Status Report | Resources Utilization is OK on ABC-PROD-NGINX

Update and Patch

Server Name	ABC-PROD-NGINX
mWatcher Version	v0.2.4
TimeStamp	Sat, 27 Feb 21, 12:27 IST
Status	**Resources Utilization is OK**
Upgradable Packages	105 Packages
Restart Required	No Restart Required

Server IP (65.0.1.2) Details

COUNTRY	India
CITY	Mumbai
REGIONNAME	Maharashtra
REVERSE	ec2-65-0-1-2.ap-south-1.compute.amazonaws.com
ISP	ATu0026T Corp.

OS Details / System Utilization

Operating System	Host Name	Public IP	Uptime	# of Processes	Root FS Usage	iNode Status	Used Disk
Ubuntu 20.04.1 LTS	abc-prod-nginx	65.0.1.2	5 days	107	22%	5%	**22%**

System Details / Resources Utilization

Disk Size	Load Average	Total RAM (MB)	Used RAM(in MB)	Used Memory	Used CPU
20G	0.00 0.00 0.00	978	567	**57%**	**6%**

SSH|NGINX - Service Status

Timestamp	Service	Satus	Severity
2021-02-27 12:27:04	ssh	Running	**Info**
2021-02-27 12:27:04	nginx	Running	**Info**

Disk Utilization

Filesystem	Size	Used	Available	Use (%)	Mounted on
/dev/root	20G	4.3G	16G	22%	/
devtmpfs	486M	0	486M	0%	/dev
tmpfs	490M	0	490M	0%	/dev/shm
tmpfs	98M	836K	98M	1%	/run
tmpfs	5.0M	0	5.0M	0%	/run/lock
tmpfs	490M	0	490M	0%	/sys/fs/cgroup
/dev/loop1	34M	34M	0	100%	/snap/amazon-ssm-agent/3552
/dev/loop0	33M	33M	0	100%	/snap/amazon-ssm-agent/2996
/dev/loop2	56M	56M	0	100%	/snap/core18/1944
/dev/loop3	56M	56M	0	100%	/snap/core18/1988
/dev/loop4	70M	70M	0	100%	/snap/lxd/19032
/dev/loop5	70M	70M	0	100%	/snap/lxd/19188
/dev/loop6	32M	32M	0	100%	/snap/snapd/10707
/dev/loop7	32M	32M	0	100%	/snap/snapd/11036
tmpfs	98M	0	98M	0%	/run/user/1000

High Memory Consumption

PID	PPID	Mem (%)	CPU (%)	Command
1154060	1	37.8	0.1	/usr/sbin/mysqld
1275643	1275631	4.9	0.0	php-fpm: pool www
1275642	1275631	4.8	0.0	php-fpm: pool www
1366901	1275631	4.8	0.0	php-fpm: pool www
160	1	2.5	0.2	/lib/systemd/systemd-journald
486	1	2.5	0.0	/usr/lib/snapd/snapd
267	1	1.7	0.0	/sbin/multipathd -d -s
725	470	1.6	0.8	/snap/amazon-ssm-agent/3552/ssm-agent-worker
1275631	1	1.5	0.0	php-fpm: master process (/etc/php/7.3/fpm/php-fpm.conf)

All Open Ports and Services

Service Type	Source IP:Port	PID:Service Name
tcp	0.0.0.0:22	698/sshd: /usr/sbin
tcp	0.0.0.0:443	1167136/nginx: mast
tcp	0.0.0.0:3306	1154060/mysqld
tcp	0.0.0.0:80	1167136/nginx: mast
tcp6	:::22	698/sshd: /usr/sbin
tcp6	:::33060	1154060/mysqld

Attacker's Source IP Details [From Latest 50 Failed Requests]

Attacker IP	Request Count	Risk Level	Blocked	City Name	Source Country	Region	Autonomous System Number
122.177.86.156	9	Low - 18%	No	Noida	India	Uttar Pradesh	AS24560 Bharti Airtel Ltd., Telemedia Services
45.155.205.225	8	Low - 16%	Yes	St Petersburg	Russia	St.-Petersburg	AS49505 OOO Network of data-centers Selectel
51.141.111.74	2	Normal - 4%	Yes	Cardiff	United Kingdom	Wales	AS8075 Microsoft Corporation
45.151.144.113	2	Normal - 4%	Yes	Moscow	Russia	Moscow	AS9002 RETN Limited
185.12.95.70	2	Normal - 4%	Yes	Moscow	Russia	Moscow	AS49189 LLC RuWeb
103.70.81.158	2	Normal -	No	Delhi	India	National Capital Territory of	AS132116 Ani Network Pvt Ltd

