Tempest

ACADEMY

Conference

2023

Técnicas de anti-flapping e correlação no zabbix para mitigar falsos positivos em um SOC

Classificação da Informação: PÚBLICA
Autor da apresentação: <Lucas Deodato>

01 Panorama de monitoração das plataformas

02 Monitorando a disponibilidade de um host

03 Correlação de métricas para redução de falsos positivos

04 Classificação de criticidade

05 Técnicas de anti-flapping

06 Conclusão e referências

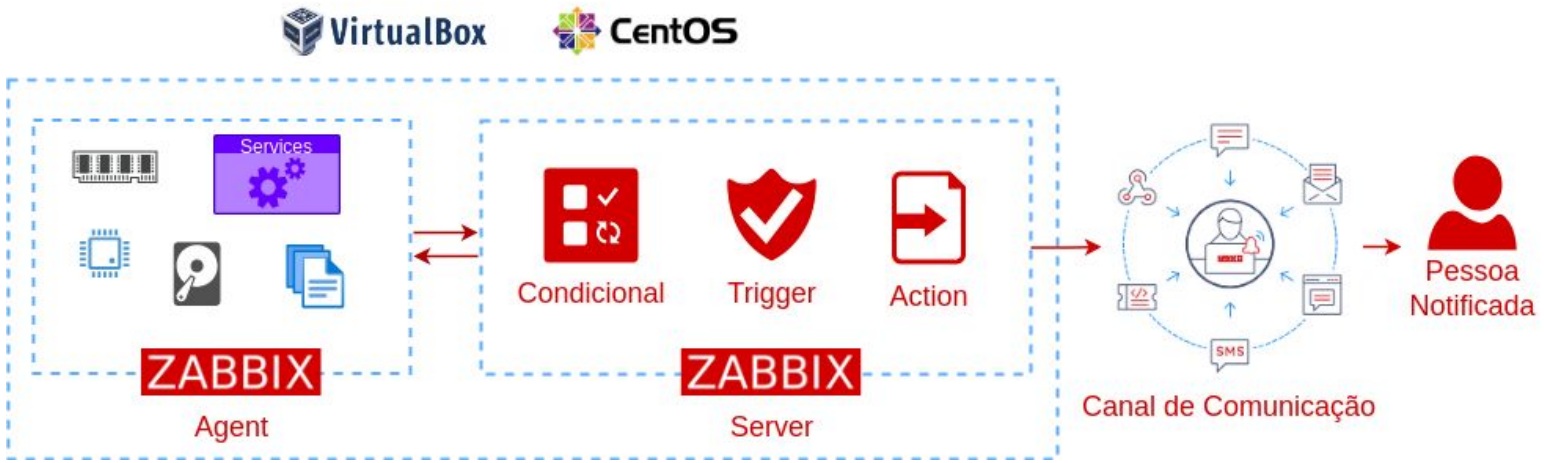
Tempest

:ACADEMY:

