10.6 SNMP Monitoring

10.6.1 TE SNMP OIDs

Currently these values can be queried by SNMP but are not part of the official Check Point MIB:

Description	OID	Blade
Threat Emulation Status Fields	1.3.6.1.4.1.2620.1.49	
Threat Emulation Status Code	1.3.6.1.4.1.2620.1.49.101	TE
Threat Emulation Status Short Description	1.3.6.1.4.1.2620.1.49.102	TE
Threat Emulation Status Long Description	1.3.6.1.4.1.2620.1.49.103	TE
Threat Emulation Engine Major Version	1.3.6.1.4.1.2620.1.49.29	TE
Threat Emulation Engine Minor Version	1.3.6.1.4.1.2620.1.49.30	TE
Threat Emulation Mode	**.1.3.6.1.4.1.2620.1.49.19.0**	TE
Threat Emulation Queue Information	1.3.6.1.4.1.2620.1.49.1	TE
Threat Emulation Download Information	1.3.6.1.4.1.2620.1.49.2	TE
Threat Emulation Average Download Percentage	1.3.6.1.4.1.2620.1.49	TE
Threat Emulation Download Percentage	1.3.6.1.4.1.2620.1.49.3	TE
Threat Emulation Update Status	**1.3.6.1.4.1.2620.1.49**	TE
Threat Emulation Status	1.3.6.1.4.1.2620.1.49.16	TE
Threat Emulation Status Description	1.3.6.1.4.1.2620.1.49.17	TE
Threat Emulation Queue Info	1.3.6.1.4.1.2620.1.49.1	TE
	1.3.6.1.4.1.2620.1.49.1.1.1.0	TE
Threat Emulation Download Info	1.3.6.1.4.1.2620.1.49.2	TE
	.1.3.6.1.4.1.2620.1.49.2.1.2.x.0	
Threat Emulation Download Percentage	**1.3.6.1.4.1.2620.1.49.3**	TE
Threat Emulation Scanned Files (Quantity)	**1.3.6.1.4.1.2620.1.49.4**	TE
Threat Emulation Scanned Files Total Count	1.3.6.1.4.1.2620.1.49.4.1	TE
Threat Emulation Scanned Files Count Last Day	1.3.6.1.4.1.2620.1.49.4.2	TE
Threat Emulation Scanned Files Count Last Week	1.3.6.1.4.1.2620.1.49.4.3	TE
Threat Emulation Scanned Files Count Last Month	1.3.6.1.4.1.2620.1.49.4.4	TE
Threat Emulation Malware Detected (Quantity)	**1.3.6.1.4.1.2620.1.49.5**	TE
Threat Emulation Malware Detected Total Count	1.3.6.1.4.1.2620.1.49.5.1	TE
Threat Emulation Malware Detected Count Last Day	1.3.6.1.4.1.2620.1.49.5.2	TE

