

Systemüberwachung mit Nagios und SNMP

Die Serversysteme der m-privacy GmbH verfügen über Sensoren für NRPE-basierte Monitoringsysteme (z. B. Nagios) oder für SNMP-basiertes Monitoring-Systeme. Damit lassen sich wichtige Betriebszustände aus der Ferne prüfen, sodass bereits vor einer Überschreitung kritischer Grenzwerte Gegenmaßnahmen ergriffen werden können. Nachfolgende Aufstellung gibt einen Überblick über die implementierten Prüfpunkte (Checks).

Nicht jedes System verfügt über die Gesamtzahl der möglichen Sensoren, sodass nicht immer alle Prüfpunkte aktiv sein müssen. Die angegebenen Schwellwerte sind vordefiniert, können jedoch bei Bedarf geändert werden.

Hinweis

Damit TightGate-Pro mit einem Monitoring-System überwacht werden kann, muss die Überwachung als Administrator **config** unter **Dienste > Nagios-NRPE-Unterstützung bzw. SNMP-Dienst starten** aktiviert werden. Zusätzlich muss unter **config > Netzwerk > Nagios/SNMP IP** die IP-Adresse des Monitoring-Servers hinterlegt sein.

Manuelle Überprüfung von NRPE Prüfpunkten

Als **root** in der Konsole folgenden Befehl eingeben:

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

```
./check_nrpe -H [IP-Adresse des TightGate-Pro] -c check_[Name des Prüfpunktes]
```

Bsp. für den Prüfpunkt maint:

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

Manuelle Überprüfung von SNMP Prüfpunkten

Folgenden Befehl vom überwachenden Rechner eingeben, zum Auslesen sämtlicher verfügbaren Checks:

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

Folgenden Befehl vom überwachenden Rechner eingeben, zum Auslesen einzelner Checks:

```
snmpget -v3 -u snmp-user -A [PASSWORD] -a SHA -l authnoPriv [IP-Adresse des
```

TightGate-Pro] [einzelne MIB oder OID]

Hinweis

Hier finden Sie eine [vollständige Liste aller MIBs und OIDs der Prüfpunkte von TightGate-Pro](#).

Grundlegende Prüfpunkte

| Prüfpunkt | Beschreibung | Zustand OK | Zustand Warning | Zustand Critical | Aktivität bei Warning | Aktivität bei Critical |
|-----------|--|---|--|--|---|---------------------------|
| maint | Prüft, ob ein Node verfügbar ist und sich nicht im Wartungsmodus befindet. Zeigt ggf. den Zeitpunkt einer geplanten Wartung an. | Node verfügbar und nicht im Wartungsmodus | Node im Wartungsmodus | | Nach beendeter Wartung als Administrator maint anmelden und Wartungsmodus beenden. | |
| load | Gibt die durchschnittliche Systemlast zurück für die Zeitpunkte: 1, 5 und 15 Minuten. | Die Systemlast ist geringer als der vom Administrator config unter den Systemvorgaben gesetzte Wert | Die Systemlast ist höher als der vom Administrator config unter den Systemvorgaben gesetzte Wert aber geringer als das doppelte des Wertes | Die Systemlast ist höher als das Doppelte des vom Administrator config unter den Systemvorgaben gesetzten Wertes | Als Administrator root anmelden und eine Konsole öffnen. Der Befehl atop zeigt die Prozessübersicht unter Angabe der Last pro Prozess. Die Liste kann durch Eingabe von p im Fenster nach dem Lastwert sortiert werden. Prozesse, die besonders hohe Last verursachen, können mittels kill beendet werden. Auch ein Neustart des Systems kann helfen. In jedem Fall ist bei übermäßiger Systemlast der technische Kundendienst der m-privacy GmbH zu informieren. | |
| softmode | Prüft, ob sich der Node im Softmode befindet, d.h. in einem nicht durch RSBAC geschützten Zustand. | Softmode ist nicht aktiviert | | Softmode ist aktiviert | Bitte Softmode als Benutzer Security deaktivieren. | |
| users | Prüft auf die als config hinterlegte maximale Anzahl von VNC-Verbindungen (TightGate-Viewer) und gibt die aktuelle Anzahl der Viewer- und Schleusen-Verbindungen aus. | < Max VNC | Über Max VNC aber unter Max VNC +10 | > Max VNC +10 | Bei Überschreitung der Grenzwerte ist mit Performance-Einbußen zu rechnen. | |
| disks | Prüft freien Speicher auf den Festplatten. | > 20% frei | Zwischen 20% und 10% frei | < 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. | |

