# Dienstauswahl und Aktivitäten

Als Administrator ***config*** kann über das Nagios-Menü die Nutzung von Statistiken aktiviert werden. Diese Funktion erhebt Daten zur Laufzeit eines Serverrechners und stellt diese grafisch dar. Durch Klick auf das Grafik-Symbol auf der Hostseite der Nagios-Webseite können die Statistikdaten zum jeweils überwachten Service angezeigt werden. Es werden nicht für alle Services Statistiken angeboten.

## Dienstauswahl für TightGate-Server

Nachfolgende Aufstellung gibt einen Überblick über die implementierten Nagios-Prüfpunkte (Checks) bei TightGate-Systemen.

**Warnung:**
Zum Erhalt der CC-Konformität ist es bei TightGate-Pro (CC) Version 1.4 Server zwingend erforderlich, dass sich der als Nagios-Überwachunsstation agierende Rechner außerhalb des Klientennetzwerks befindet. Damit eine Verbindung mit TightGate-Pro (CC) Version 1.4 Server dennoch erfolgen kann, muss die IPv4-Adresse dieses Rechners unter ***config > Einstellungen > Wartung und Updates > Nagios / Storage IP*** hinterlegt sein.

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. Wird ein Nagios-Prüfpunkt nicht benötigt oder ist dessen Überwachung bzw. Anzeige nicht erwünscht, kann dieser Prüfpunkt aus den generierten Übersichten entfernt werden. Nähere Informationen erteilt der technische Kundendienst der m-privacy GmbH.

| **Prüfpunkt** | **Beschreibung** | **OK** | **Warnung (warning)** | **Problem (critical)** | **Aktivität, falls Warnung ausgegeben** | **Aktivität, falls Problem gemeldet** |
|---|---|---|---|---|---|---|
| backup | Prüft auf vorhandenes Backup und eventuell aufgetretene Fehler. Gibt Datum und Uhrzeit des zuletzt angelegten Backups zurück, falls gefunden. | Backup vorhanden und fehlerfrei. | Backup fehlerhaft. | 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. |
| bug | Sucht in der Datei kern.log nach Schlüsselworten, die auf Kernfehler hindeuten. | Kein Schlüsselwort gefunden. | — | Schlüsselwort(e) gefunden. | Technischen Kundendienst der m-privacy GmbH informieren. | |

| | | | | | |
|---|---|---|---|---|---|
| cron | Prüft, ob und wie viele Cron-Jobs laufen. | 1 bis 10 Cron-Jobs laufen | 11 bis 20 Cron-Jobs laufen | mehr als 20 oder keine Cron-Jobs laufen | Als Administrator ***root*** anmelden und Konsole aufrufen. Befehlsfolge ***ps tree -ah*** lokalisiert den blockierten Cron-Job.<br>Infrage kommende Dienste prüfen und entsprechende Maßnahmen ergreifen, z. B. als Administrator ***config Sanft Anwenden*** oder auch Neustart des Systems. |
| disk | Prüft freien Speicher auf den Festplatten für / und inode. | > 20 % frei | > 10 %, aber < 20 % frei | < 10 % frei | Statusseite des entsprechenden Systems aufrufen und Massenspeicher auf Belegung überprüfen.<br>Bei Platzmangel sollten insbesondere die Benutzerverzeichnisse in /home geprüft werden. Evtl. können z. B. alte Backups gelöscht werden.<br>Weiterhin sollten die Logdateien in /var/log geprüft werden. Zu große Logdateien können gelöscht werden, um Platz auf dem Datenträger zu schaffen. |
| 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. |
| homeusermount | Prüft, ob /home/user im Verzeichnisbaum eingehängt ist. Gibt den Pfad von /home/user zurück. | Eingehängt. | — | Nicht eingehängt. | Festplatte überprüfen, ggf. Benutzerverzeichnisse probehalber von Hand einhängen.<br>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 probehalber von Hand einhängen.<br>Es könnte sich um einen Dateisystemfehler handeln, daher wird die Benachrichtigung des technischen Kundendienstes der m-privacy GmbH empfohlen. |
| license | Prüft auf gültige Lizenz und gibt das Ablaufdatum zurück. | Lizenz gültig. | — | Lizenz ungültig. | Die Lizenz muss über den technischen Kundendienst der m-privacy GmbH erneuert werden. |