Threat Emulation Malware Detected Count Last Week	1.3.6.1.4.1.2620.1.49.5.3	TE
Threat Emulation Malware Detected Count Last Month	1.3.6.1.4.1.2620.1.49.5.4	TE
Threat Emulation Scanned Files On Threat Cloud (Quantity)	**1.3.6.1.4.1.2620.1.49.6**	TE
Threat Emulation Scanned Files On Threat Cloud Total Count	1.3.6.1.4.1.2620.1.49.6.1	TE
Threat Emulation Scanned Files On Threat Cloud Last Day	1.3.6.1.4.1.2620.1.49.6.2	TE
Threat Emulation Scanned Files On Threat Cloud Last Week	1.3.6.1.4.1.2620.1.49.6.3	TE
Threat Emulation Scanned Files On Threat Cloud Last Month	1.3.6.1.4.1.2620.1.49.6.4	TE
Threat Emulation Malware Detected On ThreatCloud (Quantity)	**1.3.6.1.4.1.2620.1.49.7**	TE
Threat Emulation Malware Detected On ThreatCloud Total Count	1.3.6.1.4.1.2620.1.49.7.1	TE
Threat Emulation Malware Detected On ThreatCloud Last Day	1.3.6.1.4.1.2620.1.49.7.2	TE
Threat Emulation Malware Detected On ThreatCloud Last Week	1.3.6.1.4.1.2620.1.49.7.3	TE
Threat Emulation Malware Detected On ThreatCloud Last Month	1.3.6.1.4.1.2620.1.49.7.4	TE
Threat Emulation Average Process Time (Quantity)	**1.3.6.1.4.1.2620.1.49.8**	TE
Threat Emulation Average Process Time Total Count	1.3.6.1.4.1.2620.1.49.8.1	TE
Threat Emulation Average Process Time Last Day	1.3.6.1.4.1.2620.1.49.8.2	TE
Threat Emulation Average Process Time Last Week	1.3.6.1.4.1.2620.1.49.8.3	TE
Threat Emulation Average Process Time Last Month	1.3.6.1.4.1.2620.1.49.8.4	TE
Threat Emulation Emulated File Size (File size - bytes)	**1.3.6.1.4.1.2620.1.49.9**	TE
Threat Emulation Emulated File Size Total	1.3.6.1.4.1.2620.1.49.9.1	TE
Threat Emulation Emulated File Size Last Day	1.3.6.1.4.1.2620.1.49.9.2	TE
Threat Emulation Emulated File Size Last Week	1.3.6.1.4.1.2620.1.49.9.3	TE
Threat Emulation Emulated File Size Last Month	1.3.6.1.4.1.2620.1.49.9.4	TE
Threat Emulation Queue Size (Quantity)	**1.3.6.1.4.1.2620.1.49.10**	TE
Threat Emulation Queue Size Total Count	1.3.6.1.4.1.2620.1.49.10.1	TE
Threat Emulation Queue Size Last Day	1.3.6.1.4.1.2620.1.49.10.2	TE
Threat Emulation Queue Size Last Week	1.3.6.1.4.1.2620.1.49.10.3	TE
Threat Emulation Queue Size Last Month	1.3.6.1.4.1.2620.1.49.10.4	TE
Threat Emulation Peak Size (Quantity)	**1.3.6.1.4.1.2620.1.49.11**	TE
Threat Emulation Peak Size Total Count	1.3.6.1.4.1.2620.1.49.11.1	TE

Threat Emulation Peak Size Last Day	1.3.6.1.4.1.2620.1.49.11.2	TE
Threat Emulation Peak Size Last Week	1.3.6.1.4.1.2620.1.49.11.3	TE
Threat Emulation Peak Size Last Month	1.3.6.1.4.1.2620.1.49.11.4	TE
Threat Emulation General Status Fields		
Threat Emulation Email Scanned	1.3.6.1.4.1.2620.1.49.12	TE
Threat Emulation Downloaded Files Scanned	1.3.6.1.4.1.2620.1.49.13	TE
Threat Emulation Files In Queue	1.3.6.1.4.1.2620.1.49.14	TE
Threat Emulation Number Of Emulation Environments	1.3.6.1.4.1.2620.1.49.15	TE
		TE
Threat Emulation Contract Status Fields		
Contract Name	1.3.6.1.4.1.2620.1.49.19	TE
Cloud Subscription Expire Date	1.3.6.1.4.1.2620.1.49.20	TE
TE Cloud Hourly Quota	1.3.6.1.4.1.2620.1.49.21	TE
TE Cloud Monthly Quota	1.3.6.1.4.1.2620.1.49.22	TE
TE Cloud Remaining Quota	1.3.6.1.4.1.2620.1.49.23	TE
TE Maximal VMs Number	1.3.6.1.4.1.2620.1.49.24	TE
TE Subscription Status	1.3.6.1.4.1.2620.1.49.25	TE
TE Cloud Quota Status	1.3.6.1.4.1.2620.1.49.26	TE
TE Subscription Description	1.3.6.1.4.1.2620.1.49.27	TE
TE Cloud Quota Description	1.3.6.1.4.1.2620.1.49.28	TE
TE Cloud Quota Identifier	1.3.6.1.4.1.2620.1.49.31	TE
TE Cloud Monthly Quota Period Start	1.3.6.1.4.1.2620.1.49.32	TE
TE Cloud Monthly Quota Period End	1.3.6.1.4.1.2620.1.49.33	TE
TE Cloud Monthly Quota Usage for This GW	1.3.6.1.4.1.2620.1.49.34	TE
TE Cloud Hourly Quota Usage for this GW	1.3.6.1.4.1.2620.1.49.35	TE
Threat Emulation Is First Download	1.3.6.1.4.1.2620.1.49.36	TE
TE Cloud Monthly Quota Usage for Quota ID	1.3.6.1.4.1.2620.1.49.37	TE
TE Cloud Hourly Quota Usage for Quota ID	1.3.6.1.4.1.2620.1.49.38	TE
TE Cloud Monthly Quota Exceeded	1.3.6.1.4.1.2620.1.49.39	TE
TE Cloud Hourly Quota Exceeded	1.3.6.1.4.1.2620.1.49.40	TE
TE Cloud Last Quota Update GMT Time	1.3.6.1.4.1.2620.1.49.41	TE

