TightGate-Monitoring

Integrierte Systemüberwachung auf Nagios-Basis
für Server der TightGate-Produktlinie
sowie weiterer Serverrechner

Herausgeber:
m-privacy GmbH
Technische Redaktion
Werner-Voß-Damm 62
12101 Berlin

Fon: +49 30 243423-34
Fax: +49 30 99296856

support@m-privacy.de
https://help.m-privacy.de/doku.php/tightgate-monitor

Inhaltsverzeichnis

Versionshistorie

Ver.	Datum	Änderung	Redakteur
0.50	05.12.2013	Dokument erstellt	ple
1.00	09.12.2013	Dokument freigegeben	ple
1.01	06.11.2014	Erweiterung Monitoring Windows	hom
1.02	20.11.2014	Detailkorrekturen	ple
1.10	23.06.2015	Erweiterung ZenTiV	hom
1.15	24.06.2015	Detailkorrekturen	ple
1.16	25.06.2015	Detailkorrekturen	hom
1.17	30.06.2015	Ergänzungen ZenTiV	hom
1.18	30.11.2015	Ergänzungen ZenTiV	hom

Allgemeine Hinweise zu diesem Handbuch

Alle Materialien und Ausführungen wurden mit größter Sorgfalt erarbeitet und zusammengestellt. Dennoch sind Fehler nicht auszuschließen. Die m-privacy GmbH übernimmt keine Haftung für Schäden, die aus Unrichtigkeit einzelner Angaben entstehen.

Im Sinne einer raschen Orientierung und zur Vermeidung von Sicherheitsrisiken werden besonders wichtige Aspekte durch wiederkehrende Stichworte gekennzeichnet. Diese sind:

Hinweis
Unter diesem Stichwort werden nützliche Details zur rationellen Verwendung von TightGate-Servern erläutert.

Achtung
Unter diesem Stichwort erfolgen Hinweise zur Problemvermeidung bzw. zur Vorbeugung von Betriebsstörungen bei TightGate-Servern.

Warnung
Unter diesem Stichwort erfolgen Hinweise auf mögliche Fehler bei der Konfiguration und Verwendung von TightGate-Servern, die weitreichende Sicherheitsrisiken bergen oder zu schwerwiegenden Betriebsstörungen führen können.

1 Einführung

Die Server der TightGate-Produktlinie sowie weitere Server sind im Systembetrieb komfortabel mittels des TightGate-Monitorings auf Nagios-Basis zu überwachen. Der Monitoring-Server ist separat zu erwerben und kann virtualisiert werden. Die Sensoren zur Erfassung der Prüfpunkte sind standardmäßig in die Server der TightGate-Produktlinie integriert. Bei anderen Serverrechnern müssen die Prüfpunkte nachinstalliert werden; alternativ lassen sich auch ohne gesonderte Prüfpunkte grundlegende Serverfunktionen überwachen. Über die regulären Sensoren zur Überwachung der Serverparameter hinaus stehen weitere Sensoren zur Verfügung, welche spezifische Prüfpunkte im Zusammenhang mit TightGate-Servern registrieren und dem Monitoring zugänglich machen.

Neu hinzugekommen sind Prüfpunkte zur Überwachung von Windows-Servern, sodass über TightGate-Monitoring im Idealfall die gesamte Serverlandschaft eines Netzwerks integriert überwacht werden kann.

2 Konfiguration

Die gesamte Konfiguration von TightGate-Monitoring erfolgt menübasiert. Es ist hierzu die Anmeldung über ein Terminalprogramm (z. B. „puTTY“) am Monitoring-Server erforderlich. Die Konfigurationseinstellungen werden als Administrator ***config*** vorgenommen. Das Administrationskonzept entspricht grundsätzlich dem der anderen Server der TightGate-Produktlinie.

Das wird benötigt:

→ Betriebsbereit konfigurierter E-Mail-Versand für E-Mail-Benachrichtigung

→ Für SMS-Versand: Zugriff über Port 443 (TCP) zum SMS-Expert-Provider

2.1 Monitoring aktivieren

Bevor ein Server mittels TightGate-Monitoring überwacht werden kann, muss dieser als neuer Host dem Monitoring-System bekannt gemacht werden. Folgende Einstelloptionen stehen zur Verfügung:

config > Einstellungen > Nagios	
Menüpunkt	**Beschreibung**
Nagios starten	Starten/Stoppen des Nagios-Dienstes.
Nagios Statistiken	Start/Stop des Nagios-Graphers, der für einzelne Sensoren grafische Statistiken liefert.
Globale Kontakte	Liste aller verfügbaren Kontakte, an die Nagios-Meldungen versendet werden können. **Hinweis:** Kontakte sind nur verfügbar, wenn sie als globale Kontakte eingetragen wurden.
Anzeigen	Zeigt alle von diesem Nagios-System überwachten Hosts mit allen Einstellungen am Bildschirm an.
Dienste aktualisieren	Aktualisiert alle Dienste der überwachten Hosts, sofern bei diesen die automatische Aktualisierung aktiviert ist. Die automatische Dienstaktualisierung arbeitet nur an TightGate-Servern mit Ausnahme von TightGate-Pro.
Neu	Legt einen neuen zu überwachenden Host an.
Kopieren	Kopiert einen bestehenden Host.
Löschen	Löscht einen zu überwachenden Host.
nagiosamin-Passwort	Setzt das Passwort für den „nagiosadmin“-Benutzer zu Nutzung der Web-Oberfläche neu.
---	Beginn der Host-Übersicht
1	Erster von Nagios überwachter Host. Es werden alle registrierten (d. h. zu überwachenden) Hosts angezeigt. Die Sortierung erfolgt aufsteigend anhand der laufenden Nummer, die bei der initialen Konfiguration eines neuen Hosts gesetzt werden muss.
...	Ggf. weitere überwachte Hosts

