Προδιαγραφές S-AI Server και οδηγός εγκατάστασης

Γιώργος Νικολαΐδης, gnikolaidis@ergobyte.gr
Βασίλης Τσάπας, btsapas@ergobyte.gr

Έκδοση 1.0, 22 Ιουνίου 2008

1 - Εισαγωγή

Ο οδηγός αυτός απευθύνεται στον εγκαταστάτη/συντηρητή ενός S-AI Server. Περιέχει τις προδιαγραφές που πρέπει να πληροί ένας S-AI Server, καθώς και έναν συνοπτικό οδηγό εγκατάστασης (how-to).

Παρακαλώ στείλετε προτάσεις ή συνεισφορές μέσω e-mail στον Γιώργο Νικολαΐδη. Αυτός ο οδηγός θα ανανεώνεται συχνά με τις νέες συνεισφορές και βελτιώσεις.

1.1 - Γενικά περί S-AI

Η τυποποίηση S-AI Server προήλθε από τον τρόπο που η Ergobyte Πληροφορική εγκαθιστά τους server των πελατών της. Είναι το αποτέλεσμα διαδοχικών βελτιώσεων έπειτα από αξιοποίηση της εμπειρίας από την λειτουργία τους.

Η ένδειξη S-AI σε έναν server είναι συνώνυμη με μεγαλύτερη αξιοπιστία και πιο εύκολη συντήρηση. Καθώς η τυποποίηση είναι ελεύθερα διαθέσιμη για μη εμπορική χρήση, η χρησιμότητά της είναι δεδομένη στις περισσότερες περιπτώσεις.

1.2 - Διαφορετικά είδη server

Ανάλογα με την τελική τους χρήση, οι S-AI Server χωρίζονται σε διαφορετικα είδη. Στην παρούσα έκδοση αναγνωρίζονται τα εξής είδη:

- Unconfigured S-AI Server
- S-AI File Server
- S-AI Backup Server

Εκτός εάν αναφέρεται διαφορετικά, όλες οι προδιαγραφές εφαρμόζονται σε όλα τα είδη S-AI Server χωρίς παρεκκλίσεις.

1.3 - Εκδόσεις του κειμένου

Η τελευταία έκδοση του κειμένου αυτού είναι πάντα διαθέσιμη στην διεύθυνση developer.ergobyte.gr/specs.

Πιθανές νέες τεχνικές και τεχνολογικές λύσεις για την εγκατάσταση ενός S-AI Server θα γίνουν μέρος επόμενης έκδοσης του οδηγού αυτού. Σε περίπτωση που εγκαταστάσεις που έχουν πιστοποιηθεί με την παρούσα έκδοση και χρειάζεται να μετακυλίσουν σε οποιαδήποτε επόμενη, η ενέργεια πρέπει να γίνει εξ΄ολοκλήρου και σε σύντομο χρονικό διάστημα ώστε να μην βρεθεί η εγκατάσταση σε ενδιάμεση μεταξύ των εκδόσεων κατάσταση.

1.4 - Συμβάσεις στο παρόν κείμενο

Στο παρόν κείμενο οι χρήση των όρων ΠΡΕΠΕΙ, ΔΕΝ ΠΡΕΠΕΙ, ΑΠΑΙΤΕΙΤΑΙ, ΠΡΟΤΕΙΝΕΤΑΙ, ΔΕΝ ΠΡΟΤΕΙΝΕΤΑΙ, ΜΠΟΡΕΙ, ΠΡΟΑΙΡΕΤΙΚΑ γίνεται σύμφωνα με το RFC2119.

Όπου αναφέρεται πακέτο Debian, αυτό γράφεται με πλάγια γράμματα, πχ *laptop-detect*.

Οι διαδρομές (paths) σε φακέλους και αρχεία του συστήματος γράφονται με διαφορετική γραμματοσειρά και χρώμα, πχ `/etc/apache2/sites-enabled/`.

Οι συμβολοσειρές που πρέπει να χρησιμοποιηθούν χωρίς καμία τροποποίηση (literals) γράφονται με διαφορετική γραμματοσειρά και χρώμα, πχ `[mysqld]`.

1.5 - Άδεια χρήσης

2 - Προδιαγραφές S-AI Server

2.1 - Hardware

Οι ελάχιστες δυνατότητες hardware ενός S-AI Server πρέπει να είναι οι εξής:

- Επεξεργαστής Intel x86 συμβατός, γενιάς 6 και πάνω (τουλάχιστον Pentium Pro, Pentium II, Celeron, K6-2)
- Μνήμη RAM τουλάχιστον 256MB
- Δύο ή περισσότεροι σκληροί δίσκοι ίδιας χωρητικότητας τουλάχιστον 80GB. Κατ' εξαίρεση, ένας S-AI Backup Server μπορεί να έχει έναν μόνο δίσκο.
- 1000MBps LAN

Προαιρετικά ο S-AI Server μπορεί να διαθέτει:

- Serial Modem
- DVD Writer
- PSTN/ISDN PCI cards για VoIP
- Επιπλέον LAN cards για routing

2.2 - Λειτουργικό σύστημα

Ο S-AI Server πρέπει να φέρει stable διανομή του Debian, και συγκεκριμένα την "Etch". Πιθανές μελλοντικές εκδόσης της stable διανομής θα υιοθετηθούν σε επόμενη έκδοση του οδηγού. Στην παρούσα έκδοση απαιτείται η επιλογή της 32bit έκδοσης.