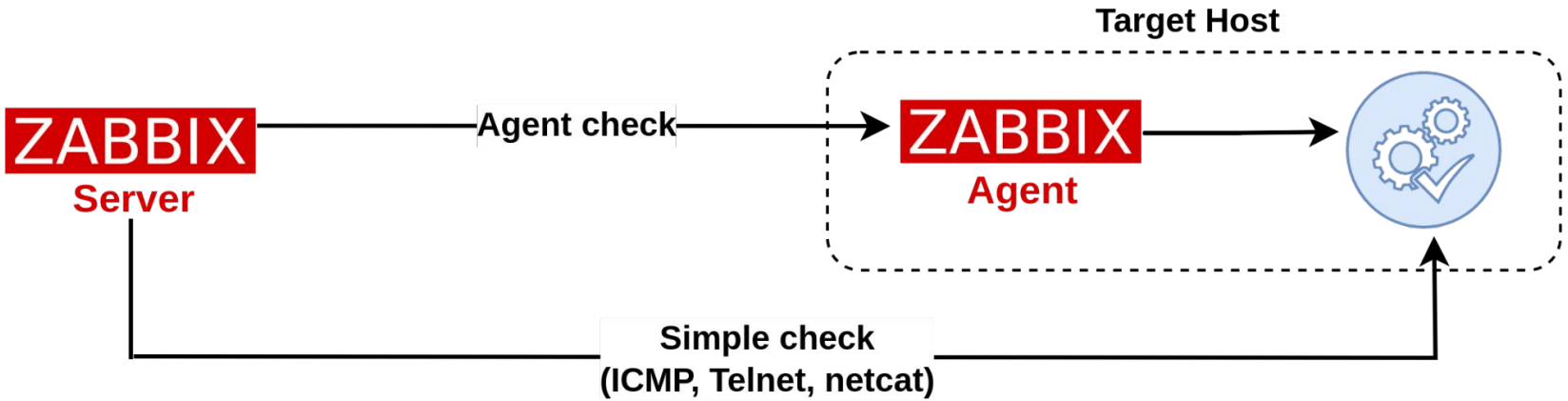
Conference

Panorama de monitoração das plataformas

Fluxo de monitoração Zabbix



Tipos de coletas de dados



Implicações na monitoração

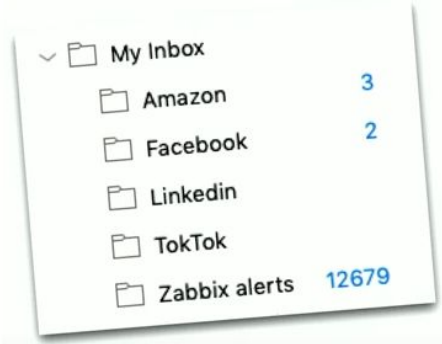
Tempest
[ACADEMY]
Conference

False positives and notification floods

Customers need to receive notifications when problems arise. However, if more than five or ten percent of total notifications are false positives, users generally stop trusting information from Zabbix. Most likely, they will create inbox filters to get rid of Zabbix messages.

- False positives undermine monitoring system reputation among your users.
- Notification flood makes your monitoring system inefficient.

By Nicola Mauri — August 6, 2020



Fonte: MAURI, Nicola. Zabbix Conference 2020

Monitorando a disponibilidade de um host

ICMP ping

Tempest
[ACADEMY]
Conference

Network Working Group
Request for Comments: 792

J. Postel
ISI
September 1981

Updates: RFCs 777, 760
Updates: IENs 109, 128

INTERNET CONTROL MESSAGE PROTOCOL

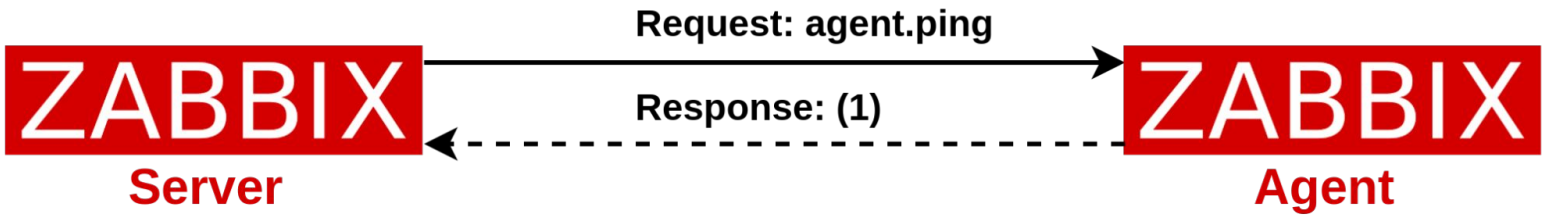
DARPA INTERNET PROGRAM
PROTOCOL SPECIFICATION

Fonte: POSTEL, Jon. RFC 792

```
osboxes@osboxes:~$ ping -c8 192.168.0.103
PING 192.168.0.103 (192.168.0.103) 56(84) bytes of data.
64 bytes from 192.168.0.103: icmp_seq=1 ttl=64 time=0.932 ms
64 bytes from 192.168.0.103: icmp_seq=2 ttl=64 time=1.28 ms
64 bytes from 192.168.0.103: icmp_seq=3 ttl=64 time=1.23 ms
64 bytes from 192.168.0.103: icmp_seq=4 ttl=64 time=0.703 ms
64 bytes from 192.168.0.103: icmp_seq=5 ttl=64 time=1.05 ms
64 bytes from 192.168.0.103: icmp_seq=6 ttl=64 time=1.04 ms
64 bytes from 192.168.0.103: icmp_seq=7 ttl=64 time=1.28 ms
64 bytes from 192.168.0.103: icmp_seq=8 ttl=64 time=0.469 ms

--- 192.168.0.103 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 18ms
rtt min/avg/max/mdev = 0.469/0.998/1.282/0.270 ms
osboxes@osboxes:~$
```

agent.ping



* Expression

```
nodata(/host/agent.ping,3m)=1
```

O que realmente aconteceu?

