Πλάνο υλοποίησης Virtual υποδομής για παροχή VPS (virtual private servers)

Ανδρέας Φιλίππου, Άντρη Μιχαηλίδου

Έκδοση 1η

20 Ιουνίου 2014

Περιεχόμενα

ΠΛΑΝΟ ΥΛΟΠΟΙΗΣΗΣ VIRTUAL ΥΠΟΔΟΜΗΣ ΓΙΑ ΠΑΡΟΧΉ VPS (VIRTUAL PRIVATE SERVERS)

ΣΚΟΠΟΣ ΕΡΓΟΥ

Σκοπός του έργου αυτού είναι η παροχή **VPS (Virtual Private Servers)** σε χρήστες του τμήματος με απλό και γρήγορο τρόπο. Επιπλέον τίθεται ως στόχος και η αυτοεξυπηρέτηση των χρηστών ούτως ώστε να μπορούν οι ίδιοι να δημιουργούν τις μηχανές τους με ασφαλή τρόπο.

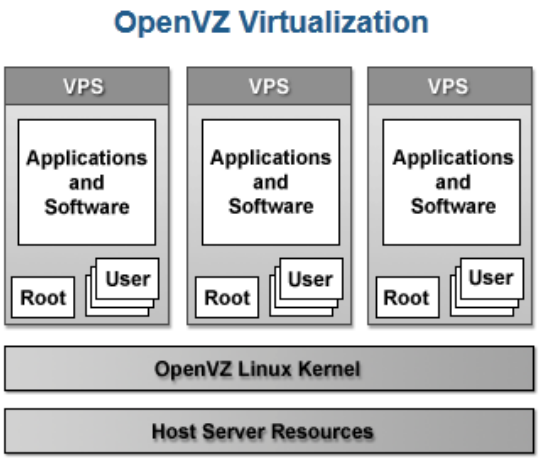
OPERATING SYSTEM-LEVEL VIRTUALIZATION

Για την υλοποίηση του σκοπού του έργου αποφασίστηκε όπως υιοθετηθεί operating system-level virtualization. Πρόκειται στην ουσία για τεχνολογία virtualization που χρησιμοποιούν αρκετοί **VPS** providers. Στην πραγματικότητα δεν πρόκειται για πλήρες Virtualization, δεν δημιουργούνται ανεξάρτητες εικονικές μηχανές, αλλά πλήρως απομονωμένα κελιά, καθένα από τα οποία τρέχει Linux και αυτό επιτρέπεται από τον πυρήνα του λειτουργικού συστήματος. Τα συστήματα εντός των κελιών μοιράζονται τον ίδιο πυρήνα, πρόκειται δηλαδή στην ουσία σαν εξελιγμένα root jails.

Αυτά τα απομονωμένα στιγμιότυπα, θεωρούνται σαν user space instances, φέρουν την ονομασία containers, virtualization engines (VE), **virtual private servers (VPS)** ή αλλιώς jails. Από την πλευρά του ο χρήστης ή ο owner του κελιού, έχει την εντύπωση αλλά και την ελευθερία που του παρέχει το περιβάλλον ενός server με δικαιώματα root. Στα UNIXοειδή λειτουργικά συστήματα αυτή η τεχνολογία μπορεί να θεωρηθεί ως μια προχωρημένη υλοποίηση του standard chroot μηχανισμού. Με την χρήση τέτοιου συστήματος βασικό προτέρημα είναι ότι η κατανάλωση της RAM είναι ελάχιστη, αφού το κάθε κελί δεν χρειάζεται να φορτώνει έναν ολόκληρο πυρήνα στην μνήμη, μαζί με τους απαραίτητους device drivers. Όλα βρίσκονται ήδη στην μνήμη γιατί στην ουσία τα έχει

φορτώσει το host OS και επομένως δεν χρειάζεται να δημιουργηθούν αντίγραφα. Επιπρόσθετα η διαχείριση των εικονικών μηχανών γίνεται εύκολα και ταχύτατα. Μπορείς να τρέχεις *πολλές* εικονικές μηχανές, σε ένα σύστημα με πραγματικά περιορισμένους πόρους.