| Prüfpunkt | Beschreibung | Zustand OK | Zustand Warning | Zustand Critical | Aktivität bei Warning | Aktivität bei Critical |
|----------------------|--|-----------------------------------|---|--|---|---------------------------|
| disk_load | Plattenaktivität aller verfügbaren Platten in % | < 70% | Zwischen 70% und 90% | > 90% | Bei HDD problematisch, bei SSD eher unwahrscheinlich | |
| zombie_procs | Untermirierte Zombieprozesse, können auf Fehler hinweisen. | Keine Zombieprozesse | Unter 10 Zombieprozessen | Über 10 Zombieprozessen | Zombieprozesse können gelegentlich auftreten und beeinträchtigen den Systembetrieb in der Regel nicht. Gehäuftes Auftreten von Zombieprozessen deutet auf Fehler in der Dateibehandlung hin. Es wird empfohlen, den technischen Kundendienst der m-privacy GmbH zu informieren. | |
| 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 Sekunden | Insbesondere in Clustersystemen müssen alle Nodes dieselbe Systemzeit aufweisen. Ist die Zeitdifferenz zur Referenz des hinterlegten NTP-Servers > 1 Minute, besteht Handlungsbedarf! Bitte als Administrator config anmelden und mit dem Menüpunkt Netzwerk prüfen das Problem verifizieren und ggf. die Zeit gleich anpassen. Ggf. sollte ein alternativer externer NTP-Server konfiguriert werden, um einwandfreien Systembetrieb sicherzustellen. | |
| memavailable | Anzeige des verfügbaren Speichers in kByte. | über 1.000.000 (1 GB RAM) | Wert zwischen 1.000.000 und 100.000 | Wert unter 100.000 (100 MB RAM) | Erhöhung des Arbeitsspeichers oder Verringerung der Anzahl der User auf dem Server. | |
| memorypressurekilled | Anzahl der Benutzer-Sitzungen, welche auf Grund akuten Speichermangels innerhalb der letzten 24 Stunden automatisch abgemeldet wurden. | 0 | Wert kleiner 0 | | Erhöhung des Arbeitsspeichers oder Verringerung der Anzahl der User auf dem Server. | |
| pressure_cpu | Prüft, ob Anfragen auf Grund eines Engpasses in der CPU verzögert bearbeitet werden. | Verzögerungen <20% aller Anfragen | Verzögerungen zwischen 20%>50% aller Anfragen | Verzögerungen >50% aller Anfragen | Die Anzahl der zugelassenen Benutzer sollte auf dem Node gesenkt werden. | |
| pressure_io | Prüft, ob Anfragen auf Grund eines Lese-/Schreib-Engpasses oder auf Grund von Netzwerkengpässen verzögert bearbeitet werden. | Verzögerungen <20% aller Anfragen | Verzögerungen zwischen 20%>50% aller Anfragen | Verzögerungen >50% aller Anfragen | Sofern SSDs verwendet werden, sind treten Engpässe meist im Zusammenhang mit Netzwerkengpässen aus. | |
| pressure_memory | Prüft, ob Anfragen auf Grund eines Engpasses im Speicher verzögert bearbeitet werden. | Verzögerungen <2% aller Anfragen | Verzögerungen zwischen 2%>10% aller Anfragen | Verzögerungen >10% aller Anfragen | Das verfügbare RAM sollte erweitert werden oder die Anzahl der zugelassenen Benutzer auf dem Node gesenkt werden. | |

