



paedML[®] Plus-Paket

Fernüberwachung mit Nagios – Vorbemerkungen und
Voraussetzungen / Stand 8.12.2008



Baden-Württemberg
MINISTERIUM FÜR KULTUS, JUGEND UND SPORT



Impressum

Herausgeber

Landesmedienzentrum Baden-Württemberg (LMZ)
Support-Netz
Rotenbergstraße 111
70190 Stuttgart

Autoren

der Zentralen Expertengruppe Netze (ZEN)
Support-Netz, LMZ
Peter Klein

Endredaktion

Elke Albrecht

Weitere Informationen

www.support-netz.de
www.lmz-bw.de

Veröffentlicht: **2008**

© Landesmedienzentrum Baden-Württemberg

Inhaltsverzeichnis

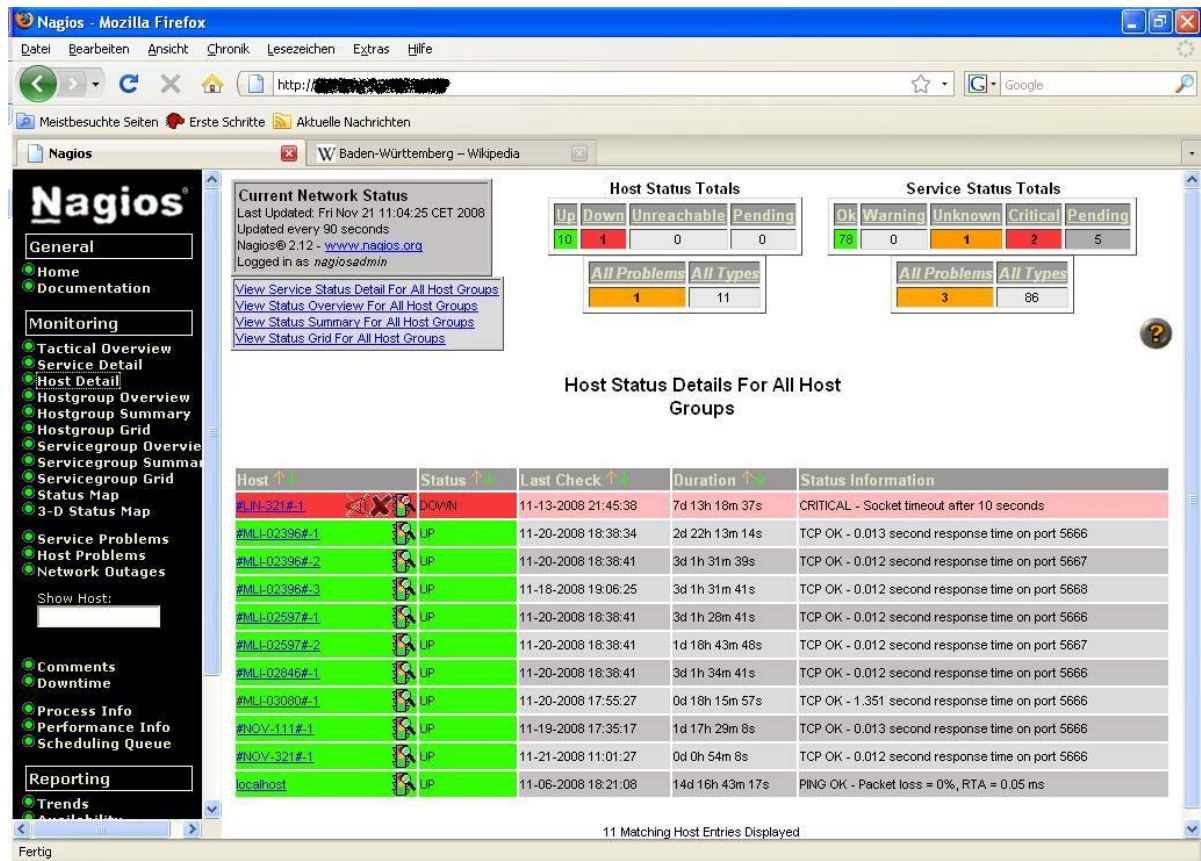
1.	Allgemeines zur Fernüberwachung	1
2.	Ziel der Fernüberwachung	2
3.	Systemvoraussetzungen zur Fernüberwachung	4
3.1.	Software-Voraussetzungen	4
3.2.	Internetanbindung	4
3.2.1.	Statische IP-Adresse	4
3.2.2.	Dynamische IP-Adresse	5
4.	Organisatorischer Ablauf der Fernüberwachung	6

1.

Allgemeines zur Fernüberwachung

Im Rahmen des paedML Plus-Paketes besteht die Möglichkeit, den Zustand Ihrer Musterlösungs-Installation durch das Support-Netz per automatisierter Fernüberwachung in regelmäßigen Zeitintervallen überprüfen zu lassen.