- Rede indisponível?
- Host indisponível?
- Host up, mas agent indisponível?
- Agent up, mas não retorna dados?

Tempest

ACADEMY

Conference

Correlação de métricas para redução de falsos positivos

Uma abordagem combinada

Tempest
[ACADEMY]
Conference

Porta 10050	ICMP ping	agent.ping	Possível causa raiz
–	❌	❌	Host indisponível
–	✅	❌	Agent indisponível
✅	–	❌	Sobrecarga ou má configuração
–	❌	✅	Provável bloqueio de ICMP ping

1. Identificando host indisponível

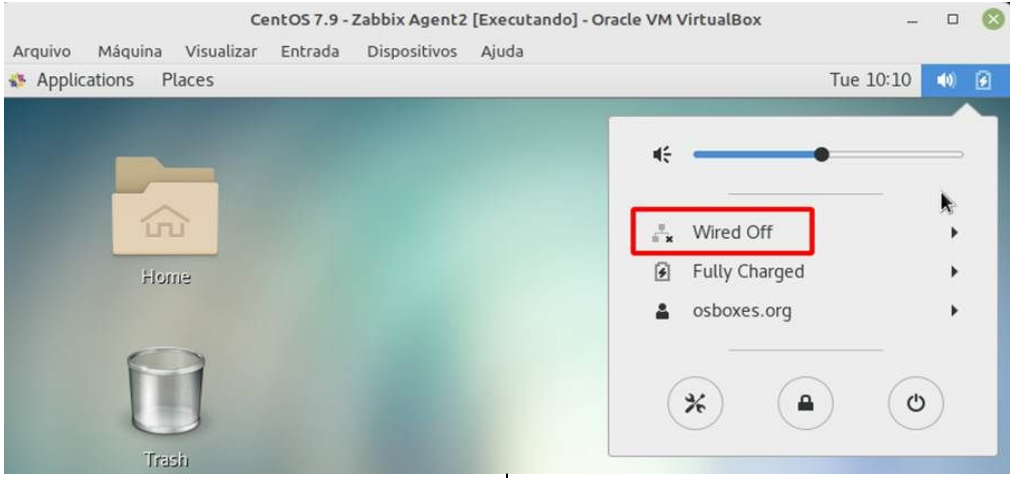
Tempest
[ACADEMY]
Conference

ICMP ping	agent.ping	Possível causa raiz
❌	❌	Host indisponível

1. Trigger “O host está indisponível por 5 minutos”

```
max(/CentOS/icmpping,5m)=0 and nodata(/CentOS/agent.ping,5m)=1
```

Cenário de host indisponível



2. Identificando agent indisponível

ICMP ping	agent.ping	Possível causa raiz
✅	❌	Agent indisponível

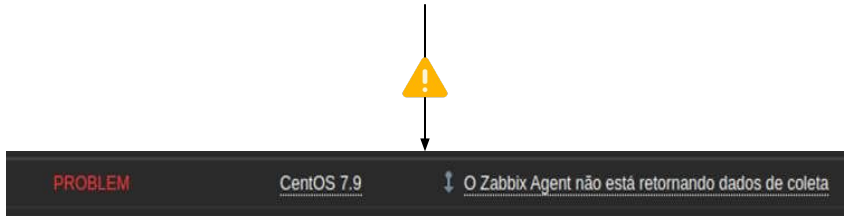
2. Trigger “O Zabbix Agent não está retornando dados de coleta”

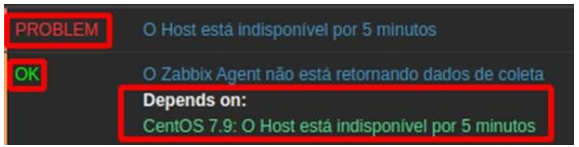
nodata(/CentOS/agent.ping,10m)=1

Cenário de agent indisponível

Tempest
[ACADEMY]
Conference

```
[root@osboxes osboxes]# systemctl stop zabbix-agent2
[root@osboxes osboxes]# systemctl status zabbix-agent2
● zabbix-agent2.service - Zabbix Agent 2
   Loaded: loaded (/usr/lib/systemd/system/zabbix-agent2.service; enabled; vendor prese
t: disabled)
   Active: inactive (dead) since Mon 2023-05-15 18:08:17 -03; 6s ago
  Process: 21644 ExecStop=/bin/kill -SIGTERM $MAINPID (code=exited, status=0/SUCCESS)
  Process: 20712 ExecStart=/usr/sbin/zabbix_agent2 -c $CONFFILE (code=exited, status=0/
SUCCESS)
```