2.2 Globale Kontakte und Warnstufen

Das Anlegen globaler Kontakte dient als Vorgabe, welche Adressen per E-Mail oder SMS benachrichtigt werden sollen. Es kann ebenfalls festgelegt werden, für welche Art von Warnstufen das Nagios-System die Kontakte benachrichtigt. Bevor ein Nagios-Host definiert werden kann, muss mindestens ein globaler Kontakt definiert sein, maximal können 999 Kontakte angelegt werden. Nachfolgende Einstelloptionen bestehen:

config > Einstellungen > Nagios > Globale Kontakte > neu	
Menüpunkt	**Beschreibung**
Nummer	Laufende Nummer des Kontakts. Es kann eine Nummer zwischen 1 und 999 frei gewählt werden.
Name	Name des Kontakts
Kommentar	Kommentar zum Kontakt
Alias	Alias-Name zum Kontakt
E-Mail	E-Mail-Adressen, an welche die Benachrichtigungen versandt werden. Mehrere E-Mail-Adressen sind durch Leerzeichen voneinander zu trennen.
SMS-Nummern*	Mobilrufnummer(n), an welche die Benachrichtigungen versandt werden. Mehrere Rufnummern sind durch Leerzeichen voneinander zu trennen. Das Format der Rufnummer ist dabei eine fortlaufende Nummer mit Ländervorwahl. Beispiel für eine Mobilrufnummer im deutschen Netz: 0049 (Ländervorwahl) 0178 (Vorwahl Mobilfunknetz) 1234567 (Rufnummer) → einzutragen ist: 491781234567
Zeit	Auswahl einer Zeit, bzw. eines Zeitraumes, in der das Nagios-System Benachrichtigungen an den Kontakt versenden darf.
Host-Optionen	Auswahl der Host-Ereignisse, zu denen Meldungen vom Nagios-System versendet werden.
Dienst-Optionen	Auswahl der Dienst-Ereignisse, zu denen Meldungen vom Nagios-System versendet werden.

*Zur Nutzung der SMS-Funktionalität ist ein gültiger Account bei der Firma SMS-Expert, Hamburg, notwendig. Durch Inanspruchnahme des SMS-Dienstes entstehen weitere Kosten. Je nach Einstellung können sehr viele SMS versandt werden. Da es sich um einen Prepaid-Dienst handelt, ist der SMS-Versand nur bei bestehendem Guthaben möglich. Die notwendigen Einstellungen zur Übermittlung der SMS via SMS-Expert werden auf der Hauptseite unter ***config > Einstellungen > Nagios > Globale Kontakte*** vorgenommen.

2.3 Nagios-Hosts anlegen

Bevor ein Server mittels TightGate-Monitoring überwacht werden kann, muss er dem Monitoring-Server bekannt gemacht werden. Dies geschieht über nachfolgende Einstelloptionen:

config > Einstellungen > Nagios > Neu	
Menüpunkt	**Beschreibung**
Nummer	Nummer des zu überwachenden Hosts. Es kann eine Nummer zwischen 1 und 999 frei gewählt werden. Die Nummer des Hosts beeinflusst die Anzeige in der Webansicht. Die Hosts werden der Nummer nach aufsteigend angezeigt.
Aktiviert	Aktiviert oder deaktiviert die Überwachung des Hosts.