OPENVZ - ΓΕΝΙΚΗ ΕΙΚΟΝΑ

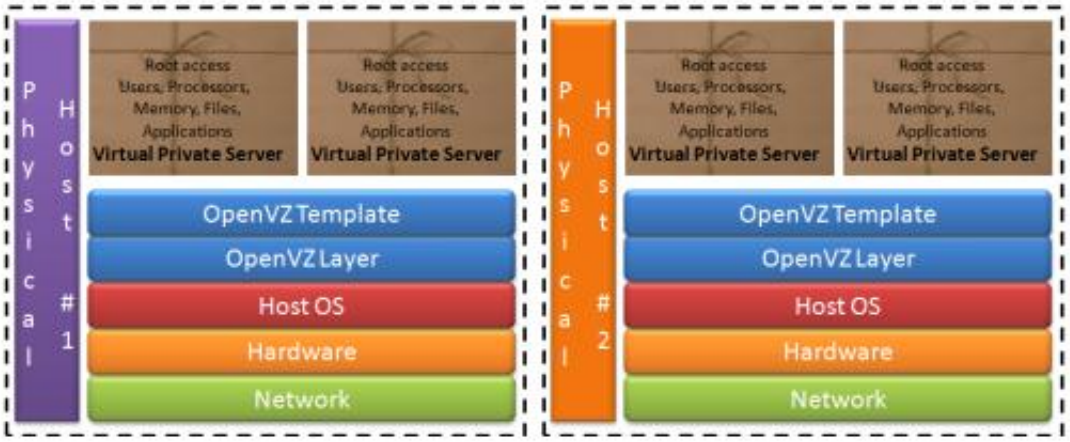


Απαραίτητος κανόνας είναι ότι όλα τα εικονικά μηχανήματα θα πρέπει να τρέχουν Linux. Ο περιορισμός αυτός επιβάλλεται από τον τρόπο λειτουργίας του OpenVZ. Κάθε virtual machine του OpenVZ αποτελεί ένα ξεχωριστό κελί και εκτελείται αυτόνομα από το υπόλοιπο σύστημα.

Σημαντικό είναι ότι όλα τα κελιά μοιράζονται τον ίδιο πυρήνα. Με το OpenVZ μπορούμε να δημιουργούμε εικονικές μηχανές οι οποίες θα τρέχουν οποιαδήποτε διανομή Linux. Στις εικονικές μηχανές του OpenVZ δεν πραγματοποιείται κάποιου είδους εγκατάσταση του λετουργικού. Το OpenVZ δημιουργεί εικονικές μηχανές κάνοντας στην ουσία χρήση έτοιμων προτύπων - templates. Κάθε template αποτελεί ουσιαστικά ένα archive με τα αρχεία της εκάστοτε διανομής. Στην ακόλουθη σελίδα υπάρχουν templates που έχουν δημιουργήσει οι προγραμματιστές του OpenVZ καθώς επίσης και άλλα templates που έχουν συνεισφέρει προγραμματιστές και χρήστες (contributed): http://wiki.openvz.org/Download/template/precreated

.

Αρχιτεκτονική του OpenVZ



ΓΙΑΤΙ OPENVZ?

Έχει επίσης μελετηθεί σε θεωρητικό επίπεδο και η μέθοδος **LXC (LinuX Containers),** η οποία υπάγεται στην κατηγορία του operating system-level virtualization, αλλά δεν έχει επιλεχθεί για υιοθέτηση καθώς είναι ακόμη σε νηπιακό στάδιο.

Το **OpenVZ** χρησιμοποιείται ευρέως και γίνεται develop για περισσότερα από 8 χρόνια και θεωρείται πιο ώριμο σύστημα από το LXC. Παρόλα αυτά το πρώτο stable release του LXC ολοκληρώθηκε τον Φεβρουάριο και είναι πολύ υποσχόμενο σύστημα. Ίσως στο μέλλον και αφότου ωριμάσει αρκετά το LXC να μελετηθεί εκ νέου η επιλογή αυτή για παροχή VPS.

ΥΛΟΠΟΙΗΣΗ ΈΡΓΟΥ - ΣΤΟΧΟΙ

Η υλοποίηση virtual υποδομής η οποία θα στηρίζεται στο OpenVZ, θα ολοκληρωθεί σταδιακά και μέσα σε πλαίσιο τριών φάσεων υλοποίησης του έργου.

Ο διαχωρισμός της υλοποίησης του έργου virtual υποδομής OpenVZ και η σύνθεση του σε τρείς φάσεις, θα προσδώσει σε καλύτερη μελέτη προς την υλοποίηση του τελικού

έργου, αλλά και στον εντοπισμό καλύτερων λύσεων στα προβλήματα που θα συναντηθούν κατά την υλοποίηση της κάθε επιμέρους φάσης.