3. Identificando sobrecarga ou má configuração no agent

Tempest
[ACADEMY]
Conference

Porta 10050	agent.ping	Possível causa raiz
✅	❌	Sobrecarga ou má configuração

3. Trigger “O Zabbix Agent está indisponível devido à uma sobrecarga no sistema ou má configuração”

```
max(/CentOS/net.tcp.service[tcp,,10050],5m)=1 and nodata(/CentOS/agent.ping,5m)=1
```

Cenário de sobrecarga ou má configuração no agent

Tempest
[ACADEMY]
Conference

```
### Option: Server
#       List of comma delimited IP addresses, opt
#       Incoming connections will be accepted onl
#       If IPv6 support is enabled then '127.0.0.
#       and '::/0' will allow any IPv4 or IPv6 ad
#       '0.0.0.0/0' can be used to allow any IPv4
#       Example: Server=127.0.0.1,192.168.1.0/24,
#
# Mandatory: yes
# Default:
# Server=

Server=ipincorreto
```

Status	Info	Host	Problem
PROBLEM		CentOS 7.9	O Zabbix Agent está indisponível devido à uma sobrecarga no sistema ou má configuração

4. Possível bloqueio de ICMP ping

Tempest
[ACADEMY]
Conference

ICMP ping	agent.ping	Possível causa raiz
❌	✅	Possível bloqueio de ICMP ping

4. Trigger “Possível bloqueio de ICMP ping”

`max(/CentOS/icmpping,10m)=0 and nodata(/CentOS/agent.ping,10m)=0`

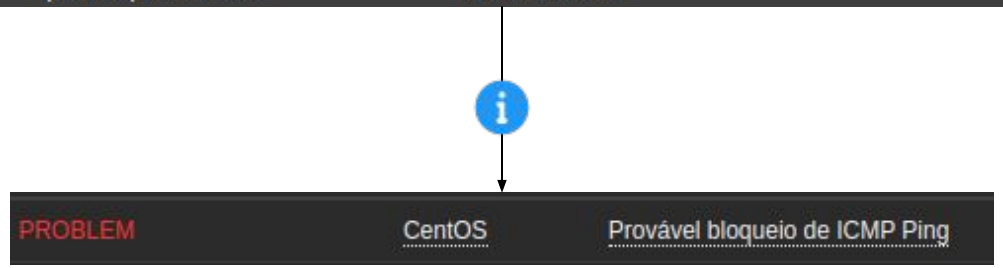
Cenário de possível bloqueio de ICMP ping

