Лабораторна робота №16

Налаштування Zabbix SNMP-моніторингу.

Мета: набути практичних навичок з налаштування системи моніторингу Zabbix для збору даних через протокол SNMP у віртуалізованому середовищі.

Інструменти: гіпервізор VirtualBox, модель комп'ютерної мережі.



Теоретичні відомості

Рис. 16.1. Топологія мережі

На рис. 16.1 наведена модель комп'ютерної мережі, побудована під час виконання попередніх лабораторних робіт. На сервері Serv-G-N-2 розгорнуто систему моніторингу на базі Nagios 4.X. На сервері Zabbix-G-N працює сервер Zabbix з базовими налаштуваннями. В обох моніторингових системах налаштоване спостереження за Serv-G-N-1, WS-G-N-1, Serv-G-N-3. На хосту Serv-G-N-3 налаштований сервіс SNMP-серверу. У попередній лабораторній роботі на сервері Nagios 4.X (Serv-G-N-2) налаштовано моніторинг для збору даних через протокол SNMP.

Інструменти та можливості Zabbix для SNMP-моніторингу.

Zabbix підтримує SNMP через вбудовані можливості, які дозволяють зчитувати дані з пристроїв та серверів, які працюють як SNMP-агенти. Основні інструменти та можливості Zabbix для роботи з SNMP:

- Шаблони (Templates). Zabbix має готові шаблони для багатьох пристроїв, які використовують SNMP: Template Net SNMP або індивідуальні шаблони для різних пристроїв і серверів. Шаблони включають попередньо налаштовані елементи даних, тригери, графіки та екрани.
- Елементи даних (Items), що використовуються для збирання інформації через SNMP. Типи елементів:
 - ✓ SNMPv1 agent
 - SNMPv2 agent
 - SNMPv3 agent (з підтримкою аутентифікації та шифрування).
- Виклики SNMP OID, через які можливо вручну додати OID, якщо необхідні показники не охоплені стандартними шаблонами. Zabbix дозволяє зчитувати дані з різних таблиць SNMP (наприклад, інтерфейси, статус процесів).
- Автодетекція (Discovery). Zabbix може автоматично сканувати пристрої в мережі для виявлення SNMP-пристроїв та їхніх інтерфейсів. Автодетекція працює через SNMP LLD (Low-Level Discovery).
- SNMP Trap: Zabbix може отримувати SNMP-трапи (повідомлення, які ініціює сам агент). Для цього потрібно налаштувати службу SNMP Trap на сервері Zabbix.
- Графіки, тригери та сповіщення. На основі отриманих SNMP-даних можна налаштовувати сповіщення про події, а також створювати графіки продуктивності чи стану пристроїв.

Налаштування SNMP-моніторингу Linux-хосту у Zabbix.

												Hosts			
													VIEW	_	
$\epsilon \rightarrow G$, Не защищено 192.168	3.22.129:81/zabbix.php?na	me=&ip=&idn	= & port = & status = -	1&evaltype=0&tags%5B0%5D	%5Btag%5[D=&tags%5B0%	5D%5Bo 🛱	QÊ	☆ 角 🛛	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	< 7	Dashboards		
	Hosts									2 500	te bost 55		Problems		
Zabbix-22-40	110363												Latest data	Name	
	< 7										\sim >		Graphs	. and the	turne here to re-
~		No.			(mar. 6)	all a Consta	-						Web	. groops	type nere to set
🗄 Dashboards		name			status Hiy En	abred Disable	•						Inventory	IP	
Maniforing +		Host groups type here to sean	ch	Select	Tags /nd/Or	Or								DNS	
C Noncomy .		IP			tag	C	ontains 👻	value	Remove				CONFIGURATION		
Problems		DNS			940								Hust	Port	
Hosts		Port			Show hosts in maintenance 🗹	Show suppress	ed problems						nems T	severity	Not classified
Latest data		Secondary Net also rited	Mining	- Histo									inggers		Information
Maps		Information	Average	Disaster									oraphs		
Discovery													Liscovery		
着 Services 🔹 👻				(Save as Apply Reset							_	UVED	-	
A	Name -	Interface	Australia	Thur		Otation	Intert data	Broblems	Granhe	Darbhoaste	1000	Name 🔺	SCRIFTS	oe	
Twentory *			Joanny	inda.	_		Latest Gata	Tionalis	orapita -			Gateway	Detect operating system		
🔐 Reports 🔹 👻	Gateway NAL Network			ouss: network target: or	-	Brabked	Latest data 3	Problems	urapns	Lashboards	1160		Ping		
Data collection	Serv-22-40-1	192.168.40.131:10050	ZBX	class: os target: uindous	3	Enabled	Latest data 105	1	Graphs 12	Dashboards 3	10.6P	Serv-22-	Traceroute	8.40.131	:10060
-	Serv-22-40-3	192.168.40.137:10050	Zex	class: os target: linux		Enabled	Latest data 15	1	Graphs 15	Dashboards 3	Web	Serv-22	182.	08.40.137	:10050
슈 Alerts ㆍ	WS-22-40-1		ZIX	class: os target: uindows	3	Enabled	Latest data 107	1	Graphs 12	Dashboards 3	Web	WS-22-40	-1		
🔐 Users 👻	Zabbix-22-40	127.0.0.1:10050	ZIX	olass: os olass: software	target: linux +++	Enabled	Latest data 161	1	Graphs 20	Dashboards 4	Web				
										Direlavia	A of A found	∠abbix-22	4U 127.	J.U.1:10050	J