| | | | | | |
|---|---|---|---|---|---|
| load | Gibt die durchschnittliche Systemlast der letzten Minute, der letzten 5 bzw. 15 Minuten zurück. | Last < 40 | Last > 40 (1,5,15 min) | Last > 80,70,70 (1,5,15 min) | 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 dazu führen, dass diese Prozesse nicht mehr gestartet werden oder deutlich weniger Last verursachen.<br>In jedem Fall ist bei übermäßiger Systemlast der technische Kundendienst der m-privacy GmbH zu informieren. |
| ntp | Prüft die Erreichbarkeit des lokalen NTP-Zeitservers des jeweiligen Nodes und gibt spezifische Parameter zurück. | Erreichbar, Anzeige der Zeitdifferenz. | | Nicht erreichbar oder erreichbar und Zeitdifferenz > 1h. | Insbesondere in Clustersystemen müssen alle Nodes dieselbe Systemzeit aufweisen. Ist die Zeitdifferenz zur Referenz des externen NTP-Servers > 1 h, besteht unbedingt Handlungsbedarf! In diesem Fall als ***root*** anmelden, eine Konsole aufrufen und folgende Schritte ausführen:<br>* Lokalen NTP-Server anhalten: // **/etc/init.d/ntp stop**//<br>* Lokalen NTP-Server aktualisieren: ***ntpdate IP_des_externen_Zeitservers***<br>* Lokalen NTP-Server wieder starten: ***/etc/init.d/ntp start***<br><br>Schlägt dieses Verfahren fehl, könnte der externe NTP-Server unerreichbar sein. Dies kann als Administrator ***config*** mit dem Menüpunkt ***Netzwerk prüfen*** festgestellt werden. Ggf. sollte ein alternativer externer NTP-Server konfiguriert werden, um einwandfreien Systembetrieb sicherzustellen. |
| smart_sd*<br>smart_hd* | Prüft den SMART-Status der jeweiligen Festplatte und gibt den festgestellten Status zurück. | Festplatte OK + aktuelle Temperatur | Temperatur > 45 °C | Temperatur > 50 °C | Wird eine zu hohe Temperatur ausgegeben, sollte die Kühlung des Systems geprüft werden. Falls Festplatte nicht ok ist, werden auch die Fehler des S.M.A.R.T.-Checks der Platte ausgegeben.<br>Maßnahmen können ein Systemstart vom Rettungssystem oder Ausführung eines ***fsck*** sein. |

| | | | | | |
|---|---|---|---|---|---|
| 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. |
| 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 ***Sanft Anwenden*** ausgeführt werden.<br>Wird SSH danach weiterhin in Nagios 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. |
| swap | Prüft auf freien Swap-Speicher und gibt den Wert des gesetzten Maximalwerts und des freien Speicherplatzes zurück. | > 50% des gesetzten Maximalwerts frei | < 50%, aber > 20% des gesetzten Maximalwerts frei | < 20% des gesetzten Maximalwerts frei | Bei dauerhafter Überschreitung der Grenzwerte zunächst lastreduzierende 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. |
| total_procs | Prüft die Anzahl laufender Prozesse. | < 4000 | > 4000 und < 6000 | > 6000 | Ein Neustart des Systems kann die Zahl laufender Prozesse vermindern.<br>**Hinweis:** Dieser Prüfpunkt ist eher weniger aussagekräftig, da eine Warnung erst bei sehr hohen Werten erfolgt. |
| user | Prüft die Anzahl der aller angemeldeten Benutzer (VNC, SSH und SFTP) | < 80 | 80 bis 90 | > 90 | Bei dauerhafter Überschreitung der Grenzwerte ist mit Performance-Einbußen zu rechnen. |
| versions | Vergleicht die installierte Softwareversion mit dem aktuell verfügbaren Softwarestand. | 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.<br>Wird VNC danach weiterhin in Nagios 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. |

| | | | | | |
|---|---|---|---|---|---|
| zombie_procs | Unterminierte Zombieprozesse, können auf Fehler hinweisen. | Keine unterminierten Zombieprozesse vorhanden. | Bis zu 10 Zombieprozesse vorhanden. | Mehr als 10 Zombieprozesse vorhanden. | 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. |
| maint | Prüft, ob ein Node verfügbar und nicht im Wartungsmodus ist. Gibt ggf. den Zeitpunkt einer geplanten Wartung zurück. | Node verfügbar und nicht im Wartungsmodus. | Node im Wartungsmodus. | | Nach beendeter Wartung als Administrator ***maint*** anmelden und Wartungsmodus beenden. |
| 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. |

