# System monitoring with Nagios and SNMP

The server systems of m-privacy GmbH have sensors for NRPE-based monitoring systems (e.g. Nagios) or for SNMP-based monitoring systems. This allows important operating states to be checked remotely so that countermeasures can be taken before critical limit values are exceeded. The following list provides an overview of the implemented checks.

Not every system has the total number of possible sensors, so not all check points must always be active. The specified threshold values are predefined, but can be changed if necessary.

**Hinweis**

In order for TightGate-Pro to be monitored with a monitoring system, the monitoring must be activated as administrator *config* under **Services > Nagios NRPE Support/Start SNMP Service**. In addition, the IP address of the monitoring server must be stored under **Services > Maintenance and Updates > Remote Administrator IP**.

# Manual check of NRPE checkpoints

As *root* enter the following command in the console:

```
cd /usr/lib/nagios/plugins/
```

```
./check_nrpe -H [IP address of TightGate-Pro] -c check_[name of checkpoint]
```

Ex. for the checkpoint maint:

```
./check_nrpe -H 192.168.4.1 -c check_maint
```

# Manual check of SNMP checkpoints

Enter the following command from the monitoring machine to read out all available checks:

```
 snmpwalk -v3 -u snmp-user -A [PASSWORD] -a SHA -l authnoPriv [IP address of
TightGate-Pro] .1.3.6.1.4.1.8072.1.3.2.3.1.1 [or MIB NET-SNMP-EXTEND-
MIB::nsExtendStatus]
```

Enter the following command from the monitoring computer to read out individual checks:

```
 snmpget -v3 -u snmp-user -A [PASSWORD] -a SHA -l authnoPriv [IP address of
TightGate-Pro] [single MIB or OID]
```

**Hinweis**

Here you will find a complete list of all MIBs and OIDs of the test points from TightGate-Pro.

# Basic checkpoints

| Checkpoint | Description | State OK | State Warning | State Critical | Activity at Warning | Activity at Critical |
|---|---|---|---|---|---|---|
| maint | Checks whether a node is available and not in maintenance mode. If applicable, displays the time of a scheduled maintenance. | Node available and not in maintenance mode | Node in maintenance mode | | Log in as administrator **maint** and exit maintenance mode after maintenance is complete. | |
| load | Returns the average system load for the time points: 1, 5 and 15 minutes. | The workload is lower than the value set by the administrator config under the system preferences | The workload is higher than the value set by the administrator config under the system preferences but less than twice the value | The workload is higher than twice the value set by the administrator config under the system preferences | | Log in as administrator **root** and open a console. The command **atop** displays the process overview, indicating the load per process. The list can be sorted by load value by entering **p** in the window. Processes that cause particularly high load can be terminated using **kill** . Restarting the system can also help. In any case, if the system load is excessive, inform the technical customer service of m-privacy GmbH . |
| softmode | Checks whether the node is in softmode, i.e. in a state not protected by RSBAC. | Softmode is not activated | | Softmode is activated | Please deactivate softmode as user **Security**. | |
| users | Checks for the maximum number of VNC connections (TightGate viewer) stored as **config** and outputs the current number of viewer and lock connections. | < Max VNC | Über Max VNC aber unter Max VNC +10 | > Max VNC +10 | If the limit values are exceeded, performance losses are to be expected. | |

