Tuesday October 3, 2023

Houston office

IBM QRadar

SAR sentinel threshold crossed

38750073 - SAR Sentinel: threshold crossed.

Explanation

The system activity reporter (SAR) utility detected that your system load is above the threshold. Your system can experience reduced performance.

User response

Review the following options:

- In most cases, no resolution is required.

  For example, when the CPU usage over 90%, the system automatically attempts to return to normal operation.

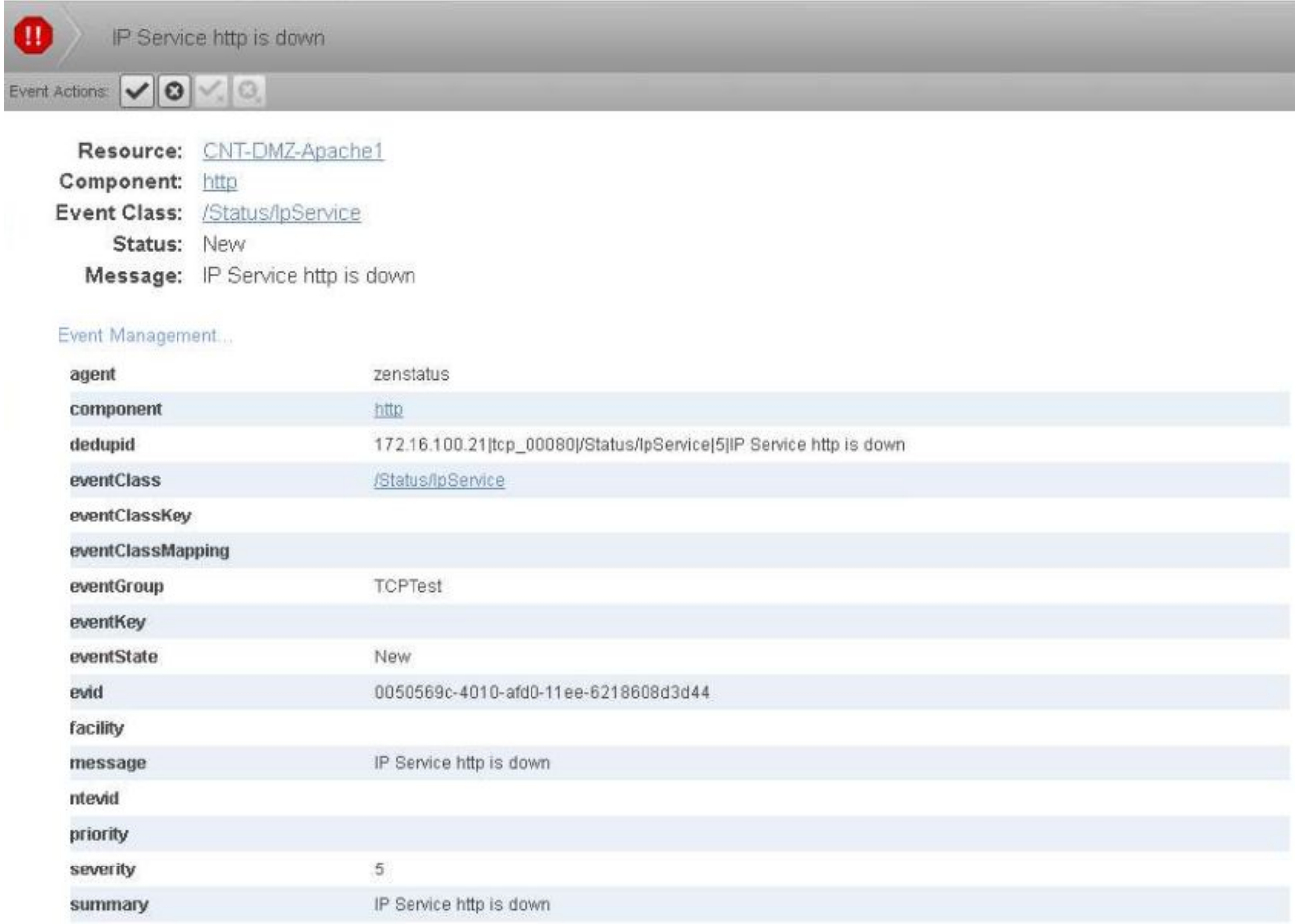
- If this notification is recurring, increase the default value of the SAR sentinel.