# Dienstauswahl für Server ohne Nagios-Sensoren

Bei manchen Servern besteht mitunter nicht die Möglichkeit, die für das Monitoring notwendigen Nagios-Plugins zu installieren und damit entsprechende Prüfpunkte zu etablieren. Einige Funktionen dieser Server können aber dennoch durch TightGate-Monitoring überwacht werden. Dies betrifft regelmäßig solche Server, die beim Anlegen des Hosts in der Nagios-Konfiguration den TYP „anderer" haben.

Die nachfolgende Liste gibt eine Übersicht über die in diesen Fällen verfügbaren Prüfpunkte:

| Prüfpunkt | Statistiken | Beschreibung |
|---|---|---|
| ssh | Nein | Prüfung über Port 22 (TCP), ob ein SSH-Server antwortet |
| http | Ja | Prüfung über Port 80 (TCP), ob ein Webserver antwortet |
| https | Ja | Prüfung über Port 443 (TCP), ob ein Webserver antwortet |
| pop | Nein | Prüfung über Port 110 (TCP), ob ein Mailserver antwortet |
| imap | Ja | Prüfung über Port 993 (TCP), ob ein Mailserver antwortet |
| smtp | Ja | Prüfung über Port 25 (TCP), ob ein Mailserver antwortet |
| ftp | Ja | Prüfung über Port 21 (TCP), ob ein FTP-Server antwortet |

# Dienstauswahl für Windows-Server

Das TightGate-Monitoring erlaubt es, auch Windows-Server mit in die Überwachung mit aufzunehmen. Dabei unterstützt TightGate-Monitoring die Prüfpunkte der Standard-Windows-Überwachung von NSClient++. Alle von dieser Software unterstützten Alias-Prüfpunkte sind im TightGate-Monitoring bereits vordefiniert und können bei der Dienstauswahl direkt selektiert werden.

Folgende Voraussetzungen zur Nutzung der NSClient++-Prüfpunkte müssen erfüllt sein:

- Installation und Konfiguration des Pakets NSClient++ auf dem jeweiligen Windows Server.

Download via http://www.nsclient.org/download/ Im Installationsverzeichnis des Programms NSClient++ auf dem jeweiligen Windows Server befinden sich auch PDF-Dokumente zur Konfiguration der einzelnen Prüfpunkte.

- Zugriff des TightGate-Monitoring auf den Windows-Server über Port 5666 (TCP); ggf. muss das Regelwerk einer lokalen Firewall auf dem Windows-System angepasst werden.

Die nachfolgende Liste enthält alle verfügbarer Prüfpunkte für Windows-Server, welche im TightGate-Monitoring vordefiniert sind. Die Prüfpunkte korrespondieren mit den Vorgaben der *nsclient.ini* auf dem zu überwachenden Windows-Server.

| ***Prüfpunkte*** | ***Prüfpunkte*** | ***Prüfpunkte*** |
|---|---|---|
| alias-cpu | alias-sched_all | alias-process |
| alias-disk | alias-sched_long | alias-process-count |
| alias-event_log | alias-sched_task | alias-process-hung |
| alias-file_age | alias-service | alias-process-stopped |
| alias-file_size | alias-up | alias-volumes |
| alias-mem | alias-updates | alias-counter |

Die Einstellungen zu den einzelnen Prüfpunkten werden direkt auf den Windows-Server in der Datei *nsclient.ini* definiert.

From:
https://help.m-privacy.de/ -

Permanent link:
**https://help.m-privacy.de/doku.php/tightgate-monitor:checks**

Last update: **2021/10/29 12:16**