config > Einstellungen > Nagios > Neu	
Name	Name des zu überwachenden Hosts. Sofern es sich bei dem zu überwachende System um ein TightGate-Pro Server handelt, sollte der auflösbare DNS-Name des zu überwachenden Hosts eingetragen werden, damit die Schaltfläche zum direkten Aufruf der „TightGate-Administration“ über die Web-Oberfläche korrekt arbeitet. **Achtung:** Der auflösbare DNS-Name muss derselbe sein, der im Active Directory (AD) hinterlegt ist und über den sich auch etwaige TightGate-Viewer auf den Klientenrechnern mit einem TightGate-Pro Server verbinden. Andernfalls ist Single Sign-on (SSO) beim Direktzugriff auf die Administrationsoberfläche des überwachten Servers nicht möglich. Bei Nutzung der entsprechenden Schaltfläche im Web-Frontend der Monitoring-Ansicht erfolgt in diesem Fall ein Login mit Zugangsdaten (Benutzername / Passwort).
ZenTiV-Kommentar	Der Kommentar kann frei gewählt werden und wird als Beschreibung in der ZenTiV-Weboberfläche zu dem Host angezeigt.
Alias	Der Alias kann frei gewählt werden und wird als Beschreibung in der Web-Oberfläche zu dem Host angezeigt.
Typ	Auswahl des Host-Typs, welcher überwacht werden soll. Es stehen folgende Host-Typen zur Auswahl:
	anderer – Unbekannter / anderer Host (nicht in dieser Liste aufgeführt) fw – TightGate-Firewall mail – TightGate-Mailserver web – TightGate-Webserver pro – TightGate-Pro win – Windows-Host
Adresse	IPv4-Adresse oder auflösbarer Hostname des zu überwachenden Hosts.
Port	Port, über das der Nagios-Server mit dem Host kommunizieren kann. Standard-Port ist 5666.
Gateway	Sofern ein Gateway vor dem zu überwachenden Host liegt, so ist es hier auszuwählen. **Achtung:** Das Gateway muss ebenfalls als Host definiert sein.
Dienste	Auswahl der Dienste für den Host. Die Liste der verfügbaren Dienste für die jeweils zu überwachenden Server befindet sich im Kapitel 3.
Dienst-Auto-Update	Auswahl, ob die Dienste des zu überwachenden Hosts durch den Nagios-Server automatisch aktualisiert werden sollen. Diese Funktion setzt voraus, dass der Host diese Funktion unterstützt. Bei TightGate-Systemen unterstützen alle TightGate-Server außer TightGate-Pro diese Funktion.
Kontakte	Auswahl der Kontakte, die über Meldungen im Nagios informiert werden sollen. Es können beliebig viele Kontakte ausgewählt werden. **Hinweis:** Kontakte können nur ausgewählt werden, wenn sie vorher als „Globale Kontakte“ angelegt wurden.
Prüf-Zeiten	Auswahl der Zeiten, in denen der Host überwacht wird.
Nachrichten-Abstand	Abstand in Minuten zwischen zwei Nachrichten, sofern ein Dienst oder Host nicht wieder verfügbar ist. Wert 0 sendet keine weiteren Nachrichten, beim Maximalwert 1440 wird einmal täglich eine Nachricht versandt.

Exkurs „Nachrichten-Abstand“:
Sofern ein Dienst ausfällt, ein Host nicht mehr verfügbar ist oder ein anderer, als Abweichung definierter Zustand auftritt, wird dies vom Nagios-System erkannt. Eine Alarmierung per E-Mail oder SMS erfolgt zu diesem Zeitpunkt noch nicht, stattdessen wird die Abweichung in der entsprechenden Log-Datei vermerkt. So werden (ggf. Kosten verursachende) Fehlalarme vermieden, zumal Dienste aus Sicht des Nagios-Systems vorübergehend unerreichbar sein können, auch ohne dass eine schwerwiegende Fehlerbedingung (beispielsweise ein Rechnerausfall) gegeben ist.

Ist ein Dienst über einen längeren Zeitraum nicht verfügbar, generiert das Nagios-System im Minutenabstand weitere Einträge in der Log-Datei. Dabei werden die Anzahl der Meldungen hochgezählt. Eine Alarmierung des hinterlegten Kontakts erfolgt nach dem 10. Eintrag derselben Abweichung.

Webansicht der Monitoring-Oberfläche

TightGate-Monitoring gibt die Statusanzeige der Prüfpunkte in einer übersichtlichen Webansicht aus. Diese Übersicht kann mit allen gängigen Webbrowsern abgerufen und dargestellt werden. Um den Zugang zu schützen und Unbefugten eine Einsichtnahme in die Betriebsparameter der überwachten Hosts zu verwehren, ist der Aufruf der Webansicht passwortgeschützt. Sie ist erreichbar über

https://[IPv4-Adresse des TightGate-Monitoring-Servers]/nagios3/

Hinweis:
Die Webansicht kann nur SSL-gesichert aufgerufen werden (https://).

Es wird ein Anmeldedialog angezeigt. Der Benutzername lautet stets ***nagiosadmin***. Das Passwort kann durch den Administrator *config* unter ***config > Einstellungen > Nagios > nagiosadmin Passwort*** gesetzt werden. Es wird eine Übersicht angezeigt, die nachfolgendem Beispiel entspricht:

Im Navigationsbereich auf der linken Seite sind die wesentlichen Funktionen direkt erreichbar. Unter Hosts kann der Server ausgewählt werden, der überwacht werden soll. Mittels Services können die einzelnen Dienste angezeigt werden. Ist der Administrations-Direktzugriff eingerichtet, wird zusätzlich eine entsprechende Schaltfläche angezeigt. Über diese Schaltfläche kann direkt in die Administrationsoberfläche des zu überwachenden Servers gewechselt werden, sofern es sich um einen TightGate-Pro Server handelt.

2.4 Administrations-Direktzugriff

Sollten in der Web-Ansicht von TightGate-Monitoring Betriebszustände bei zu überwachenden TightGate-Pro-Systemen festgestellt werden, die den Eingriff eines Administrators erfordern, kann unmittelbar zur Administrationsoberfläche des betreffenden Servers gewechselt werden. Dort kann das ursächliche Problem behoben und der Systemzustand über TightGate-Monitoring sofort kontrolliert werden.