2.3 - Partitioning και mount points

Ένας S-AI Server στηρίζει την αξιοπιστία του στο software RAID των Linux kernels, συγκεκριμένα του `md` driver. Το paritioning, το οποίο γίνεται συνήθως κατά την διάρκεια της εγκατάστασης της Debian διανομής, πρέπει να ακολουθεί τις εξής γενικές αρχές:

- Όλοι οι δίσκοι πρέπει να έχουν τα ίδια partition (πλήθος, διάταξη, χωρητικότητα)
- Το πρώτο partition κάθε δίσκου σχηματίζει το πρώτο md array, το δεύτερο partition κάθε δίσκου το δεύτερο md array και ούτω κάθε εξής
- Όταν οι δίσκοι είναι δύο, πρέπει να χρησιμοποιηθεί RAID 1 για όλα τα arrays. Όταν οι δίσκοι είναι περισσότεροι, μπορούν να επιλεγούν επίσης RAID 5, RAID 6. Προτείνεται να έχουν όλα τα arrays το ίδιο RAID σχήμα προκειμένου να είναι πιο απλή η εγκατάσταση.
- Πρέπει να υπάρχουν τουλάχιστον 3 md partitions: το root που γίνεται mount στο /, το swap και το home που γίνεται mount στο /home
- Η χωρητικότητα του root partition πρέπει να είναι τουλάχιστον 2GB και το πολύ 8GB
- Η χωρητικότητα του swap partition πρέπει να είναι ίση ή μεγαλύτερη με την μνήμη RAM του συστήματος
- Δεν προδιαγράφεται συγκεκριμένο filesystem. Ωστόσο απαιτείται η χρήση journaling filesystem και προτείνεται η χρήση του EXT3

Σημειώνεται ότι από την υποχρέωση για χρήση του md driver και των RAID array εξαιρείται ο S-AI Backup Server, όταν αυτός έχει μόνο έναν δίσκο.

2.4 - Πολιτική ονομάτων

Στα πλαίσια των εγκαταστάσεων S-AI ορίζονται οι εξής βασικές παράμετροι :

1. **Αναγνωριστικό τελικού χρήστη** : κάθε τελικός χρήστης που γίνεται αποδέκτης ενός S-AI Server έχει ένα μοναδικό αναγνωριστικό που αποτελείται από μικρά λατινικά γράμματα και την κάτω ή πάνω παύλα. Όταν ο τελικός χρήστης είναι κάτοχος ενός καταχωρημένου και έγκυρου domain name, τότε χρησιμοποιείται το τελευταίο συνθετικό αυτού ως αναγνωριστικό τελικού χρήστη. Για παράδειγμα έαν ο τελικός χρήστης Example Corporation έχει το domain name example.com, τότε το αναγνωριστικό του είναι το example.
2. **Κωδικός τοποθεσίας** : ένας μοναδικός ακέραιος αριθμός που προέρχεται από τα μητρώα τελικών χρηστών, είναι μοναδικός για κάθε S-AI εγκατάσταση.
3. **Όνομα server** : Κάθε S-AI Server φέρει ένα μοναδικό όνομα που αποτελείται από ακριβώς τρία (3) μικρά λατινικά γράμματα. Το όνομα επιλέγεται ελεύθερα από τον εγκαταστάτη, προσέχοντας όμως να μην συμπέσει με άλλα ήδη υπάρχονται ονόματα.

Οι υπόλοιπες παράμετροι που ορίζονται και εξάγονται από τις βασικές είναι

1. **FQDN όνομα server** : Το fully qialified domain name του server είναι το όνομα του server με την κατάληξη `.ddns.bsod.gr`
2. **server root password** : Προδιαγράφεται ότι είναι ένας τριψήφιος αριθμός συν το όνομα του server συν έναν άλλο τριψήφιο αριθμό. Τα 4 πρώτα keystrokes γίνονται με το SHIFT πατημένο.

2.5 - Πολιτική πακέτων και αρχείων

Για την εγκατάσταση ή απεγκατάσταση πακέτων πρέπει να χρησιμοποιείται αποκλειστικά το *aptitude*, ρυθμισμένο έτσι ώστε να μην εγκαθιστά αυτόματα τα προτεινόμενα πακέτα.

Η οργάνωση των αρχείων και των φακέλων στο σύστημα γίνεται ακολουθώντας τις αρχές του Linux Standard Base / Filesystem Hierarchy Standard.