| Checkpoint | Description | State OK | State Warning | State Critical | Activity at Warning | Activity at Critical |
|---|---|---|---|---|---|---|
| disks | Checks free memory on the hard disks. | > 20% free | Between 20% and 10% free | < 10% frei | Statusseite des entsprechenden Systems aufrufen und Massenspeicher auf Belegung überprüfen. Bei Platzmangel sollten insbesondere die Benutzerverzeichnisse in /home geprüft werden. Evtl. können z. B. alte Backups gelöscht werden. Weiterhin sollten die Logdateien in /var/log geprüft werden. Zu große Logdateien können gelöscht werden, um Platz auf dem Datenträger zu schaffen. | |
| disk_load | Plattenaktivität aller verfügbaren Platten in % | < 70% | Zwischen 70% und 90% | > 90% | Problematic with HHD, unlikely with SSD. | |
| zombie_procs | Undermined zombie processes, can indicate errors. | No zombie processes | Under 10 zombie processes | Over 10 zombie processes | Zombie processes can occur occasionally and usually do not affect system operation. Frequent occurrence of zombie processes indicates errors in file handling. It is recommended to inform the technical customer service of m-privacy GmbH . | |
| total_procs | Checks the number of running processes. | < 4.000 | Zwischen 4.000 und 10.000 | > 10,000 | Restarting the system may reduce the number of running processes. **Note:** This checkpoint is rather less meaningful, as a warning is only given at very high values. | |
| swap | Checks for free swap memory and returns the value of the maximum value set and the free memory. | > 50% of the maximum value free | Between 50% and a minimum of 20% of the maximum value free | < 20% des Maximalwerts frei | Bei dauerhafter Überschreitung der Grenzwerte zunächst Last reduzierende Maßnahmen ergreifen (z. B. Nutzung der Browser-Add-ons "Flashblock", "AdBlock" und dergl.). Auch eine Erweiterung des Arbeitsspeichers kann Abhilfe schaffen. Es wird empfohlen, die Maßnahmen mit dem technischen Kundendienst der m-privacy GmbH zu erörtern. | |

| Checkpoint | Description | State OK | State Warning | State Critical | Activity at Warning | Activity at Critical |
|---|---|---|---|---|---|---|
| smtp | Prüft die Erreichbarkeit des SMTP-Servers und gibt dessen Antwortzeit zurück | Erreichbar | | Nicht erreichbar | Nach Anmeldung als Administrator **config** steht der Menüpunkt **Netzwerk prüfen** zur Verfügung. Damit kann auch erkannt werden, ob ein SMTP-Server erreichbar ist. Ggf. Konfiguration des Systems prüfen oder Erreichbarkeit des SMTP-Servers sicherstellen. |
| ntp | Prüft die Erreichbarkeit von NTP-Zeitservern und zeigt Abweichungen zur lokalen Systemzeit an. | Zeitdifferenz < 60 Sekunden | Zeitdifferenz zwischen 60 und 120 Sekunden | Nicht erreichbar oder Zeitdifferenz > 120 seconds | Especially in cluster systems, all nodes must have the same system time. If the time difference to the reference of the stored NTP server is > 1 minute, action is required! Please log in as administrator **config** and use the menu item **Check network** to verify the problem and adjust the time if necessary. If necessary, an alternative external NTP server should be configured to ensure proper system operation. |
| memavailable | Display the available memory in kByte. | over 1,000,000 (1 GB RAM) | Value between 1,000,000 and 100,000 | Value under 100,000 (100 MB RAM) | Increase the memory or reduce the number of users on the server. |
| memorypressurekilled | Number of user sessions that were automatically logged off due to acute memory shortage within the last 24 hours. | 0 | Value less than 0 | | Increase in memory or decrease in the number of users on the server. |
| pressure_cpu | Checks whether requests are delayed due to a bottleneck in the CPU. | Delays <20% aller Anfragen | Verzögerungen zwischen 20%>50% of all requests | Delays >50% of all requests | The number of authorised users should be reduced on the node. |
| pressure_io | Checks whether requests are delayed due to a read/write bottleneck or network bottlenecks. | Delays <20% aller Anfragen | Verzögerungen zwischen 20%>50% of all requests | Delays >50% of all requests | If SSDs are used, bottlenecks usually occur in connection with network bottlenecks. |
| pressure_memory | Checks whether requests are delayed due to a memory bottleneck. | Delays <2% aller Anfragen | Verzögerungen zwischen 2%>10% of all requests | Delays >10% of all requests | The available RAM should be extended or the number of authorised users on the node should be reduced. |