2.4.1 Vorarbeiten

Zunächst ist das MSI-Paket ***TG-Pro nagios*** auf dem Klientensystem zu installieren, welches die Web-Ansicht von TightGate-Monitoring darstellen soll. Dieses Programmpaket steht derzeit für Microsoft Windows bis Version 8.1 zur Verfügung. Es registriert auf dem Klientensystem ein neues Protokoll namens „tgpro“.

Weiterhin ist die Anbindung des zu überwachenden Host-Systems an ein Active Directoy (AD) obligatorisch, falls eine automatische Anmeldung an der Administrationsoberfläche per Single Sign-on (SSO) gewünscht wird. Andernfalls ist nur die Anmeldung mit Zugangsdaten (Benutzername / Passwort) möglich.

Hinweis:
Der Administrations-Direktzugriff aus der Web-Ansicht von TightGate-Monitoring heraus ist nur auf Hosts der TightGate-Pro-Reihe möglich.

Wird nach Abschluss der Vorarbeiten die Web-Ansicht von TightGate-Monitoring auf dem Klientensystem aufgerufen, erscheint zusätzlich die Schaltfläche zum Administrations-Direktzugriff.

2.4.2 Nutzung

Durch Betätigung der Schaltfläche zum Administrations-Direktzugriff wird automatisch ein Konsolenfenster geöffnet und eine Verbindung zum überwachten Host hergestellt. Der Systemadministrator wird automatisch als Administrator ***config*** am Host angemeldet und kann notwendige Verwaltungsarbeiten ausführen.

Hinweis:
Hinweise und Sicherheitsabfragen des Browsers müssen akzeptiert werden, da andernfalls die Verbindung nicht an den Host übergeben werden kann.

3 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.

3.1 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.	
check_apply	Zeigt an, ob ein ***Sanft Anwenden*** für den Administrator ***config*** aussteht und nachgeholt werden muss.	No config apply needed.	Config apply needed.	---	Fehlendes ***Sanft Anwenden*** sollte umgehend nachgeholt werden. Insbesondere im Rechnerverbund (Cluster) kann andernfalls instabiler Systembetrieb die Folge sein.	
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	Eine sehr große Zahl laufender Cron-Jobs kann auf nicht korrekt terminierende Jobs hindeuten. 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*** ***Sanft Anwenden*** oder auch Neustart des Systems.	

Prüfpunkt	Beschreibung	OK	Warnung (warning)	Problem (critical)	Aktivität, falls Warnung ausgegeben	Aktivität, falls Problem gemeldet
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. 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. Sie werden automatisch neu angelegt.	
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.	
homeuser-mount	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. Es könnte sich auch um einen Dateisystemfehler handeln, daher wird die Benachrichtigung des technischen Kundendienstes der m-privacy GmbH empfohlen.	
glusterhomeuser	Prüft, ob der für den Betrieb des Dateisystems entscheidende GlusterFS-Server für /home/user auf diesem System läuft.	Läuft.	---	Läuft nicht.	Sollte sich das Problem durch ***Sanft Anwenden*** nicht lösen lassen, ist der technische Kundendienst der m-privacy GmbH zu benachrichtigen.	
gluster-backup		Erreichbar.	---	Nicht erreichbar.	Sollte sich das Problem durch ***Sanft Anwenden*** nicht lösen lassen, ist der technische Kundendienst der m-privacy GmbH zu benachrichtigen.	
backup-mount	Prüft, ob /home/backuser /backup korrekt im Verzeichnisbaum eingehängt wurde.	Eingehängt.	---	Nicht eingehängt.	Festplatte überprüfen, ggf. Benutzerverzeichnisse probehalber von Hand einhängen. 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. In jedem Fall ist bei übermäßiger Systemlast der technische Kundendienst der m-privacy GmbH zu informieren.	

Prüfpunkt	Beschreibung	OK	Warnung (warning)	Problem (critical)	Aktivität, falls Warnung ausgegeben	Aktivität, falls Problem gemeldet
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: 1. Lokalen NTP-Server anhalten: ***/etc/init.d/ntp stop*** 2. Lokalen NTP-Server aktualisieren: ***ntpdate IP_des_externen_Zeitservers*** 3. Lokalen NTP-Server wieder starten: ***/etc/init.d/ntp start*** 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* 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. 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. 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.	
timedupdate	Anzeige de Datums und der Uhrzeit geplanter Updates bzw. Deaktivierung geplanter Updates.	OK: Timed update is disabled oder OK: Timed update on [Zeitstempel]	---	---		
total_procs	Prüft die Anzahl laufender Prozesse.	< 4000	> 4000 und < 6000	> 6000	Ein Neustart des Systems kann die Zahl laufender Prozesse vermindern. **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.	