Tempest
[ACADEMY]
Conference

```
root@osboxes:/home/osboxes# iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
root@osboxes:/home/osboxes# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             anywhere             icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```



Recapitulando...

Tempest
[ACADEMY]
Conference

Porta 10050	ICMP ping	agent.ping	Possível causa raiz
–	❌	❌	Host indisponível
–	✅	❌	Agent indisponível
✅	–	❌	Sobrecarga ou má configuração
–	❌	✅	Provável bloqueio de ICMP ping

Classificação de criticidade

Definindo um modelo padrão

Tempest
[ACADEMY]
Conference

Severidade	Critério
Not classified	Fora do escopo de monitoração do SOC ou classificação de severidade em análise
Information	Eventos que não são problemas, mas contém informações úteis para possível análise e investigação (TBSH)
Warning	Eventos de sobrecarga e alto consumo de recursos que podem gerar perdas de dados casuais
Average	Indisponibilidade em serviços importantes para o SOC
High	Indisponibilidade em um host crítico
Disaster	Indisponibilidade ou perda de dados na rede inteira

Severidade dos alertas

Tempest
[ACADEMY]
Conference

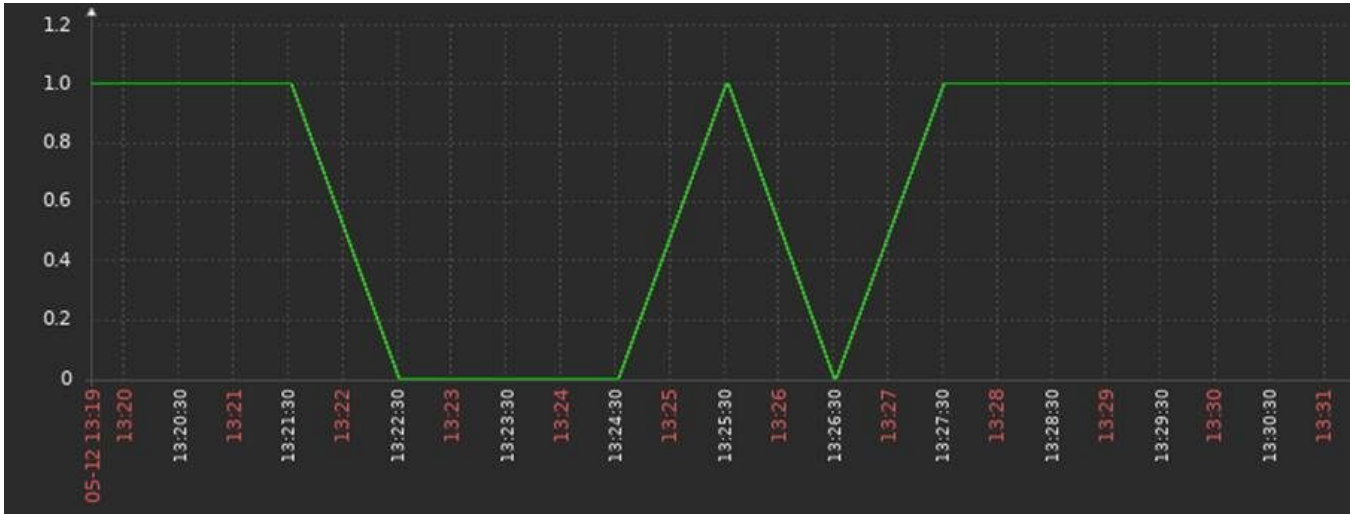
Porta 10050	ICMP ping	agent.ping	Possível causa raiz	Severidade
–	❌	❌	Host indisponível	High
–	✅	❌	Agent indisponível	Average
✅	–	❌	Sobrecarga ou má configuração	Warning
–	❌	✅	Provável bloqueio de ICMP ping	Information

Matriz de acionamento

Possível causa raiz	Time Acionado	Tipo de acionamento
Host indisponível	Infraestrutura 1	24x7
O Agent não está retornando dados de coleta	Monitoramento ou responsável pelo serviço	24x7
Sobrecarga ou má configuração	Responsável pelo serviço	Horário comercial
Provável bloqueio de ICMP ping	Infraestrutura 2	Horário comercial

Técnicas de anti-flapping

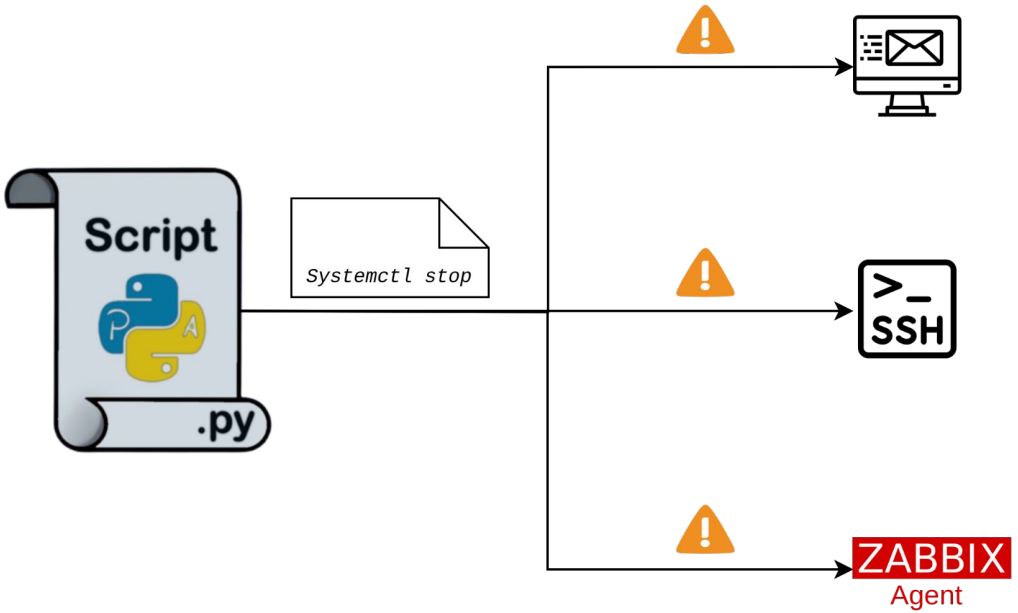
Flapping e anti-flapping



Expressões sensíveis

Expressão de trigger	Descrição
last(/CentOS 7.9/net.tcp.service[tcp,,25])=0	Serviço SMTP indisponível
last(/CentOS 7.9/net.tcp.service[tcp,,22])=0	Serviço SSH indisponível
last(/CentOS 7.9/net.tcp.service[tcp,,10050])=0	Serviço Zabbix Agent indisponível

Simulando oscilações nos serviços



Alertas e oscilações