10.6.2 Extend SNMP Monitoring

10.6.2.1 Enable SNMP

1. # cpconfig
   a. enable "SNMP Extension"
2. Clish
   - set snmp community <*community-name*> read-only
   - save config

Check OIDs for TE
TE OIDs => .1.3.6.1.4.1.2620.1.49

Show all TE related OIDs
snmpwalk -v 2c -c <*community-name*> localhost .1.3.6.1.4.1.2620.1.49

Enable SNMP Agent
1. Clish
   - set snmp agent on
   - save config

10.6.2.2 Extend available SNMP OIDs

Select free OID for Postfix queue value
Free OID => .1.3.6.1.4.1.2620.1.250.1

Extend available SNMP values
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk78360

Add the following lines to /etc/snmp/userDefinedSettings.conf file:

```
extend .1.3.6.1.4.1.2620.1.250.1 postfix_queue /bin/sh
/home/admin/mailqueue.sh
extend .1.3.6.1.4.1.2620.1.250.2 emaild_queue /bin/sh
/home/admin/emaild_tmpdir.sh
extend .1.3.6.1.4.1.2620.1.252 vm /bin/sh /home/admin/running_vm.sh
```


10.6.2.3 Postfix mailqueue monitoring script

/home/admin/mailqueue.sh

```
# Extract Postfix queue size value
#!/bin/bash

MAILQ=$(/opt/postfix/usr/sbin/postqueue -c /opt/postfix/etc/postfix/ -p |
egrep '^--.*Request|^Mail.*empty')

if [[ $MAILQ =~ "empty" ]] ; then
  RESPONSE=0
  echo $RESPONSE
elif [[ $MAILQ =~ "Request" ]] ; then
  RESPONSE=$(echo $MAILQ|awk '{print $5}')
  echo $RESPONSE
else
  RESPONSE=error
fi
```

10.6.2.4 Emaild queue monitoring script

/home/admin/emaild_tmpdir.sh

```
# Extract emaild temp file queue amount
#!/bin/bash
. /opt/CPshared/5.0/tmp/.CPprofile.sh
ls -l $FWDIR/tmp/email_tmp/ |grep emailtemp |wc -l
```

10.6.2.5 Running VM instances monitoring script

/home/admin/running_vm.sh

```
#  Extract amount of running VM Instances
#!/bin/bash
. /opt/CPshared/5.0/tmp/.CPprofile.sh
tecli s e e | grep "Running virtual machines"|awk '{print $4}'
```


10.6.2.6 Test extended SNMP values

Test new values
MAILQUEUE
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2620.1.250.4.1.2.2.109.113.1

EMAILD_TEMPDIR
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2620.1.251.4.1.2.3.101.109.102.1