Prüfpunkt	Beschreibung	OK	Warnung (warning)	Problem (critical)	Aktivität, falls Warnung ausgegeben	Aktivität, falls Problem gemeldet
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. 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.	Sogenannte 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.	
gluster_error_user	Prüft auf Fehler in den Klienten-Logdateien und gibt sie (wenn vorhanden) aus.	Keine Fehler.	---	Fehler vorhanden.	Zunächst System neu starten. Falls danach weiterhin Fehler auftreten: Als Administrator *root* anmelden und /home/user/ manuell aus- und wieder einhängen. Dieser Vorgang kann nur als Administrator *root* manuell ausgeführt werden, nachdem alle Benutzer abgemeldet wurden. In jedem Fall sollte der technische Kundendienst der m-privacy GmbH benachrichtigt werden.	
gluster_error_backup	Prüft auf Fehler in den Logdateien des Administrators *backuser* und gibt sie (wenn vorhanden) aus.	Keine Fehler.	---	Fehler vorhanden.	Zunächst System neu starten. Falls danach weiterhin Fehler auftreten: Als Administrator *root* anmelden und /home/backuser manuell aus- und wieder einhängen. Dieser Vorgang kann nur als Administrator *root* manuell ausgeführt werden, nachdem alle Benutzer abgemeldet wurden. In jedem Fall sollte der technische Kundendienst der m-privacy GmbH benachrichtigt werden.	
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.	
fpupdate	Prüft, ob die Schadcodedefinitionen des F-Prot aktuell sind und ob der F-Prot-Monitor läuft.	Definitionen aktuell (oder nicht älter als 3 Tage) und F-Prot-Prozess (fpmon) läuft.	> 3 Tage alte Definitionen	F-Prot-Prozess (fpmon) läuft nicht.	Aktualität der F-Prot Lizenz überprüfen und Virendefinitionen gemäß Administrationshandbuch aktualisieren.	Korrekte Konfiguration als Administrator *config* entsprechend Administrationshandbuch vornehmen.
cups	Prüft auf Verfügbarkeit des CUPS-Dienstes.	CUPS- Prozess läuft.		CUPS- Prozess läuft nicht.	Sollte sich das Problem durch ***Sanft Anwenden*** nicht lösen lassen, ist der technische Kundendienst der m-privacy GmbH zu benachrichtigen.	

3.2 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

3.3 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:

1. 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.
2. 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.

4 ZenTiV (Zentrale TightGate-Verwaltung)

ZenTiV ist die Verwaltungszentrale zur gemeinsamen Administration mehrerer TightGate-Pro-Server.

4.1 Initiale Einrichtung von ZenTiV

Das wird benötigt:

→ Ein aktuelles TightGate-Monitoring-System mit gültiger Lizenz muss betriebsbereit vorliegen.

So geht's:

1. Als Administrator ***update*** unter **Kundendienst > Optionale Pakete** das Paket **zentiv** installieren.
2. Als ***config*** neu anmelden und unter **Einstellungen > Laufenden Dienste > ZenTiV-Fernverwaltung** ZenTiV starten. Nach dem Starten von ZenTiV erweitert sich das Menü unter Laufende Dienste um weitere Menüpunkte.
3. Den neuen Menüpunkt **ZenTiV-SSH-Key** auswählen. Dadurch wird ein neuer SSH-Key erzeugt.

   ACHTUNG:
   Der SSH-Key wird verwendet, um alle TightGate-Pro-Server an die ZenTiV zu binden. Wird dieser Key erneuert, können alle bisher über ZenTiV verwalteten TightGate-Pro-Server nicht mehr über das Werkzeug erreicht werden!
4. Über den Menüpunkt **ZenTiV-SSH-Pub-Export** den erzeugten SSH-Key in das transfer-Verezichnis des Administrators ***config*** exportieren.
5. Als Administrator ***config*** die Einstellungen **Speichern** und **Sanft Anwenden**.

Nächste Schritte:

→ ZenTiV-Benutzer hinzufügen

→ TightGate-Pro-Server zu ZenTiV hinzufügen

4.2 ZenTiV-Benutzer hinzufügen

Zur Anmeldung an der Weboberfläche von ZenTiV werden gültige Zugangsdaten (Benutzername und Passwort) eines Benutzers benötigt, welcher im TightGate-Monitoring angelegt sein muss.

Für das Anlegen eines neuen Benutzers ist zumindest ein Benutzername notwendig. Vor- und Nachname sind optional. Das Anlegen von neuen Benutzern geschieht als Administrator ***maint*** in der Benutzerverwaltung.

Das wird benötigt:

→ Benutzername und Passwort für den neuen ZenTiV-Benutzer

So geht's:

1. Als Administrator ***maint*** unter **Benutzerverwaltung > Neu> 20000 ZentiV** einen neuen ZenTiV-Benutzer für die Domäne „ZenTiV" anlegen. Der Benutzer ist sofort nach Ausführung des Assistenten aktiv.

Ergebniskontrolle:

Nach der Anlage des neuen Benutzers als Administrator ***maint*** ist es möglich, sich mit dem neuen Benutzer an der ZenTiV-Oberfläche anzumelden.