Рис. 16.2. Меню [Monitoring]-[Hosts]WEB-інтерфейсу серверу Zabbix-22-40

Хост Serv-22-40-3, де налаштовано сервіс SNMP-серверу, вже моніториться у Zabbix через Zabbix Agent. Додавання SNMP-моніторингу можна зробити саме через інтерфейс цього хосту. Відкриваємо Zabbix вебінтерфейс та переходимо у меню [Monitoring] – [Hosts]. Обираємо у переліку хостів Serv-22-40-3 та натискаючи його потрапляємо у список контекстного меню, де обираємо пункт [Configuration]-[Host]. У дочірньому вікні [Host] натискаємо меню [Add] для додавання інтерфейсів [Interfaces]. Ця дія викликає контекстне меню, де ми обираємо пункт SNMP. У якості IP Address нового інтерфейсу дублюємо адресу хосту, яка використовується для Zabbix Agent (192.168.40.137).

Port: стандартний порт для SNMP — 161. Якщо на сервері SNMP налаштований для прослуховування на іншому порту, вам слід вказати цей порт.

SNMP Version: - SNMPv2. Якщо в конфігурації SNMP-сервера на хосту зазначено іншу версію (наприклад, SNMPv3), потрібно вибрати відповідну версію.

SNMP Community: ви правильно вказали параметр {\$SNMP_COMMUNITY}. Це змінна, яку ви можете визначити у шаблоні або глобальних налаштуваннях Zabbix. Якщо використовуєте конкретне значення для community string, можна ввести його напряму (наприклад, public 192.168.40.137 або інше, залежно від конфігурації SNMP на сервері).



Рис. 16.3. Меню [Monitoring]-[Hosts]WEB-інтерфейсу серверу Zabbix-22-40

Додавання SNMP-Items до системи моніторингу Zabbix.

Host

Перейдемо у меню [Data collection]-[Hosts] WEB-інтерфейсу серверу Zabbix-22-40 та порівняємо кількість Items хосту Serv-22-40-3 до та після додавання SNMP-інтерфейсу у налаштування .На рис. 16.4 ми бачимо, що це значення не змінилося і дорівнює у даному випадку 75. Таким чином, підключення SNMP-інтерфейсу не впливає на елементи моніторингу хосту.

Serv-22-40-3	Items 75 Trig	ggers 30 (Graphs 16	Discovery 3	Web	192.1	168.40.137:10050	Linux by Zabbix agent active	Enabled	Z8X]
Serv-22-40-3	Items 7	5 Triggers	30 Graph:	s 16 Discovery	з W	/eb	192.168.40.137:10050	Linux by Zabbix agent active	Enabled	ZBX SNMP

Рис. 16.4. Меню [Data collection]-[Hosts]WEB-інтерфейсу серверу Zabbix-22-40. Порівняння кількості Items до та після додавання SNMP-інтерфейсу у налаштуваннях хосту Serv-22-40-3.

Самий простий метод автоматичного додавання Items через додавання Template до існуючого хосту у поточній на поточній версії Zabbix не працює. Є системна проблема з можливістю додавання до хосту додаткових Templates. У нашому випадку хост використовує шаблон "Linux by Zabbix agent active". При спробі додавання шаблону "Linux by SNMP" виникає помилка "Cannot inherit item with key "system.name" of template "Linux by SNMP" to host "Serv-22-40-3", because an item with the same key is already inherited from template "Linux by Zabbix agent active". Проблема є системною і криється у структурі бази даних Zabbix.



Puc. 16.5. Меню [Monitoring]-[Hosts]WEB-iнтерфейсу серверу Zabbix-22-40. Спроба додавання Template "Linux by SNMP" до шаблонів хосту Serv-22-40-3.

Для поточної версії Zabbix, якщо потрібно використовувати обидва шаблони без змін, можна створити окремі хости. У меню [Monitoring]-[Hosts]WEB-інтерфейсу серверу Zabbix-22-40 натискаємо кнопку [Create host] (верхній правий куток вікна) та створюємо тестовий хост Serv-22-40-3-SNMP:

Host IPMI Ta	gs Maoros Inventory Encryption Value mapping					
* Host name	Serv-22-40-3-SMNP					
Visible name	Serv-22-40-3-SMNP					
Templates	Name Action					
	Linux by SNMP Unlink Unlink and clear					
	type here to search	Select				
* Host groups	Linux servers X type here to search	Select				
Interfaces	Type IP address DNS name	Connect to Port Default				
	~ SNMP 192.108.40.137	IP DNS 161 Remove				
	* SNMP version SNMPv2 ~					
	* SNMP community public					
	Max repetition count (2) 10					
	Use combined requests					
	Add		Name 🔺	Interface	Availability	Tags
Description	Test version of Serv-22-40-3 for SNM/P		Gateway NAT Network			class: network target: icmp
			Serv-22-40-1	192.168.40.131:10050	ZBX	class: os target: windows
			Serv-22-40-3	192.168.40.137:10050	ZBX SNMP	class: os target: linux
			Serv-22-40-3-SMINP	192.168.40.137:161	SNUP	class: os target: linux
Monitored by	Server Proxy Proxy group		WS-22-40-1		ZBX	class: os target: windows
		Undate Clone	Zabbix-22-40	127.0.0.1:10050	Z8X	class: os class: software target: linux •

На рис.16.7 показано як видалити помилково створений, або тестовий хост у контексті меню

[Data collection]-[Hosts]

Спробуємо додати SNMP-показники до вже існуючого в системі Zabbix хосту, замість створення окремого, додаткового SNMP-хосту.

