Open-Source-Logserver für Windows- und Cisco- Clients

Zentrale Kontrolle

Ein zentraler Linux-Logserver sichert die Protokolldateien der Windows-Server und einer Cisco-Firewall. Für den Admin gibt's übersichtliche Web-GUIs dazu. David Rupprechter

Auch wenn das Netzwerk sicher scheint, muss der Admin alle Möglichkeiten ausschöpfen, um beim Eindringen eines Angreifers die Spuren zurückverfolgen zu können. Ein zentraler Linux-Loghost ist da sinnvoll, Ressourcen-sparend und sicher. Die Logs sind sofort auf einem zweiten Server, ein Angreifer müsste beide Systeme hacken, um seine Spuren zu verwischen. Auch beim Fahnden nach harmloseren Beeinträchtigungen macht sich ein zentraler Loggingdienst gut.

Auf Linux-Maschinen ist das keine Hexerei, der moderne Protokolldienst Syslog-NG [1] bringt alles mit, was für einen zentralen Loghost notwendig ist. Spannend wird es, wenn der Server auch die Protokolle von anderen Betriebssystemen sichern soll, denn heterogene Landschaften mit Windows- und Linux-Maschinen sowie Appliances wie Ciscos Pix-Geräte sind der Normalfall im Unternehmen. In der Standardeinstellung protokolliert jedes System seine Fehler brav auf seine Art im lokalen Dateisystem.

Eine Suche in den Eventlogs – sei es zur Fehlerdiagnose oder nach einem Einbruch – gestaltet sich da schwierig. Allein das Prüfen und die Sicherung von Windows-Eventlogs stellt ein größeres Problem dar und gestaltet sich bei komplexen Netzwerk-Topologien aufwändig. Wer da nicht auf teure kommerzielle Softwarepakete zurückgreifen will, findet in der Open-Source-Welt Ressourcen-sparende Programme, die den kostenpflichtigen Lösungen in keiner Weise nachstehen.

Sicherheit und Komfort

Ein Linux-Logserver für Windows- und Cisco-Clients hat aber noch zwei weitere Vorteile: Der Admin legt einem potenziellen Eindringling eine weitere Schwelle in den Weg: Wenige Angreifer auf Windows-Netzwerke sind in der Lage, in einen Linux-Syslog-Server mit ausgefeilter IPtables-Firewall und einer minimalen Anzahl laufender Dienste einzudringen, um die eigenen Spuren zu verwischen. Kommt noch eine Firewall-Appliance hinzu, braucht er schon Know-how über drei verschiedene Architekturen.

Aber das wichtigste Argument für die meisten Admins ist der Komfort. Alle Logdateien an einem Platz zu archivieren und zu überblicken, am besten bequem und jederzeit erreichbar per Webfrontend, vereinfacht und beschleunigt die Suche und Kontrolle der Systeme enorm.

Modernes Syslog-NG

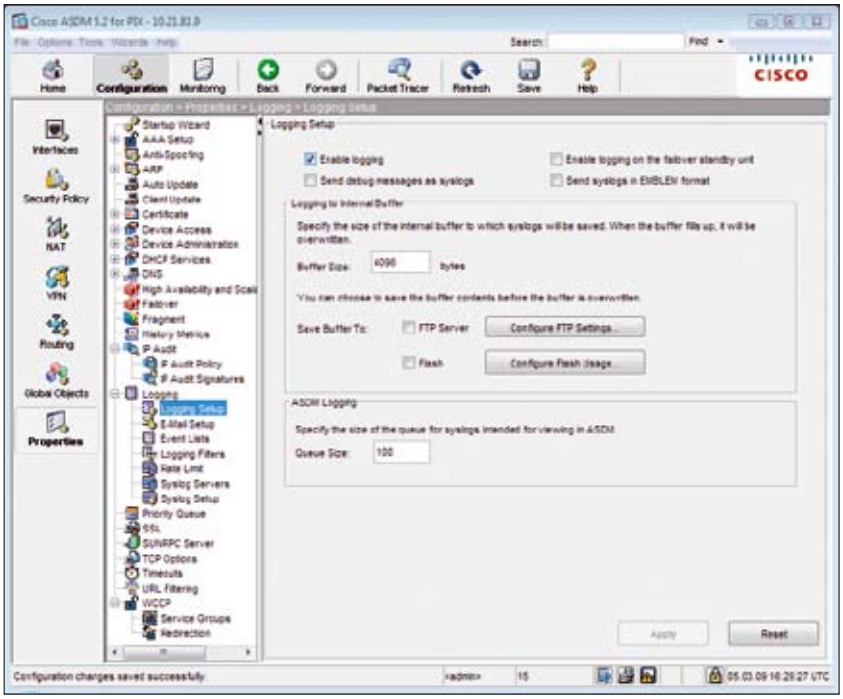
Der Standard-Protokolldienst aller neueren Linux-Systeme ist die zentrale Schnittstelle für eingehende Logs. In der Defaultkonfiguration überwacht er aber nur den lokalen Rechner. Damit er auch die Logs anderer Hosts annimmt, sind nur wenige Änderungen nötig. Mehr Details zu Syslog-NG, seinen Vorgängern und der kommerziellen Version von Balabit namens Premium Edition finden sich unter [2]. Im vorliegenden Beispiel braucht der Admin dem Dienst nur in der Konfiguration mitzuteilen, von wem er Protokolldaten annehmen soll. Das geschieht im Bereich »sources« der Konfigurationsdatei. Unter »sources_all« fügt er innerhalb der Klammern seine IP-Adresse(n), Protokoll und Port hinzu:

```
# Remote-Logs empfangen
Udp(port(514));
Tcp(ip("192.168.0.1") keep-alive(yes));
```