| Checkpoint | Description | State OK | State Warning | State Critical | Activity at Warning | Activity at Critical |
|---|---|---|---|---|---|---|
| ssh | Checks the reachability of a Secure Shell and returns the SSH version. | Reachable | | Not reachable | | If SSH is reported as unreachable, the administrator **config** should first execute a **Apply** . If SSH is still reported as unreachable, the system must be restarted in recover mode. In this case, it is recommended to contact the technical customer service of m-privacy GmbH . |
| dns | Checks the DNS server entered. Returns the IP address and the response time of the DNS server. | Resolution of the IP address possible. | | Resolution of the IP address not possible. | Check DNS server, enter alternative DNS server if necessary. | |
| bug | Searches the kern.log file for keywords that indicate kernel errors. | No errors found | | Error found | Inform technical customer service of m-privacy GmbH . | |
| cron | Checks the number of running cron jobs. | 1 to 10 cron jobs | Between 11 and 20 cron jobs | > 20 or no cron jobs | | Log in as administrator **root** and call console. Command sequence **ps tree -ah** locates the blocked cron job. Check possible services and take appropriate action, e.g. as administrator **config Apply** or restart the system. |

| Checkpoint | Description | State OK | State Warning | State Critical | Activity at Warning | Activity at Critical |
|---|---|---|---|---|---|---|
| versions | Compares the installed software version with the currently available software version. **Note:** This check can only be called up **directly a maximum of 2 times a day**. Each additional call returns the last result with the note "**(cached)**". If you want to force the call, you can call up "Available updates" once beforehand ( **update** do not forget to log off again). The check is then run again. | No newer version available | Updates available | Updates available for more than 6 months | Log in as administrator **update** and **Perform autoupdate** | |
| vnc | Checks the accessibility of the VNC server and returns its response time and the port set. | Reachable | | Not reachable | If VNC is activated in the configuration and is still reported as unreachable, the administrator **config** should first execute a **Full Apply** . If VNC is still shown as unreachable, the system must be restarted in recover mode. In this case, it is advisable to consult the technical customer service of m-privacy GmbH . | |
| diskerror | Searches the kern.log file for keywords that indicate hard disk errors. | No errors found | | Errors found | Warnings indicate faulty hard disks. This can lead to data inconsistencies or data loss. Please contact technical support at m-privacy GmbH . | |
| licence | Checks for a valid licence and returns the number of licences used and the expiry date. | Licence valid | | Licence invalid | The licence must be renewed via the technical customer service of m-privacy GmbH . | |
| apply | Checks whether it is necessary to apply as Administrator Config. | No apply necessary | | Apply necessary | If Nagios signals that an apply is necessary, please log in as administrator **config** and execute an **apply**. | |

| Checkpoint | Description | State OK | State Warning | State Critical | Activity at Warning | Activity at Critical |
|---|---|---|---|---|---|---|
| slabs | Check for memory areas in the core. | < 10 Mio. | Zwischen 10 und 100 Mio. | > 100 million | Indicates memory leaks and core errors. | |
| backup | Checks for existing backup and any errors that may have occurred. Returns date and time of the last backup created, if found. | Backup exists and is free of errors | Backup is faulty or no automatic backup has been configured | Backup does not exist or service is not available | As administrator *backuser* Log in and check log for errors. It can be called up with the command **Show last log**. | Check whether as administrator *backuser* under **Configuration > Frequency** inappropriate settings may have been selected. Then, for example, check in the log whether a backup was created and check for errors if necessary. |
| smart_sd* | Checks the SMART status of the respective hard disk and returns the detected status. Replace the * character with the respective purchase plant letter. | Hard disk OK + current temperature | Temperature > 45 °C | Temperature > 50 °C | | If the temperature is too high, the cooling of the system should be checked. If the hard disk is not OK, the errors of the S.M.A.R.T. check of the disk are also output. Measures can be a system start from the rescue system or execution of a **fsck**. |
| check_definedusers | Checks the number of created users in TightGate-Pro and shows how many user IDs are currently created in TightGate-Pro. | At least 5 new user IDs can still be created. | Only a maximum of 5 new users can be created. | A maximum of one new identifier can still be created or the maximum number of user identifiers has already been reached. | | Please purchase additional licences from TightGate-Pro. |

# Optional checkpoints

Optimal checkpoints can be used depending on the system configuration to monitor specific processes.