Das Support-Netz des Landesmedienzentrums Baden-Württemberg hat seit Oktober 2008 einen zentralen Nagios-Server in Karlsruhe im Testbetrieb, welcher das Herzstück der oben genannten Dienstleistung darstellt. Dieser Server ist seinerseits bei einem entsprechend spezialisierten IT-Dienstleister gehostet.



Weiterführende Informationen über die zu diesem Zwecke eingesetzte „Open Source“-Software Nagios finden Sie unter <http://de.wikipedia.org/wiki/Nagios> bei Wikipedia im Internet.

2. Ziel der Fernüberwachung

Ziel der Fernüberwachung ist es, den Zustand ausgewählter Dienste und Hardware-Ressourcen auf Ihren Servern zu überwachen, welche in der Gesamtheit die „Vitalität“ Ihrer Musterlösungs-Installation ausmachen. Einen Überblick bezüglich der überwachten Dienste und Ressourcen der paedML Windows gewährt Ihnen die nachstehend aufgeführte Tabelle:

Parameter	Typ
CPU-Auslastung in Prozent	Hardware-Ressource
Festplattenfüllstand in Prozent	Hardware-Ressource
Arbeitsspeicherbelegung über Swap / Auslagerungsdatei in Prozent	Hardware-Ressource
DHCP	Dienst
DNS	Dienst
Webserver (IIS)	Dienst
Mailserver SMTP (Exchange)	Dienst
Verzeichisdienst (Active Directory)	Dienst
Remoteinstallationsdienst (RIS/WDS)	Dienst
Firewall / Proxy (ISA)	Dienst

In der paedML Novell werden folgende Parameter überwacht:

Parameter	Typ
CPU-Auslastung in Prozent	Hardware-Ressource
Festplattenfüllstand in Prozent	Hardware-Ressource
Arbeitsspeicherbelegung über Swap / Auslagerungsdatei in Prozent	Hardware-Ressource
DHCP	Dienst
DNS	Dienst
Webserver (Apache)	Dienst
Verzeichnisdienst (eDirectory)	Dienst
Druckermanager für Netzwerkdrucker (iPrint)	Dienst
Treiberablage für Netzwerkdrucker (iPrint)	Dienst
Web-Proxy (Squid)	Dienst

Die paedML Linux wird auf nachfolgende Werte überprüft:

Parameter	Typ
Festplattenfüllstand in Prozent	Hardware-Ressource
Arbeitsspeicherbelegung über Swap / Auslagerungsdatei in Prozent	Hardware-Ressource
Prozessorauslastung (CPU) in Prozent	Hardware-Ressource
DHCP	Dienst
DNS	Dienst
Erreichbarkeit der Schulkonsole	Dienst
Verfügbarkeit der Imaging Dienste (Rembo/Linbo)	Dienst
Verzeichnisdienst (LDAP)	Dienst
Web-Proxy (Squid)	Dienst
Postgresql Benutzerdatenbank	Dienst

3. Systemvoraussetzungen zur Fernüberwachung

3.1. Software-Voraussetzungen

Die Plugins des auf Ihren Musterlösungs-Servern zu installierenden Nagios-Dienstes sind ausschließlich auf Basis der aktuellsten Versionen der jeweiligen paedMLs entwickelt und getestet worden. Von einer Installation des Dienstes sowie der zugehörigen Plugins auf älteren Musterlösungsversionen wird in diesem Zusammenhang explizit abgeraten. Zur Nutzung des Fernüberwachungs-Features muss zwingend auf die aktuelle Musterlösungsversion umgestellt werden.

3.2. Internetanbindung

Für die Durchführung der Fernüberwachung ist entscheidend, wie Ihre Schule an das Internet angebunden ist. Grundsätzlich wird die Fernüberwachung für die nachfolgend genannten Internet-Anbindungsarten unterstützt:

- 1) Permanente Internetanbindung über Statische IP-Adresse (z.B. durch Provider „BelWü“)
=> im Folgenden kurz „Statische IP-Adresse“ genannt.
- 2) Permanente Internetanbindung über Dynamische IP-Adresse (z.B. Telekom DSL-Flatrate)
=> im Folgenden kurz „Dynamische IP-Adresse“ genannt.

