A DNSSEC Signing tool for RDNS

Mark Elkins

Posix Systems

mje@posix.co.za

Problem to solve

There are a number of solutions for automating the DNS Signing of zones – usually for when the Zone is a Forward zone (posix.co.za).

Many are GUI orientated.

(A home-grown example – the DNS management for the domain “diver.co.za” - from my “vweb” system)

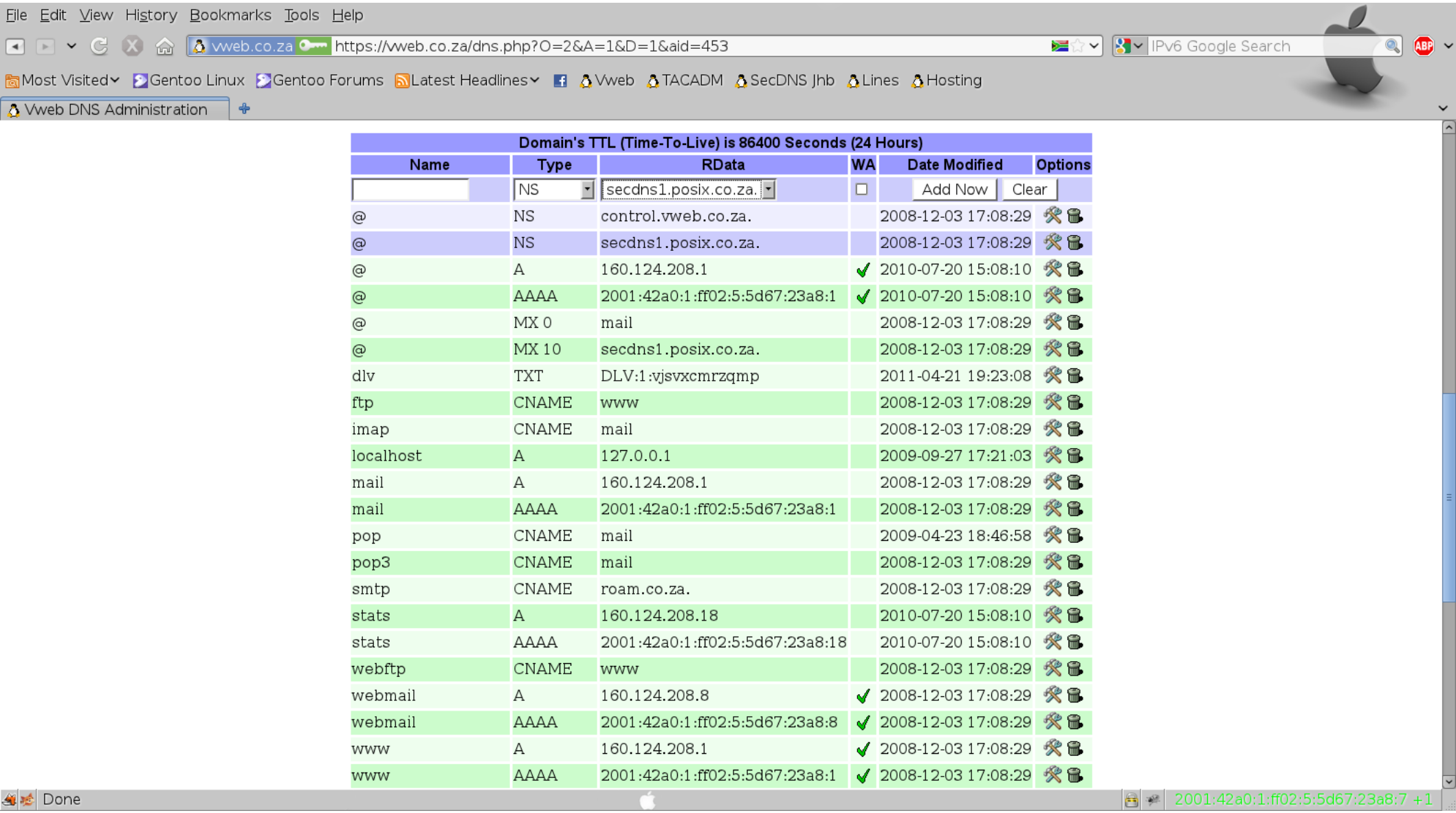
Registration Applicant Information on diver.co.za

Server Time: 21:09:24 Browser Time: 21:09:23
Next potential VWEB/DNS Rebuild: 0:36