	Name 🔺	Items	Triggers	Graphs	Discovery	Web	Interface
	Gateway NAT Network	Items 3	Triggers 3	Graphs	Discovery	Web	
	Serv-22-40-1	Items 108	Triggers 74	Graphs 12	Discovery 4	Web	192.168.40.131:10050
	Serv-22-40-3	Items 76	Triggers 30	Graphs 16	Discovery 3	Web	192.168.40.137:10050
2	Serv-22-40-3-SMNP	Items 62	Triggers 20	Graphs 11	Discovery 5	Web	192.168.40.137:161
	NS-22-40-1	Items 107	Triggers 73	Graphs 12	Discovery 4	Web	
	Zabbix-22-40	Items 161	Triggers 92	Graphs 20	Discovery 6	Web	127.0.0.1:10050



Такий підхід дозволить уникнути дублювання об'єктів моніторингу та підтримувати актуальність інформації в одному місці, що є кращою практикою з точки зору організації та ефективності моніторингу. Уникаючи створення зайвих хостів, адміністратор зберігає прозорість у налаштуванні та підвищує ефективність управління мережею.

Переходимо у меню [Data collection]-[Hosts] та натискаємо підменю Items відповідного хосту. У нашому випадку це Items (75) хосту Serv-22-40-3. Відкривається вікно [Items], де у правому верхньому кутку є кнопка [Create item]. Потрапляємо у дочірнє вікно, де заповнюємо характеристики об'єкту моніторингу. Назва Item – «CPU Load 1 min SNMP», тип – «SNMP agent», key – «cpu.load.1min.snmp». У якості SNMP OID вказуємо відповідний рядок – «.1.3.6.1.4.1.2021.10.1.3.1». Після натискання кнопки [Update], при умові вірного заповнення всіх полів, маємо активований для моніторингу Item. У даному прикладі це у відповідності до значення рядку SNMP OID – «Перевірка завантаження CPU за 1 хв»



Рис. 16.8. Створення SNMP Item для SNMP OID – «Перевірки завантаження CPU за 1 хв».

Натискання трьох крапок ліворуч від назви Item дозволяє викликати контекстне меню для нього. Тут можливо примусово отримати дані моніторингу, переглянути отримані дані, відредагувати чи переглянути значення Host та самого Item.

До речі, перегляд Items хосту Serv-22-40-3 показує, що їх стало на 1 більше ©

VIEW		
Latest data		
Graph	1	
\alues		
500 latest values	Name 🔺	Items
CONFIGURATION	Gaterolay NAT Network	Items 3
ltem		
Host	Sept 22.40.1	Items 10
Triggers	1 0010-22-40-1	nems ibi
Create trigger	C 800/22/40/2	Home 78
Create dependent item	5810-22-40-5	items ro
Create dependent discovery rule	WS-22-40-1	Items 107
ACTIONS		
Execute now	Zabbix-22-40	Items 16
Check CHO load in Timin		

Рис. 16.9. Контекстне меню Item хосту

Аналогічно додаємо Item, що нас цікавлять у системі моніторингу для даного хосту. Орієнтуємося на обрані у попередній лабораторній роботі при налаштуванні SNMP моніторингу хосту Serv-G-N-3 у Nagios.

Не забуваємо, що для обробки системою моніторингу вказується повний, точний OID-рядок. Перед додаванням перевіряємо його у командному рядку за допомогою snmpwalk. На рис 16.10 показана така перевірка для кількох OID. Наприклад для OID .1.3.6.1.4.1.2021.4.3 у цьому конкретному випадку рядок буде мати значення .1.3.6.1.4.1.2021.4.3.0

₽°	student@serv-22-40-3: ~
student@serv-22-40-3:~\$ snmpwalk -v 2c	-c public localhost .1.3.6.1.4.1.2021.4.5
iso.3.6.1.4.1.2021.4.5.0 = INTEGER: 980	0492
student@serv-22-40-3:~\$ snmpwalk -v 2c	-c public localhost .1.3.6.1.4.1.2021.4.5
iso.3.6.1.4.1.2021.4.5.0 = INTEGER: 980	0492
student@serv-22-40-3:~\$ snmpwalk -v 2c	-c public localhost .1.3.6.1.4.1.2021.4.4
iso.3.6.1.4.1.2021.4.4.0 = INTEGER: 196	50956
student@serv-22-40-3:~\$ snmpwalk -v 2c	-c public localhost .1.3.6.1.4.1.2021.4.3
iso.3.6.1.4.1.2021.4.3.0 = INTEGER: 196	50956

Рис. 16.10. Приклад перевірки кількох OID використання пам'яті хосту

Створення графіку з показниками на прикладі отриманих через SNMP

Створення графіків у Zabbix, і не тільки у Zabbix ^(©), є потужним інструментом для аналізу продуктивності та спрощення моніторингу інфраструктури. У цій лабораторній роботі ми розглянемо приклад аналізу продуктивності серверу, побудувавши графік з використанням таких метрик завантаження CPU (%), використання оперативної пам'яті (%) та використання SWAP (%). Вивчення такого графіку дозволить виявити "вузькі місця" у ресурсах (наприклад, недостатньо оперативної пам'яті, що призводить до активного використання SWAP) та визначити час для планування масштабування чи оптимізації.