  Click the **Admin** tab, then click **Global System Notifications**. Increase the notification threshold.

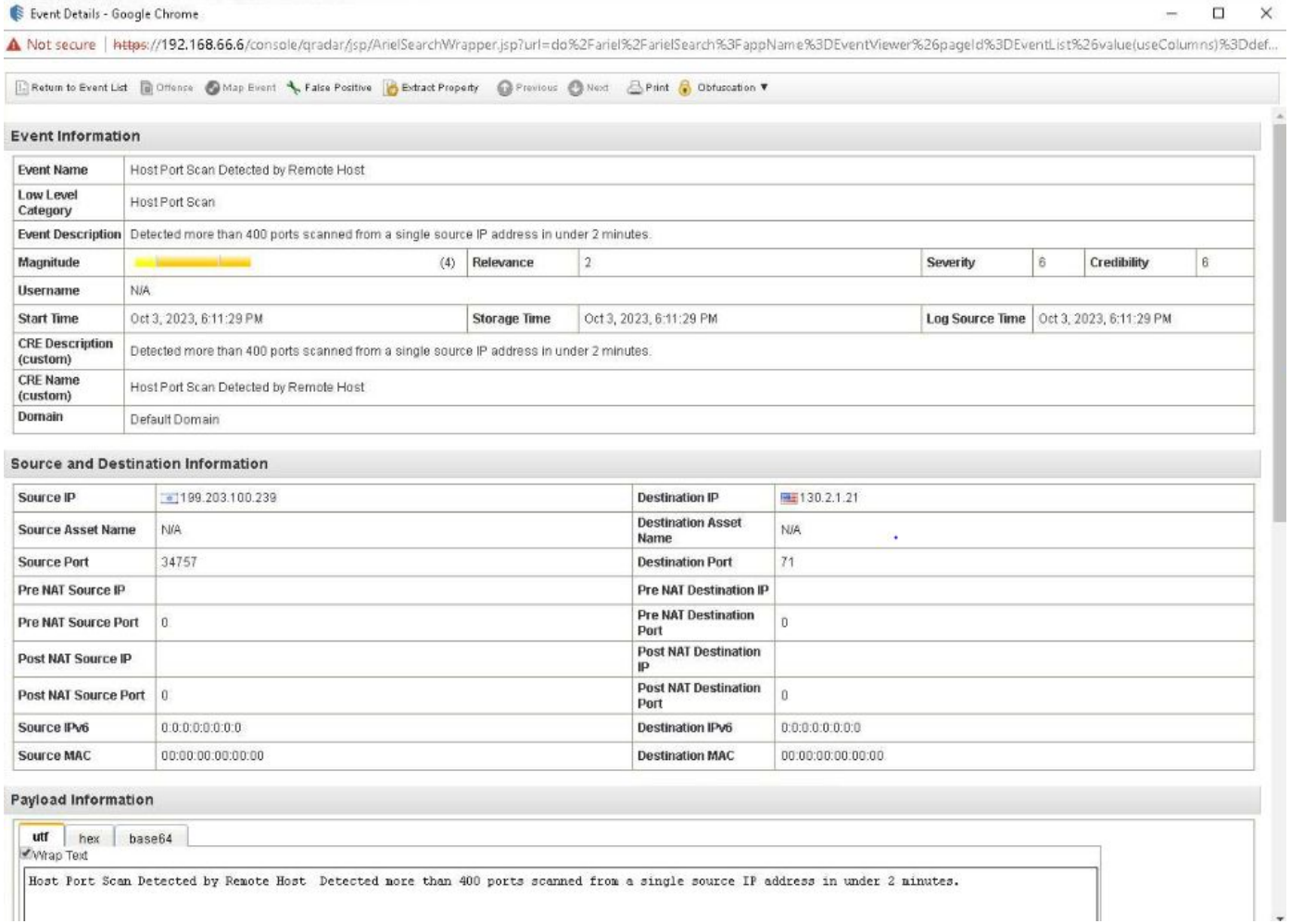
- For system load notifications, reduce the number of processes that run simultaneously.

