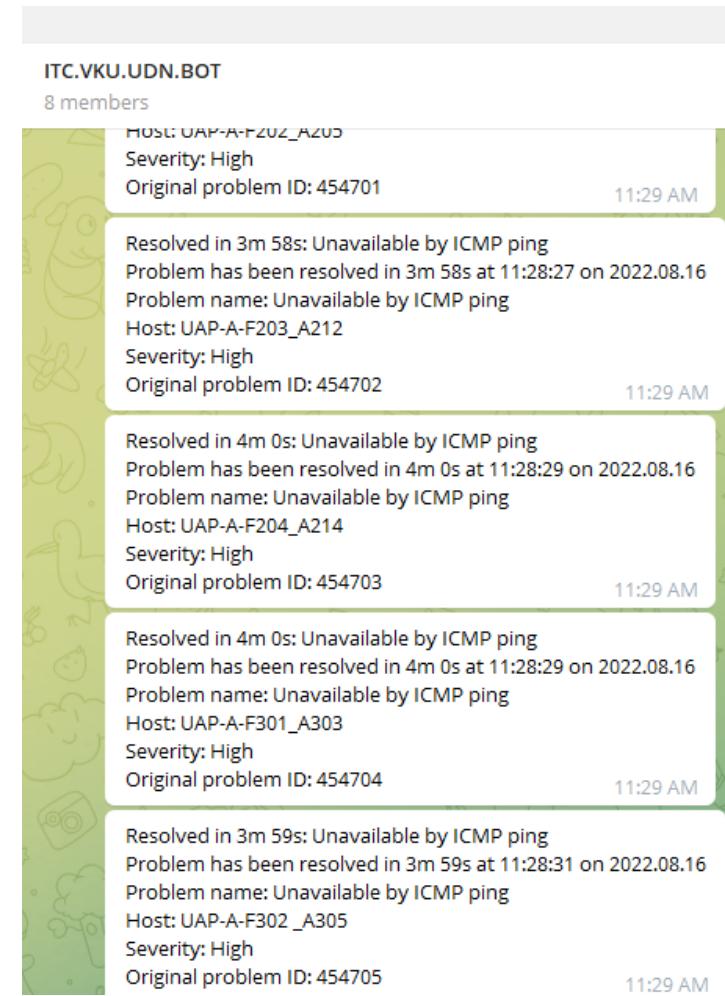
CHƯƠNG 6. HỆ THỐNG CẢNH BÁO

6.2. Cảnh báo qua telegram

Telegram là ứng dụng nhắn tin, gọi điện video, chia sẻ file đa nền tảng và miễn phí. Telegram có rất nhiều máy chủ trên toàn thế giới để đảm bảo hoạt động ổn định, nhanh chóng với trung tâm dữ liệu được đặt tại Dubai. Telegram có mặt trên các hệ điều hành phổ biến nhất hiện nay như Android, iOS, Windows, macOS và Linux

CHƯƠNG 6. HỆ THỐNG CẢNH BÁO

Ví dụ: Cảnh báo qua telegram



CHƯƠNG 6. HỆ THỐNG CẢNH BÁO

ZABBIX

Server Zabbix

Monitoring Services Inventory Reports Configuration Administration General Proxies Authentication User groups User roles Users Media types Scripts Queue Support Integrations Help User settings Sign out

Media types

Name	Type	Status	Used in actions	Details
Brevi's one	Webhook	Enabled		
Discord	Webhook	Enabled		
Email	Email	Enabled		SMTP server: "mail.example.com", SMTP helo: "example.com", SMTP email: "zabbix@example.com"
Email (HTML)	Email	Enabled		SMTP server: "mail.example.com", SMTP helo: "example.com", SMTP email: "zabbix@example.com"
Express.ms	Webhook	Enabled		
Github	Webhook	Enabled		
GLPI	Webhook	Enabled		
iLert	Webhook	Enabled		
iTop	Webhook	Enabled		
Jira	Webhook	Enabled		
Jira ServiceDesk	Webhook	Enabled		
Jira with CustomFields	Webhook	Enabled		
ManageEngine ServiceDesk	Webhook	Enabled		
Mattermost	Webhook	Enabled		
MS Teams	Webhook	Enabled		
Opsgenie	Webhook	Enabled		
OTRS	Webhook	Enabled		
PagerDuty	Webhook	Enabled		
Pushover	Webhook	Enabled		
Redmine	Webhook	Enabled		
Rocket.Chat	Webhook	Enabled		
ServiceNow	Webhook	Enabled		
SIGNAL4	Webhook	Enabled		
Slack	Webhook	Enabled		