3.2.1. Statische IP-Adresse

Ist Ihr paedML-Server mit der externen Netzwerkkarte über eine statische IP-Adresse direkt an das Internet angebunden, so müssen Sie bei Ihrem ISP (Internet Service Provider) eingehende TCP-Verbindungen auf den nachfolgend genannten Ports für Ihre externe IP-Adresse (sogenannte „Public IP“) freischalten lassen:



Port 5666

(paedML Windows Zwei-Server-Lösung: Port 5666 und 5667,
paedML Windows Drei-Server-Lösung: Port 5666, Port 5667, Port 5668)

Dies ist erforderlich, da der Nagios-Server des Support-Netzes den auf Ihren Servern zu installierenden Nagios-Dienst genau über diese Schnittstellen abfragt. In der Regel kann dies per Email beantragt werden und dauert meist nicht länger als einen Werktag (z.B. bei BelWü).

3.2.2.

Dynamische IP-Adresse

Ist Ihr paedML-Server mit der externen Netzwerkkarte beispielsweise über eine Telekom-DSL-Flatrate an das Internet angebunden, so bekommt er in regelmäßigen Zeitabständen (spätestens über Nacht) zwangsweise dynamisch eine neue IP-Adresse von Ihrem Provider zugeteilt. Da Ihre Musterlösungsinstallation somit nicht konstant über eine gleichbleibende Adresse von außen angesprochen werden könnte, würde eine Fernüberwachung vom Nagios-Server des Support-Netzes aus nicht zuverlässig funktionieren, da dieser Server vom Wechsel Ihrer IP-Adresse nichts „mitbekommen“ würde.

Dieser Umstand lässt sich durch Registrierung eines Dynamischen DNS-Namen beheben (siehe nächster Abschnitt 3.2.2.1.).

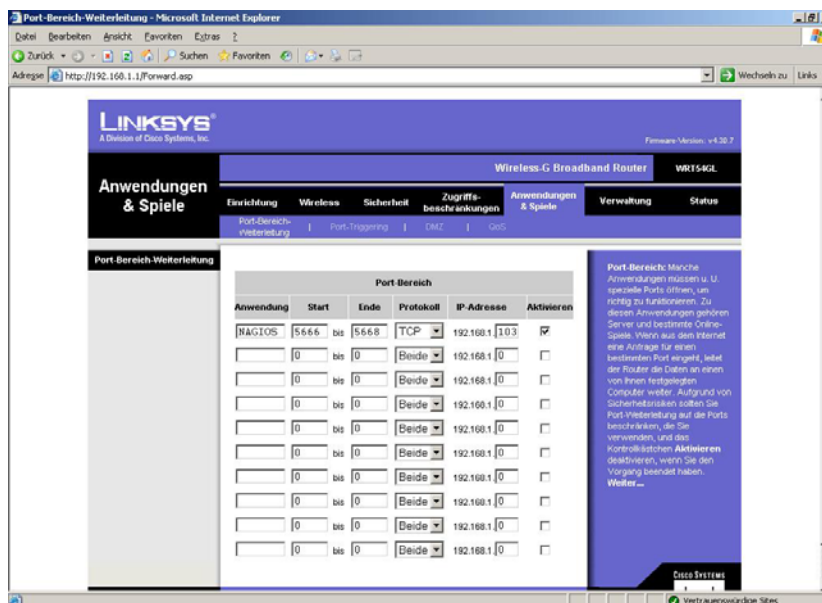
Da Ihr Server mit der externen Netzwerkkarte in der Regel über einen DSL-Router an das Internet angebunden ist, muss dieser Router so konfiguriert werden, dass er eingehende TCP-Verbindungen auf dem nachfolgend aufgeführten Port für Ihre externe IP-Adresse (sogenannte „Public IP“) zulässt:



Port 5666

(paedML Windows Zwei-Server-Lösung: Port 5666 und 5667,
paedML Windows Drei-Server-Lösung: Port 5666, Port 5667, Port 5668)

Die nachstehende Abbildung zeigt dies beispielhaft an einem handelsüblichen Linksys-Router:



The screenshot shows the 'Port-Bereich-Weiterleitung' (Port Range Forwarding) page in a Linksys router's web interface. The page is titled 'Wireless-G Broadband Router WRT54GL'. The main content area is a table for configuring port forwarding. The first row is pre-filled with the following data:

Anwendung	Start	Ende	Protokoll	IP-Adresse	Aktivieren
NAGIOS	5666	bis 5666	TCP	192.168.1.103	<input checked="" type="checkbox"/>
	0	bis 0	Beide	192.168.1.0	<input type="checkbox"/>
	0	bis 0	Beide	192.168.1.0	<input type="checkbox"/>
	0	bis 0	Beide	192.168.1.0	<input type="checkbox"/>
	0	bis 0	Beide	192.168.1.0	<input type="checkbox"/>
	0	bis 0	Beide	192.168.1.0	<input type="checkbox"/>
	0	bis 0	Beide	192.168.1.0	<input type="checkbox"/>
	0	bis 0	Beide	192.168.1.0	<input type="checkbox"/>
	0	bis 0	Beide	192.168.1.0	<input type="checkbox"/>
	0	bis 0	Beide	192.168.1.0	<input type="checkbox"/>

