

Konsolenserver von Opendgear

Down under

Dirk Wetter

Unter der Reihe der Konsolenserver fällt die Lösung von Opendgear aus Australien durch zwei Punkte trotz ihres unscheinbaren Äußeren auf: durch den Preis und den Umgang mit Open Source.



Konsolenserver unterscheiden sich von außen betrachtet nur geringfügig: Eine Serie von RJ45-Ports dient zum seriellen Anschluss der Knoten, ein bis zwei zur Anbindung ans Ethernet, in der Regel über ein separates Verwaltungsnetz, sowie ein eigener serieller Konsolenanschluss. *iX* hatte in der 8/05 [1] Geräte von sieben Herstellern vorgestellt. Im Test fiel auf, dass einige Hersteller hemmungslos Open-Source-Software verwenden, ohne sich um die GPL zu scheren. Zum anderen hatten einige der Produkte erhebliche Sicherheitsmängel.

Quasi als Nachzügler zum Test kam der CM4148 von Opendgear aus Toowong (bei Brisbane, Australien) ins Haus. Neben der gedruckten Quickstart-Anleitung war eine CD-ROM im Paket, die nicht nur das Handbuch als PDF enthält, sondern auch als Live-CD-ROM mit Installationsmöglichkeit dient.

Beim CM4148 ist eine IP-Adresse vorkonfiguriert, was hinderlich sein kann, wenn die bereits vergeben wurde; da wäre ein Hinweis im Quick-Start auf den gleichzeitig lauschenden DHCP-Klienten hilfreich gewesen. Zwar sind alle 48 Ports ab Werk vor dem Zugriff aus dem Netz geschützt, aber die Admin-Zugänge Telnet- und

HTTP sind offen, trotz aktiviertem SSH- und HTTPS-Zugang.

Bei der groben Grundkonfiguration nimmt ein Vier-Punkte-Menü im Webbrowser den Admin an die Hand: hier kann er das Werkspasswort, die IP-Konfiguration sowie die der seriellen Ports ändern und die Benutzerzugriffe auf die Ports regeln. Alternativ lässt sich der Konsolenserver mit dem Werkzeug `config -set=` nebst Parametern auf der Linux-Kommandozeile administrieren.

Ohne die nachgeordneten zusätzlichen Adapter fanden die DB25- und RJ45-Buchsen der Testumgebung (Sparc-Hardware und ein Cisco-Switch) keinen Anschluss. Die Adapter sind extra zu bestellen oder gemäß der Pinbelegung im Handbuch selbst anzufertigen. Nur für den Server-PC war ein DB9-Adapter dabei. Fehlbelegungen kommt man mit dem Webbrowser oder über das Kommando `pmsell -signals` auf die Schliche, die über den Status von CTS, RTS, DCD, DSR und DTR informieren.

Im Labor musste, wie im Rechenzentrum angeraten, der CM4148 per Syslog alle Meldungen an einen zentralen Log-Server weiterleiten. Wenn konfiguriert, liefert der CM sogar die Statusänderun-

gen der seriellen Leitungen. Vorsicht sollte der Admin aber walten lassen: Auf dem höchsten Log-Level erscheinen alle über den seriellen Draht gesendete Daten inklusive der Passwörter einzelner Knoten; wenn der Admin es partout befiehlt, sogar auf dem konfigurierten Syslog-, NFS- oder CIFS-Server.

Opendgears Konsolenserver kann zwar auf Zeichenketten im Portpuffer hin per E-Mail einen Alarm auslösen, aber bis dato keine SNMP-Traps verschicken. In der Beta-Firmware 2.10 (im Live-Demo-Test getestet) lässt sich der SNMP-Agent per Web-Oberfläche konfigurieren.

Zugriff von außen fest geregelt

Beim NTP leistete sich der CM4148 einen kleinen Patzer, verursacht durch die schwache Batterie der Hardwareuhr: Beim Start der Appliance stellt der `ntpd` die Systemzeit nicht sofort, sondern ließ sie in Richtung reale Zeit driften. Ein Neustart des NTP-Dämons sorgte für Abhilfe.

