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.

Voraussetzungen zum Betrieb:

- Betriebsbereit konfigurierter E-Mail-Versand für E-Mail-Benachrichtigung
- Für SMS-Versand: Zugriff über Port 443 (TCP) zum SMS-Expert-Provider

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

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.

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.|| |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.

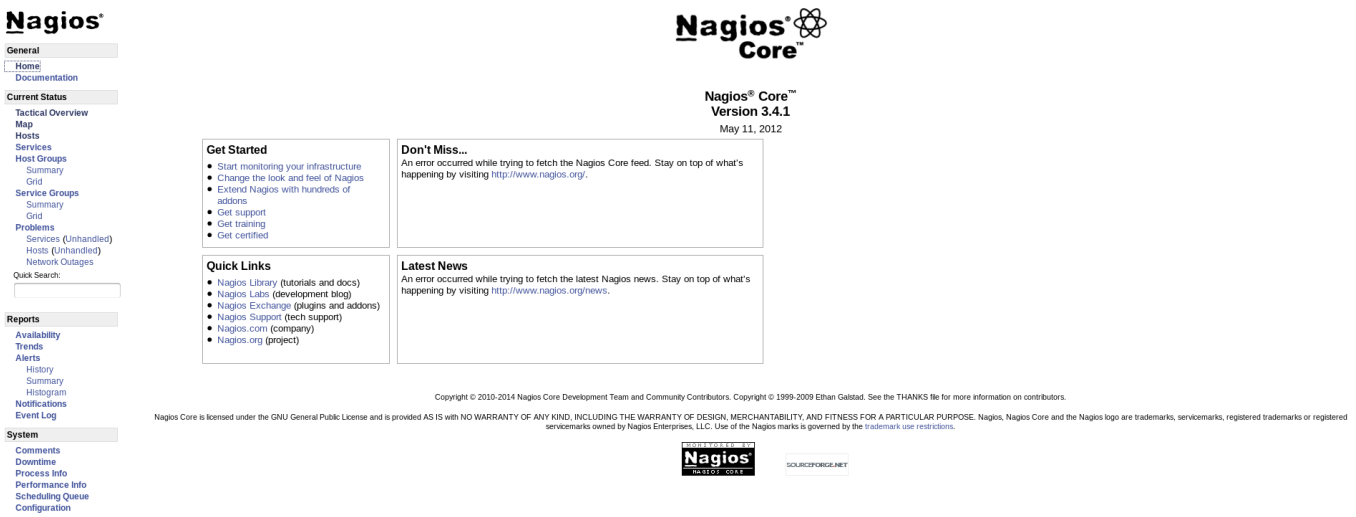
Ist ein Dienst über einen längeren Zeitraum nicht verfügbar, generiert das Nagios-System im Minutenabstand weitere Einträge in der Log-Datei. Dabei werden die Anzahl der Meldungen hochgezählt. Eine Alarmierung des hinterlegten Kontakts erfolgt nach dem 10. Eintrag derselben Abweichung.

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. 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.

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.

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.



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.

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

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

Last update: **2020/09/25 07:58**