

paedML[®] Die Musterlösung für
schulische Computernetze

Linux **paedML[®] Linux 4.x für schulische Netzwerke**



**Installationsanleitung
zur Fernüberwachung (paedML[®] Plus-Paket)
in der paedML Linux 4.x**

Stand: 04.06.2009

Impressum

Herausgeber

Landesmedienzentrum Baden-Württemberg (LMZ)

Support-Netz

Rotenbergstr. 111

70190 Stuttgart

Autoren

der Zentralen Expertengruppe Netze (ZEN),

Support-Netz, LMZ

Frank Schiebel

Roland Walter

Endredaktion

Birgit Mikley

Weitere Informationen

www.support-netz.de

www.lmz-bw.de

Veröffentlicht: **2009**

© Landesmedienzentrum Baden-Württemberg

Inhaltsverzeichnis	3
1. Vorbemerkungen und Voraussetzungen	4
1.1. Allgemeines zur Fernüberwachung	4
1.2. Ziel der Fernüberwachung	4
1.3. Systemvoraussetzungen zur Fernüberwachung	5
1.3.1. Software-Voraussetzungen	5
1.3.2. Internetanbindung	5
1.3.2.1 Statische IP-Adresse	5
1.3.2.2. Dynamische IP-Adresse	6
2. Installation auf dem paedML-Server	8
3. Organisatorischer Ablauf der Fernüberwachung	9
4. Kundeninterface zur Fernüberwachung mit Nagios	10
Anhang	11

1. Vorbemerkungen und Voraussetzungen

1.1. Allgemeines zur Fernüberwachung

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

Das Support-Netz des Landesmedienzentrums Baden-Württemberg betreibt hierzu einen zentralen Nagios-Server, 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.

Ziel dieser Anleitung ist es, auf Ihrer paedML-Installation die nötigen technischen Voraussetzungen zur Inanspruchnahme dieser Dienstleistung zu schaffen. Diese Anleitung richtet sich an den für Ihre paedML-Installation zuständigen Netzwerkberater bzw. EDV-Fachbetrieb.

1.2. Ziel der Fernüberwachung

Ziel der Fernüberwachung ist es, den Zustand ausgewählter Dienste und Hardware-Ressourcen auf Ihrem System zu überwachen, welche in der Gesamtheit die „Vitalität“ Ihrer paedML-Installation ausmachen. Einen Überblick bezüglich der überwachten Dienste und Ressourcen erhalten Sie mit der nachstehend aufgeführten 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
Erreichbarkeit der Schulkonsole	Dienst
Verfügbarkeit der Imaging-Dienste (Linbo/Rembo)	Dienst
Verzeichnisdienst (LDAP)	Dienst
Postresql Benutzerdatenbank	Dienst

1.3.

Systemvoraussetzungen zur Fernüberwachung

Um Ihren Server von außen überwachen zu können, müssen die folgenden Voraussetzungen erfüllt sein:

- Anmeldung für das paedML Plus Leistungspaket
- paedML Linux ab Version 4.0.0
- Ihr Server muss dauerhaft mit dem Internet verbunden sein
- Der Zugriff auf den Server muss entweder über eine statische IP-Adresse oder einen DNS Eintrag bei einem DynDNS Provider möglich sein
- Alle Firewalls vor dem Server müssen derart konfiguriert sein, dass der TCP-Port 5666 vom Internet aus erreichbar ist
- Das Nagios-Paket muss installiert sein

1.3.1.

Software-Voraussetzungen

Die Plugins des auf Ihren paedML-Servern zu installierenden Nagios-Dienstes (siehe Abschnitt 2.2.1) sind ausschließlich auf Basis der paedML Linux 4.0.0 und der Nachfolgeversionen entwickelt und getestet worden.

Vom Versuch einer Installation des Dienstes sowie der zugehörigen Plugins auf älteren paedML-Versionen wird in diesem Zusammenhang explizit abgeraten, da dies nicht möglich ist. Zur Nutzung des Fernüberwachungs-Features muss zwingend auf die aktuelle paedML-Version umgestellt werden.

1.3.2.

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 „BeWü“)
=> 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.

1.3.2.1

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 für Ihre externe IP-Adresse (sogenannte „Public IP“) auf dem Port 5666 freischalten lassen:

Dies ist erforderlich, da der Nagios-Server des Support-Netzes den auf Ihren Servern zu installierenden Nagios-Dienst genau über diese Schnittstelle anspricht. In der Regel kann die Freischaltung per E-Mail beantragt werden und dauert meist nicht länger als einen Werktag (siehe Textvorlagen im Anhang).

Wenn Ihr System eine statische IP-Adresse hat, können Sie die nachfolgenden Abschnitte zum Thema Dynamische IP-Adresse und DynDNS überspringen und direkt mit dem Kapitel 2 fortfahren.