2.6 - Υπηρεσίες συστήματος

Υποχρεωτικά σε κάθε S-AI Server πρέπει να έχουν ρυθμιστεί οι εξής υπηρεσίες

SSH Access	Πρέπει να γίνονται δεκτά τα root login. Προκειμένου για συνδέσεις με προέλευση εκτός του τοπικού δικτύου, η θύρα πρέπει να είναι η `222` αντί της γνωστής 22. Όταν το δίκτυο ενός τελικού χρήστη έχει περισσότερους του ενός S-AI Server, η SSH πόρτα αυξάνεται προοδευτικά κατά 1 για κάθε επιπλέον server. Για παράδειγμα, ο δεύτερος κατά σειρά S-AI Server ακούει στην θύρα 223.
Time Syncronization	Πρέπει να υπάρχει υπηρεσία συγχρονισμού του ρολογιού του συστήματος βάσει του πρωτοκόλλου NTP. Η σωστή ρύθμιση του timezone είναι αναγκαία.
Dynamic DNS	Στην πλειονότητα των περιπτώσεων ο server βρίσκεται πίσω από router που έχει μεταβλητή εξωτερική IP. Η ανάγκη να γνωρίζει ο συντηρητής του server ανά πάσα στιγμή την πραγματική WAN IP του server οδηγεί στην χρήση εργαλείων Dynamic DNS update. Κάθε S-AI server οφείλει να έχει τουλάχιστον μία (1) υπηρεσία ανανέωσης ενός domain με την εκάστοτε εξωτερική IP του δικτύου στο οποίο βρίσκεται.
Power Management	Πρέπει να υπάρχει σωστή ρύθμιση ώστε ο Server να μην

	λειτουργεί στην μέγιστη απόδοση όταν αυτό δεν χρειάζεται.
Mail Transport	Το σημαντικότερο κανάλι επικοινωνίας του server με τον διαχειριστή του είναι το ηλεκτρονικό ταχυδρομείο. Είναι κεφαλαιώδους σημασίας λοιπόν να υπάρχει ένας trasport agent που να αναλαμβάνει την αποστολή των email εκ μέρους των υπηρεσιών που τρέχουν στον server στον κατάλληλο παραλήπτη. Προτείνεται ένας light-weight smart-host only MTA όπως ο *nullmailer* ή ο *ssmtp*.
Remote Administration	Ειδική μέριμνα πρέπει να δοθεί ώστε ο διαχειριστής να μην βρεθεί ποτέ σε locked-out κατάσταση. Προτείνεται σθεναρά η εγκατάσταση PSTN modem και η σύνδεσή του με τηλεφωνική γραμμή σαν last-resort λύση όταν αποτύχουν οι συμβατικότερες προσβάσεις (μέσω Dynamic DNS, static IP, κ.α.)

2.7 - Παρακολούθηση λειτουργίας (monitoring)

TODO

2.8 - Αντίγραφα ασφαλείας (backup)

TODO

2.9 - Υπηρεσίες για τον τελικό χρήστη

Ο αριθμός και το είδος των υπηρεσιών που προσφέρονται προς τον τελικό χρήστη διαφέρουν σημαντικά από εγκατάσταση σε εγκατάσταση. Παρόλα αυτά, για επιλεγμένες υπηρεσίες που συναντώνται συχνά στην πράξη, το παρόν κείμενο δίνει μερικές προτεινόμενες πρακτικές.

Web Server

Προτείνεται η χρήση του *apache2* χωρίς κάποια ιδιαίτερη ρύθμιση.

3 - Οδηγός εγκατάστασης (how-to)

3.1 - Ρυθμίσεις BIOS

Μόλις τελειώσουμε την συναρμολόγηση του hardware και πριν αρχίσουμε την εγκατάσταση του software, αφιερώνουμε λίγο χρόνο στα μενού του BIOS. Εκεί ενδιαφέρει:

- το σύστημα να κάνει boot ακόμα και αν λείπουν ποντίκι ή πληκτρολόγιο,
- το σύστημα να κάνει boot μετά από διακοπή ρεύματος, και
- οι ανεμιστήρες να δουλέουν στην χαμηλότερη δυνατή ταχύτητα

3.2 - Εγκατάσταση Debian

Σε περίπτωση που ο S-AI Server διαθέτει οπτικό drive, αρχίζουμε με CD εγκατάστασης του Debian Etch. Έχουν δοκιμαστεί επιτυχώς τα "network install", "business card" και το πρώτο CD από το πλήρες set. Εάν δεν υπάρχει οπτικό drive, μπορεί να γίνει χρήση των δισκετών εγκατάστασης μέσω δικτύου. Οι δισκέτες υπάρχουν σε μορφή image file στο site του Debian και μπορούν να γραφτούν με το Rawrite for Windows (`rwwrtwin.exe`).

Δίνουμε βαρύτητα στα εξής σημεία της εγκατάστασης:

- timezone : προσοχή να γίνει η σωστή επιλογή `Europe/Athens`
- hostname : προσοχή να δοθεί το πλήρες hostname σύμφωνα με τις προδιαγραφές ονομάτων
- parititioning : ίσως το σημαντικότερο βήμα, πρέπει να ρυθμιστεί σωστά το md RAID
- networking : σε αυτό το στάδιο λογικά εργαζόμαστε στο εσωτερικό μας δίκτυο, οπότε επιλέγουμε DHCP
- package install : εκτός από το base σύστημα προτείνεται να μην εγκατασταθεί κανέναν άλλο πακέτο
- root password : σύμφωνα με τις προδιαγραφές
- user account : προτείνεται η χρήση του συνηθέστερου nickname/login name μας με το αντίστοιχο password για να μην έχουμε να θυμόμαστε επιπλέον credentials
- debian mirrors : να γίνει λογική επιλογή