ID=453 (uid:5076) - Added 2003-01-26 20:57:36 by 0.0.0.0

Action	Update Domain details · Save Data · Refresh Auto fill from COZA · Submit Application to COZA Applications sent: 1 Last sent on: 2002-09-28 00:00:00 Click this just ONCE (COZA)
Domain Registrant (Owner) Details. (Phone details are taken from Vweb system)	
Organisation/Owner	Posix Systems (Pty) Ltd
Postal Address	P.O. Box 73892, Lynnwoodridge, 0040, South Africa
Street Address *Domicilium Citandi et Executandi*	Suite 86, Wapadrand Office Park, Wapadrand, Pretoria, Gauteng, ZA
Billing Details	
Organisation to bill	Posix Systems (Pty) Ltd
E-Mail	dns-billing@posix.co.za VAT: 466016620
Invoice address	P O Box 73892, Lynnwood Ridge, Gauteng, 0040, ZA
Administrator Details	
Name (last, first)	Elkins, Mark J
Organisation	Posix Systems (Pty) Ltd
Postal address	P.O. Box 73892, Lynwoodridge, 0040, South Africa
Phone	+27.128070590 Fax: +27.128075324
E-Mail	dns-admin@posix.co.za
The Domains Technical Contact details are automatically supplied by Posix Systems	
Domain Registration Status	Created:**2002-12-27**, Renewal Month:**01**, Renewal Freq:**12**(Mth) ExpireOn: **2012-01-03**, LastTran:**2011-01-03**, PaidOn:**2011-01-06**

To Modify( ) or Delete( ) a DNS entry - click on the appropiate **Icon**
To Add a new DNS Entry - fill in the first entry below and Click on 'Add Now'


File Edit View History Bookmarks Tools Help
vweb.co.za https://vweb.co.za/dns.php?O=2&A=1&D=1&aid=453
IPv6 Google Search
Most Visited Gentoo Linux Gentoo Forums Latest Headlines Vweb TACADM SecDNS Jhb Lines Hosting
Vweb DNS Administration
Domain's TTL (Time-To-Live) is 86400 Seconds (24 Hours)
Name Type RData WA Date Modified Options
NS secdns1.posix.co.za. Add Now Clear
@ NS control.vweb.co.za. 2008-12-03 17:08:29
@ NS secdns1.posix.co.za. 2008-12-03 17:08:29
@ A 160.124.208.1 2010-07-20 15:08:10
@ AAAA 2001:42a0:1:ff02:5:5d67:23a8:1 2010-07-20 15:08:10
@ MX 0 mail 2008-12-03 17:08:29
@ MX 10 secdns1.posix.co.za. 2008-12-03 17:08:29
dlv TXT DLV:1:vjsvxcmrzqmp 2011-04-21 19:23:08
ftp CNAME www 2008-12-03 17:08:29
imap CNAME mail 2008-12-03 17:08:29
localhost A 127.0.0.1 2009-09-27 17:21:03
mail A 160.124.208.1 2008-12-03 17:08:29
mail AAAA 2001:42a0:1:ff02:5:5d67:23a8:1 2008-12-03 17:08:29
pop CNAME mail 2009-04-23 18:46:58
pop3 CNAME mail 2008-12-03 17:08:29
smtp CNAME roam.co.za. 2008-12-03 17:08:29
stats A 160.124.208.18 2010-07-20 15:08:10
stats AAAA 2001:42a0:1:ff02:5:5d67:23a8:18 2010-07-20 15:08:10
webftp CNAME www 2008-12-03 17:08:29
webmail A 160.124.208.8 2008-12-03 17:08:29
webmail AAAA 2001:42a0:1:ff02:5:5d67:23a8:8 2008-12-03 17:08:29
www A 160.124.208.1 2008-12-03 17:08:29
www AAAA 2001:42a0:1:ff02:5:5d67:23a8:1 2008-12-03 17:08:29
Done
2001:42a0:1:ff02:5:5d67:23a8:7 +1

webftp	CNAME	www		2008-12-03 17:08:29
webmail	A	160.124.208.8	✓	2008-12-03 17:08:29
webmail	AAAA	2001:42a0:1:ff02:5:5d67:23a8:8	✓	2008-12-03 17:08:29
www	A	160.124.208.1	✓	2008-12-03 17:08:29
www	AAAA	2001:42a0:1:ff02:5:5d67:23a8:1	✓	2008-12-03 17:08:29