4.3 Einen neuen TightGate-Pro-Server zu ZenTiV hinzufügen

4.3.1 TightGate-Pro für ZenTiV vorbereiten

Das wird benötigt:

→ Die lokale Zeitzone, in der sich TightGate-Pro befindet

→ SSH-Public-Key vom TightGate-Monitoring zur Authentisierung von ZenTiV an TightGate-Pro

→ IP-Adresse des TightGate-Monitoring-Servers, auf der ZenTiV läuft

So geht's:

1. Den SSH-Public-Key vom TightGate-Monitoring in das Transfer-Verzeichnis des Administrators ***config*** von TightGate-Pro kopieren.
2. Als Administrator ***config*** im Hauptmenü über den Menüpunkt **Zeitzone setzen** die Zeitzone festlegen.
3. Als Administrator ***config*** unter **Einstellungen > Wartung und Updates > Ferne Administrator-IP** die IP-Adresse des TightGate-Monitoring-Servers eintragen.
4. Als Administrator ***config*** unter **Einstellungen > ZenTiV-Job-Verarbeitung** die ZenTiV-Verwaltung für diesen TightGate-Pro-Server aktivieren. Sobald die ZenTiV-Job-Verarbeitung auf **ja** gesetzt wurde, erscheint ein neuer Menüpunkt (ZenTiV-Job-Upload-Schlüssel).
5. Den Menüpunkt ZenTiV-Job-Upload-Schlüssel auswählen, den SSH-Public-Key des TightGate-Monitoring-Servers auswählen und damit importieren.
6. Als Administrator ***config*** die Einstellungen **Speichern** und **Sanft Anwenden**.
7. Als Administrator ***update*** über den Menüpunkt **Zeitgest. Download: Beginn/Ende** festlegen, in welchen Intervallen TightGate-Pro Updates herunterladen soll.
8. Als Administrator ***update*** über den Menüpunkt **Zeitgest. Update: Beginn** festlegen, zu welchem Zeitpunkt TightGate-Pro Updates installieren soll.

4.3.2 TightGate-Pro zu ZenTiV (TightGate-Monitoring) hinzufügen

Das Hinzufügen eines TightGate-Pro-Servers zu ZenTiV erfolgt ebenso wie das Anlegen eines neuen Hosts für die Nagios-Überwachung. → Siehe Kapitel 2.3 Nagios-Hosts anlegen.

Das wird benötigt:

→ IP-Adresse vom TightGate-Pro

→ Grundkonfiguriertes NAGIOS auf TightGate-Monitoring

So geht's:

1. Server als Administrator ***config*** im Nagios anlegen. Zusätzlich kann das Feld **ZenTiV-Kommentar** genutzt werden. Diese Informationen werden auf der ZenTiV-Weboberfläche mit angezeigt.
2. Als Administrator ***config*** die Einstellungen **Speichern** und **Sanft Anwenden**.

Ergebniskontrolle:

Nachdem das **Sanft Anwenden** abgeschlossen ist, wird der hinzugefügte TightGate-Pro-Server in der ZenTiV-Weboberfläche angezeigt.

4.4 TightGate-Pro über die ZenTiV-Weboberfläche verwalten

Das wird benötigt:

→ Die zu verwaltenden TightGate-Pro-Server müssen bereits in der ZenTiV eingetragen sein

→ Gültige Zugangsdaten eines ZenTiV-Benutzers

So geht's:

1. Anmeldung an der ZenTiV-Weboberfläche, per Webbrowser auf IP-Adresse https://IP-Adresse/zentiv/ (bei ZenTiV sind nur verschlüsselte Verbindung per HTTPS erlaubt)
2. Auswahl der zu bearbeitenden TightGate-Pro-Server (über Suche oder Gruppe)
3. Markierung der zu verwaltenden TightGate-Pro-Server. Es können dabei einzelne oder mehrere Server ausgewählt werden. → Siehe dazu 4.6 ZenTiV - Server auswählen.
4. Auswahl der durchzuführenden Aufgabe aus der Liste **Administration** oder **Aufträge senden**. → Siehe dazu 4.8 ZenTiV – TightGate-Pro administrieren
   Hinweis: Es kann für den/die markierten Server nur jeweils eine Aktion durchgeführt werden.
5. Eine Übersicht gibt eine Zusammenfassung der ausgewählten Server und der durchzuführenden Aktion. Die Freigabe/Bestätigung der ausgewählten Aufgabe erfolgt über den Button **Auftrag absenden bestätigen**.

Ergebniskontrolle:

Nach der Bestätigung des Auftrags wird dieser in der Übersicht **Aufträge** angezeigt. Solange der Auftrag noch nicht auf dem jeweiligen TightGate-Pro-Server ausgeführt wurde, kann er ausgewählt und gelöscht werden.

4.5 ZenTiV - Gruppen anlegen / löschen

In der ZenTiV-Oberfläche kann über den Menübutton **Gruppen** die Gruppenverwaltung für die Server aufgerufen werden. Beim Aufruf des Gruppen-Buttons zeigt das System eine Liste aller verfügbaren Gruppen. In der Grundinstallation gibt es vorgegebene Gruppen, die nicht verändert werden können. Folgende Gruppen sind fest vorgegeben:

Gruppenname	**Beschreibung**
Alle Server	Liste aller Server
Server mit verfügbaren Updates	Server mit verfügbaren Updates
Server mit unvollständigen Updates	Server mit unvollständig heruntergeladen Updates

Eine neue Gruppe kann über die Schaltfläche **Neue Gruppe anlegen** hinzugefügt werden. Neben dem Namen der Gruppe, welcher obligatorisch ist, kann noch eine Beschreibung für die Gruppe hinzugefügt werden. Über den Button **Gruppe anlegen** wird die Gruppe angelegt.

Um eine Gruppe zu löschen, markiert man in der Gruppenverwaltung die zu löschende Gruppen und betätigt die Schaltfläche **Ausgewählte Gruppen löschen**. Nach der Bestätigung der Eingabe wird die Gruppe (nicht die Server in der Gruppe) gelöscht.