| Prüfpunkt | Beschreibung | Zustand OK | Zustand Warning | Zustand Critical | Aktivität bei Warning | Aktivität bei Critical |
|-----------|---|-----------------------------------|------------------------------|---|--|---------------------------|
| ssh | Prüft die Erreichbarkeit einer Secure Shell und gibt die SSH-Version zurück. | Erreichbar | | Nicht erreichbar | Falls SSH als unerreichbar moniert wird, sollte zunächst als Administrator config ein Anwenden ausgeführt werden. Wird SSH danach weiterhin als nicht erreichbar ausgewiesen, ist ein Neustart des Systems im Recover-Modus erforderlich. Es empfiehlt sich in diesem Fall eine Rücksprache mit dem technischen Kundendienst der m-privacy GmbH. | |
| dns | Prüft den eingetragenen DNS-Server. Gibt die IP-Adresse und die Antwortzeit des DNS-Servers zurück. | Auslösung der IP-Adresse möglich. | | Auflösung der IP-Adresse nicht möglich. | DNS-Server überprüfen ggf. alternativen DNS-Server eintragen. | |
| bug | Sucht in der Datei kern.log nach Schlüsselworten, die auf Kernfehler hindeuten. | Keine Fehler gefunden | | Fehler gefunden | Technischen Kundendienst der m-privacy GmbH informieren. | |
| cron | Prüft die Anzahl der laufenden Cron-Jobs. | 1 bis 10 Cron-Jobs | Zwischen 11 und 20 Cron-Jobs | > 20 oder keine Cron-Jobs | Als Administrator root anmelden und Konsole aufrufen. Befehlsfolge ps tree -ah lokalisiert den blockierten Cron-Job. Infrage kommende Dienste prüfen und entsprechende Maßnahmen ergreifen, z. B. als Administrator config Anwenden oder auch Neustart des Systems. | |
| versions | Vergleicht die installierte Softwareversion mit dem aktuell verfügbaren Softwarestand. Hinweis: Dieser Check kann nur noch maximal 2 mal täglich direkt aufgerufen werden. Jeder weitere Aufruf liefert das letzte Ergebnis mit dem Hinweis " (cached) ". Möchte man den Abruf erzwingen, kann man vorher einmal "Verfügbare Updates" aufrufen (update wieder abmelden nicht vergessen). Anschließend wird der Check einmal neu ausgeführt. | Keine neuere Version verfügbar | Updates verfügbar | Updates seit mehr als 6 Monaten verfügbar | Als Administrator update anmelden und Autoupdate durchführen | |
| vnc | Prüft die Erreichbarkeit des VNC-Servers und gibt dessen Antwortzeit sowie den gesetzten Port zurück. | Erreichbar | | Nicht erreichbar | Ist VNC in der Konfiguration aktiviert und wird dennoch als unerreichbar moniert, sollte zunächst als Administrator config ein Voll Anwenden ausgeführt werden. Wird VNC danach weiterhin als nicht erreichbar ausgewiesen, ist ein Neustart des Systems im Recover-Modus erforderlich. Es empfiehlt sich in diesem Fall eine Rücksprache mit dem technischen Kundendienst der m-privacy GmbH. | |