So verwendet Syslog-NG den Standardport 514 zum Empfang der Logs. Damit es den DNS-Namen beim Loggen heranzieht, sollte unter »options« der Eintrag »keep_hostname(yes);« stehen.

Zu guter Letzt bestimmt der Admin die Orte für die Logdateien, indem er die Zeilen aus Listing 1 am Ende der Datei »syslog-ng.conf« hinzufügt. Wie in Zeile

▲ **Abbildung 1: Das GPL-Tool Snare bringt Windows-Systeme dazu, einem Linux-Loghost über die eigenen Fehler und Warnungen Auskunft zu geben. Das Werkzeug verlangt aber nach der vollen Kontrolle über die Windows-Eventlogs.**



▶ **Abbildung 2: Das Administrations-GUI der Cisco-Pix-Geräte ASDM ist zwar nicht in allen Varianten enthalten, bietet aber alle Möglichkeiten, Logs auf einen Linux-Logserver zu exportieren.**

7 zu erkennen ist, legen Variablen wie »$YEAR« oder »$MONTH« den Speicherort beliebig fest. Hier ist es jedem Admin überlassen, eine für seine Netzwerktopologie passende Verzeichnisstruktur zu entwickeln. Noch ein Restart des Syslog-Daemon mit »/etc/init.d/syslog-ng restart«, und schon läuft der Server und wartet auf eingehende Logdaten.

Die Windows-Rechner passend konfigurieren

Damit die Windows-Maschinen ihre Eventlogs an den Server weiterleiten, braucht Windows Extrasoftware, zum Beispiel das GPL-Programm Snare [3]. Dessen Installation verläuft problemlos, der Admin braucht nur zwei Entscheidungen zu treffen (Abbildung 1). Auf die Frage »Do you want SNARE to take over control of your Eventlog Configuration?« antwortet er mit einem beherzten »Yes«, gleich danach wählte er bei »Would you like to password protect access to the interface?« den Eintrag »Yes – with NO password, local access only«.

Lokaler Zugriff reicht hier aus, da Snare die Logs ja ohnehin an den Syslog-Server senden soll. Mit »Start | Programme | InterSect Alliance | Snare for Windows« startet das Tool, und der Benutzer gelangt direkt in dessen Web-GUI, dem Snare Remote Admin Interface. Hier wählt er noch die Einstellungen, die Tabelle 1 erläutert. Anschließend übernimmt er die neuen Einstellungen mit »Change Configuration« und aktiviert sie mit »Apply the Latest Audit Configuration«.

Alle neuen Eventlogs sendet Snare ab sofort auch an den Syslog-Server. Je nach dessen Konfiguration landen die Logs jetzt auf dem Linux-Server unter »/var/log/hosts/*Jahr-Monat*/*Hostname*/«.

Tabelle 1: Snare-Konfiguration

Feld	Erklärung
Destination Snare Server address	Die IP-Adresse des Syslog-Servers angeben
Destination Port	Den Zielport von 6161 auf 514 (Syslog) ändern
SYSLOG Facility	Syslog
SYSLOG Priority	Detailtiefe (»Notice«, »Alert«, »Critical«, »?«) auswählen
Enable SYSLOG Header	Aktivieren

Eine Pix-Firewall einrichten

Eine Cisco-Firewall vom Typ Pix lässt sich am intuitivsten über die grafische Benutzeroberfläche Adaptive Security Device Manager (ASDM, [4]) administrieren, allerdings verfügen nicht alle Modelle über dieses GUI. In ASDM finden sich die Einstellungen für die Zusammenarbeit mit einem Syslog-Server unter »Configuration | Properties«, vor allem unter »Logging« und seinen Unterpunkten (siehe Abbildung 2).