# Checkpoints for cluster system "Ceph

Depending on how many Ceph servers are in use, all Nagios checkpoints are provided for each Ceph server. The following table lists all checks for the first Ceph server. The checkpoints for the second and further Ceph servers are to be used in the same way, but the number given in the checkpoint is to be incremented in each case.

| Checkpoint | Description | State OK | Status Warning | State Critical | Activity at Warning | Activity at Critical |
|---|---|---|---|---|---|---|
| homeusermount | Checks whether /home/user is mounted in the directory tree. Returns the path of /home/user. | Mounted | | Not mounted | | Check hard disk, if necessary mount user directories manually as a test. It could also be a file system error, so notifying technical support at m-privacy GmbH is recommended. |
| backupmount | Checks whether /home/backuser/backup has been correctly mounted in the directory tree. | Mounted | | Not mounted | | Check hard disk, if necessary mount user directories manually as a test. This could be a file system error, so notifying technical support at m-privacy GmbH is recommended. |
| ceph | Check ceph status for internal Ceph data storage | Ceph is running normally | There are errors | There are errors | | Notify the technical support of m-privacy GmbH . |
| check_ceph_hu_1_disks | Checks free memory on the hard disks of the first Ceph server. | > 20% free | Between 20% and 10% free | < 10 % frei | | Ist der Speicher voll, nehmen Sie bitte Kontakt mit dem technischen Kundendienst der m-privacy GmbH auf. |
| check_ceph_hu_1_disk_load | Plattenaktivität aller verfügbaren Platten in %. | < 70% | Zwischen 70% und 90% | > 90% | | Problematic with HHD. |

| Checkpoint | Description | State OK | Status Warning | State Critical | Activity at Warning | Activity at Critical |
|---|---|---|---|---|---|---|
| check_ceph_hu_1_zombie_procs | Undermined zombie processes, can indicate errors. | No zombie processes | Under 10 zombie processes | Over 10 zombie processes | Zombie processes may occur occasionally and usually do not affect system operation. Frequent occurrence of zombie processes indicates errors in file handling. It is recommended to inform the technical customer service of m-privacy GmbH . | |
| check_ceph_hu_1_ntp | Checks the accessibility of NTP time servers and displays deviations from the local system time. | Time difference < 60 Sekunden | Zeitdifferenz zwischen 60 und 120 Sekunden | Nicht erreichbar oder Zeitdifferenz > 120 seconds | In the event of deviations, it is essential to restore synchronicity, otherwise cluster failures may occur. | |
| check_ceph_hu_1_ssh | Checks the accessibility of a Secure Shell and returns the SSH version. | Reachable | | Not reachable | If SSH is reported as unreachable, the administrator **config** should first execute a **Apply** . If necessary, contact the technical customer service of m-privacy GmbH . | |
| check_ceph_hu_1_cron | Checks the number of running cron jobs. | 1 to 10 cron jobs running | 11 to 20 cron jobs running | > 20 or no cron jobs running | | |
| check_ceph_hu_1_raid | Checks for the presence of a software RAID. | RAID is running without errors | RAID is being synchronised | Disks are missing in the RAID | If errors occur, check the RAID. Individual disks may be defective. | |
| check_ceph_hu_1_ceph | Displays the HEALTH status of the entire external Ceph. | Ceph is OK | Ceph has a problem | Ceph is not intact | Yes, depending on the problem, the error messages of the Ceph must be responded to individually. If necessary, contact the technical customer service of m-privacy GmbH . | |

| Checkpoint | Description | State OK | Status Warning | State Critical | Activity at Warning | Activity at Critical |
|---|---|---|---|---|---|---|
| check_ceph_hu_1_smart_sd* | Checks the SMART status of the respective hard disk and returns the detected status. The * sign is to be replaced by the respective purchase plant letter. | Hard disk OK + current temperature | temperature > 45 °C | temperature > 50 °C | | If the hard disk is too hot, the fan settings or the air flow in the server must be checked. |