CHƯƠNG 6. HỆ THỐNG CẢNH BÁO

ZABBIX < >

Server Zabbix

Monitoring Services Inventory Reports Configuration Administration

- General
- Proxies
- Authentication
- User groups
- User roles
- Users
- Media types

<input type="checkbox"/>	OTRS	Webhook	Enabled
<input type="checkbox"/>	PagerDuty	Webhook	Enabled
<input type="checkbox"/>	Pushover	Webhook	Enabled
<input type="checkbox"/>	Redmine	Webhook	Enabled
<input type="checkbox"/>	Rocket.Chat	Webhook	Enabled
<input type="checkbox"/>	ServiceNow	Webhook	Enabled
<input type="checkbox"/>	SIGNAL4	Webhook	Enabled
<input type="checkbox"/>	Slack	Webhook	Enabled
<input type="checkbox"/>	SMS	SMS	Enabled GSM modem: "/dev/ttyS0"
<input type="checkbox"/>	SolarWinds Service Desk	Webhook	Enabled
<input type="checkbox"/>	SysAid	Webhook	Enabled
<input type="checkbox"/>	Telegram	Webhook	Enabled
<input type="checkbox"/>	Telegram VKU	Webhook	Enabled Telegram Notification
<input type="checkbox"/>	TOPdesk	Webhook	Enabled
<input type="checkbox"/>	VictorOps	Webhook	Enabled
<input type="checkbox"/>	Zammad	Webhook	Enabled
<input type="checkbox"/>	Zendesk	Webhook	Enabled

CHƯƠNG 6. HỆ THỐNG CẢNH BÁO

6.3. Xây dựng chính sách cảnh báo

Việc xây dựng chính sách cảnh báo rất quan trọng, thông qua chính sách cảnh báo người quản trị viên dễ dàng sàng lọc được các thông tin cần cảnh báo. Các thông tin cần cảnh báo thường là các thông tin quan trọng và có ảnh hưởng nghiêm trọng đến hệ thống.

CHƯƠNG 6. HỆ THỐNG CẢNH BÁO

Phân tích hệ thống (phục vụ xây dựng chính sách cảnh báo)

- Các thiết bị mạng, dịch vụ mạng cần đưa vào cảnh báo
- Các thông số quan trọng cần cảnh báo
- Các ngưỡng “chịu đựng” của thiết bị

CHƯƠNG 6. HỆ THỐNG CẢNH BÁO

Ví dụ: Chính sách cảnh báo

- Up, Down hệ thống
- CPU, RAM, Disk hoạt động vượt ngưỡng 80%
- Tốc độ mạng chậm dưới ngưỡng (do người quản trị mạng thiết lập)
- Hệ thống quá nhiệt
-