```
root@osboxes:/home/osboxes# ss -tl
State                                  Local Address:Port
LISTEN                                       *:http
LISTEN                                     [::]:ssh
LISTEN                                    [::1]:ipp
LISTEN                                     [::]:smtp
LISTEN                                       *:zabbix-agent
root@osboxes:/home/osboxes#
```

Antes da execução do script

```
root@osboxes:/home/osboxes# ss -tl
State                                  Local Address:Port
LISTEN                                 127.0.0.1:ipp
LISTEN                                       *:http
LISTEN                                    [::1]:ipp
root@osboxes:/home/osboxes#
```

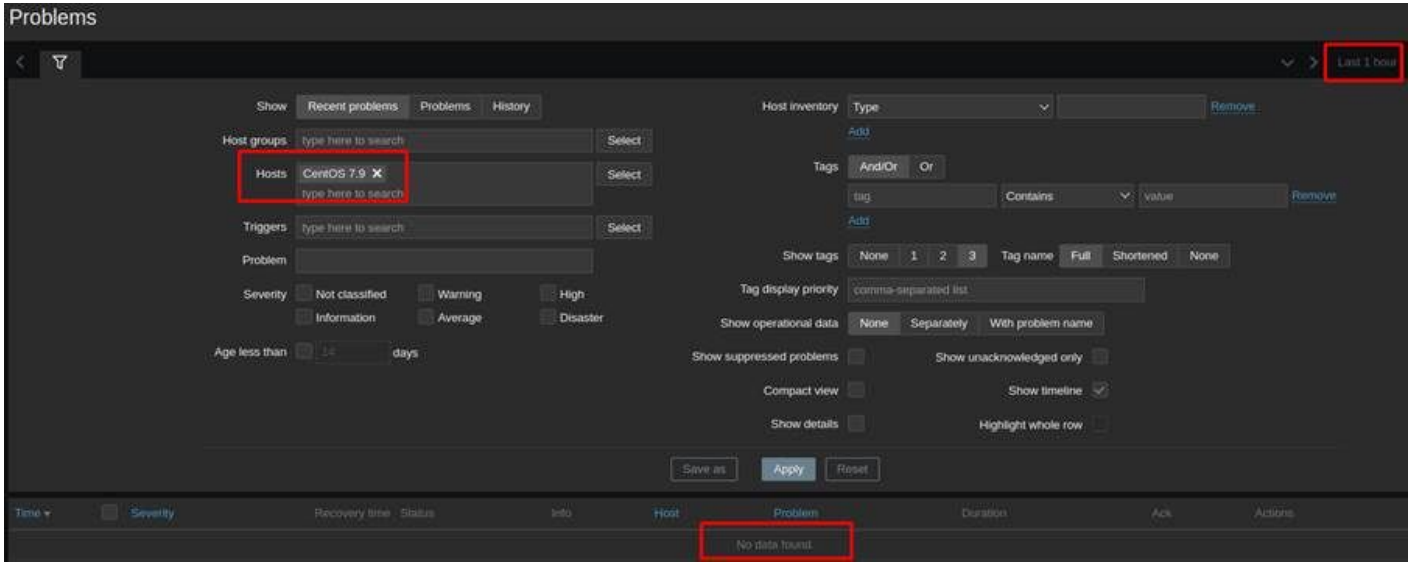
Após a execução do script

Recovery time	Status	Info	Host	Problem	Duration
			CentOS 7.9	SMTP Service is not running	1m 21s
15:05:35	RESOLVED		CentOS 7.9	SSH Service is not running	1m
15:06:33			CentOS 7.9	Zabbix Agent Service is not running	2m
15:03:35	RESOLVED		CentOS 7.9	SSH Service is not running	1m
15:03:33	RESOLVED		CentOS 7.9	Zabbix Agent Service is not running	2m

Tornando menos sensível

Expressão de trigger	Descrição
max(/CentOS 7.9/net.tcp.service[tcp,,25],10m)=0	Serviço SMTP indisponível
max(/CentOS 7.9/net.tcp.service[tcp,,22],10m)=0	Serviço SSH indisponível
max(/CentOS 7.9/net.tcp.service[tcp,,10050],10m)=0	Serviço Zabbix Agent indisponível

Problemas mitigados



Conclusão e referências

Conclusão

- É de suma importância analisar detalhadamente o panorama geral do ambiente monitorado;
- O monitoramento deve ser inteligente (isso é um processo de evolução contínua);
- Os stakeholders devem atuar de forma conjunta para definir alguns aspectos da monitoração;
- Reduzir falsos positivos e acionamentos indevidos evita prejuízos financeiros para as partes envolvidas, bem como quebras de SLA (do inglês: Service Level Agreement);
- Assertividade contribui para melhoria de indicadores de desempenho como MTTA (do inglês, Mean Time To Acknowledge) e MTTR (do inglês, Mean Time To Respond) e diminui substancialmente a incidência de falsos positivos e inundações de notificações;