3.3 - Πρώτα βήματα μετά την εγκατάσταση

3.3.1 - Αρχικές ρυθμίσεις πακέτων

Ρυθμίζουμε το αρχείο `/etc/apt/sources.list` ώστε να περιέχει και τα `contrib` και `non-free` repositories

```
deb http://debian.otenet.gr/debian/ etch main contrib non-free
deb-src http://debian.otenet.gr/debian/ etch main contrib non-free
deb http://security.debian.org/ etch/updates main contrib non-free
deb-src http://security.debian.org/ etch/updates main contrib non-free
```

Ανοίγουμε το aptitude

```
# aptitude
```

και εκτελούμε τις εξής εργασίες

1. Εκτελούμε ένα update των πακέτων (πλήκτρο "u")
2. Απενεργοποιούμε τις αυτόματες εγκαταστάσεις των προτεινόμενων πακέτων, πηγαίνονται στα μενού με F10 και επιλέγοντας "Options", "Dependency Handling", "Install Recommended packages automatically"
3. Ζητάμε την αναβάθμιση των πακέτων που έχουν security updates
4. Αφαιρούμε περιττά πακέτα όπως : *`tasksel`*, *`dselect`*, *`vim-tiny`*, *`installation-report`*, *`libsasl2`*, *`laptop-detect`*
5. Προσθέτουμε μερικά πακέτα που κρίνονται χρήσιμα όπως : *`tcsh`*, *`less`*

3.3.2 - Hostname

Αλλάζουμε το hostname ώστε να περιέχει το Fully Qualified Domain Name, δηλαδή δίνουμε:

```
# hostname <fqdn>
```

και επεξεργαζόμαστε αναλογα το `/etc/hostname`

3.3.3 - SSH

Εγκαθιστούμε τον SSH server (πακέτο *`openssh-server`*) καθώς θα μας επιτρέψει να μεταφερθούμε στην άνεση του αγαπημένου μας desktop.

Επεξεργαζόμαστε το `/etc/ssh/sshd_config` προσθέτοντας κάτω από την γραμμή

```
Port 22
```

την

```
Port 222
```

Σημειωτέον ότι για τον δεύτερο S-AI server εντός του δικτύου ενός τελικού χρήστη, το νούμερο της θύρας είναι 223, για τον τρίτο 224 και ούτω κάθε εξής.

3.3.4 - Power Management

Ακολουθούμε τις οδηγίες του πολύ καλού how-to για το power-management σε 2.6 kernel και σε Debian Etch αυτής της σελίδας. Συγκεκριμένα :

```
# aptitude install cpufrequtils sysfsutils
# cat /proc/cpuinfo
```

Ανάλογα με την οικογένεια CPU διαλέγουμε ένα speedstep module από την λίστα

```
AMD K6 processors : powernow_k6
AMD K7 processors (Athlon, Duron, Sempron 32 bits) : powernow_k7
AMD K8 processors (Athlon 64, Turion 64, Sempron 64, Opteron 64) : powernow_k8
Pentium 4, Celeron D, Pentium D, Celeron M : p4_clockmod
Pentium M, Core Duo, Core 2 Duo : speedstep_centrino
```

και ανάλογα με τον επιθυμητό τρόπο διαχείρισης της ενέργειας ένα module από την λίστα

```
cpufreq_performance : highest possible frequency
cpufreq_powersave : lowest frequency
cpufreq_ondemand : dynamical, depending on the work load
cpufreq_conservative : dynamical, less aggressive, ideal for laptops
```

Προσθέτουμε τις επιλογές μας στο `/etc/modules`. Τέλος προσθέτουμε στο `/etc/sysfs.conf` την γραμμή:

```
devices/system/cpu/cpu0/cpufreq/scaling_governor = ondemand
```

πιθανώς αλλάζοντας το `ondemand` με την επιλογή μας παραπάνω.

3.3.5 - Inittab

Μπορούμε να αφαιρέσουμε τα επιπλέον TTY από το `/etc/inittab` κάνοντας comment-out τις γραμμές

```
2:23:respawn:/sbin/getty 38400 tty2
3:23:respawn:/sbin/getty 38400 tty3
4:23:respawn:/sbin/getty 38400 tty4
5:23:respawn:/sbin/getty 38400 tty5
6:23:respawn:/sbin/getty 38400 tty6
```

και δίνοντας

```
# kill -HUP 1
```

3.3.6 - Επανεκκίνηση

Σε αυτό το σημείο προτείνεται να κάνουμε reboot, ιδίως αν στα προηγούμενα βήματα άλλαξε ο kernel του συστήματος.