Переходимо у меню [Data collection]-[Hosts] та натискаємо підменю Graphs відповідного хосту. У нашому випадку це Graphs (16) хосту Serv-22-40-3. Відкривається вікно [Graphs], де у правому верхньому кутку є кнопка [Create graph]. Потрапляємо у дочірнє вікно, де заповнюємо характеристики об'єкту моніторингу: назву графіку, його розміри, тип, додаємо Items, взаємозалежність яких буде відображатися на ньому.



Рис. 16.11. Створення графіку взаємозалежності SNMP показників навантаження ЦП, вільної RAM та вільного SWAP для хосту Serv-22-40-3

Існуючі графіки зручно переглядати у меню [Monitoring]-[Hosts]-[Graphs] відповідного хосту. У вікні, що завантажиться обираємо період, який буде відображатися на графіках.

Graphs						? 53
				< Z0	om out > 🕓 La	est 1 day 🔽 Filter
From	now-24h	i	Last 2 days	Yesterday	Today	Last 5 minutes
To	now	□曲	Last 7 days	Day before yesterday	Today so far	Last 15 minutes
	_		Last 30 days	This day last week	This week	Last 30 minutes
	P	oply	Last 3 months	Previous week	This week so far	Last 1 hour
			Last 6 months	Previous month	This month	Last 3 hours
			Last 1 year	Previous year	This month so far	Last 6 hours
			Last 2 years		This year	Last 12 hours
					This year so far	Last 1 day

Рис. 16.12. Вибір звітного періоду для відображення графіків у меню [Monitoring]-[Hosts]-[Graphs]

Створення класичного Dashboard

У Zabbix дашборди використовуються для швидкого огляду стану інфраструктури, а також для аналізу її продуктивності. Основні типи корисних дашбордів: оглядовий дашборд (Overview Dashboard), мережевий дашборд, що аналізує стан мережевих пристроїв та інтерфейсів, дашборд для моніторингу сервісів, що слідкує за доступністю та продуктивністю окремих сервісів, безпековий дашборд, що відстежує інцидентів безпеки та спроб проникнення та інші.

Створимо новий користувацький DashBoard на основі побудованого нами графіку. До нього включимо графік Server Performance Analysis, відображення логу проблем хосту, годинник та географічну мапу. Переходимо у меню [DashBoards] та обираємо у меню кнопки [Actions] пункт [Create New].

Власника залишаємо без змін, назва Serv-G-N-3 SNM-N, де N-номер варіанту. Період оновлення залишаємо 30 сек, або змінюємо на 1 хв. Після цього у робочій області створюваного DashBoard з'являється фрейм першого елементу. Налаштовуємо його тип як Graph (classic) з назвою серверу та обираємо у якості графіку створений нами на попередніх кроках графік [Server Performance Analysis].

	Global view					Edit dashboard 📃 🕵
Zabbi×22-40	All dashboards / Global view				ACTIONS Sharing	
<u>ч</u>	Top hosts by CPU utilization		System information		Create new Clone	
88 Dashboards	Host name Utilization 1m avg 5m avg 15m avg Processes	2 05	Parameter	Value	Det. Delete	
🚇 Monitoring 🗸 🗸	Zabbix22:40 32.08 % 0.93 0.93 0.64 242	J.35	Zabbix server is running	Yes	loca Create new report	0.07
🚓 Services 🗸		Values per second	Zabbix server version	7.0.6	New View related reports	9.37
s			Zabbix frontend version	7.0.6	New update available	
Unventory *			Number of hosts (enabled/disabled)	5	5/0	Kiev
🔐 Reports 🛛 👻			Number of templates	329		1001
Data collection			Number of items (en abled/disabled/not supp	orted) 460	446 / 0 / 14	
~			Number of triggers (enabled/disabled [probl-	em/ok]) 272	272/0 8/284	
			Serv-22-40-3 SNM-40	Add widget	sph (classic) 👻	? 🗙 Show header 🗹
New dashboard			All dashboards / Serv-22-40-3 SNM-40	Name Se	n+22-40-3	
All dashboards / New Deshboard p	properties	? >	Page 1 ***	Refresh interval Det Source 0	fault (1 minute) 👻 raph Simple graph	
	*Owner Admin (Zabšo Administrator) × Select			* Graph Se	rv-22-40-3: Server Performance Analysis ×	Select ¥
Default page	• Name Service-Russ SNM-RU		G	Show legend	ashboard wreget Custom	
Start slidesho	wautomatically 🕑		Click and drag to	Override host typ	e here to search	Select 🛩
Add a new w		Apply Cancel	desired size.			Add Cancel

Рис. 16.13. Створення DashBoard "Serv-22-40-3 SNM-40" та налаштування першого елементу – графіку.

У якості другого елементу DashBoard налаштовуємо «віджет проблем» хосту. Третій елемент – віджет годинника. Четвертий елемент – географічна мапа, де у полі "Initial View" задано координати м. Житомир ©. Якщо Ви розміщаєте свій сервер Serv-G-N-3 у Бангкоку, введіть його координати в цьому полі ©.