Den Sun-Break-Test bestand der CM4148 – es geht darum zu verhindern, dass bestimmte Sparcs (wie SGIs) auf den Stromausfall eines Konsolenservers hin in den „OK“-Prompt gehen. Den im Labor angelegten lokalen Testbenutzern – die angebotenen externen Authentifizierungen RADIUS, TACACS+, LDAP blieben außen vor – erlaubt er nur den Zugriff auf die zugewiesenen Ports, egal, ob er es via SSH (Public Key/Passwort) oder Telnet versucht. Die Web-Oberfläche dient nur zur Administration.

Neu ist das Secure Desktop Tunneling (SDT), das zunächst ein wenig an KVM-over-IP erinnert: Ein RDP- oder VNC-Client tunnelt sein Desktop-Protokoll durch eine SSH-Verbindung zum Konsolenserver, der es über PPP an seinen seriell angeschlossenen Kno-

Daten und Preise

Konsolenserver: CM4148**Hardware:** 166MHz ARM922T-CPU (System on a Chip Centaur), KS8695P von Micrel, inkl. 5-Port-Ethernetswitch, PCI-Bridge, UART, MMU), keine Lüfter; Firmware 2.0.9**Hersteller:** Opendgear (www.opengear.com)**Vertrieb:** Sphinxcomputer (www.sphinxcomputer.de/opengear.de)**Preis:** CM4148 (Teststellung) 1295 Euro

-Wertung

- ⊕ Preis/Leistungsverhältnis
- ⊕ sicheres Desktop-Tunneling
- ⊖ Default-Klartextprotokolle

ten weiterleitet. SDT ist keine Out-Of-Band-Anwendung, da dafür auf Knotenseite ein laufendes Betriebssystem mit einer PPP-Schnittstelle nötig ist. Opengear bewirbt es als sicheren Fernzugriff auf Windows-PCs, obwohl die Technik nicht wirklich neu ist. Ähnliches hat kürzlich Digi implementiert.

Es wäre für Performance-Untersuchungen sicherlich spannend gewesen, SDT im Labor zu erproben. Aus Zeitgründen fand stattdessen eine Live-Demo statt, in der sich die WAN-Verbindung zu einem Open-gear mit angeschlossenem Windows-2000-Knoten in Ostaustralien erproben ließ, was mit der richtigen Komprimierung im Linux-VNC-Viewer ohne allzu große Verzögerungen über die Bühne ging.

Im Handbuch steht GPL-konform erklärt und verlinkt, was Opengear für seinen Konsolenserver aus der Open Source verwendet hat: Als Embedded-Linux-BIOS kommt „uboot“ zum Einsatz (u-boot.sf.net), als Kernel dient „uClinux“, das aus dem Embedded Linux Kernel Mikrocontroller Project (www.uclinux.org) stammt. Den Werkzeugsatz stellen die Multi-Binaries aus der „Busybox“ (www.busybox.net) auf Benutzerebene zur Verfügung. Ergänzungen wie die Open Source-Konsolen- und KVM-Managementsoftware *okvm* sind bei Sourceforge (okvm.sf.net) untergebracht. Laut Handbuch sollen die Quellen proprietären Codes (wie die Programme des Webservers und Konfigurationswerkzeuge) für Kunden unter NDA erhältlich sein.

Fazit

Legt man die Maßstäbe aus dem Vergleichstest [1] an, braucht sich Opengear wegen seiner Technik, seines niedrigen Preises und seines jun-

gen Alters von weniger als einem Jahr nicht zu verstecken. Es fehlen ein paar Optionen wie SNMP-Traps, Kerberos-Authentifizierung und PCMCIA-Slots, wie sie Server anderer Anbieter haben – bei denen der Griff in die Tasche aber etwa dreimal tiefer ausfallen kann. Abgesehen von den monierten Punkten bietet der CM4148 ein gutes Preis-/Leistungsverhältnis. Erhältlich sind bis dato nur 8-, 16- und 48-Port-Varianten ohne Redundanz. Ein CM4248 mit 48 Ports, zwei Netzteilen und redundanten Ethernet-Schnittstellen sowie einem USB-Port soll Herstellerangaben zufolge in etwa acht Wochen vom Stapel laufen. (rh)

DR. DIRK WETTER

ist selbstständiger Berater im Bereich IT-Sicherheit und Open Source.

Literatur

- [1] Dirk Wetter; Systemverwaltung; Außer Rand und Band; Gesicherte Fernsteuerung serieller Zugänge per Konsolenserver; iX 8/2005, S. 99 