- Apesar de ser uma ferramenta bastante robusta e eficaz, o Zabbix é apenas um meio;

Referências

LONTONS, Arturs. Handy Tips #19: Preventing alert storms with trigger dependencies. Disponível em: <https://blog.zabbix.com/handy-tips-19-preventing-alert-storms-with-trigger-dependencies/18696/>. Acesso em: 05 jan 2023.

MAURI, Nicola. Fighting notification floods and misleading alerts in distributed Zabbix deployments. Disponível em: <https://blog.zabbix.com/fighting-notification-floods-and-misleading-alerts-in-distributed-zabbix-deployments/11600/>. Acesso em: 14 jan 2023.

POSTEL, Jon. RFC 792 – Internet Control Message Protocol. 1981. Disponível em <https://datatracker.ietf.org/doc/html/rfc792>

Secure Users & Access. Disponível em: <https://www.checkpoint.com/cyber-hub/threat-prevention/>. Acesso em: 19 maio 2023.

SUNDARAMURTHY, Sathya Chandran et al. A tale of three security operation centers. In: Proceedings of the 2014 ACM workshop on security information workers. 2014. p. 43-50.

VLADISHEV, Alexei. No more flapping. Define triggers the smart way. Disponível em: <https://blog.zabbix.com/no-more-flapping-define-triggers-the-smart-way/1488/>. Acesso em: 11 fev 2023.

WUTZL, Eduardo. [Noc] Chuva de Alertas, qual Remédio? Disponível em: <https://pt.linkedin.com/pulse/noc-chuva-de-alertas-qual-rem%C3%A9dio-eduardo-wutzl>. Acesso em: 13 jan 2023.

Referências

WUTZL, Eduardo. [Noc] Chuva de Alertas, qual Remédio? Disponível em: <https://pt.linkedin.com/pulse/noc-chuva-de-alertas-qual-rem%C3%A9dio-eduardo-wutzl>. Acesso em: 13 jan 2023.

Zabbix Manual. Disponível em: <https://www.zabbix.com/documentation/6.0/en/manual>. Acesso em: 26 mar 2023.

Bloqueio de ICMP: camada de segurança ou uma medida ruim? Disponível em: <https://www.defcon-lab.org/bloqueio-de-icmp-camada-de-seguranca-ou-uma-medida-ruim/>. Acesso em: 02 nov. 2023.

Falso positivo. Disponível em: <https://pt.wikipedia.org/wiki/Falso_positivo>. Acesso em: 14 nov. 2023.

Tempest

:ACADEMY:

Conference

2023