Στο γενικότερο πλαίσιο υλοποίησης της virtual υποδομής θα δοθεί έμφαση στην ασφάλεια των συστημάτων για να μην μπορεί η ιδεατή υποδομή να επηρεάζει είτε τις υπάρχουσες υποδομές ή άλλα συστήματα εντός και εκτός ΠΚ.

1η Φάση – Γενική Περιγραφή Στόχου Υλοποίησης

Δημιουργία με απλό και γρήγορο τρόπο ιδεατών μηχανών που θα παραχωρούνται σε χρήστες (ερευνητές ή και φοιτητές).

2η Φάση – Γενική Περιγραφή Στόχου Υλοποίησης

Δημιουργία από χρήστες δικών τους μηχανών με βάση πολιτική και διαδικασίες που θα δημιουργηθούν.

3η Φάση – Γενική Περιγραφή Στόχου Υλοποίησης

Συμπερίληψη ιδέας του myCS portal στην πιο πάνω υλοποίηση. Αναθεώρηση και βελτιστοποίηση του συστήματος.

Στη συνέχεια του εγγράφου αυτού αναλύονται οι φάσεις που αναφέρονται πιο πάνω, περιλαμβάνοντας και όλες τις απαραίτητες παραμέτρους που καθορίζονται για την κάθε μία.

1Η ΦΑΣΗ ΥΛΟΠΟΙΗΣΗΣ ΤΗΣ VIRTUAL ΥΠΟΔΟΜΗΣ OPENVZ

Η 1η φάση περιλαμβάνει την εγκατάσταση Centos 6.5 σε μηχανή 64bit και την διενέργεια των απαραίτητων ρυθμίσεων για την λειτουργία του OpenVZ όπως καθορίζεται από τους στόχους πιο κάτω.

ΣΤΟΧΟΙ 1ΗΣ ΦΑΣΗΣ

- Δημιουργία με απλό και γρήγορο τρόπο εικονικών μηχανών από τον διαχειριστή του συστήματος - Άμεση παροχή εικονικών μηχανών
- Διαχείριση του OpenVZ node από τον διαχειριστή του συστήματος
- Εποπτεία του συστήματος

ΑΝΑΛΥΣΗ ΣΥΣΤΗΜΑΤΟΣ

Πιο κάτω αναφέρονται και αναλύονται οι ρυθμίσεις για τις πιο σημαντικές παραμέτρους του συστήματος.

HARD DISKS

Για την ομαλή λειτουργία προτείνεται όπως ο host έχει 2 δίσκους με configuration RAID 1. Εάν δεν παρέχεται RAID controller τότε θα ενεργοποιηθεί software raid.

FILE SYSTEM

Για την λειτουργία του OpenVZ χρειάζεται όπως υπάρχει ένα **/vz ξεχωριστό partition** στη μηχανή για την αποθήκευση των εικονικών μηχανών, των templates και των backups.

Προτείνεται όπως στην φάση αυτή να χρησιμοποιηθεί ο τοπικός δίσκος της μηχανής που θα εξυπηρετεί το OpenVZ, νοουμένου ότι ο ελεύθερος χώρος για τον σκοπό αυτό είναι τουλάχιστον 100GB. Το /vz θα δημιουργηθεί σε ξεχωριστό volume group.

Download των απαραίτητων templates, στην μηχανή host , προεργασία από admin (/vz/template/cache)

- centos-6-x86_64.tar.gz (signature)
- debian-7.0-x86_64.tar.gz (signature)
- fedora-20-x86_64.tar.gz (signature)

- scientific-6-x86_64.tar.gz (signature)
- suse-13.1-x86_64.tar.gz (signature)
- ubuntu-14.04-x86_64.tar.gz (signature)

QUOTA

Από δοκιμές που έχουν γίνει στο πρωτότυπο cs992 φαίνεται ότι κάθε μηχανή ακόμη και με αρκετά πακέτα εγκατεστημένα δεν ξεπερνά το 1GB σε μέγεθος. Προτείνεται όπως για αρχή ξεκινήσουμε να παρέχουμε την υπηρεσία με **quota 2GB ανά μηχανή**.