Im Bereich »Logging Setup« aktiviert der Admin das Optionsfeld »Enable logging«, damit die kleine Appliance überhaupt

Listing 1: Syslog-NG-Konfiguration

```
01 # Filter/Destination für PIX-Firewall
02 filter f_pix {
03         host(pix);
04 };
05 # Zielort der Log-Dateien
06 destination loghost {
07         file ("/var/log/hosts/$YEAR-$MONTH/$HOST
   /$FACILITY-$YEAR-$MONTH-$DAY"
08                 owner(root) group(root) perm(0600)
   dir_perm(0700) create_dirs(yes)
09         );
10 };
11 log {
12         source(s_all);
13         destination(loghost);
14 };
15 # Pix
16 log {
17         source(s_all);
18         filter(f_pix);
19         destination(loghost);
20         flags(final);
21 };
```

Protokoll führt. Im Unterpunkt »Logging Filters« definiert er passende Filter, indem er die Logging-Destination »Syslog Servers« auswählt und per »Edit« editiert. Wichtig ist hier nur, einen »Filter on severity« zu setzen. »Debugging« gibt am meisten Information an den Syslog-Server weiter, eignet sich dadurch aber nur bedingt für den Dauerbetrieb. Die Einstellung »Alerts« gibt nur Alarmierungen an den Loghost weiter.

Im letzten Schritt muss die Pix noch erfahren, welchen Loghost sie beglücken soll. Dies geschieht mit einem einfachen Klick unter »Syslog Servers« auf die Schaltfläche »Add«. Hier trägt der Admin das passende »Interface« ein, in Ciscos Namenswelt zum Beispiel »inside«, »outside« oder »dmz«. IP-Adresse des Loghost, der Port 514 und UDP als Protokoll komplettieren die Änderungen. Ab sofort sendet die Firewall-Appliance ihre Logs parallel an den Syslog-Server.

Admins, die Modelle ohne ASDM besitzen oder lieber die eingebaute Shell des Geräts nutzen, können diesen Vorgang auch per Terminal ausführen. In der Regel geschieht dies über unsichere Telnet-Tools, doch ist dies die schnellere und flexibelste Art, eine Pix zu steuern. Für die Logging-Funktionen braucht es beispielsweise nur wenige Befehle:

```
logging enable
logging trap alerts
logging host inside 10.21.81.8
```

Die erste Zeile aktiviert das Logging, hinter »logging trap« steht der Informationsgrad und die dritte Zeile definiert die IP des Loghost und das passende Interface. Speichern lassen sich die Einstellungen mit »write memory« und »reload«. Jetzt ist ein guter Zeitpunkt, um den Erfolg der Aktionen auf dem Linux-Server zu begutachten. Unter »/var/log/hosts/...« treffen sicherlich schon Nachrichten ein.

Listing 2: Logs an MySQL übergeben

```
01 # Created by Tadghe Patrick Danu
02 #
03 #!/bin/bash
04 If [ -e /var/log/sql.pipe ]; then
05 while [ -e /var/log/sql.pipe ]
06 do
07 mysql -u root -password=PASSWORT syslog < /var/log/
   sql.pipe
08 done
09 else
10 mkfifo /var/log/sql.pipe
11 fi
```

Ein Webinterface oder in eine Datenbank loggen

Wer eine größere Serverlandschaft verwalten muss, stellt bald fest, dass sich die Ablage der Logfiles in den Unterverzeichnissen (trotz fehlender Log-Rotation bei Syslog-NG) zwar gut für die Archivierung eignet, vermisst aber Übersichtlichkeit bei der Suche nach Einträgen.

Um den Komfort zu erhöhen, empfiehlt es sich, die Logfiles in eine MySQL-Datenbank zu leiten und ein passendes Webinterface für den Syslog-Daemon zu installieren. Die beiden Programme PHP Logcon [5] und PHP-Syslog-NG [6] sind gut dokumentiert und besitzen nützliche Funktionen. Als netter Nebeneffekt beschleunigt die Datenbank dahinter auch alle Abfragen, vor allem im Vergleich zur Suche in lokalen Logdateien.