CHƯƠNG 6. HỆ THỐNG CẢNH BÁO

	Severity	value	ivalue ▲	Operational data	expression
<input type="checkbox"/>	Warning	OK	CPU discovery: #1: High CPU utilization	Current utilization: {ITEM.LASTVALUE1}	<code>min(/Mikrotik CCR1036-12G-4S/system.cpu.util[hrProcessorLoad.1],5m)>{\$CPU.UTIL.CRIT}</code>
<input type="checkbox"/>	Warning	OK	CPU discovery: #2: High CPU utilization	Current utilization: {ITEM.LASTVALUE1}	<code>min(/Mikrotik CCR1036-12G-4S/system.cpu.util[hrProcessorLoad.2],5m)>{\$CPU.UTIL.CRIT}</code>
<input type="checkbox"/>	Warning	OK	CPU discovery: #3: High CPU utilization	Current utilization: {ITEM.LASTVALUE1}	<code>min(/Mikrotik CCR1036-12G-4S/system.cpu.util[hrProcessorLoad.3],5m)>{\$CPU.UTIL.CRIT}</code>
<input type="checkbox"/>	Warning	OK	CPU discovery: #4: High CPU utilization	Current utilization: {ITEM.LASTVALUE1}	<code>min(/Mikrotik CCR1036-12G-4S/system.cpu.util[hrProcessorLoad.4],5m)>{\$CPU.UTIL.CRIT}</code>
<input type="checkbox"/>	Warning	OK	CPU discovery: #5: High CPU utilization	Current utilization: {ITEM.LASTVALUE1}	<code>min(/Mikrotik CCR1036-12G-4S/system.cpu.util[hrProcessorLoad.5],5m)>{\$CPU.UTIL.CRIT}</code>
<input type="checkbox"/>	Warning	OK	CPU discovery: #6: High CPU utilization	Current utilization: {ITEM.LASTVALUE1}	<code>min(/Mikrotik CCR1036-12G-4S/system.cpu.util[hrProcessorLoad.6],5m)>{\$CPU.UTIL.CRIT}</code>
<input type="checkbox"/>	Warning	OK	CPU discovery: #7: High CPU utilization	Current utilization: {ITEM.LASTVALUE1}	<code>min(/Mikrotik CCR1036-12G-4S/system.cpu.util[hrProcessorLoad.7],5m)>{\$CPU.UTIL.CRIT}</code>
<input type="checkbox"/>	Warning	OK	CPU discovery: #8: High CPU utilization	Current utilization: {ITEM.LASTVALUE1}	<code>min(/Mikrotik CCR1036-12G-4S/system.cpu.util[hrProcessorLoad.8],5m)>{\$CPU.UTIL.CRIT}</code>
<input type="checkbox"/>	Warning	OK	CPU discovery: #9: High CPU utilization	Current utilization: {ITEM.LASTVALUE1}	<code>min(/Mikrotik CCR1036-12G-4S/system.cpu.util[hrProcessorLoad.9],5m)>{\$CPU.UTIL.CRIT}</code>
<input type="checkbox"/>	Warning	OK	CPU discovery: #10: High CPU utilization	Current utilization: {ITEM.LASTVALUE1}	<code>min(/Mikrotik CCR1036-12G-4S/system.cpu.util[hrProcessorLoad.10],5m)>{\$CPU.UTIL.CRIT}</code>
<input type="checkbox"/>	Warning	OK	CPU discovery: #11: High CPU utilization	Current utilization: {ITEM.LASTVALUE1}	<code>min(/Mikrotik CCR1036-12G-4S/system.cpu.util[hrProcessorLoad.11],5m)>{\$CPU.UTIL.CRIT}</code>