NETWORK

Όσον αφορά την δικτύωση των μηχανών προτείνεται όπως δημιουργηθεί **ένα νέο εσωτερικό VLAN** και όλες οι εικονικές μηχανές τοποθετηθούν εκεί.
Το VLAN αυτό θα είναι **περιορισμένο** για την καλύτερη ασφάλεια της υποδομής του τμήματος. Ο περιορισμός αυτός θα συμφωνηθεί με τον αρμόδιο για θέματα δικτύου. Προτείνεται όπως είναι εντελώς αποκλεισμένο από όλα τα εσωτερικά δίκτυα, ενώ για πρόσβαση για updates και άλλη πρόσβαση προς τα έξω να δίδεται πρόσβαση μόνο μέσω του proxy.
Εάν χρειαστεί στη συνέχεια μπορούμε να ανοίξουμε από συγκεκριμένα IPs των VPS την πρόσβαση στα δικά τους ερευνητικά εργαστήρια.

Όσον αφορά την διαμόρφωση για την παροχή δικτύου προτείνεται όπως χρησιμοποιηθεί **Virtual Ethernet Device (veth) με χρήση bridge.** [1] [2] [3]

Η χρήση **Virtual Network Device (venet),** η οποία είναι και η default δεν προτείνεται στην δική μας περίπτωση λόγω των περιορισμών που έχει. (Παροχή MAC address, VPS network administration κλπ.) [4]**,** [5]

Στην 1^{η} φάση όλες οι μηχανές που θα παρέχονται θα είναι καθαρά για ερευνητικούς και διδακτικούς σκοπούς και η πρόσβαση θα είναι μόνο από το εσωτερικό δίκτυο**.**

Στην 2η φάση θα μελετηθεί κατά πόσον μπορούμε να παρέχουμε μηχανές σε δίκτυα που είναι διαθέσιμα και από το εξωτερικό δίκτυο (πχ DMZ) και κατά πόσον είναι ασφαλές, τόσο για την υποδομή και συστήματα του Πανεπιστημίου, όσο και για τα συστήματα εκτός Πανεπιστημίου.

WEB INTERFACE

Για την 1η φάση του έργου προτείνεται όπως χρησιμοποιήσουμε **το OpenVZ Web Panel**, το οποίο και δοκιμάστηκε. Πρόσβαση στο interface αυτό θα έχει μόνο ο διαχειριστής της υποδομής OpenVZ για εύκολη διαχείριση των εικονικών μηχανών.

Το OpenVZ Web Panel είναι OpenSource σύστημα και προτείνεται ως web interface control panel από το OpenVZ. [6]

BACKUP

Προτείνεται όπως στην 1η φάση παρέχεται μόνο ένα daily backup για τις εικονικές μηχανές, το οποίο by default γίνεται αυτόματα με cron job στον host. Για κάθε εικονική μηχανή υπολογίζεται ότι χρειάζεται όσος χώρος καταλαμβάνει και για το backup. πχ. εικονική μηχανή 512MB χρειάζεται περίπου 512MB χώρο για το backup της.

Το backup σχεδιάζεται όπως μελετηθεί ενδελεχώς στην 2η φάση του έργου, σε συνδυασμό ίσως και με το TSM.

MONITORING

Για την 1η φάση του έργου προτείνεται όπως το Monitoring των VPS γίνεται με την χρήση του **Nagios** όπου είναι σύστημα ήδη εγκατεστημένο και σε χρήση στο τμήμα. Το monitoring θα αφορά την παρακολούθηση για υπερκατανάλωση πόρων, το οποίο μπορεί να γίνει εύκολα με την παρακολούθηση των **"/proc/user_beancounters"** [7] Εάν κριθεί απαραίτητο μπορεί επίσης να γίνεται monitor και το bandwidth. [8] Ενδεικτικά αναφέρεται το πακέτο vzmonitor [9]

2η ΦΑΣΗ ΥΛΟΠΟΙΗΣΗΣ ΤΗΣ VIRTUAL ΥΠΟΔΟΜΗΣ OPENVZ

Η 2η φάση περιλαμβάνει την δημιουργία υποδομής έτσι ώστε οι ίδιοι οι χρήστες να είναι σε θέση να δημιουργούν τις δικές τους εικονικές μηχανές. Στη φάση αυτή θα πρέπει επίσης να καθοριστούν όλες οι διαδικασίες που θα ακολουθούνται για τον σκοπό αυτό.

Η πολιτική θα περιλαμβάνει στοιχεία όπως:

- Ποιοι δικαιούνται VPS
- Οι VPS τι προδιαγραφές θα έχουν
- Σε ποια δίκτυα θα είναι ενωμένες
- Ποιο το εύρος ζωής των μηχανών (expiry)
- Πρόσβαση σε διαφορετικά OpenVZ nodes αναλόγως κατηγοριών (Φοιτητές, Ερευνητές, Καθηγητές)
- κλπ

Ο καθορισμός της πολιτικής και των διαδικασιών θα κριθούν από τις ανάγκες του τμήματος, αλλά και την εξέλιξη της 1ης φάσης του έργου.