In der Syslog-Konfiguration definiert dieser Bereich, dass Syslog-NG seine Logs in die Tabelle »logs« schreibt:

```
destination dot_mysql {
pipe("/var/log/sql.pipe"
template("INSERT INTO logs (host, facility,➥
 priority, level, tag, date, time, program,➥
 msg)
VALUES ('$HOST', '$FACILITY', '$PRIORITY',➥
 '$LEVEL', '$TAG', '$YEAR-$MONTH-$DAY',➥
 '$HOUR:$MIN:$SEC','$PROGRAM','$MSG');\n")➥
 template-escape(yes));
```

Anschließend muss der Admin den Logbereich anpassen, damit der Syslog-Dienst in eine MySQL-Pipe schreibt:

```
log {
      source(s_all);
      destination(dot_mysql);
};
```

Syslog-Ng neu starten, und schon landen die Logs in »/var/log/sql.pipe«. Ein Transfer in die SQL-Datenbank erfolgt jedoch noch nicht. Das erledigt ein Bash-Skript von der Webseite von PHP-Syslog-NG [6], wo sich auch Konfigurationen für Oracle-, PostgreSQL oder andere Datenbanken finden. An die vorhandene Syslog-Konfiguration angepasst, gestaltet sich das Skript wie Listing 2.

Mit dieser Konfiguration schreibt Syslog-NG die Logs in die Datenbank »syslog«, Tabelle »logs«. Vor dem ersten Aufruf sollte der Admin die Datei »sql.pipe« mit »mkfifo /var/log/sql.pipe« erstellen. Um Lücken beim Logging zu vermeiden, empfiehlt es sich, nach einem Funktionstest das Skript in »/etc/init.d/mysqlpipe.sh« abzulegen und mittels »update-rc.d mysqlpipe.sh defaults« beim Start automatisch ausführen zu lassen.

Puristisch und übersichtlich: PHP-Syslog-NG

Das Webinterface von PHP-Syslog-NG bedient sich der SQL-Datenbank und kann Logdateien nicht direkt auslesen.

Abbildung 3: Die Meldungen der Pix-Firewall sind auf dem Linux-Server angekommen. Der Syslog-NG-Dienst hat sie in eine MySQL-Datenbank geschickt, wo PHP-Syslog-NG eine einfache, aber flotte Oberfläche mit Suchfunktionen bietet.

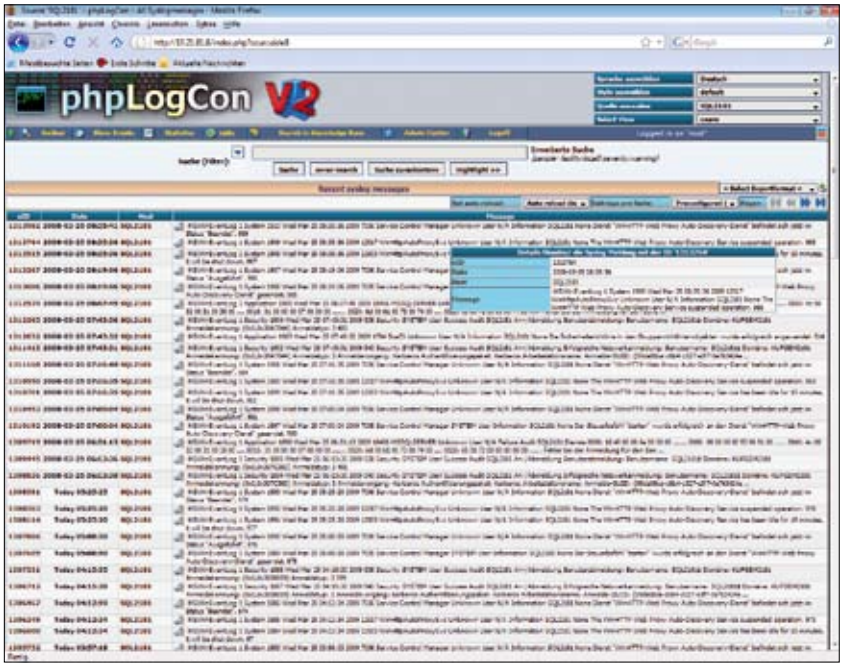


Abbildung 4: PHP Logcon unterstützt Datenbanken, kann aber auch direkt die Logfiles auslesen. Fehlermeldungen aller lokalen Windows- und Linux-Systeme sowie angeschlossener Cisco-Firewalls lassen sich damit in einer gefälligen, flotten Oberfläche überblicken.

Eine Installationsroutine gibt es nicht, die benötigten MySQL-Tabellen richtet der Admin manuell in der Konsole oder mittels PHP MyAdmin ein. In der Datei »db_fns.php« landen die Zugangsdaten der jeweiligen SQL-Datenbank, detailliertere Informationen stehen auf der Webseite des Projekts [6].