CHƯƠNG 6. HỆ THỐNG CẢNH BÁO

	Severity	Value	Name ▲	Operational data	Expression	Status
	Information	OK	Cisco IOS SNMP: Device has been replaced		<code>last(/SG300_ITC/system.hw.serialnumber,#1)<>last(/SG300_ITC/system.hw.serialnumber,#2) and length(last(/SG300_ITC/system.hw.serialnumber))>0</code>	Unknown
	Warning	OK	Cisco IOS SNMP: has been restarted Depends on: SG300_ITC: No SNMP data collection		<code>last(/SG300_ITC/system.uptime sysUpTime.0) <10m</code>	Enabled
	Warning	OK	Cisco IOS SNMP: High ICMP ping loss Depends on: SG300_ITC: Unavailable by ICMP ping	Loss: {ITEM.LASTVALUE1}	<code>min(/SG300_ITC/icmpingloss,5m)>{\$ICMP_LOSS_WARN} and min(/SG300_ITC/icmpingloss,5m)<100</code>	Enabled
	Warning	OK	Cisco IOS SNMP: High ICMP ping response time Depends on: SG300_ITC: High ICMP ping loss SG300_ITC: Unavailable by ICMP ping	Value: {ITEM.LASTVALUE1}	<code>avg(/SG300_ITC/icmpingsec,5m)>{\$ICMP_RESPONSE_TIME_WARN}</code>	Enabled
	Information	OK	Network interfaces discovery: Interface 1: Ethernet has changed to lower speed than it was before Depends on: SG300_ITC: Interface 1(): Link down	Current reported speed: {ITEM.LASTVALUE1}	<p>Problem: <code>change(/SG300_ITC/net.if.speed[ifHighSpeed.100000])<0 and last(/SG300_ITC/net.if.speed[ifHighSpeed.100000])>0 and (last(/SG300_ITC/net.if.type[ifType.100000])=6 or last(/SG300_ITC/net.if.type[ifType.100000])=7 or last(/SG300_ITC/net.if.type[ifType.100000])=11 or last(/SG300_ITC/net.if.type[ifType.100000])=62 or last(/SG300_ITC/net.if.type[ifType.100000])=69 or last(/SG300_ITC/net.if.type[ifType.100000])=117) and (last(/SG300_ITC/net.if.status[ifOperStatus.100000])<>2)</code></p> <p>Recovery: <code>(change(/SG300_ITC/net.if.speed[ifHighSpeed.100000])>0 and last(/SG300_ITC/net.if.speed[ifHighSpeed.100000])#2)>0 or (last(/SG300_ITC/net.if.status[ifOperStatus.100000])=2)</code></p>	Enabled
	Information	OK	Network interfaces discovery: Interface 1: Ethernet has changed to lower speed than it was before Depends on: SG300_ITC: Interface 1(): Link down	Current reported speed: {ITEM.LASTVALUE1}	<p>Problem: <code>change(/SG300_ITC/net.if.speed[ifHighSpeed.300000])<0 and last(/SG300_ITC/net.if.speed[ifHighSpeed.300000])>0 and (last(/SG300_ITC/net.if.type[ifType.300000])=6 or last(/SG300_ITC/net.if.type[ifType.300000])=7 or last(/SG300_ITC/net.if.type[ifType.300000])=11 or last(/SG300_ITC/net.if.type[ifType.300000])=62 or last(/SG300_ITC/net.if.type[ifType.300000])=69 or last(/SG300_ITC/net.if.type[ifType.300000])=117) and (last(/SG300_ITC/net.if.status[ifOperStatus.300000])<>2)</code></p> <p>Recovery: <code>(change(/SG300_ITC/net.if.speed[ifHighSpeed.300000])>0 and last(/SG300_ITC/net.if.speed[ifHighSpeed.300000])#2)>0 or (last(/SG300_ITC/net.if.status[ifOperStatus.300000])=2)</code></p>	Enabled
	Warning	OK	Network interfaces discovery: Interface 1: High bandwidth usage Depends on: SG300_ITC: Interface 1(): Link down	In: {ITEM.LASTVALUE1}, out: {ITEM.LASTVALUE3}, speed: {ITEM.LASTVALUE2}	<p>Problem: <code>(avg(/SG300_ITC/net.if.in[ifHCInOctets.100000],15m)>{\${IF.UTIL.MAX."1"}/100}*last(/SG300_ITC/net.if.speed[ifHighSpeed.100000]) or avg(/SG300_ITC/net.if.out[ifHCOutOctets.100000],15m)>{\${IF.UTIL.MAX."1"}/100}*last(/SG300_ITC/net.if.speed[ifHighSpeed.100000])) and last(/SG300_ITC/net.if.speed[ifHighSpeed.100000])>0</code></p> <p>Recovery: <code>avg(/SG300_ITC/net.if.in[ifHCInOctets.100000],15m)<{\${IF.UTIL.MAX."1"}-3}/100)*last(/SG300_ITC/net.if.speed[ifHighSpeed.100000]) and avg(/SG300_ITC/net.if.out[ifHCOutOctets.100000],15m)<{\${IF.UTIL.MAX."1"}-3}/100)*last(/SG300_ITC/net.if.speed[ifHighSpeed.100000])</code></p>	Enabled