ΣΤΟΧΟΙ 2ΗΣ ΦΑΣΗΣ

- Καθορισμός πολιτικής και διαδικασιών
- Δημιουργία υποδομής για δημιουργία εικονικών μηχανών από τους χρήστες
  - Ασφάλεια συστημάτων και υποδομής
  - Εποπτεία της κίνησης, φιλτράρισμα
  - Web interface διαχείριση
  - Traffic Shaping

ΑΝΑΛΥΣΗ ΣΥΣΤΗΜΑΤΟΣ

Πιο κάτω αναφέρονται και αναλύονται οι ρυθμίσεις για τις πιο σημαντικές παραμέτρους του συστήματος.

FILE SYSTEM

Από την εμπειρία που θα μας παρέχει η υλοποίηση της 1ης φάσης θα αποφασιστεί κατά πόσον το **/vz ξεχωριστό partition** είναι προτιμότερο να παρέχεται από κάποιο κεντρικό storage αντί για τον τοπικό δίσκο του host. Αυτό θα εξαρτηθεί και από τη ζήτηση που θα έχουμε για τη δημιουργία μηχανών, αλλά και άλλους παράγοντες όπως το backup και το performance.

WEB INTERFACE

Στην φάση αυτή θα μελετηθούν άλλα web interfaces, τα οποία μπορούν να ενσωματωθούν στην υποδομή και με χρήση και άλλων συστημάτων υποδομής όπως για παράδειγμα το LDAP. Θα πρέπει να μπορεί να υποστηρίξει authentication αλλά και authorization αν είναι δυνατόν, με βάση το group ή άλλες παραμέτρους σε χρήστες για δημιουργία μηχανών. Για την υιοθέτηση του web interface πρέπει να ληφθεί υπόψη και ο στόχος της 3ης φάσης που είναι η συμπερίληψη της διαχείρισης ή μέρος της από το myCSportal.

Θα προτιμηθεί μια Open source λύση εάν παρέχει όσα χρειάζονται, αλλά πιθανό ενδεχομένως να μελετηθούν και λύσεις εμπορικές. [6] [10]

Ενδεικτικά αναφέρονται τα **OpenNode** [7], Proxmox [7], SolusVM, Plesk κλπ.

BACKUP

Στην φάση αυτή θα μελετηθεί ενδελεχώς το backup σύμφωνα με τις ανάγκες που θα προκύψουν. Σε συνδυασμό και με τον TSM θα αποφασιστεί κατά πόσον θα συνεχίσουμε με ένα ή περισσότερα daily backup για τις εικονικές μηχανές, καθώς και τον χώρο που θα αποθηκεύονται.

NETWORK

Στην φάση αυτή θα μελετηθεί κατά πόσον μπορούμε να παρέχουμε μηχανές σε δίκτυα που είναι διαθέσιμα και από το εξωτερικό δίκτυο (πχ DMZ) και κατά πόσον είναι

ασφαλές, τόσο για την υποδομή και συστήματα του Πανεπιστημίου, όσο και για τα συστήματα εκτός Πανεπιστημίου.

Βασικό στην νέα υποδομή του OpenVZ virtualization να λειτουργεί ένα είδος παρακολούθησης/φιλτραρίσματος της κίνησης του δικτύου.

Για να καταστεί αυτό δυνατόν και να είναι ασφαλές και για την υποδομή εντός και εκτός Πανεπιστημίου πιθανό να χρειαστεί να εγκατασταθεί/χρησιμοποιηθεί και κάποιο σύστημα IPS/IDS ή software firewall (pfSense), όπου σε συνάρτηση με το monitoring θα βοηθά στην αποτροπή κακόβουλων ενεργειών. Το pfsense φέρει με την εγκατάσταση του ένα web interface το οποίο εκτός από πλήρεις υπηρεσίες Firewall συμπεριλαμβάνει ταυτόχρονα κατάλληλη διαχείριση δημοφιλών third party πακέτων λογισμικού για επιπρόσθετα functionalities, ένα εκτων οποίων και portal το οποίο μπορείς να επεξεργαστείς κατάλληλα με προσθήκες κώδικα.