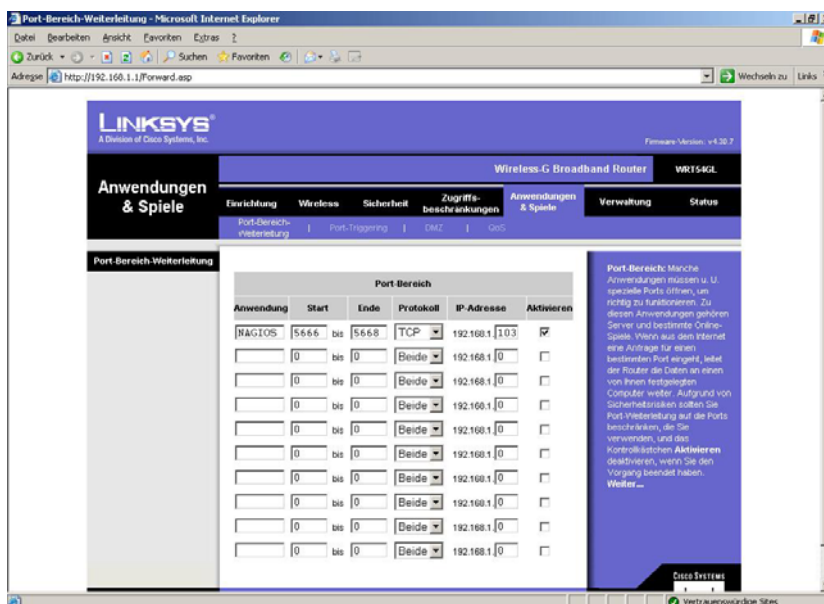
1.3.2.2.

Dynamische IP-Adresse

Ist Ihr paedML-Server beispielsweise über eine DSL Flatrate mit dem Internet verbunden (z.B. über T@School), so bekommt Ihr Netzwerk in regelmäßigen Zeitabständen (spätestens über Nacht) zwangsweise dynamisch eine neue IP-Adresse von Ihrem Provider zugeteilt. Da Ihre paedML-Installation somit nicht konstant über eine gleichbleibende Adresse von außen angesprochen werden kann, 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-Namens (DnYDNS-Alias) beheben. 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 Port 5666 für Ihre externe IP-Adresse (sogenannte „Public IP“) zulässt:

Die nachstehende Abbildung zeigt die Einrichtung des „port-forwarding“ (Portweiterleitung) beispielhaft an einem handelsüblichen Linksys-Router:



Außerdem ist in diesem Fall die Registrierung bei einem DynDNS-Dienst notwendig.

Mithilfe dynamischer DNS (DynDNS, vgl. <http://de.wikipedia.org/wiki/DynDNS>) können Sie Ihr System im Internet verfügbar machen, auch wenn dieses über keine statische öffentliche IP-Adresse verfügt.

Um DynDNS verwenden zu können, müssen Sie sich zunächst bei einem DynDNS-Anbieter für eine Unterdomäne registrieren. Anschließend muss der IPCop so konfiguriert werden, dass er jedes Mal, wenn eine Verbindung zum Internet hergestellt und ihm dabei von Ihrem Internetdienstanbieter eine neue IP-Adresse zugewiesen wird, dem DynDNS-Server diese IP-Adresse mitteilt. Der IPCop unterstützt die fortlaufende Aktualisierung Ihrer DynDNS-Adresse durch die automatische Aktualisierung bei zahlreichen DynDNS-Anbietern. Die Konfiguration wird im Menü *Dienste | Dynamischer DNS* auf dem IPCop vorgenommen:

Konfiguration

Dynamic DNS Anbieter werden eine IP-Adresse für diesen IPCop erhalten von:

- Die klassische ROTE IP, welche von IPCop während der Verbindung verwendet wird
- Schätze die echte öffentliche IP-Adresse mit Hilfe eines externen Servers **•**
- Updates minimieren: Vergleicht vor einem Update die DNS-IP-Adresse für Hostname "[host.]domain" gegen der ROTEN IP-Adresse.

• Benutzen Sie diese Option nicht mit Dial on Demand! Wird hauptsächlich verwendet, wenn ihr IPCop sich hinter einem Router befindet. Ihre ROTE IP muß sich innerhalb eines der drei reservierten Netzwerkbereiche befinden z.B. 10/8, 172.16/12, 192.168/16.