CHƯƠNG 6. HỆ THỐNG CẢNH BÁO

<input type="checkbox"/>	Name ▲	Triggers	Key	Interval	History	Trends	Type	Status	Tags
<input type="checkbox"/>	... Cisco IOS SNMP: Hardware model name		system.hw.model	1h	2w		SNMP agent	Not supported	component: system
<input type="checkbox"/>	... Cisco IOS SNMP: Hardware serial number	Triggers 1	system.hw.serialnumber	1h	2w		SNMP agent	Not supported	component: system
<input type="checkbox"/>	... Cisco IOS SNMP: ICMP loss	Triggers 1	icmppingloss	1m	1w	365d	Simple check	Enabled	component: health component: network
<input type="checkbox"/>	... Cisco IOS SNMP: ICMP ping	Triggers 1	icmpping	1m	1w	365d	Simple check	Enabled	component: health component: network
<input type="checkbox"/>	... Cisco IOS SNMP: ICMP response time	Triggers 1	icmppingsec	1m	1w	365d	Simple check	Enabled	component: health component: network
<input type="checkbox"/>	... Network interfaces discovery: Interface 1(): Bits received	Triggers 1	net.if.in[ifHCInOctets.100000]	3m	7d	365d	SNMP agent	Enabled	component: network description interface: 1
<input type="checkbox"/>	... Network interfaces discovery: Interface 1(): Bits received	Triggers 1	net.if.in[ifHCInOctets.300000]	3m	7d	365d	SNMP agent	Enabled	component: network description interface: 1
<input type="checkbox"/>	... Network interfaces discovery: Interface 1(): Bits sent	Triggers 1	net.if.out[ifHCOutOctets.100000]	3m	7d	365d	SNMP agent	Enabled	component: network description interface: 1
<input type="checkbox"/>	... Network interfaces discovery: Interface 1(): Bits sent	Triggers 1	net.if.out[ifHCOutOctets.300000]	3m	7d	365d	SNMP agent	Enabled	component: network description interface: 1
<input type="checkbox"/>	... Network interfaces discovery: Interface 1(): Inbound packets discarded		net.if.in.discard[ifInDiscards.300000]	3m	7d	365d	SNMP agent	Enabled	component: network description interface: 1
<input type="checkbox"/>	... Network interfaces discovery: Interface 1(): Inbound packets discarded		net.if.in.discard[ifInDiscards.100000]	3m	7d	365d	SNMP agent	Enabled	component: network description interface: 1
<input type="checkbox"/>	... Network interfaces discovery: Interface 1(): Inbound packets with errors	Triggers 1	net.if.in.errors[ifInErrors.100000]	3m	7d	365d	SNMP agent	Enabled	component: network description interface: 1
<input type="checkbox"/>	... Network interfaces discovery: Interface 1(): Inbound packets with errors	Triggers 1	net.if.in.errors[ifInErrors.300000]	3m	7d	365d	SNMP agent	Enabled	component: network description interface: 1
<input type="checkbox"/>	... Network interfaces discovery: Interface 1(): Interface type	Triggers 1	net.if.type[ifType.100000]	1h	7d	0d	SNMP agent	Enabled	component: network description interface: 1
<input type="checkbox"/>	... Network interfaces discovery: Interface 1(): Interface type	Triggers 1	net.if.type[ifType.300000]	1h	7d	0d	SNMP agent	Enabled	component: network description interface: 1
<input type="checkbox"/>	... Network interfaces discovery: Interface 1(): Operational status	Triggers 2	net.if.status[ifOperStatus.100000]	1m	7d	0	SNMP agent	Enabled	component: network description interface: 1
<input type="checkbox"/>	... Network interfaces discovery: Interface 1(): Operational status	Triggers 2	net.if.status[ifOperStatus.300000]	1m	7d	0	SNMP agent	Enabled	component: network description interface: 1