| Prüfpunkt | Beschreibung | Zustand OK | Zustand Warning | Zustand Critical | Aktivität bei Warning | Aktivität bei Critical |
|--------------|---|---|--|---|--|--|
| diskerror | Sucht in der Datei kern.log nach Schlüsselworten, die auf Festplattenfehler hindeuten. | Keine Fehler gefunden | | Fehler gefunden | Warnungen deuten auf fehlerhafte Festplatten hin. Dies kann zu Dateninkonsistenzen oder Datenverlust führen. Kontaktieren Sie bitte den technischen Kundendienst der m-privacy GmbH. | |
| license | Prüft auf gültige Lizenz und gibt die Anzahl der genutzten Lizenzen sowie das Ablaufdatum zurück. | Lizenz gültig | | Lizenz ungültig | Die Lizenz muss über den technischen Kundendienst der m-privacy GmbH erneuert werden. | |
| apply | Prüft, ob ein Anwenden als Administrator Config notwendig ist. | Kein Anwenden notwendig | | Anwenden notwendig | Wird im Nagios signalisiert, dass ein Anwenden notwendig ist, bitte als Administrator config anmelden und ein Anwenden ausführen. | |
| slabs | Prüfung auf Speicherbereiche im Kern. | < 10 Mio. | Zwischen 10 und 100 Mio. | > 100 Mio. | Deutet auf Speicherlecks und Kernfehler hin. | |
| backup | Prüft auf vorhandenes Backup und eventuell aufgetretene Fehler. Gibt Datum und Uhrzeit des zuletzt angelegten Backups zurück, falls gefunden. | Backup ist vorhanden und fehlerfrei | Backup ist fehlerhaft, bzw. es wurde keine automatisches Backup konfiguriert | Backup nicht vorhanden oder Dienst nicht verfügbar | Als Administrator backuser anmelden und Protokoll auf Fehler überprüfen. Es kann mit dem Befehl Letztes Protokoll anzeigen aufgerufen werden. | Überprüfen, ob als Administrator backuser unter Konfiguration > Häufigkeit eventuell unpassende Einstellungen gewählt wurden. Dann z. B. im Protokoll nachsehen, ob ein Backup erstellt wurde und ggf. Fehler überprüfen. |
| smart_sd* | Prüft den SMART-Status der jeweiligen Festplatte und gibt den festgestellten Status zurück. Das *-Zeichen ist durch den jeweiligen Kaufwerksbuchstaben zu ersetzen. | Festplatte OK + aktuelle Temperatur | Temperatur > 45 °C | Temperatur > 50 °C | Wird eine zu hohe Temperatur ausgegeben, sollte die Kühlung des Systems geprüft werden. Falls die Festplatte nicht OK ist, werden auch die Fehler des S.M.A.R.T.-Checks der Platte ausgegeben. Maßnahmen können ein Systemstart vom Rettungssystem oder Ausführung eines fsck sein. | |
| definedusers | Prüft die Anzahl an angelegten Benutzer in TightGate-Pro und zeigt an, wie viele Benutzerkennungen derzeit im TightGate-Pro angelegt sind. | Es können noch mindestens 5 neue Benutzerkennungen angelegt werden. | Es können nur noch maximal 5 neue Benutzer angelegt werden. | Es kann maximal noch eine neue Kennung angelegt werden oder die maximale Anzahl von Benutzerkennungen ist bereits erreicht. | Bitte erwerben Sie weitere Lizenzen von TightGate-Pro. | |

Optionale Prüfpunkte

Optimale Prüfpunkte können je nach Systemkonfiguration verwendet werden, um spezifische Prozesse zu überwachen.

Prüfpunkte für Clustersystem "Ceph"

Je nachdem wie viele Ceph-Server im Einsatz sind werden für jeden Ceph-Server alle Nagios-Prüfpunkte bereit gestellt. Nachfolgende Tabelle listet alle Checks für den ersten Ceph-Server auf. Die Prüfpunkte für den zweiten und weitere Ceph-Server sind analog zu verwenden, jedoch ist die im Prüfpunkt angegebene Nummer jeweils hochzuzählen.