3.4 - Υπηρεσίες συστήματος

3.4.1 - Αυτόματες ενημερώσεις ασφαλείας

Δημιουγούμε το αρχείο `/etc/apt/apt.conf.d/10periodic` με τα εξής περιεχόμενα:

```
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Download-Upgradeable-Packages "1";
APT::Periodic::AutocleanInterval "0";
APT::Periodic::Unattended-Upgrade "1";
```

3.4.2 - Mail transfer agent

Στον οδηγό αυτό χρησιμοποιούμε τον *nullmailer*.

```
# aptitude install nullmailer
# dpkg-reconfigure nullmailer
```

Στις ερωτήσεις του dpkg απαντάμε ως εξής:

```
Mail name of your system   : [fqdn όνομα server]
Smarthosts                 : mail.ergobyte.gr
Where to send local emails : [όνομα server]-admin@ergobyte.gr
```

Ο παραλήπτης των μηνυμάτων για τις εφαρμογές ρυθμίζεται να είναι ο [όνομα server]-admin@ergobyte.gr. Μπορούμε να δοκιμάσουμε τις ρυθμίσεις μας με το πακέτο *mailx*:

```
# aptitude install mailx
# echo "Hello, World!" | mail -s "Test Message" [όνομα server]-admin@ergobyte.gr
```

3.4.3 - Monit

Το *monit* είναι ένα system monitoring εργαλείο που μπορεί να προλάβει πολλά προβλήματα την ώρα που γεννιούνται.

```
# aptitude install monit
```

Ξαναγράφουμε το `/etc/monit/monitrc` ώστε να περιέχει μόνο τα εξής:

```
set daemon 120
set logfile syslog facility log_daemon
set mailserver mail.ergobyte.gr timeout 30 seconds
set eventqueue
    basedir /var/monit
    slots 100

set mail-format {
    from: monit@[fqdn όνομα server]
    subject: [όνομα server] $SERVICE $EVENT at $DATE
}

set alert [όνομα server]-admin@ergobyte.gr

set httpd port 2812 and
    allow admin:288[όνομα server]

include /etc/monit/monit.d/*
```

Δημιουργούμε τον φάκελο `/etc/monit/monit.d` και τοποθετούμε μέσα configuration files για κάθε service που θέλουμε να παρακολουθήσουμε. Μία εκτενής λίστα από έτοιμα configuration υπάρχει στην διεύθυνση developer.ergobyte.gr/monit

```
# mkdir /etc/monit/monit.d
# cd /etc/monit/monit.d
# wget http://developer.ergobyte.gr/monit/[filename].conf
```

Απαραίτητα αρχεία θεωρούνται τα system, process-ssh, device-md0 και device-md2. Τέλος, για την ολοκλήρωση της ρύθμισης του monit, αλλάζουμε το `/etc/default/monit` ώστε να τρέχει αυτόματα κατά την εκκίνηση. Επίσης τροποποιούμε το configuration του firewall `/etc/ferm/ferm.conf` ώστε να δέχεται συνδέσεις στην 2812.

3.4.4 - NTP

Κάνουμε εγκατάσταση του *ntpdate*.

```
# aptitude install ntpdate
```

Τρέχουμε την υπηρεσία για πρώτη φορά

```
# /etc/network/if-up.d/ntpdate
```

Περιμένουμε μερικά δευτερόλεπτα και ελέγχουμε την ορθότητα της ώρας

```
# date
```

3.4.5 - Dynamic DNS update

Η λύση που προτείνεται εδώ στηρίζεται σε ένα άρθρο του swisslinux.org (σελίδα στα Γαλλικά), σε συνδυασμό με ένα PHP script που τρέχει στον TTL. Μετά το τέλος των ρυθμίσεων το όνομα που θα αντιστοιχεί στην εκάστοτε IP θα είναι το

```
[server].ddns.bsod.gr
```

όπου [server] είναι το όνομα τριών γραμμάτων του server. Πρώτα κάνουμε root login στον TTL και πηγαίνουμε στον φάκελο `/tmp`. Εκεί δίνουμε την εντολή (προσοχή στην τελεία στο τέλος!)

```
# dnssec-keygen -r /dev/urandom -a HMAC-MD5 -b 512 -n HOST [server].ddns.bsod.gr.
```

Παράγονται δύο αρχεία:

```
/tmp/K[server].ddns.bsod.gr.[some-stuff].key
/tmp/K[server].ddns.bsod.gr.[some-stuff].private
```

Τυπώνουμε στην οθόνη τα περιεχόμενα του `K[server].ddns.bsod.gr.[some-stuff].private`:

```
# cat K[server].ddns.bsod.gr.[some-stuff].private
```

και κάνουμε copy στο clipboard (Ctrl-C) ότι γράφει μετά το "Key: ". Ανοίγουμε το αρχείο `/etc/bind/named.conf` και προσθέτουμε στο τέλος

```
key "[server].ddns.bsod.gr." {
     algorithm HMAC-MD5;
     secret "[paste από το clipboard]";
};
zone "[server].ddns.bsod.gr." IN { type master; file "ddns.[server]";
     update-policy { grant [server].bsod.gr. name [server].bsod.gr. A; };
     allow-transfer { none; }; notify no;
};
```

Δημιουργούμε το αρχείο `/etc/bind/ddns.[server]` με τα εξής περιεχόμενα

```
@       IN SOA  [server].ddns.bsod.gr. root.bsod.gr. (
                        1
                        28800
                        7200
                        2419200
                        86400
                )
        NS      ns1.bsod.gr.
        A       0.0.0.0
```

Ζητάμε από τον BIND να ξαναδιαβάσει τα configuration files του:

```
# rndc reload
```

Μεταφερόμαστε στην κονσόλα του υπό εγκατάσταση server και αντιγράφουμε τα δύο αρχεία K[server].bsod.gr.[some-stuff].* στον φάκελο `/usr/local/etc/` με secure copy:

```
# scp root@ttl.bsod.gr:/tmp/K[server].ddns.bsod.gr.[some-stuff].key .
# scp root@ttl.bsod.gr:/tmp/K[server].ddns.bsod.gr.[some-stuff].private .
```