Das Webinterface PHP-Syslog-NG beschränkt sich auf das Nötigste und ist eng mit der SQL-Datenbank verknüpft, was sich schon in den Auswahlmöglichkeiten der diversen Filter wie Datum, Zeit oder Meldungstyp zeigt. Die Suchergebnisse sind übersichtlich dargestellt, der Meldungstyp wird durch unterschiedliche Farben gekennzeichnet. Leider fehlen erweiterte Einstellungsmöglichkeiten und Feinheiten wie das farbliche Darstellen von URLs (Abbildung 3).

Wer keinen SQL-Dienst am Loghost betreiben will und genügend Geduld mitbringt, für den stellt PHP Logcon eine Alternative dar. Es kann auch direkt die Logdateien auslesen, was aber vor allem im Vergleich zum Abfragen einer Datenbank deutlich länger dauert.

Flexibel: PHP Logcon

Nach dem Upload der Installationsdateien ins Webserver-Verzeichnis startet der Admin die Installationsskripte »configure.sh« und »secure.sh«. Der Rest der Installation erfolgt bequem über ein Webinterface, wobei in manchen Fällen noch das Anpasssen einiger Dateirechte nötig ist. Das Installationsinterface gibt dazu detailliertes Feedback. Die zu verwendenden Datenbanken oder Logdateien lassen sich anschließend über den Menüpunkt »Sources« hinzufügen.

Im Vergleich zum PHP-Syslog-NG wirkt PHP Logcon nicht so minimalistisch. Fährt der Benutzer mit der Maus über eine Zeile, dann zeigt ihm das Tool den jeweiligen Logeintrag in einem kleineren Fenster an (Abbildung 4). Diverse Farben heben weiterführende Informationen wie URLs hervor. Derartige Kleinigkeiten fehlen der Konkurrenz und erleichtern dem Admin die Arbeit ungemein.

Die Ansichten von PHP Logcon lassen sich flexibel gestalten. Wer seine Logfiles gerne etwas strukturierter betrachten möchte, als dies in der Standardansicht der Fall ist, der fügt im Admin Center unter »Views« eine neue Ansicht hinzu (Abbildung 5) und stellt die neue Ansicht im Modul »Sources« als Standard ein.

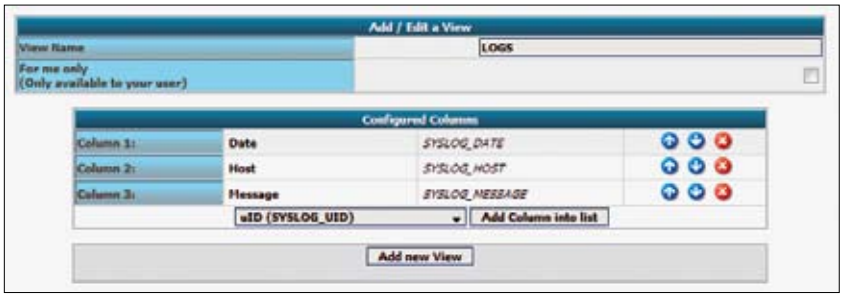


Abbildung 5: Damit PHP Logcon die Spalten so übersichtlich darstellt wie in Abbildung 4, ist allerdings eine neue Standardview im Admin Center erforderlich.

Gratis, aber nicht umsonst

Mit Linux, MySQL und anderer freier Software lässt sich ein zentralisierter Logserver einrichten, der kaum Rechenleistung benötigt. Admins stellen so die Integrität von Logs sicher und durchstöbern die Fehlermeldungen bequem vom Browser aus. Das Archivieren alter Logs übernimmt zum Beispiel ein einfacher Export aus PHP MyAdmin. *(mfe/jk)* ■

Infos

[1] Syslog-NG: [http://www.balabit.com/network-security/syslog-ng]
[2] Ralf Spenneberg, „Protokollfrage – Die kommerzielle Premium Edition von Syslog-NG im Test“: Linux-Magazin 10/07, S. 88
[3] Snare-Logging-Client für Windows: [http://www.intersectalliance.com/projects/BackLogNT/index.html]
[4] Cisco Adaptive Security Device Manager: [http://www.cisco.com/en/US/products/ps6121/index.html]
[5] PHP Logcon: [http://www.phplogcon.org]
[6] PHP-Sylog-NG: [http://vermeer.org/docs/1]

Der Autor

David Rupprechter ist Systemadministrator bei einem Großhändler für Laptoptaschen und Computerzubehör und befasst sich mit Netzwerktechnik, Programmierung und Linux. [http://www.dotlike.net]