| Prüfpunkt | Beschreibung | Zustand OK | Zustand Warning | Zustand Critical | Aktivität bei Warning | Aktivität bei Critical |
|------------------------|--|----------------------|---------------------------|----------------------------|---|-------------------------------------|
| homeusermount | Prüft, ob /home/user im Verzeichnisbaum eingehängt ist. Gibt den Pfad von /home/user zurück. | Eingehängt | | Nicht eingehängt | Festplatte überprüfen, ggf. Benutzerverzeichnisse probeweise von Hand einhängen. Es könnte sich auch um einen Dateisystemfehler handeln, daher wird die Benachrichtigung des technischen Kundendienstes der m-privacy GmbH empfohlen. | |
| backupmount | Prüft, ob /home/backuser/backup korrekt im Verzeichnisbaum eingehängt wurde. | Eingehängt | | Nicht eingehängt | Festplatte überprüfen, ggf. Benutzerverzeichnisse probeweise von Hand einhängen. Es könnte sich um einen Dateisystemfehler handeln, daher wird die Benachrichtigung des technischen Kundendienstes der m-privacy GmbH empfohlen. | |
| ceph_hu_1_disks | Prüft freien Speicher auf den Festplatten des ersten Ceph-Servers. | > 20% frei | Zwischen 20% und 10% frei | < 10 % frei | Ist der Speicher voll, nehmen Sie bitte Kontakt mit dem technischen Kundendienst der m-privacy GmbH auf. | |
| ceph_hu_1_disk_load | Plattenaktivität aller verfügbaren Platten in %. | < 70% | Zwischen 70% und 90% | > 90% | Bei HDD problematisch. | |
| ceph_hu_1_zombie_procs | Unterminierte Zombieprozesse, können auf Fehler hinweisen. | Keine Zombieprozesse | Unter 10 Zombieprozessen | Über 10 Zombieprozessen | Zombieprozesse können gelegentlich auftreten und beeinträchtigen den Systembetrieb in der Regel nicht. Gehäuftes Auftreten von Zombieprozessen deutet auf Fehler in der Dateibehandlung hin. Es wird empfohlen, den technischen Kundendienst der m-privacy GmbH zu informieren. | |

| Prüfpunkt | Beschreibung | Zustand OK | Zustand Warning | Zustand Critical | Aktivität bei Warning | Aktivität bei Critical |
|---------------------|---|-------------------------------------|--|--|--|------------------------------|
| ceph_hu_1_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 Sekunden | Bei Abweichungen sollte unbedingt die Synchronizität wieder hergestellt werden, da sonst Cluster-Ausfälle drohen. | |
| ceph_hu_1_ssh | Prüft die Erreichbarkeit einer Secure Shell und gibt die SSH-Version zurück. | Erreichbar | | Nicht erreichbar | Falls SSH als unerreichbar moniert wird, sollte zunächst als Administrator config ein Anwenden ausgeführt werden. Ggf. ist eine Rücksprache mit dem technischen Kundendienst der m-privacy GmbH zu nehmen. | |
| ceph_hu_1_cron | Prüft die Anzahl der laufenden Cron-Jobs. | 1 bis 10 Cron-Jobs laufen | 11 bis 20 Cron-Jobs laufen | > 20 oder keine Cron-Jobs laufen | | |
| ceph_hu_1_ceph | Gibt den HEALTH-Status des gesamten externen Ceph aus. | Ceph ist in Ordnung | Ceph hat ein Problem | Ceph ist nicht intakt | Ja, nach Problem muss auf die Fehlermeldungen des Ceph individuell reagiert werden. Ggf. mit dem technischen Kundendienst der m-privacy GmbH Kontakt aufnehmen. | |
| ceph_hu_1_smart_sd* | Prüft den SMART-Status der jeweiligen Festplatte und gibt den festgestellten Status zurück. Das *-Zeichen ist durch den jeweiligen Kaufwerksbuchstaben zu ersetzen. | Festplatte OK + aktuelle Temperatur | Temperatur > 45 °C | Temperatur > 50 °C | Wird die Festplatte zu heiß, müssen die Lüftereinstellungen bzw. der Luftstrom im Server überprüft werden. | |