SECDNS (Secure DNS) status for this zone: NSEC Commit

The zone **diver.co.za** is signed with NSEC keys. The Parent of this zone is the **CO.ZA Administrator**. Click on for more info. There are 2 ZSK's, ages: 3, 24 (of max 34 days).The Key Signing Keys (**KSK**) are:

DNSKEY Key ID = 3429 Age 197 (of max 370 days) Born 2010-10-28 00:01:31	257 3 5 BQEAAAABsEUWFqFBY804vwGBLoG7WU5H/bT1mc /151b07VfxaiieyVj0 YPUNNcjoWi3Jw8Kdi1rFywNqVe3QrKsZ0CRG0RIa5uHu4Lz7y4V20Elz c0N/TrbONm2zXQZVXhcfQDgLgybjFUxHak/QLOTTrN1Msm2uT8PEkdbj wscvAqPWbXk=
DNSKEY Key ID = 18804 Age 32 (of max 370 days) Born 2011-04-11 00:01:25	257 3 5 BQEAAAAByP0Jzpn6fr+4HwYqxPL4rJBY77uUNQI8x+kmUhS8PsPPSzR5 XgSbqN8YxbSccmYKXthi0UeXVsVmvmgtxZnOm/hh+6oyNnamAwJElcd+ ngLyu3McLteYp/O0JB+91/4HxCHv38U3QxKP5vhA8i/szUdQdr0R8sms MExPqGrB//U=
DS Key ID = 18804 ✓	18804 5 2 9C7A2D534BCD06B4B6F40509E0DF951B88E134904D0A17FF2107E591 2595F384
DS Key ID = 18804 ✓	18804 5 1 D32B9F1529088306835AFBB4080C4EABE9AEE285
DS Key ID = 3429 ✓	3429 5 2 36DB0DA6B58164CF443D66D1483DDEAE20B750F795D45AB026B4022B F0124E25
DS Key ID = 3429 ✓	3429 5 1 D425D0F4D47F416C730FAB6CF6F0B0CB442E1196

Default DNS Back to DOMAIN

Last modified: Thursday, 12th May, 2011 @ 05:25pm

Goals

To create a script that...

- ***Allow non-gui-ified zones to be signed***
- ***Simple directory structure***
- ***Work for both “forward” and “reverse” zones***
- ***Detect zone changes and update the SOA Serial Number appropriately***
- ***Maintain DNSKEY Records as appropriate***
- ***(Re)Sign a zone if needed***
- ***Work with Unsigned, Dynamic, NSEC and NSEC3 zone types***
- ***Manage the grouping of Child and Parent zones (the DS records of local children need to be given to local parents)***
- ***Manage non-local Parents (give DS records to remote parents)***

Solutions

- **Allow non-gui-ified zones to be signed**
  - Bash is my friend!

- **Simple directory structure**
  - /etc/bind/pri/<zone_name>/<Zones-Data>

- **Work for both “forward” and “reverse” zones**
  - Forward zones are easy – 'diver.co.za' is just that.
  - Reverse zones – by their arpa name so '192.96.28.X' is named as '28.96.192.in-addr.arpa'

- **Detect zone changes and update the SOA Serial Number appropriately**
  - Record and maintain an md5sum of each zone
    - for each “db.<zone_name>”
    - manage “md5sum-<zone_name>” and “soa-<zone_name>”

- **Maintain DNSKEY Records as appropriate**
  - ZSK – alive for 34 days, create a new one every 17 days, remove any that are older than 34 days (there are usually two)
  - KSK – alive for 370 days, create a new one every 185 days, remove any that ae older than 370 days...

Solutions

- *(Re)Sign a zone if needed*
  - *run dnssec-signzone only if there was some sort of data change (Child DS, SOA Update)*

- *Work with Unsigned, Dynamic, NSEC and NSEC3 zone types*
  - *Use dnssec-<zone_name> with appropriate value*

