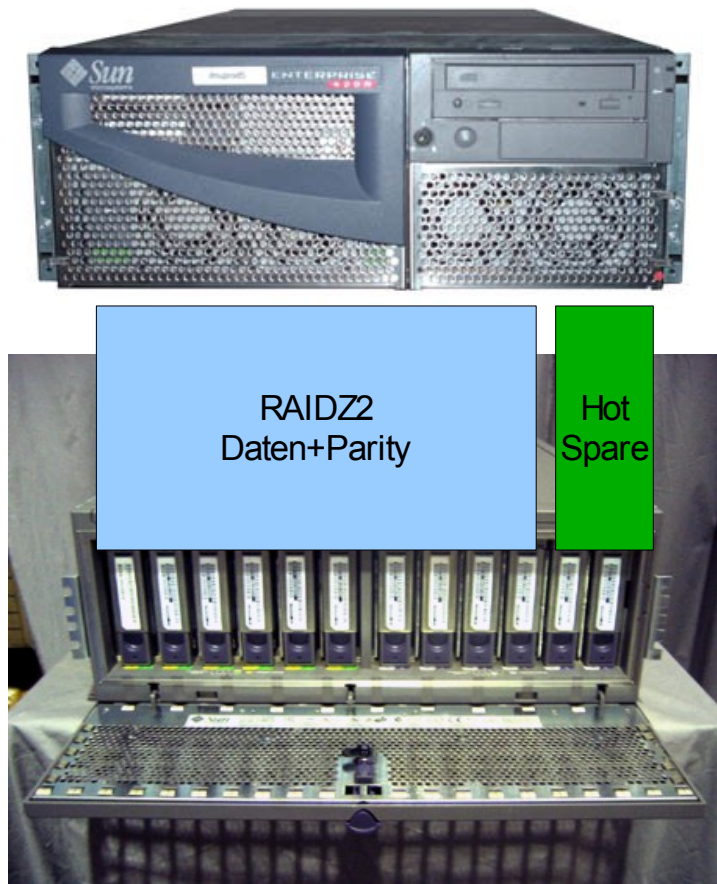


E420R mit D1000 als Loghost für Firewalls und Router



Der alte Loghost war ein alter Linux-Server, dessen Plattenplatz mit jedem weiteren Router immer knapper wurde. Der Cronjob, der die älteren Logs per gzip komprimierte, half auch nur am Anfang.

Durch die Ablösung eines Servers wurde eine E420R mit 2 CPUs, 4GB RAM, einer QFE-Karte und einem D1000 mit 12 Platten á 36GB frei.

Im Zuge der Ablösung war auch geplant, diesen Loghost für alle Router und Firewalls im gesamten Netz zu verwenden, daher wurde das Hauptaugenmerk auf verfügbaren Plattenplatz und Ausfallsicherheit gelegt.

Das Resultat war ein RAIDZ2 mit 2 Hot Spares, so dass netto 8 Platten für die Daten übrig blieben, also etwas über 250GB.

Ein Test mit den alten Log-Dateien ergab mit der Default-Kompression (LZHB) ein Verhältnis von 1:4, mit gzip auf Anhieb 1:12, also ging der Server mit dieser Konfiguration produktiv.

Das komprimierte Filesystem machte auch den Cronjob überflüssig, der vorher die alten Logs komprimiert hatte; nur der Cronjob zum Löschen nach (zur Zeit) 35 Tagen ist noch aktiv.

Als positiver Nebeneffekt hat sich das Arbeiten mit den Log-Dateien vereinfacht und vereinheitlicht - es ist kein gzcat mehr erforderlich.

```
# df -k
Filesystem          kbytes  used  avail capacity  Mounted on
syslogng/logs      278014464 87490868 190445986   32%   /var/log/HOSTS

# zfs get compressratio
NAME                PROPERTY          VALUE          SOURCE
syslogng            compressratio     14.75x        -
syslogng/logs       compressratio     14.76x        -

# zpool status -v
  pool: syslogng
state: ONLINE
  scrub: scrub completed after 4h2m with 0 errors on Tue Sep  8 21:43:58 2009
config:

NAME                STATE              READ  WRITE  CKSUM
syslogng            ONLINE             0     0     0
  raidz2            ONLINE             0     0     0
    c2t0d0           ONLINE             0     0     0
    c2t1d0           ONLINE             0     0     0
    c2t2d0           ONLINE             0     0     0
    c2t3d0           ONLINE             0     0     0
    c2t4d0           ONLINE             0     0     0
    c2t5d0           ONLINE             0     0     0
    c2t8d0           ONLINE             0     0     0
    c2t9d0           ONLINE             0     0     0
    c2t10d0          ONLINE             0     0     0
    c2t11d0          ONLINE             0     0     0
spares
  c2t12d0           FAULTED           corrupted data
  c2t12d0           AVAIL
  c2t13d0           AVAIL

errors: No known data errors
```

Inzwischen ist ein halbes Jahr vergangen; die Kompressionsrate hat sich auf gut 1:14 eingependelt, der ARC-Cache bei 2GB. Die Load liegt im Durchschnitt bei knapp 1, also ist der Server mit zwei CPUs ausreichend dimensioniert. Diese System-/Platten-Auslastung bei etwas über 300 Routern lässt noch genügend Luft für weitere 600.

Die syslog-ng.conf entspricht dem Auslieferungszustand, ergänzt um je einen Eintrag für die IPs der einzelnen Netzwerkinterfaces, die alle über den gleichen Eintrag in die gleiche Verzeichnisstruktur im RAIDZ2 schreiben.

syslog-ng.conf:

```
source r_pix {
    udp(ip("10.175.159.49" ) port(514) ); }; # hme0
source r_ext {
    udp(ip("10.175.100.32" ) port(514) ); }; # qfe0
source r_ex1 {
    udp(ip("10.175.128.46" ) port(514) ); }; # qfe1
source r_ex2 {
    udp(ip("10.175.229.99" ) port(514) ); }; # qfe2
source r_ex3 {
    udp(ip("10.175.178.57" ) port(514) ); }; # qfe3
destination l_pix {
    file("/var/log/HOSTS/$HOST/$YEAR/$MONTH/$HOST-$YEAR-$MONTH-$DAY-$HOUR"
        owner(root) group(sys) dir_group(sys) perm(0640) dir_perm(0750) create_dirs(yes)
    );
};
log { source(r_pix); destination(l_pix); };
log { source(r_ext); destination(l_pix); };
log { source(r_ex1); destination(l_pix); };
log { source(r_ex2); destination(l_pix); };
log { source(r_ex3); destination(l_pix); };
```