Εγκαθιστούμε το πακέτο *host* αντικαθιστώντας το *bind9-host* αν χρειαστεί. Επίσης εγκαθιστούμε το *dnsutils*. Δημιουργούμε το παρακάτω script στον φάκελο `/usr/local/bin/` με το όνομα `dynamic-dns-update.sh`:

```
#!/bin/bash
HOSTNAME='[server].ddns.bsod.gr'
PRIVATE_KEY='/usr/local/etc/K[server].ddns.bsod.gr.[some-stuff].private'
CURRENT_IP=`wget -q -O - http://www.bsod.gr/ipinfo.php`
OLD_IP=`host $HOSTNAME ns1.bsod.gr | cut -f 3`
if [ "$CURRENT_IP" = "$OLD_IP" ]
then
     echo "DNS record is up to date."
else
     (echo "server ns1.bsod.gr"
      echo "zone $HOSTNAME"
      echo "update delete $HOSTNAME A"
      echo "update add ${HOSTNAME}. 60 A $CURRENT_IP"
      echo "send" ) | nsupdate -k $PRIVATE_KEY
      echo "DNS record updated successfully."
fi
```

Κάνουμε το αρχείο εκτελέσιμο:

```
# chmod +x dynamic-dns-update.sh
```

Μπορούμε σε αυτό το σημείο να τρέξουμε το script δύο φορές. Την πρώτη πρέπει να απαντήσει "updated successfully" και την δεύτερη "record is up to date".

Το τελευταίο βήμα είναι να εγκατατήσουμε μια εντολη crontab. Δίνουμε:

```
# crontab -e
```

και στην συνέχεια εισάγουμε την γραμμή

```
*/5 * * * * /usr/local/bin/dynamic-dns-update.sh >/dev/null
```

3.4.6 - Firewall

Μια πολύ αποτελεσματική και συνάμα απλή ρύθμιση firewall μπορεί να επιτευχθεί με το *ferm*:

```
# aptitude install ferm
```

Απαντήστε yes ώστε να ξεκινάει στην εκκίνηση του συστήματος. Επεξεργαστείτε το αρχείο `/etc/ferm/ferm.conf`, συγκεκριμένα αλλάξτε τις γραμμές

```
# allow SSH connections
proto tcp dport ssh ACCEPT;
```

ως εξής:

```
# allow SSH connections
proto tcp dport 222 ACCEPT;
```

Στο ίδιο σημείο πρέπει να ανοίξουν όσες πόρτες χρειάζονται τα άλλα services, πχ για MySQL προσθέτουμε:

```
proto tcp dport (222 3036) ACCEPT;
```

Μετά από κάθε αλλαγή στο `ferm.conf` χρειάζεται μια επανεκκίνηση του firewall με:

```
# /etc/init.d/ferm restart
```

3.4.7 - PSTN Modem Dial-in

Πολλά modem (softmodem) απαιτούν ειδικούς drivers που παρέχει η Linuxant σε δωρεάν έκδοση για ταχύτητες μέχρι 14400. Σε περίπτωση που το modem σας έχει ήδη αναγνωρισθεί από τον kernel μπορείτε να αγνοήσετε τα επόμενα βήματα.

Επισκεπτόμαστε το site της Linuxant και κατεβάζουμε το πιο πρόσφατο DEB πακέτο. Για την εγκατάσταση θα χρειαστούν τα πακέτα *make*, *gcc* και τα linux kernel headers που ταιριάζουν στον kernel. Μόλις αυτά γίνουν διαθέσιμα, η εγκατάσταση των Linuxant drivers απαιτεί τις εντολές:

```
# wget http://www.linuxant.com/drivers/hsf/full/archive/hsfmodem-7.68.00.07full/hsfmodem_7.68.00.07fu
# unzip hsfmodem_7.68.00.07full_i386.deb.zip
# dpkg -i hsfmodem_7.68.00.07full_i386.deb
```

Το πακέτο *mgetty* παρέχει έναν απλό στην χρήση dial-in server. Επεξεργαζόμαστε το `/etc/inittab` αρχείο ώστε να κάνει spawn το mgetty:

```
T3:23:respawn:/sbin/mgetty -x0 -s 57600 modem
```

αλλάζοντας την λέξη modem ώστα να αντιστοιχεί στο device name του modem μας. Το init process θέλει επανεκκίνηση:

```
# telinit q
```

3.4.8 - Reverse SSH

Προαιρετικά για τις εγκαταστάσεις όπου η απ'έξω σύνδεση στο τοπικό δίκτυο του τελικού χρήστη και συγκεκριμένα στον S-AI Server δεν είναι δυνατή, προτείνεται η λύση του reverse ssh ώστε ο διαχειριστής να έχει πάντα πρόσβαση στον κύριο S-AI Server και κατά προέκταση στους υπόλοιπους hosts του τοπικού δικτύου του τελικού χρήστη.

Για να λειτουργήσει η παρακάτω μέθοδος απαιτήται ένας "μεσάζοντας" server στον οποίο θα δημιουργηθεί ένας χρήστης για κάθε S-AI Server στον οποίο απαιτήται πρόσβαση με αυτό τον τρόπο.