Add widget		?	× Ad	d widget		? ×
Туре	Problems V S	ihow header 🗹	1	Туре	Clock ~	Show header 🗹
Name	Sen-22-40-3. Problems	1		Name	default	
Refresh interval	Default (1 minute)		R	efresh interval	1 minute 👻	
Show	Recent problems Problems History			Time type	Local time 👻	
Underwood		0.1.1.1.1.1		Clock type	Analog Digital	
Host groups	type here to search	Select 👻				Add Cancel
Exclude host groups	type here to search	Select				
Hotte	Serv22.40.3 V	Salart V				
11035	type here to search	Jeleor	Ad	d widget		
Problem		7		Туре	Geomap 👻	Show header 🗹
Severity	Not classified Warping High			Name	Zhytomyr SNM-40	
occomy	Information Average Disaster		R	efresh interval	Default (1 minute) Y	
Problem taos	And/Or Or			Host groups	Linux servers × type here to search	Select 👻
	Ann Castring and Leafus	Bernun		Hosts	Serv-22-40-3 ×	Select 🗸
	Add	Kennove		[type here to search	
Show tags	None 1 2 3			Tags	And/Or Or	
T				[tag Contains V Value	Remove
Taginame	Full Shortened None			5 nitial view 🙆 🗍	50 25444 28 85778	
Tag display priority	comma-separated list				Ad	d Cancel
Show operational data	None Separately With problem name					
	A	dd Cancel				

Рис. 16.14. Додавання до DashBoard "Serv-22-40-3 SNM-40" наступних елементів.



Рис. 16.15. Загальний вигляд створеного DashBoard "Serv-22-40-3 SNM-40".

Налаштування тригерів

Тригери (Triggers) — це механізм у Zabbix, який використовується для автоматичного аналізу даних, що надходять від елементів (Items), і визначення, чи є стан моніторингу нормальним або проблемним. Тригер спрацьовує на основі заданого логічного виразу (expression), який оцінює отримані дані та порівнює їх із певними пороговими значеннями.

Тригери використовуються для виявлення проблем - визначення аномалій, наприклад, завантаження СРU понад 80%, низький вільний простір на диску, або відсутність даних від пристрою. З тригерами пов'язані дії (Actions), які можуть надсилати повідомлення (email, Telegram, Slack) або виконувати команди (наприклад, перезапуск служби). Тригери мають рівні важливості (severity), що дозволяє класифікувати проблеми за критичністю (наприклад, від «Not classified» до «Disaster»). Тригери сприяють автоматичному реагуванню на інциденти без потреби постійного ручного втручання.

Алгоритм роботи тригера наступний - дані отримуються від Item: Zabbix збирає дані через SNMP, агентів, скрипти тощо. Вираз тригера аналізує дані: наприклад, перевіряє, чи значення CPU > 80%. Якщо вираз оцінюється як true, тригер змінює стан на Problem. Коли умова більше не виконується, тригер повертається до стану OK. Для створення цього тригеру переходимо у меню [Data Collection] – [Hosts] та обираємо меню [Triggers] відповідного хосту. У нашому випадку це буде [Serv-22-40-3] – [Triggers(30)]. У правому верхгьому кутку завантаженого вікна [Triggers] натискаємо кнопку [Create Trigger]. Вантажиться дочірнє вікно [New trigger], де пишемо назву тригеру «High CPU Usage» та натискаємо Add для написання вмісту поля Expression. По кнопці [Select] обираємо створений нами раніше Item "SNMP. Check CPU Load 5 min" і у виразі Result ставимо умову >80.

Data collection 、										
				New tri	gger		Condition			×
Template groups	Name 🔺	Items	Triggers	Triance	Trees	Descedenci				
Host groups	Gatemay NAT Network	Items 3	Triggers 3	mgger	lays	Dependenci	^ Item	Serv-22-40-3: SNMP, Check CPU Load 6 min	Select	
-		active o	mggers v			* N	Function	last() - Last (most recent) T value	~	
lemplates	Senv-22-40-1	Items 108	Triggers 74			Event n	Last of (T)	5 Count		
Hosts	Serv-22-40-3	Items 81	Triggers 30			Operational	Time shift	now-h Time		
Maintenance	W/S-22-40-1	Items 107	Triggers 73			Sev	* Result	> ~ 80		
Event correlation	Zabbix-22-40	Items 161	Triggers 92			* Expres			Insert Cancel	
Discovery										

Рис. 16.16. Створення Triger «High CPU Usage» для Serv-22-40-3.

Натискаємо кнопку [Insert] вікна [Condition] і знову потрапляємо до вікна [New trigger]. Ще раз переглядаємо отримані заповнення, та обираємо значення [Severity] High.

Отриманий вираз Вираз

last(/Serv-22-40-3/cpu.load.5min.snmp.#3)>80

перевіряє, чи останнє значення метрики cpu.load.5min перевищує 80. Якщо необхідно додати резервний вираз для ситуації, коли середнє завантаження CPU на інших інтервалах часу також має перевищення, тригер може бути розширений з використанням операторів OR чи AND. Наприклад:

New trigger	
Trigger Tags Dependencies	
* Name	High CPU Usage
Event name	High CPU Usage
Operational data	
Severity	Not classified Information Warning Average High Disaster
* Expression	last(/Serv-22-40-3/cpu.load.5min.srmp;#5)>80
OK event concention	
PROBLEM event generation mode	Single Multiple
OK event closes	All problems All problems if tan values match
Allow manual close	
Menu entry name 🚳	Trioger URL
Menu entry URL	
Description	
	Add Cancel

last(/Serv-22-40-3/cpu.load.1min.snmp.#3)>90 OR last(/Serv-22-40-3/cpu.load.5min.snmp.#3)>80

Рис. 16.17. Створення Triger «High CPU Usage» для Serv-22-40-3.