Weitere Optionale Prüfpunkte

| Prüfpunkt | Beschreibung | Zustand OK | Zustand Warning | Zustand Critical | Aktivität bei Warning | Aktivität bei Critical |
|-----------|---|--|---|---|---|--|
| scanner | Prüft, ob die Schadcodedefinitionen des Virencanners aktuell sind und ob der Virencanner läuft. | Definitionen aktuell (oder nicht älter als 2 Tage) | Definitionen älter als 2 Tage aber jünger als 1 Woche | Virencanner läuft nicht oder es sind keine Definitionen verfügbar oder die Definitionen sind älter als 1 Woche. | Virendefinitionen gemäß Administrationshandbuch aktualisieren. | Korrekte Konfiguration als Administrator config entsprechend Administrationshandbuch vornehmen. |
| sensors | Prüft die Festplatten-Temperatur | Temperatur unter 110°C | Temperatur über 110°C und unter 120° C | Temperatur über 120°C | Es besteht Überhitzungsgefahr. Bitte prüfen Sie, ob die Lüfter ordnungsgemäß arbeiten. Ggf. sind dazu im BIOS des Servers Einstellungen vorzunehmen. Bitte prüfen Sie auch, dass der Luftstrom um den Server gewährleistet ist. | |
| squid | Prüft auf die Erreichbarkeit des hinterlegten Proxy-Servers und gibt die Antwortzeit sowie den Verbindungsport aus. | Alles OK | | Port nicht Nicht erreichbar | Kann der Port nicht erreicht werden ist zu prüfen, ob der Dienst läuft. | |
| http | Prüft auf die Erreichbarkeit des des HTTP-Protokolls und gibt die Antwortzeit aus. | Alles OK | | Port Nicht erreichbar | Kann der Port nicht erreicht werden ist zu prüfen, ob der Dienst läuft. | |

| Prüfpunkt | Beschreibung | Zustand OK | Zustand Warning | Zustand Critical | Aktivität bei Warning | Aktivität bei Critical |
|-------------|---|----------------------------|--|--|---|---------------------------|
| temp | Prüft die Temperatur des Mainboards (falls Sensor vorhanden) und gibt sie aus. | < 50 °C | 50 °C bis 60 °C | > 60 °C | Bei Temperaturüberschreitung gesamtes Kühlsystem der Hardware (Lüfter, Kühlkörper, Luftkanäle, etc.) sowie Klimatisierung der Betriebsumgebung prüfen. | |
| fan | Prüft, ob ein Lüfter läuft (falls Sensor vorhanden). | Läuft | | Läuft nicht | Bei Problemmeldung Hardware überprüfen. | |
| timedupdate | Prüft, ob eine Automatisches Update geplant ist. | | | | Der Prüfpunkt liefert nur Informative Werte zum geplanten Update-Zeitpunkt. | |
| identd | Prüfung des Ident-Deamon für die Protokollierung von Proxy-Verbindungen. | ok | Keine Protokollierung konfiguriert, aber Proxy läuft | Protokollierung ist konfiguriert, aber der Proxy läuft nicht | Korrektur der Einstellungen oder Neustart des Dienstes durch Anwenden als config . | |
| adldap | Prüfung auf Erreichbarkeit des LDAP-Servers / AD-Servers bei der Benutzerverwaltung | | | | Gibt Hinweise auf Fehler bei der Verwendung von Active Directory oder LDAP-Servern. Es sind Maßnahmen entsprechend der Hinweise des Checks durchzuführen. | |
| nodesavail | Prüft auf die Verfügbarkeit aller Nodes innerhalb eines Clusters von TightGate-Pro Systemen | Alles Nodes sind verfügbar | Es sind weniger Nodes verfügbar als definiert, aber die Mindestanzahl ist noch gegeben | Es sind keine Nodes Erreichbar/Verfügbar. | Informativ. | |

From:

<https://help.m-privacy.de/> -

Permanent link:

<https://help.m-privacy.de/doku.php/tightgate-pro:anhang:nagios>

Last update:

2024/05/23 09:04