Για την αλληλουχία εντολών που ακολουθεί προσέξτε πως το prompt είναι στην μορφή user@host, όπου host είναι είτε `middle` για τον μεσάζοντα server, είτε `natted` για τον υπολογιστή στον οποίο θέλουμε να αποκτήσουμε πρόσβαση και είναι πίσω από firewall/nat. Όπου εμφανίζεται ο κωδικός `1234` αντιστοιχεί στον κωδικό τοποθεσίας του παραδείγματος και μπορεί να αντικατασταθεί ελεύθερα. Ο αριθμός θύρας και των δύο SSH servers είναι ο 222.

```
root@natted# ssh-keygen -t rsa
root@natted# scp -P 222 ~/.ssh/id_rsa.pub root@middle.example.com:/root

root@middle# adduser rssh1234
root@middle# mv /root/id_rsa.pub ~rssh1234
root@middle# chown rssh1234 ~rssh1234/id_rsa.pub
root@middle# su rssh1234

rssh1234@middle$ cd ~
rssh1234@middle$ mkdir .ssh
rssh1234@middle$ cat id_rsa.pub >> .ssh/authorized_keys
rssh1234@middle$ exit
```

Καλό είναι να δοκιμάσουμε σε αυτό το σημείο πως μπορεί να συνδεθεί με SSH ο root του natted ως rssh1234 στον middle χωρίς να ζητηθεί password:

```
root@natted# ssh -p 222 rssh1234@middle.example.com
```

Για να λειτουργήσει το reverse SSH πρέπει να ορίσουμε έναν port forwarding και να εκτελέσουμε την παραπάνω εντολή στο παρασκήνιο. Προσθέτουμε την παρακάτω γραμμή στο `/etc/inittab` του natted:

```
RSSH:23:respawn:/usr/bin/ssh -p 222 -nNT -R 21234:127.0.0.1:222 rssh1234@middle.example.com
```

όπου το RSSH είναι ένα τυχαίο αναγνωριστικό που πρέπει να διαφέρει από τα άλλα του ιδίου αρχείου και η πόρτα 21234 είναι επίσης τυχαία (εδώ προτείνεται 2 + κωδικός τοποθεσίας).

```
root@natted# telinit q
```

Το reverse ssh tunnel μας είναι έτοιμο για χρήση. Στον middle δίνοντας την παρακάτω εντολή συνδεόμαστε στον ssh server του natted, αρκεί ο τελευταίος να έχει σύνδεση με το Internet.

```
root@middle# ssh -p 21234 localhost
```

Επειδή απαντούν πολλοί servers στο localhost του `middle` με αυτό τον τρόπο σύνδεσης, ο SSH client παράγει πολλά μηνύματα του είδους "REMOTE HOST IDENTIFICATION HAS CHANGED". Η λύση για αυτήν την ενόχληση είναι η προσθήκη της παρακάτω γραμμής στο αρχείο `/etc/ssh/ssh_config`

```
    NoHostAuthenticationForLocalhost yes
```

3.5 - Υπηρεσίες προς τον χρήστη

Για τις υπηρεσίες επιθυμούμε να προσφέρουμε προς τον χρήστη, ακολουθούμε τα ανάλογα βήματα.

3.5.1 - Apache 2

Για την εγκατάσταση αρκεί απλά:

```
# aptitude install apache2
```

Η default σελίδα "It Works!" είναι κάπως ερασιτεχνική: προτείνεται η αφαίρεση του φακέλου

```
# rm -r /var/www/apache2-default
```

και η αλλαγή της παρακάτω γραμμής στο `/etc/apache2/sites-available/default`

```
RedirectMatch ^/$ /apache2-default/
```

σε

```
RedirectMatch ^/$ http://www.ergobyte.gr
```

Για την ολοκλήρωση της εγκατάστασης απαιτείται η εκτέλεση της

```
# apache2ctl graceful
```

3.5.2 - MySQL Server

Η εγκατάσταση του πακέτου *mysql-server-5.0* είναι αρκετή. Αρχικά δεν υπάρχει root password, για να οριστεί αυτό εκτελούμε την εντολή:

```
# dpkg-reconfigure mysql-server-5.0
```

Ως database root password δίνουμε το ίδιο ακριβώς με το root password του server.

Για λόγους ασφαλείας η default εγκατάσταση εχεί ενεργοποιημένη την πρόσβαση μόνο μέσω localhost. Η ενεργοποίηση της remote πρόσβασης γίνεται κάνοντας comment out την γραμμή του αρχείου `/etc/mysql/my.cnf`:

```
bind-address = 127.0.0.1
```

Η χρήση του UTF-8 για όλες τις νέες βάσεις και τους νέους πίνακες πρέπει να είναι δεδομένη. Προσθέτουμε την παρακάτω γραμμή στις ενότητες [mysql] και [mysqld] του ίδιου αρχείου:

```
default-character-set=utf8
```

Εξ΄ορισμού η MySQL τρέχει με ενεργοποιημένο το binary log. Αυτό σπαταλά σημαντικό χώρο στο root partition του server, και αν δεν χρησιμοποιείται το replication, προτείνεται η απενεργοποίησή του κάνοντας comment out τις γραμμές:

```
#log_bin = /var/log/mysql/mysql-bin.log
#expire_logs_days = 10
#max_binlog_size = 100M
```