Host hinzufügen:

Dienst:	<input type="text" value="dyndns.org"/>	Hostname: •	<input type="text"/>
Hinter einem Proxy:	<input type="checkbox"/>	Domain:	<input type="text"/>
Wildcardcards erlauben:	<input type="checkbox"/>	Benutzername:	<input type="text"/>
Aktiviert:	<input checked="" type="checkbox"/>	Password:	<input type="text"/>
		Wiederholung:	<input type="text"/>

• Um no-ip im Gruppenmodus zu benutzen, dem Hostnamen **noipg-** hinzufügen

Wesentlich sind die Optionen

- *Klassische ROTE IP:* Verwenden Sie diese Option, wenn der IPCop selbst ein DSL Modem steuert – hierfür benötigen Sie einen dedizierten IPCop.
- *Schätze die echte öffentliche IP-Adresse:* Verwenden Sie diese Methode, wenn sich Ihr IPCop über einen vorgeschalteten Router ins Internet einwählt.

2.

Installation auf dem paedML-Server

Die erforderliche Software wird bei der Installation des Paketes „linuxmuster-nagios-fernueberwachung“ automatisch auf Ihrem paedML-Server installiert. Dazu führen Sie den Befehl

```
aptitude install linuxmuster-nagios-fernueberwachung
```

auf einer Kommandozeile des Server aus. Dabei werden an Ihrem System die folgenden Änderungen vorgenommen:

- Der Nagios-nrpe-Server wird als Dienst (Daemon) auf Ihrem Server installiert
- Die Datei `/etc/nagios/nrpe.cfg` wird derart verändert, dass die Datei `/etc/nagios/nrpe_lmz_fernwartung.cfg` in die Konfiguration des nrpe-Dienstes eingebunden wird.
- Auf dem IPCop wird der Zugriff von außen auf Port 5666 des Servers als Portweiterleitung eingetragen. Ändern Sie unter keinen Umständen Einstellungen für diese Portweiterleitung (Namen der Regel oder Port)!

Sollte bei der Installation des Paketes die Meldung „The authenticity of host ‚ipcop (10.16.1.254)‘ can’t be established. RSA key fingerprint is ... Are you sure, that you want to continue connection (yes/no)?“ erscheinen, so wurde bisher noch keine Verbindung zwischen Server und dem IPCop aufgebaut. Sie müssen die Meldung mit `yes` quittieren, damit die Installation durchgeführt werden kann.

Damit die Änderungen aktiv werden, müssen Sie nun den IPCop neu starten. Dies können Sie über das IPCop Webinterface machen. Rufen Sie hierfür in einem Browser `https://ipcop:445` auf. Über *System | Herunterfahren | Neustart* können Sie den IPCop neu starten.

Mit der Installation des Paketes ist serverseitig alles erledigt, möglicherweise müssen Sie – beispielsweise bei BelWue – bei Ihrem Provider noch den Zugriff von außen auf Port 5666 freischalten lassen, wie in den Voraussetzungen beschrieben (siehe oben).

3.

Organisatorischer Ablauf der Fernüberwachung

Nach Eingang des vollständig ausgefüllten paedML Anmeldeformulars - Ihr Antrag auf Inanspruchnahme des paedML Standard-Paketes oder, wie hier erforderlich, des paedML Plus-Paketes - wird im UHD-System¹ des Support-Netzes ein entsprechender Datensatz zu Ihrer paedML-Installation angelegt. Wenn Sie das paedML Plus-Paket gewählt haben, legt der zuständige Hotline-Mitarbeiter zusätzlich auf dem Nagios-Server des Support-Netzes eine Referenz auf diesen Datensatz an.

Nach Freischaltung Ihrer paedML-Installation zur Fernüberwachung durch die Hotline werden die unter 1.2. 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 E-Mail-Nachricht an das UHD-System der Hotline versandt. Diese E-Mail-Nachrichten werden auf Seiten der Hotline in regelmäßigen Zeitabständen kontrolliert. Im Bedarfsfalle kontaktiert Sie der zuständige Mitarbeiter über die von Ihnen angegebenen Kontaktdaten, um die Störung zu beheben.

Wichtiger Hinweis:

Bitte wenden Sie sich nach Schaffung der technischen Voraussetzungen zur Fernüberwachung auf Ihrer paedML-Installation (Installationsarbeiten Kapitel 2 dieser Anleitung) an die Hotline, so dass der jeweils zuständige Mitarbeiter Ihr System zur Überwachung auf dem Nagios-Server freischalten kann.

Bitte lassen Sie bei dieser Gelegenheit auch überprüfen, ob die Hotline über Ihre aktuellen Kontaktdaten verfügt, so dass durch die Fernüberwachung entdeckte Störungen im Bedarfsfalle zeitnah abgestellt werden können.