On the right side of the interface, there is a blue box with the following text:

Port-Bereich: Manche Anwendungen müssen u. U. spezielle Ports öffnen, um richtig zu funktionieren. Zu diesen Anwendungen gehören Server und bestimmte Online-Spiele. Wenn aus dem Internet diese Anträge für einen bestimmten Port eingeht, leitet der Router die Daten an einen von Ihnen festgelegten Computer weiter. Aufgrund von Sicherheitsrisiken sollten Sie Port-Weiterleitung auf die Ports beschränken, die Sie verwenden, und das Kontrollkästchen **Aktivieren** deaktivieren, wenn Sie den Vorgang beenden wollen.

3.2.2.1.

Allgemeines zu Dynamischem DNS

Über diese Technologie ist es möglich, einen Rechner trotz dynamisch wechselnder IP-Adressen über einen gleichbleibenden Klartextnamen über das Internet erreichbar zu halten. Streng technisch gesprochen handelt es sich hierbei um die Einrichtung einer DNS-Zone mit sehr kurzer TTL-(Time To Live) Zeit, weitere Infos hierzu finden Sie unter <http://de.wikipedia.org/wiki/DynDNS> bei Wikipedia.

Heutzutage gibt es einige Anbieter im Netz, bei denen man sich kostenlos einen dynamischen DNS-Namen für seinen Rechner reservieren lassen kann. Einer der bekanntesten Anbieter eines solchen Dienstes ist derzeit DynDNS.org. Hier kann man sich beispielsweise für seinen Server einen dynamischen DNS-Namen wie PaedML-INSTALLATIONSNUMMER.dyndns.org (z.B. MLI-12345.dyndns.org) einrichten (Zwecks einfacherer Zuordnung und Verwaltung wird die Verwendung der Namenssyntax MLI-12345.dyndns.org empfohlen. Bitte erfragen Sie Ihre paedML-Installationsnummer unter hotline@lmz-bw.de).

Damit die Maschine auch tatsächlich trotz IP-Wechsel über diesen Namen konstant erreichbar bleibt, muss die Zuordnung dieses DNS-Namens zu der aktuellen dynamischen IP-Adresse ständig aktuell gehalten werden. Um dies zu erreichen, muss auf dem betreffenden Server ein Update-Client (so genannter DynDNS-Client) installiert werden, der im Falle eines IP-Wechsels die aktuelle IP-Adresse an DynDNS.org übermittelt. Weitere Details zur Einrichtung eines dynamischen DNS-Namens am Beispiel DynDNS.org finden Sie in den spezifischen Installationsanleitungen zu Ihrer paedML-Plattform

4. Organisatorischer Ablauf der Fernüberwachung

Nach Eingang Ihres Antrages auf Inanspruchnahme des paedML Plus-Paketes wird im UHD-System¹ des Support-Netzes ein entsprechender Datensatz zu Ihrer Musterlösungs-Installation angelegt. Ist in diesem Antrag die Option Fernüberwachung angekreuzt, so legt der zuständige Hotline-Mitarbeiter zusätzlich auf dem Nagios-Server des Support-Netzes eine Referenz auf diesen Datensatz an.

Die Freischaltung Ihrer Musterlösungs-Installation zur Fernüberwachung kann nach Installation des jeweiligen Fernüberwachungspaketes für Ihre paedML-Plattform (Windows, Novell oder Linux) erfolgen. Die Installationspakete werden in Kürze im geschlossenen Bereich unseres Kundenportals veröffentlicht.

Nach Freischaltung Ihrer Musterlösungs-Installation zur Fernüberwachung durch die Hotline werden die in Kapitel 2 beschriebenen Hardware-Ressourcen und Dienste auf Ihrem Server (bzw. auf Ihren Servern) durch den zentralen Nagios-Server des Support-Netzes überwacht. In Zeitintervallen von 30 Minuten wird der Zustand dieser Hardware-Ressourcen und Dienste auf Ihren Maschinen vom Nagios-Server über das Internet abgefragt (Pulling-Verfahren). Stellt der Nagios-Server im Zuge einer Abfrage fest, dass sich eine Hardware-Ressource bzw. ein Dienst auf einer Ihrer Maschinen in einem kritischen Zustand befindet, so wird postwendend eine entsprechende Email-Nachricht an das UHD-System der Hotline versandt. Diese Email-Nachrichten werden auf Seiten der Hotline in regelmäßigen Zeitabständen kontrolliert und im Bedarfsfalle kontaktiert Sie der zuständige Mitarbeiter über die von Ihnen angegebenen Kontaktdaten, um die Störung zu beheben.

¹ „User Help Desk“-System der Support-Netz-Hotline