Η MySQL φτιάχνει ένα και μοναδικό αρχείο ibdata1 με τα δεδομένα όλων των πινάκων. Αυτό δυσχεραίνει την δουλειά του διαχειριστή καθώς δεν μπορεί να επέμβει στον τρόπο που αποθηκεύονται τα δεδομένα. Προτείνεται η χρήση του InnoDB File Per Table όπως περιγράφεται στα εγχειρίδια της MySQL. Προσθέτουμε την παρακάτω γραμμή στην ενότητα [mysqld] του αρχείου:

```
innodb_file_per_table
```

Τέλος ο χρήστης root δεν έχει δικαίωμα για απομακρυσμένη πρόσβαση. Αυτό αλλάζει δίνοντας:

```
# mysql -p
> GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY '<root password>' WITH GRANT OPTION;
> EXIT
```

Για να ισχύσουν οι αλλαγές πρέπει να γίνει restart ο MySQL server:

```
# /etc/init.d/mysql restart
```

Στην περίπτωση που θέλουμε η αποθήκευση των δεδομένων να γίνεται στο μεγάλο partition, πρέπει να

εκτελέσουμε κάποια βήματα ακόμα για την μεταφορά του φακέλου `/var/lib/mysql/`:

```
# /etc/init.d/mysql stop
# mv /var/lib/mysql /home
# ln -s /home/mysql /var/lib/mysql
# /etc/init.d/mysql start
```

3.5.3 - Java Development Kit (JDK)

Το πακέτο *sun-java6-jdk* της διανομής `testing` εγκαθιστά το Java Development Kit της Sun.

```
# aptitude install sun-java6-jdk
```

Σημειωτέον ότι για 64bit εγκαταστάσεις του S-AI Server, προς το παρόν ενδείκνυται η χρήση της 32bit έκδοσης της Sun, καθώς έχει υποδιπλάσεις απαιτήσεις σε μνήμη και είναι ταχύτερη στην εκτέλεση κυρίως μεγάλων εφαρμογών.

Για τις εφαρμογές που χρειάζονται ένα σωστά ορισμένο JAVA_HOME, πρέπει να προστεθούν οι παρακάτω γραμμές στο αρχείο `/etc/profile` :

```
JAVA_HOME="/usr/lib/jvm/java-1.6.0-sun"
export JAVA_HOME
```

3.5.4 - SOLR indexing server

Το πακέτο *solr-tomcat5.5* είναι διαθέσιμο στην διανομή `unstable`. Προτείνεται η μετάβαση σε `unstable` για την εγκατάστασή του (αλλάζοντας τις αναγκαίες γραμμές στο `/etc/apt/sources.list` και αμέσως μετά η επαναφορά σε `stable`

Το πακέτο δείχνει να έχει μερικά προβλήματα με το configuration του μετά την εγκατάσταση. Συγκεκριμένα τα αρχεία `/etc/solr/*` δεν γίνονται σωστά μετονομασία ώστε να αφαιρεθεί η προέκταση dpkg-new. Μόλις γίνει αυτό πρέπει να δοθεί η εντολή

```
dpkg_reconfigure tomcat5.5
```

για να ολοκληρωθεί σωστά η εγκατάσταση του tomcat.

Πριν την επανεκκίνηση του tomcat προτείνεται η ρύθμιση του αρχείου `/etc/solr/schema.xml` ανάλογα με την εφαρμογή. Πιθανώς να χρειαστεί η αφαίρεση του φακέλου `/var/lib/solr/data/index` ώστε να ξαναδημιουργηθεί το ευρετήριο.

Για να γίνεται η αποθήκευση του ευρετηρίου στο μεγάλο partition, μεταφέρουμε τον φάκελο `/var/lib/solr/`:

```
# /etc/init.d/tomcat5.5 stop
# mv /var/lib/solr /solr
# ln -s /home/solr /var/lib/solr
# /etc/init.d/tomcat5.5 start
```

4 - Παραρτήματα

4.1 - Χρήσιμα πακέτα Debian

Υπάρχουν αναρίθμητα πακέτα Debian που κάνουν την δουλειά του system administrator πιο εύκολη. Σε αυτό το παράρτημα παραθέτουμε μια επιλογή από πακέτα που χρειάζονται συχνά κατά τις εγκαταστάσεις server. Κανένα από τα πακέτα δεν χρειάζεται γραφικό περιβάλλον.

htop	Εναλλακτική παρουσίαση της γνωστής `top`
iptraf	Εμφάνιση της ροής δεδομένων από και προς τον server με χρήσιμα στατιστικά
mtr-tiny	Το ποιό όμορφο traceroute πρόγραμμα για ncurses
nmap	Scanner δικτύου με άπειρες δυνατότητες, το απόλυτο εργαλείο του network hacker
pciutils	Περιέχει την πολύ χρήσιμη `lspci`
unzip	Η εντολή `unzip`

4.2 - Drivers για hardware που δεν υποστηρίζει ο stock kernel

HSF/HCP (soft) modems	Απαιτούν non-free closed source drivers από την linuxant