Wichtige Kontaktdaten in diesem Zusammenhang sind:

- Name des Netzwerkberaters
- Aktuelle Telefonnummer und E-Mail-Adresse des Netzwerkberaters

Ebenso sollten Sie bei Kontaktierung der Hotline zusätzlich die folgenden Daten bereithalten:

- Die externe (statische) IP-Adresse Ihrer paedML-Installation **oder** einen entsprechenden DynDNS-Namen (siehe Kapitel 1)
- Kennwort Benutzer Remote-Admin für Ihre paedML-Installation (siehe Anleitung Einrichtung Fernzugriff)

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

4.

Kundeninterface zur Fernüberwachung mit Nagios

Nach Freischaltung Ihres Systems zur Fernüberwachung durch die Hotline haben Sie auch die Möglichkeit den Zustand Ihres Servers selbst abzufragen.

Hierzu bekommen Sie einen entsprechenden Web-Link per E-Mail zugeschickt.

Auf dieser Website authentifizieren Sie sich mit Ihrem gewohnten Login für das LMZ-Kundenportal. Danach werden Sie automatisch auf die Übersicht zu den auf Ihrem System überwachten Diensten und Ressourcen geleitet.

Die folgende Abbildung veranschaulicht die Kundenübersicht für die auf einem Linux-System überwachten Ressourcen und Dienste:

Landesmedienzentrum Baden-Württemberg: Startseite - Mozilla Firefox

Landesmedienzentrum Baden-W... x

LMZ Landesmedienzentrum Baden-Württemberg
Wir bilden die Zukunft.

Nagios-Kundeninterface

paedML® Linux

Server: #MLI-XXXXX#-1

Status	Seit	letzter Check	Ausgabe des Checks
UP	27.04.09 11:30	27.04.09 14:30	TCP OK - 0.216 second response time on port 5666

Dienste auf diesem Server:

Dienstname	Status	seit	letzter Check	Ausgabe des Checks
DHCPD	OK	27.04.09 11:45	27.04.09 14:15	PROCS OK: 1 process with command name dhcpd3
DNS	OK	27.04.09 11:45	27.04.09 14:15	DNS OK: 0.003 seconds response time. www.support-netz.de returns 78.47.196.229
Festplatten	OK	27.04.09 11:45	27.04.09 14:15	DISK OK - free space: / 3977 MB (74% inode=99%); /lib/initr/w 1012 MB (100% inode=99%); /dev 9 MB (99% inode=99%); /dev/shm 1012 MB (100% inode=99%); /home 698120 MB (97% inode=99%); /var 117111 MB (82% inode=99%); /var/spool/cups 18162 MB (99% inode=99%); /tmp 1012 MB (99% inode=99%);
Imaging	OK	27.04.09 11:45	27.04.09 14:15	LINBO-Imaging OK (atftp:1Proc(s) rsync:2Proc(s))
LDAP	OK	27.04.09 11:45	27.04.09 14:15	LDAP OK - U,UU4 seconds response time
Postgres DB	OK	27.04.09 11:45	27.04.09 14:15	OK = Result returned 1 rows
Schulkonsole	OK	27.04.09 11:45	27.04.09 14:15	OK - HTTP/1.1 301 Moved Permanently - 0.028 second response time
Swap	OK	27.04.09 11:45	27.04.09 14:15	SWAP OK - 100% free (2047 MB out of 2047 MB)
System Load	OK	27.04.09 11:45	27.04.09 14:15	OK (v@0, C@0) : Average on last 60 minutes : CPU0 0.0% : CPU1 0.0% : CPU2 0.0% : CPU3 0.0%

Diese Ansicht aktualisiert sich in Ihrem Browser im Abstand von 5 Sekunden automatisch.

Anhang

Beispielantrag "Freischaltung Fernüberwachungsprotokolle und -ports beim Internetprovider"

Die nachstehend aufgeführte Textvorlage können Sie verwenden, um bei Ihrem Internet-Provider per Brief, Fax oder E-Mail die Freischaltung der für die Fernüberwachung benötigten Protokolle und Ports zu beantragen.

Ersetzen Sie einfach die Platzhalter im Text (x) durch Ihre individuellen Daten.

Betreff:

IP-Adresse xxx.xxx.xxx.xxx – Kundennummer xxxxxxxxxxxxxxxx

Freischaltung Protokolle und Ports zur Fernüberwachung

Sehr geehrte Damen und Herren,

wir sind über die von Ihnen bereitgestellte o.g. statische IP-Adresse an das Internet angebunden. Unser Server soll künftig über das Internet von unserem zuständigen Dienstleister fernüberwacht werden. Hierzu bitten wir Sie, eingehende TCP-Verbindungen auf Port 5666 für die o.g. IP-Adresse freizuschalten.

Bitte geben Sie uns umgehend Bescheid, sobald Sie die entsprechenden Änderungen an Ihrer Firewall durchgeführt haben.

Mit freundlichen Grüßen

Xxxx Xxxx