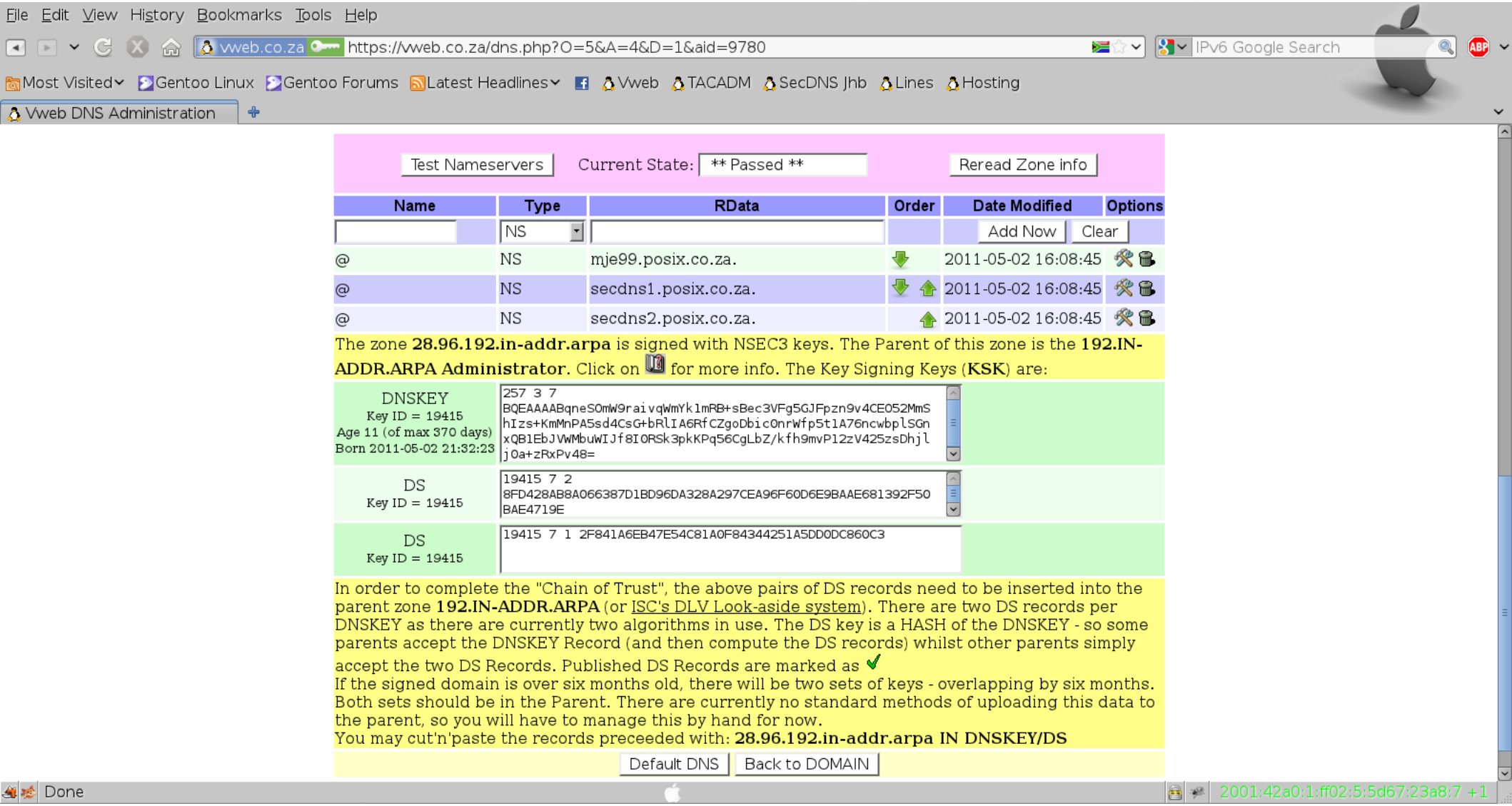
- *Manage the grouping of Child and Parent zones (the DS records of local children need to be given to local parents)*
  - *process the zones – sorted by the longest to shortest names.*
    - *children will be processed before Parents.*
  - *Children can “detect” parents and copy over their DS Records*
  - *Parents can include child's DS Records*

- *Manage non-local Parents (give DS records to remote parents)*
  - *Looks for 'parent-<zone_name>' and runs that script.*
  - *The script knows the Current and Parent zone names.*

Runs from Cron (once an hour)
Run as a visible script – whenever someone edits a zone

GUI Management?

Just works – fits into my “vweb” system just fine!



Conclusion

The Script is available for public download at:-

http://posixafrica.com/RunSign

AfriNIC resources can NOW be easily DNSSEC-signed,
DS records can be uploaded at http://my.afrinic.net

Thanks!

Mark Elkins – mje@posix.co.za