  Stagger the start time for reports, vulnerability scans, or data imports for your log sources. Schedule backups and system processes to start at different times to lessen the system load.

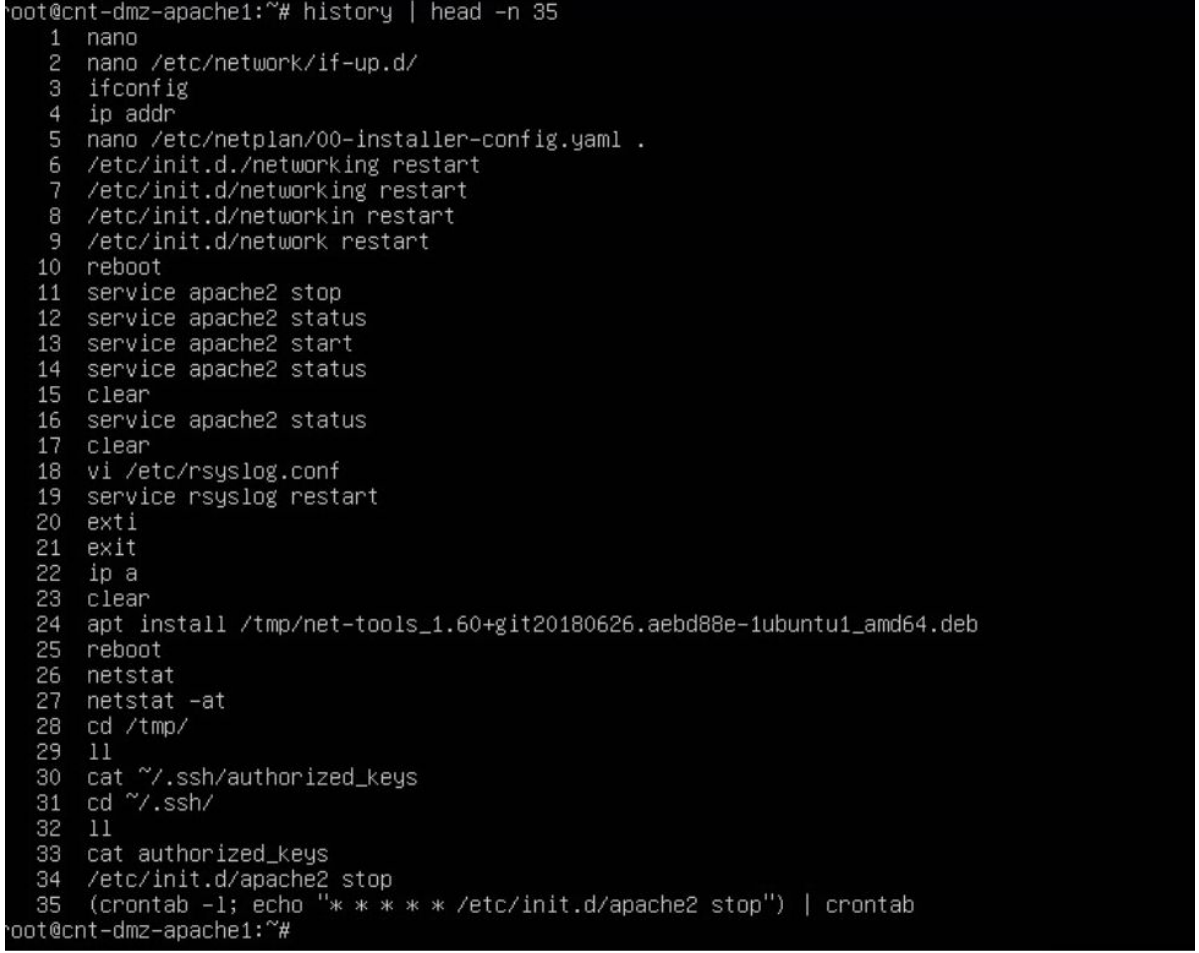
18:00



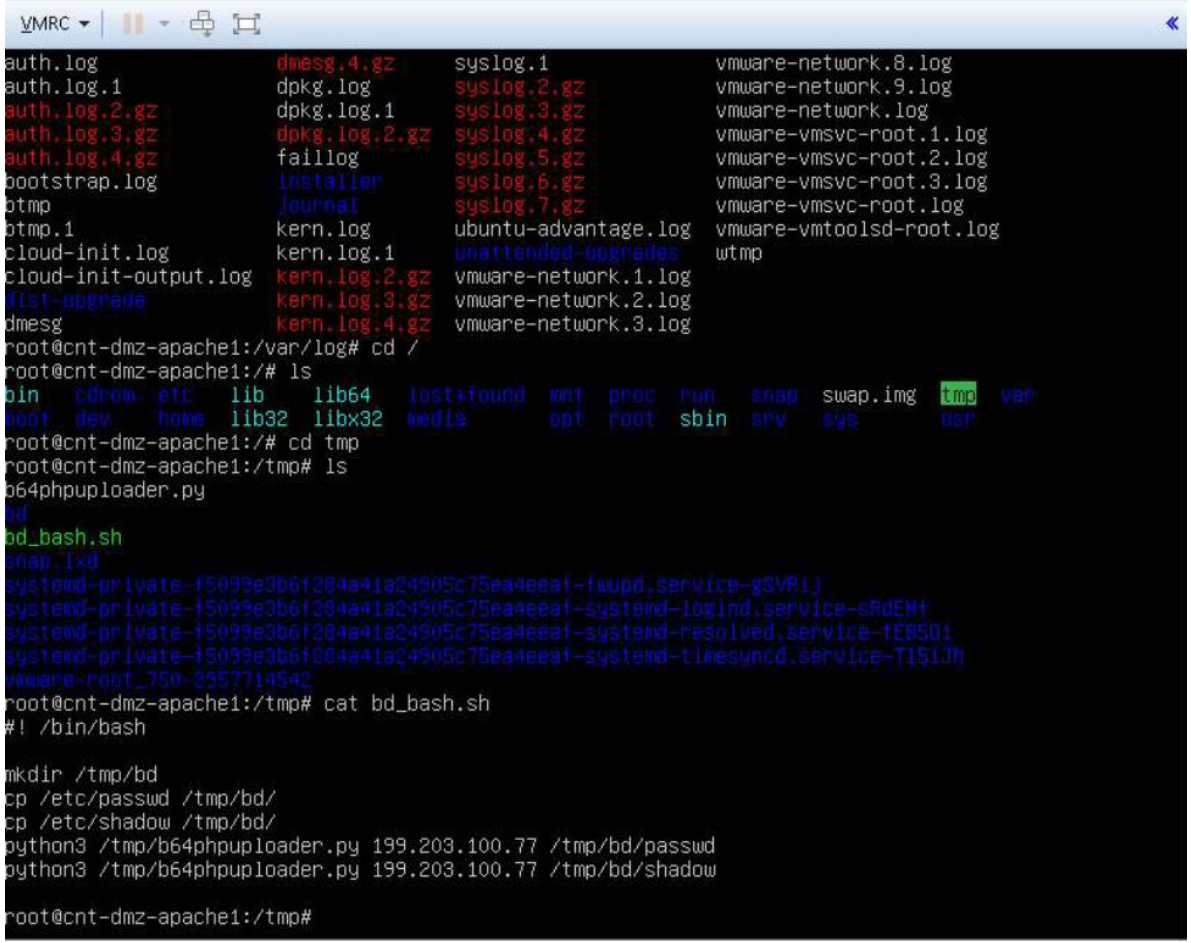
18:11 Apache 1 (www.worldnews.com)172.16.100.21