Das Hinzufügen von Servern zu einer Gruppe erfolgt über den Menübutton **Server**. Die Serverliste zeigt eine Auswahl oder alle Server an, sofern die Gruppe **Alle Server** ausgewählt wurde. Um einzelne Server einer neuen Gruppe hinzuzufügen, markiert man die gewünschten Server aus der Serverliste und bestätigt die Schaltfläche **Server zu Gruppe hinzufügen**. In der nachfolgenden Übersicht werden alle verfügbaren Gruppen aufgelistet. Um einen Server einer bestimmten Gruppe hinzufügen wählt man die Schaltfläche **Hier hinzufügen** (rechts neben der gewünschten Gruppe).

Das Entfernen eines Servers aus einer Gruppe funktioniert analog dem Anlegen. Aus der Liste der Server werden der oder diejenigen Server markiert, welche zu entfernen sind und über den Menüpunkt **Server aus Gruppe entfernen** gelangt man an die Übersicht, in welchen Gruppen der/die Server Mitglied sind. Über die Schaltfläche rechts neben der jeweiligen Gruppe lassen sich der/die Server aus der Gruppe entfernen.

4.6 ZenTiV - Server auswählen

Einzelne Server oder Gruppen von Servern können über die Schaltfläche **Server** bearbeitet werden. Die Anzeige der Server in der Serverliste richtet sich nach der jeweils ausgewählten Gruppe. Wird die Gruppe **Alle Server** ausgewählt, so listet die Übersicht alle in ZenTiV verfügbaren Server auf. Andere Gruppen zeigen eine Teilauswahl der Server, je nach zugeordneten Gruppen. → Siehe 4.5 ZenTiV - Gruppen anlegen / löschen.

4.7 ZenTiV - Serverinformationen anzeigen

Die Serverliste zeigt verschiedenen Statusinformationen zum Update-Verhalten der in ZenTiV verfügbaren TightGate-Pro-Server an. Folgende Informationen sind verfügbar:

<table>
<tr><th>Spalte</th><th>Beschreibung</th></tr>
<tr><td>Servername</td><td>Name des Servers, wie als Administrator config angelegt. Durch Anklicken des Namens gelangt man in die NAGIOS-Übersicht für den Server.</td></tr>
<tr><td>Kommentar</td><td>Beschreibung des Servers, wie als Administrator config unter ZenTiV Kommentar angelegt. Ist der Kommentar länger als 25 Zeichen, so wird dieser verkürzt in der Anzeige dargestellt. Detaillierte Informationen zum Kommentar werden angezeigt, sobald sich der Mauszeiger über dem Eintrag befindet.</td></tr>
<tr><td>Updates verfügbar</td><td>Anzeige der Anzahl der verfügbaren Updates.</td></tr>
<tr><td>Download aktiviert</td><td>Anzeige, ob der automatische Download von Updates ein- oder ausgeschaltet ist.
Hinweis: Sofern ein anderer Zustand als die Aktivierung des Downloads von TightGate-Pro signalisiert wird, ist das Tabellenfeld rot hinterlegt.</td></tr>
<tr><td>Download-Intervall</td><td>Anzeige der/des auf dem jeweiligen TightGate-Pro-Server konfigurierten Download-Zeitintervalls. Detaillierte Informationen zum konfigurierten Download-Intervall werden angezeigt, sobald sich der Mauszeiger über dem Eintrag befindet.</td></tr>
<tr><td>Download-Status</td><td>Anzeige, in welchem Status sich der automatische Download von Updates auf TightGate-Pro befindet. Folgende Zustände kann der Download-Status haben:<table><tr><td>ok
pending
active
failed
stopped</td><td>Alle verfügbaren Updates sind vollständig heruntergeladen
Es gibt neue Updates, die noch nicht heruntergeladen wurden
Das System ist gerade dabei Updates herunterzuladen
Das Herunterladen der Updates ist fehlgeschlagen
Das Herunterladen ist planmäßig unterbrochen worden</td></tr></table></td></tr>
<tr><td>Auto-Update aktiviert</td><td>Anzeige, ob das automatische Update an- oder ausgeschaltet ist.
Hinweis: Sofern ein anderer Zustand als die Aktivierung des Auto-Updates von TightGate-Pro signalisiert wird, ist das Tabellenfeld rot hinterlegt.</td></tr>
<tr><td>Auto-Update Zeiten</td><td>Anzeige der auf dem jeweiligen TightGate-Pro-Server konfigurierten Update-</td></tr>
</table>

	Zeit. Ist das Update aktiviert, so startet TightGate-Pro mit der Installation der Updates zu dem konfigurierten Zeitpunkt. Detaillierte Informationen zum konfigurierten Auto-Update werden angezeigt, sobald sich der Mauszeiger über dem Eintrag befindet.
Zeitzone	Anzeige der Zeitzone, in der sich der TightGate-Pro-Server befindet.
Verfügbare Hotfixes	Anzeige verfügbarer/installierbarer Hotfixes für TightGate-Pro. **Hinweis:** Hotfixe können nur dann installiert werden, sofern alle regulären Updates bereits eingespielt wurden.
Aktualisierung	Anzeige, zu welchem Zeitpunkt die Serverinformationen zum letzten Mal aktualisiert wurden. Die Anzeige erfolgt in Lokalzeit von ZenTiV.