Η Ιδέα αφορά την υιοθέτηση ενός ξεχωριστού firewall, υπεύθυνου για τις μηχανές εντός του OpenVZ – LAN, όπου θα μπορεί να καλύψει εκτός από υπάρχουσες και μελλοντικές ανάγκες χωρίς να επηρεάζονται ρυθμίσεις σε υπάρχουσα υποδομή που βρίσκεται σε λειτουργία.

Το σημείο αυτό χρειάζεται αρκετή μελέτη σε πολλά επίπεδα γι’ αυτό και τοποθετήθηκε στη 2^{η} φάση του έργου.

MONITORING

Από την εμπειρία που θα μας παρέχει η υλοποίηση της 1^{ης} φάσης και το Monitoring όπως καθορίστηκε στην φάση αυτή, θα εξαρτηθεί κατά πόσον θα χρειαστεί να επεκταθεί και στην παρακολούθηση άλλων παραμέτρων.

3Η ΦΑΣΗ ΥΛΟΠΟΙΗΣΗΣ ΤΗΣ VIRTUAL ΥΠΟΔΟΜΗΣ OPENVZ

Στην 3η φάση θα μελετηθεί το ενδεχόμενο συμπερίληψης της υποδομής αυτής και του web interface control panel, **myCSportal**, ούτως ώστε οι χρήστες να μπορούν να δουν τις εικονικές τους μηχανές και να εκτελέσουν σχετικές ενέργειες. Επιπλέον θα αναθεωρηθεί εκ νέου το σύστημα που δημιουργήθηκε για βελτιστοποίηση και βελτίωση του.

ΣΤΟΧΟΙ 3ΗΣ ΦΑΣΗΣ

- Συμπερίληψη ιδέας του myCS portal στην πιο πάνω υλοποίηση.
- Αναθεώρηση και βελτιστοποίηση του συστήματος.

ΑΝΑΛΥΣΗ ΣΥΣΤΗΜΑΤΟΣ

Πιο κάτω αναφέρονται και αναλύονται οι ρυθμίσεις για τις πιο σημαντικές παραμέτρους του συστήματος.

MYCSPORTAL

Η συμπερίληψη του **myCSportal** στην πιο πάνω υλοποίηση αφορά ουσιαστικά στην παροχή από το web interface κάποιου API που να μπορεί να καλείται από την σελίδα του portal (php) και μέσω του να μπορούν να διενεργηθούν ενέργειες με τις εικονικές μηχανές. Εαν αυτό δεν είναι εφικτό από το web interface που θα υιοθετηθεί, θα γίνουν προσπάθειες με custom κώδικα να παρέχονται τουλάχιστον οι βασικές πληροφορίες και για να διενεργηθούν ενέργειες στις εικονικές μηχανές να παρέχετε το Link είτε απευθείας είτε με iframe στο web interface.

OPTIMIZATION

Με την ολοκλήρωση του συστήματος θα πρέπει να γίνει μια ανασκόπηση σε όλες τις παραμέτρους και κυρίως το δίκτυο και την ασφάλεια για βελτιστοποίηση του.

REFERENCES

[1] “openvz.org,” [Online]. Available: https://openvz.org/Veth. [Accessed 06 2014].

[2] “openvz.org,” [Online]. Available: https://openvz.org/Common_Networking_HOWTOs. [Accessed 06 2014].

[3] “openvz.org,” [Online]. Available: https://openvz.org/VEs_and_HNs_in_same_subnets. [Accessed 06 2014].

[4] “openvz.org,” [Online]. Available: https://openvz.org/Virtual_network_device. [Accessed 06 2014].

[5] “openvz.org,” [Online]. Available: https://openvz.org/Differences_between_venet_and_veth. [Accessed 06 2014].

[6] “openvz.org,” [Online]. Available: http://openvz.org/Control_panels. [Accessed 06 2014].

[7] [Online]. Available: https://github.com/peletiah/openvz. [Accessed 06 2014].

[8] “openvz.org,” [Online]. Available: https://openvz.org/Category:Monitoring. [Accessed 06 2014].

[9] “vzmonitor,” [Online]. Available: http://linuxczar.com/vzmonitor/. [Accessed 06 2014].

[10] A. Kovari and P. Dukan, “KVM & OpenVZ virtualization based IaaS open source cloud virtualization platforms: OpenNode, Proxmox VE,” *Intelligent Systems and Informatics (SISY), 2012 IEEE 10th Jubilee International Symposium on , vol., no., 20-22 Sept. 2012,* pp. 335-339, 2012.