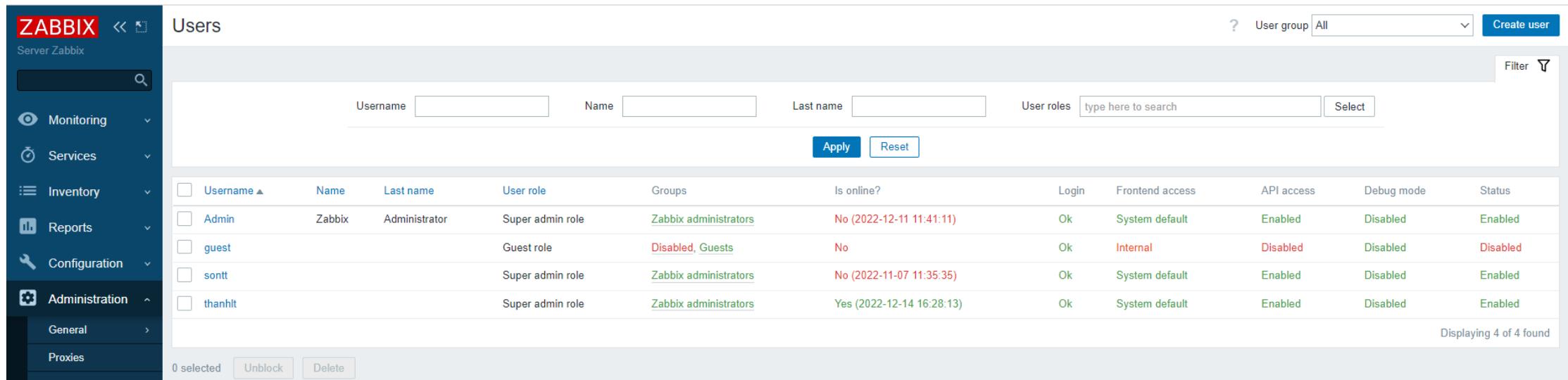
CHƯƠNG 6. HỆ THỐNG CẢNH BÁO

Phân quyền cảnh báo

Phân quyền trong cảnh báo giúp người quản trị mạng phân quyền tiếp nhận thông tin và xử lý thông tin cho các quản trị viên từ đó giúp việc giám sát và bảo trì hệ thống được tốt hơn.

CHƯƠNG 6. HỆ THỐNG CẢNH BÁO

Ví dụ: Phân quyền cảnh báo



The screenshot shows the Zabbix Administration interface, specifically the 'Users' section. The left sidebar includes links for Monitoring, Services, Inventory, Reports, Configuration, Administration (selected), General, and Proxies. The main area has search fields for Username, Name, Last name, and User roles, along with 'Apply' and 'Reset' buttons. A table lists four users:

Username	Name	Last name	User role	Groups	Is online?	Login	Frontend access	API access	Debug mode	Status
Admin	Zabbix	Administrator	Super admin role	Zabbix administrators	No (2022-12-11 11:41:11)	Ok	System default	Enabled	Disabled	Enabled
guest			Guest role	Disabled, Guests	No	Ok	Internal	Disabled	Disabled	Disabled
sontt			Super admin role	Zabbix administrators	No (2022-11-07 11:35:35)	Ok	System default	Enabled	Disabled	Enabled
thanht			Super admin role	Zabbix administrators	Yes (2022-12-14 16:28:13)	Ok	System default	Enabled	Disabled	Enabled

At the bottom, there are buttons for '0 selected', 'Unblock', and 'Delete'. A note at the bottom right says 'Displaying 4 of 4 found'.



CÁC KHÁI NIỆM CƠ BẢN VỀ QUẢN TRỊ MẠNG

Q & A