Event Details - Google Chrome
Not secure | https://192.168.66.6/console/qradar/jsp/ArielSearchWrapper.jsp?url=do%2Fariel%2FarielSearch%3FappName%3DEventViewer%26pageId%3DEventList%26value(useColumns)%3Ddef...
Return to Event List
Offense
Map Event
False Positive
Extract Property
Previous
Next
Print
Obfuscation
Event Information
Event Name
Host Port Scan Detected by Remote Host
Low Level Category
Host Port Scan
Event Description
Detected more than 400 ports scanned from a single source IP address in under 2 minutes.
Magnitude
(4)
Relevance
2
Severity
6
Credibility
6
Username
N/A
Start Time
Oct 3, 2023, 6:11:29 PM
Storage Time
Oct 3, 2023, 6:11:29 PM
Log Source Time
Oct 3, 2023, 6:11:29 PM
CRE Description (custom)
Detected more than 400 ports scanned from a single source IP address in under 2 minutes.
CRE Name (custom)
Host Port Scan Detected by Remote Host
Domain
Default Domain
Source and Destination Information
Source IP
199.203.100.239
Destination IP
130.2.1.21
Source Asset Name
N/A
Destination Asset Name
N/A
Source Port
34757
Destination Port
71
Pre NAT Source IP
Pre NAT Destination IP
Pre NAT Source Port
0
Pre NAT Destination Port
0
Post NAT Source IP
Post NAT Destination IP
Post NAT Source Port
0
Post NAT Destination Port
0
Source IPv6
0:0:0:0:0:0:0:0
Destination IPv6
0:0:0:0:0:0:0:0
Source MAC
00:00:00:00:00:00
Destination MAC
00:00:00:00:00:00
Payload Information
utf
hex
base64
Wrap Text
Host Port Scan Detected by Remote Host Detected more than 400 ports scanned from a single source IP address in under 2 minutes.

18:11


root@cnt-dmz-apache1:~# history | head -n 35
1 nano
2 nano /etc/network/if-up.d/
3 ifconfig
4 ip addr
5 nano /etc/netplan/00-installer-config.yaml .
6 /etc/init.d./networking restart
7 /etc/init.d/networking restart
8 /etc/init.d/networkin restart
9 /etc/init.d/network restart
10 reboot
11 service apache2 stop
12 service apache2 status
13 service apache2 start
14 service apache2 status
15 clear
16 service apache2 status
17 clear
18 vi /etc/rsyslog.conf
19 service rsyslog restart
20 exti
21 exit
22 ip a
23 clear
24 apt install /tmp/net-tools_1.60+git20180626.aebd88e-1ubuntu1_amd64.deb
25 reboot
26 netstat
27 netstat -at
28 cd /tmp/
29 ll
30 cat ~/.ssh/authorized_keys
31 cd ~/.ssh/
32 ll
33 cat authorized_keys
34 /etc/init.d/apache2 stop
35 (crontab -l; echo "* * * * * /etc/init.d/apache2 stop") | crontab
root@cnt-dmz-apache1:~#

18:13



- 18:17 a Bash file was uploaded to Apache 1

The Next Step

- Compromised passwords
- Impact to CIA Triad
- Impact to reputation
- Financial Impact
- Contact attorneys
- Update security policies