Налаштування сповіщень

Поточна на момент написання цього документу версія Zabbix має вбудовані шаблони для всіх основних медіа-типів сповіщень. Переглянути це можливо у меню [Data Collection] – [Media Types].

Налаштуємо сповіщення для створеного на попередньому кроці тригеру «High CPU Usage» для серверу Serv-22-40-3 за допомогою Media Type Gmail. Для цього, створимо користувача Zabbix, від імені якого буде виконуватись ця дія. Переходимо у меню [Users] – [Users] і у правому верхньому кутку вікна натискаємо кнопку [Create User]. Ім'я користувача відповідає шаблону User-G-N і він є членом групи Internal. У закладці [Permisions] додаємо роль [User Role].

Licore			Users						
03613			User Media	Permissions					
User Media Permissions					* Role	User role \times		Select	
* Username	user-22-40			U	ser type	User			
Name	Igor			Perr	nissions	Group All groups	Type Hosts		Permissions None
Last name	F alkovsky					All groups	Templates		None
Groups	Internal ×	Select				Permissions can be assigned	d for user groups o	nly.	
* Password 👔	type here to search			Das	hboards	Access to UI elements Dashboards			
* Password (once again)				Мо	nitoring	Problems Hosts Latest data	Maps		
	Password is not mandatory for non internal authentication type.			\$	Services	Services SLA report			
Language	System default 🗸 💡			In	ventory	Overview Hosts	_		
Time zone	(UTC+02:00) Europe/Kyiv				Reports	Availability report Top 100 trigg	gers		
Theme	System default 🗸 🗸		Read	l-write access to	services	Access to services			
Auto-login			Rea	d-only access to	services	Al			
Auto-logout	15m					Access to modules			
* Refresh	30s					Action log Clock Data overvi Geomap Graph Graph (classi	ieu Discovery sta ic) Graph prototyp	tus Favorite Honeycom	graphs Favorite maps Gauge b Host availability
* Rows per page	50					Host navigator Item history Problem hosts Problems Pro	tern navigator [Iter blems by severity]	n value Map SLA report S	Map navigation tree Pie chart System information Top hosts
URL (after login)						Top triggers Trigger overview	URL Web monito	ring	
	Add Cancel					Access to API Enabled			

Рис. 16.18. Створення користувача user-22-40.

Активуємо натисканням його статусу у пункті меню [Alerts] – [Media Types] тип [Telegram]. Статус має змінитися з [Disabled] на [Enabled] та редагуємо налаштування цього Media.

SysAid	Webhook Disabled a Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test
🔽 Telegram	Webhook Enabled 4 Report not supported items. Report not supported low level discovery rules. Report problems to Zabbix administrators. Report unknown triggers	Test
TOP desk	Webhook Disabled A Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix	Test

Рис. 16.19. Активація media для Telegram.

У додатку 1 описано створення та виділення Telegram bot. Для налаштування сповіщень у телеграм необхідні token та іd створеного для цього бота. Натискаємо меню Telegram та у діалозі налаштувань Media Туре для Telegram заповнюємо наступні поля:

Поле	Значення	Налаштування
Message	{ALERT.MESSAGE}	саме повідомлення, яке отримуватиме користувач.
ParseMode		форматування тексту (наприклад, Markdown, HTML, або залишити пустим).
Subject	{ALERT.SUBJECT}	заголовок повідомлення.
То	{ALERT.SENDTO}	отримувач повідомлення (сюди передається ІD чату).
Token		Token Telegram bot
	Media type	? ×

Media type Message ter	nplates 5 Options		
* Name	Telegram		
Туре	Webhook 🖌		
Parameters	Name	Value	Action
	disable_notification	false	Remove
	Message	{ALERT.MESSAGE}	Remove
	ParseMode		Remove
	Subject	{ALERT.SUBJECT}	Remove
	То	699306931	Remove
	Token	7811542868:A	Remove
	Add		
* Script	var Telegram = (
* Timeout	10s		
Process tags			
include event menu entry			
* Menu entry name			
* Menu entry URL			
Description	https://git.zabbix.com/proje <i>cts</i> /ZBX/repos/zabbix/browse/templates/media/ telegram		
		Update Clon	e Delete

Рис. 16.20. Заповнення Media Туре для Telegram.

Якщо всі поля вірно заповнено, виклик вікна Test через відповідне меню Media Type для Telegram поверне «Media type test successful.»

Telegram	Webhook	Enabled	4	Test media type	"Telegram"	×
Test				Media Message ParseMode Subject To	[ALERT.MESSA6E] [ALERT.SUBJECT] [699306931 [7811542888:AAE38wiwAe8MDuB2Y88.cov11L74xDowDRI	
@Zabbix-22-40 X	Zabbix-22-40 Alerts Bot bot		۹ 🗆 :	Response	ok	ī
CB Cabbix-22-40 Alerts B Fri (ALERT.SUBJECT) (ALERT.MES	{ALERT.SUBJECT} {ALERT.MESSAGE} 17:34 {ALERT.SUBJECT} {ALERT.MESSAGE} 17:34				Baroone hose: String	11
					Deen log	
					Test Cance	1

Рис. 16.21. Тестування Media Туре для Telegram.