## Further optional checkpoints

| Checkpoint | Description | Condition OK | State Warning | State Critical | Activity at Warning | Activity at Critical |
|---|---|---|---|---|---|---|
| backup | Checks for existing backup and any errors that may have occurred. Returns the date and time of the last backup created, if found. | Backup exists and is free of errors | Backup is faulty | Backup does not exist or service is not available. | Log in as administrator **backuser** and check log for errors. It can be called up with the command **Display last log** . | Check whether as administrator **backuser** under **Configuration > Frequency** inappropriate settings may have been selected. Then check in the log, for example, whether a backup was created and check for errors if necessary. |
| scanner | Checks whether the virus scanner's malware definitions are up-to-date and whether the virus scanner is running. | Definitions current (or not older than 2 days) | Definitions older than 2 days but younger than 1 week | Virus scanner is not running or no definitions are available or the definitions are older than 1 week. | Update virus definitions according to the administration manual. | Correctly configure as administrator **config** according to the administration manual. |
| sensors | Check the hard disk temperature | Temperature below 110°C | Temperature above 110°C and below 120°C | Temperature above 120°C | There is a danger of overheating. Please check whether the fans are working properly. If necessary, make settings in the BIOS of the server. Please also check that the air flow around the server is guaranteed. | |
| raid | Checks for the presence of a software RAID. | RAID is running without errors | RAID is being synchronised | Disks are missing in the RAID | If errors occur, check the RAID. Individual disks may be defective. | |

| Checkpoint | Description | Condition OK | State Warning | State Critical | Activity at Warning | Activity at Critical |
|---|---|---|---|---|---|---|
| squid | Checks the availability of the proxy server and displays the response time and the connection port. | All OK | | Port not accessible Not accessible | If the port cannot be reached, check whether the service is running. | |
| http | Checks for the availability of the HTTP protocol and outputs the response time. | All OK | | Port Not reachable | If the port cannot be reached, check whether the service is running. | |
| temp | Checks the temperature of the mainboard (if a sensor is present) and outputs it. | < 50 ℃ | 50 ℃ to 60 ℃ | > 60 ℃ | If the temperature is exceeded, check the entire cooling system of the hardware (fan, heat sink, air ducts, etc.) and the air conditioning of the operating environment. | |
| fan | Checks whether a fan is running (if sensor is present). | Running | | Not running | Check hardware in case of problem message. | |
| timedupdate | Checks whether an automatic update is scheduled. | | | | The checkpoint only provides informative values for the planned update time. | |
| identd | Check ident-deamon for logging of proxy connections. | ok | No logging configured, but proxy is running | Logging is configured, but proxy is not running | Correct settings or restart service by **Apply** as ***config*** . | |
| adldap | Check for accessibility of LDAP server / AD server during user administration | | | | Indicates errors when using Active Directory or LDAP servers. Measures are to be taken according to the instructions of the check. | |
| nodesavail | Checks for the availability of all nodes within a cluster of TightGate-Pro systems | All nodes are available | Fewer nodes are available than defined, but the minimum number is still present | No nodes are accessible/available. | Informative. | |

From:

[https://help.m-privacy.de/](https://help.m-privacy.de/) -

Permanent link:

**[https://help.m-privacy.de/doku.php/en:tightgate-pro:anhang:nagios](https://help.m-privacy.de/doku.php/en:tightgate-pro:anhang:nagios)**

Last update: **2023/03/02 07:47**