4.8 ZenTiV – TightGate-Pro administrieren

Folgende administrativen Aktionen stehen über die ZenTiV-Oberfläche zur Verfügung:

Aktion	Beschreibung
Informationen aktualisieren	Fordert für den/die markierten Server aktuelle Informationen über den Update-Zustand an. Damit wird eine Aktualisierung angestoßen, je nach Verbindungsgeschwindigkeit zum Server kann die Aktualisierung bis zu 10 Minuten dauern.
Server zu Gruppe hinzufügen	Fügt den/die markierten Server zu einer Gruppe hinzu.
Server aus Gruppe entfernen	Löscht den/die markierten Server aus einer Gruppe.

Folgende Aufträge können über die ZenTiV-Oberfläche ausgeführt werden:

Aktion	Beschreibung
Auto-Update ein/aus	Schaltet für den/die markierten Server das Auto-Update an bzw. aus. Je nach Verbindungsgeschwindigkeit zum Server kann die Ausführung des Auftrags bis zu 10 Minuten dauern. Der Zeitraum wann TightGate-Pro Updates durchführt soll, kann über die Aktion „Auto-Update-Zeiten einstellen“ konfiguriert werden.
Auto-Download ein/aus	Schaltet für den/die markierten Server den Auto-Download ein bzw. aus. Je nach Verbindungsgeschwindigkeit zum Server kann die Ausführung des Auftrags bis zu 10 Minuten dauern. Der Zeitraum, wann TightGate-Pro Updates herunterladen soll, kann über die Aktion „Download-Intervall einstellen“ konfiguriert werden.
Update sofort	Weist den/die markierten Server an, mit dem Update sofort zu beginnen. Je nach Verbindungsgeschwindigkeit zum Server kann die Ausführung des Auftrags bis zu 10 Minuten dauern.
Download sofort	Weist den/die markierten Server an, mit dem Download von Updates sofort zu beginnen. Je nach Verbindungsgeschwindigkeit zum Server kann die Ausführung des Auftrags bis zu 10 Minuten dauern.

Auto-Update-Zeiten einstellen	Weist den/die markierten Server an, zu den eingestellten Wochentagen zur eingestellten Uhrzeit mit der Installation von Updates zu beginnen. Je nach Verbindungsgeschwindigkeit zum Server kann die Ausführung des Auftrags bis zu 10 Minuten dauern.
Download-Intervall einstellen	Weist den/die markierten Server an, zu den eingestellten Wochentagen zur eingestellten Uhrzeit mit dem Herunterladen von Updates zu beginnen bzw. das Herunterladen abzubrechen. Je nach Verbindungsgeschwindigkeit zum Server kann die Ausführung des Auftrags bis zu 10 Minuten dauern.
Hotfixes installieren	Weist den/die markierten Server an, die ausgewählten Pakete zu den eingestellten „Auto-Download-Zeiten“ herunterzuladen und zu den eingestellten „Auto-Update-Zeiten“ zu installieren. Je nach Verbindungsgeschwindigkeit zum Server kann die Ausführung des Auftrags bis zu 10 Minuten dauern.

4.9 ZenTiV - Aufträge ansehen / löschen

Wurde über die Serverliste ein Auftrag für einen oder mehrere TightGate-Pro-Server erzeugt, so werden diese unter der Menüauswahl **Aufträge** angezeigt. Es werden nur die aktiven Aufträge angezeigt. Die neusten Aufträge befinden sich dabei oben.

Sofern die Aufträge noch nicht ausgeführt wurden (zum TightGate-Pro-Server übertragen wurden), können diese markiert und über **Administration > Ausgewählte Aufträge löschen** gelöscht werden.

Über den Link **„Gesendete Aufträge ein- und ausblenden“** können gesendete Aufträge für einen Zeitraum bis zu 7 Tagen eingeblendet werden. Die gesendeten Aufträge können nicht bearbeitet oder gelöscht werden.

Historische Aufträge ansehen

Aufträge die älter als sieben Tage alt sind, werden über die ZenTiV-Oberfläche nicht mehr angezeigt. Diese Aufträge sind aber noch bis zu 365 Tagen verfügbar und können als Archiv-Datei heruntergeladen und extern angesehen werden.

So geht’s:

1. Auswahl von **Aufträge**
2. Auswahl von **Administration > Alte Aufträge herunterladen**
3. Es wird eine Datei namens „**zentiv-jobs-archive.zip**“ zum Download angeboten
    - In dem Archiv befinden sich bis zu 12 nach Monaten geordnete CSV-Dateien mit den gesendeten ZenTiV-Aufträgen
    - Die einzelnen Dateien können mit einem Programm zur Tabellenkalkulation geöffnet werden. Dabei ist zu beachten, dass als Kodierung UTF-8 verwendet wurde und die Feldtrennung durch TAB erfolgt.

Hinweis:

Alle ZenTiV-Aufträge, die älter als 365 Tage sind, werden endgültig im TightGate-Monitoring gelöscht und können nicht mehr von Server heruntergeladen werden.