Додаємо медіа-тип Telegram до створеного на попередніх кроках користувача User-G-N. Переходимо у меню [Users] – [Users] та обираємо користувача (user_22_40). Вкладка [Media] – [Add]. Заповнюємо

Type: Telegram	Send to: 699306931
----------------	--------------------

When active: 1-7,00:00-24:00

Use if severity: обираємо всі рівні або лише потрібні для цього користувача. Enabled: Так

Users			
User Media Permissions			
* Username	user-22-40		
Last name	F alkovsky		
Groups	Internal × type here to search	Media	
Password	Change password	Туре	Telegram 🜱
Language	System default 🗸 👔	* Send to	699306931
Time zone	(UTC+02:00) Europe/Kyiv	* When active	1-7,00:00-24:00
Theme	System default 🗸	Use if severity	Vot classified
Auto-login			 ✓ Information ✓ Warning
Auto-logout	16m		V Average
* Refresh	30s		- High
* Rows per page	50		✓ Disaster
URL (after login)		Enabled	
	Update Delete Cancel		Add

Рис. 16.22. Налаштування Media для користувача User-22-40 у Zabbix

Налаштовуємо дію (Action) для сповіщень у Telegram. Переходимо у меню [Allert] – [Actions] – [Trigger Actions] та обираємо у верхньому правому кутку вікна [Trigger Actions] кнопку [Create Action]. На рис. 16.23 показаний приклад створення сповіщення для окремої події на сервері Serv-22-40-1

Operation details

Operation Send message Steps 1 . 1 (0 - infinitely)
Step duration 0 (0 - use action default) * At least one user or user group must be selected. Send to user groups type here to search Select Send to users user-22-40 (Igor Falkovsky) × Select type here to searc New action Send only to Telegram Action Operations 1 Custom message 🔽 * Name Send alert to Telegram Subject {TRIGGER.STATUS}: {TRIGGER.NAME} Message Onosiųenus si<u>a Zabbid</u> Craryo: (TRIOGER.STATUS) Проблема: (TRIOGER.MAME) Ceprep: (HOST.NAME) Чао: (EVENT.DATE) (EVENT.TIME) Type of calculation And/Or Y A and E and D Conditions Label Host equals Serv-22-40-1 Remove Remove Trigger severity equals Warning Trigger equals Serv-22-40-1: CPU interrupt time is too high Add Enabled 🔽 Conditions Label Name Action * At least one operation must exist. Add Add Cancel Add Cancel Trigger actions 🗸 Action enabled Name Status Any Enabled Disabled Apply Reset Name -Report problems to Zabbix administrators Send message to user groups: Zabbix administrators via all media Trigger equals Serv-22-40-1: CPU interrupt time is too high Send alert to Telegram Send message to users: user-22-40 (Igor Falkovsky) via Telegram Trigger severity equals Warning Host equals Serv-22-40-1 1 selected Enable Disable Delete

Якщо все налаштовано правильно, має прийти сповіщення в Telegram. 🖾

Puc. 16.23. Налаштування Trigger Actions на відправку сповіщення у Telegram для події "CPU interrupt time is too high" для серверу Serv-22-40-1

Завдання до лабораторної роботи

- 1. Налаштуйте у системі моніторингу Zabbix (Zabbix-G-N) для серверу Serv-G-N-3 стандартний SNMPv2 моніторинг. Перегляньте чи додалися автоматично Items при цьому.
- 2. Додайте нові Master Items для важливих OID (CPU, RAM), аналогічні налаштованим SNMP-items у системі моніторингу Nagios Core. Зверніть увагу, що у майбутніх завданнях будуть використовуватись наступні мережеві OID: прийняті та передані байти на інтерфейсі, кількість помилок у вхідних пакетах та кількість помилок у вихідних пакетах.
- 3. Створіть графік моніторингу мережевої активності з показниками, які отримуєте через SNMP (прийняті та передані байти на інтерфейсі, кількість помилок у вхідних пакетах та кількість помилок у вихідних пакетах). Розмістіть отримані SNMP-дані (графіки, сповіщення і т.і.) на окремому DashBoard.
- 4. Для створених SNMP-даних налаштуйте тригери визначення критичних подій. Порогові значення для критичних подій оберіть на власний розсуд.
- 5. Створіть у Telegram бот zabbixGNbot, де G числова частина імені групи, а N номер варіанту, налаштуйте та виконайте тестування Media Type для Telegram. Створення додаткових користувачів, та налаштування Media не вимагається.

Звіт має містити:

- лістинг використаних команд;
- короткий опис редагування файлів конфігурації;
- скріншоти налаштувань та підключень.

Додаток 1.

Створення та видалення Telegram-бота для використання у сповіщеннях.

Для створення Telegram-бота - входимо у Telegram і знаходимо бота BotFather. Надсилаємо команду /start, та виконуємо команду /newbot. Вводимо ім'я бота (наприклад, Zabbix-G-N Alerts Bot) та унікальне ім'я для бота, яке закінчується на bot (наприклад, zabbixGNbot).



Рис. 16.24. Створення Telegram бота zabbix2240bot.