		4%				Delhi	
45.67.230.242	1	Normal - 2%	No	Moscow	Russia	Moscow	AS44094 Webhost LLC
45.67.230.242	1	Normal - 2%	No	Moscow	Russia	Moscow	AS44094 Webhost LLC
45.67.230.242	1	Normal - 2%	No	Moscow	Russia	Moscow	AS44094 Webhost LLC
45.67.230.242	1	Normal - 2%	No	Moscow	Russia	Moscow	AS44094 Webhost LLC
45.151.144.113	1	Normal - 2%	No	Moscow	Russia	Moscow	AS9002 RETN Limited
45.151.144.113	1	Normal - 2%	No	Moscow	Russia	Moscow	AS9002 RETN Limited
45.151.144.113	1	Normal - 2%	No	Moscow	Russia	Moscow	AS9002 RETN Limited
45.151.144.113	1	Normal - 2%	No	Moscow	Russia	Moscow	AS9002 RETN Limited
45.151.144.113	1	Normal - 2%	No	Moscow	Russia	Moscow	AS9002 RETN Limited
194.87.98.91	1	Normal - 2%	No	Moscow	Russia	Moscow	AS48347 JSC Mediasoft ekspert
194.87.98.91	1	Normal - 2%	No	Moscow	Russia	Moscow	AS48347 JSC Mediasoft ekspert
194.87.98.91	1	Normal - 2%	No	Moscow	Russia	Moscow	AS48347 JSC Mediasoft ekspert
194.87.98.91	1	Normal - 2%	No	Moscow	Russia	Moscow	AS48347 JSC Mediasoft ekspert
193.124.118.53	1	Normal - 2%	No	Moscow	Russia	Moscow	AS9002 RETN Limited
193.124.118.53	1	Normal - 2%	No	Moscow	Russia	Moscow	AS9002 RETN Limited
193.124.118.53	1	Normal - 2%	No	Moscow	Russia	Moscow	AS9002 RETN Limited
193.124.118.53	1	Normal - 2%	No	Moscow	Russia	Moscow	AS9002 RETN Limited
193.124.118.53	1	Normal - 2%	No	Moscow	Russia	Moscow	AS9002 RETN Limited
185.12.95.70	1	Normal - 2%	No	Moscow	Russia	Moscow	AS49189 LLC RuWeb
185.12.95.70	1	Normal - 2%	No	Moscow	Russia	Moscow	AS49189 LLC RuWeb
185.12.95.70	1	Normal - 2%	No	Moscow	Russia	Moscow	AS49189 LLC RuWeb
185.12.95.70	1	Normal - 2%	No	Moscow	Russia	Moscow	AS49189 LLC RuWeb
157.245.100.146	1	Normal - 2%	No	Bengaluru	India	Karnataka	AS14061 DigitalOcean, LLC
122.177.86.156	1	Normal - 2%	No	Noida	India	Uttar Pradesh	AS24560 Bharti Airtel Ltd., Telemedia Services
122.177.86.156	1	Normal - 2%	No	Noida	India	Uttar Pradesh	AS24560 Bharti Airtel Ltd., Telemedia Services

- Max 10 failed requests/day is allowed from whitelisted country[India].
- Max 1 failed requests/day is allowed from Non Whitelisted country.
- Make sure you have encluded /etc/[nginx/conf.d|apache2/conf-available]/blockips.conf file in your nginx/apcahe2 config.
- Nginx/apcahe2 Service will be reload once in day

Web Request Status

Status Code	Count
200	675
301	99
404	50
405	42
302	42
500	34
400	20
401	4
304	1

Disk Utilization : /var/log/

Size	Name
617M	/var/log/journal
10M	/var/log/btmp.1
5.3M	/var/log/auth.log
4.2M	/var/log/kern.log
1.8M	/var/log/btmp
1.6M	/var/log/auth.log.1
1.4M	/var/log/nginx

Disk Utilization : /home/

Size	Name
64M	/home/ubuntu
40K	/home/harry
32K	/home/chandan
28K	/home/ram

Disk Utilization : /var/www/html/

Size	Name
436M	/var/www/html/abc-project
83M	/var/www/html/phpmyadmin
15M	/var/www/html/phpmyadmin.tgz
4.0K	/var/www/html/index.nginx-debian.html

AWS EC2 Server Details

REGION	ap-south-1
INSTANCETYPE	t2.micro
PENDINGTIME	2021-02-22T04
VERSION	2017-09-30
AVAILABILITYZONE	ap-south-1b
IMAGEID	ami-040a9ed359bb8758a
PRIVATEIP	172.31.3.51
ACCOUNTID	472873648326
INSTANCEID	i-0d2as3dfs34s3322s
ARCHITECTURE	x86_64

Disk Utilization : /tmp/

Size	Name
60K	/tmp/msg.html
56K	/tmp/mSendTML.html
52K	/tmp/health_reports
8.0K	/tmp/systemd-private-79b6e5075b36451b999451cde4a6bde4-systemd-resolved.service-7Tz6Zf
8.0K	/tmp/systemd-private-79b6e5075b36451b999451cde4a6bde4-systemd-logind.service-vVSGQi
8.0K	/tmp/systemd-private-79b6e5075b36451b999451cde4a6bde4-chrony.service-V15v4h
8.0K	/tmp/snap.lxd

Performance Check Status

Timestamp	Memory	Disk	CPU
12:26:37	57.87%	22%	6.2%
12:26:39	57.98%	22%	0%
12:26:42	57.98%	22%	6.2%
12:26:44	57.98%	22%	0%
12:26:46	57.98%	22%	6.2%
12:26:48	57.98%	22%	6.2%

12:26:50	57.98%	22%	0%
12:26:53	57.98%	22%	6.2%
12:26:55	57.98%	22%	0%
12:26:57	57.98%	22%	6.2%
12:26:59	57.98%	22%	6.2%
12:27:01	57.98%	22%	6.2%