Якщо дані у діалозі телеграм введено коректно, BotFather надасть токен вигляду 123456:ABC-DEF1234ghlkl-zyx57W2v1u123ew11

Зверніть увагу на можливість доступу до Menu графічного керування BotFather в нижній частині діалогу. Зберігаємо токен, оскільки він знадобиться для налаштування Zabbix.

Токен Telegram-бота — це фактично "пароль" для доступу до API цього бота. Хто має токен, той може керувати ботом, надсилати та отримувати повідомлення, виконувати API-запити від його імені.

Ризики витоку токена

Якщо ваш токен потрапить у чужі руки, зловмисник може:

- Використовувати вашого бота для розсилки спаму.
- Отримати доступ до ваших чатів (якщо бот зберігає повідомлення).
- Використовувати бота в шахрайських схемах або для автоматизації атак.

Щоб видалити Telegram-бота, створеного через BotFather, входимо у Telegram та знаходимо бота BotFather. Відправляємо команду /start, якщо ще не починали з ним діалог та надсилаємо команду /deletebot. BotFather попросить ввести ім'я бота, який необхідно видалити (наприклад, @Zabbix2024bot). Підтверджуємо видалення, дотримуючись інструкцій BotFather. Після цього бот буде видалено, а його токен стане недійсним. Однак Telegram не дозволяє повністю "стерти" бота – його ім'я та дані можуть залишитися на деякий час в базі, але він більше не буде працювати.

BotFather 🤡 2 312 784 monthly users	م		
	/deletebot	20:02	11
Choose a bot to delete. 20:02			
	@zabbix2240bot	20:02	11
OK, you selected @zabbix2240bot. Are you sure?			
Send 'Yes, I am totally sure.' to confirm you really want to delete this bot. 20:02			
	Yes, I am totally sure.		11
Done! The bot is gone. /help20:02			

Рис. 16.25. Видалення Telegram бота zabbix2240bot.

Якщо ви повністю видалили бота через BotFather, то Telegram відкликає його токен, і він стає недійсним. Навіть якщо хтось мав доступ до токена раніше, використати його більше не можна.

Якщо ви помітили, що токен «мав витік» (наприклад, в коді на GitHub), терміновозмініть токен через BotFather. Відкрийте BotFather і надішліть команду /token. Виберіть свого бота та запросіть новий токен. Після цього старий токен стане недійсним. Оновіть код та налаштуйте сервіси, які використовували старий токен.

Після отримання токену та імен службового боту необхідно отримати ID чату. Переходимо до нового боту в Telegram і натискаємо Start.

Знаходимо chat ID за допомогою наступної URL-адреси в браузері:

https://api.telegram.org/bot<TOKEN>/getUpdates

Замість <TOKEN> підставляємо токен вашого бота типу 123456:ABC-DEF1234ghlkl-zyx57W2v1u123ew11



{"ok":true,"result":[{"update_id":467618155,
 "message":{"message_id":1,"from":
 {"id":699306931,"is_bot":false,"first_name":"Igor","last_name":"Falkovsky","username":"FIgor2010",
 "language_code":"ru"},"chat":
 {"id":699306931,"first_name":"Igor","last_name":"Falkovsky","username":"FIgor2010","type":"private
 {"id":699306931,"first_name":"Igor","last_name":"Falkovsky","username":"FIgor2010","type":"private
 "},"date":1738938281,"text":"/start","entities":[{"offset":0,"length":6,"type":"bot_command"}]}}]}

Рис. 16.26. Отримання ID чату для бота zabbix2240bot.

Відповідно до рис.16.26 іd чату для бота zabbix2240bot має значення 699306931. Налаштування у телеграм виконано. Для налаштувань сповіщень знадобиться токен та іd чату. Остання перевірка – запуск у браузері перевірочного коду

https://api.telegram.org/bot<BOT_TOKEN>/sendMessage?chat_id=<CHAT_ID>&text=Test

де BOT_TOKEN та CHAT_ID токен та іd чату створеного боту.

← → C 🌘 api.telegram.org	g/bot781 🖻 🖈 🖬 🚳 🗄					
<pre>{"ok":true,"result":{"message_id":8,"from": {"id":7811542868,"is_bot":true,"first_name":"Zabbix-22-40 Alerts Bot","username":"zabbix2240bot"},"chat": {"id":699306931,"first_name":"Igor","last_name":"Falkovsky","username": "FIgor2010","type":"private"},"date":1738952673,"text":"Test"}}</pre>						
@zabbix-22-40 X	Zabbix-22-40 Alerts Bot bot	۹ 🗆 :				
78 • Zabbix-22-40 Alert 20:24		/start _{16:24}				
Test	Test 17:26					

Рис. 16.27. Тестування бота zabbix2240bot через браузер.

Корисні посилання

• Zabbix + SNMP.

https://www.zabbix.com/integrations/snmp

• Discovery of SNMP OIDs.

https://www.zabbix.com/documentation/3.4/en/manual/discovery/low_level_discovery/snmp_oids

• Discovery of SNMP OIDs.

http://surl.li/oywlwg

• Zabbix Graphs.

http://surl.li/lizizi

• Zabbix DashBoards.

http://surl.li/hmmceo

• Zabbix Alerts: Setup Zabbix Email Notifications & Escalations.

https://bestmonitoringtools.com/zabbix-alerts-setup-zabbix-email-notifications-escalations/

• Zabbix Media Types.

https://www.zabbix.com/documentation/current/en/manual/config/notifications/media