Αναβάθμιση Windows εξυπηρετητών και μεταφορά τους σε εικονικό περιβάλλον

Περίληψη

Σκοπός του έργου είναι η αναβάθμιση της υποδομής Windows του Τμήματος Πληροφορικής σε έκδοση Windows Server 2012/R2 και η μεταφορά των μηχανών σε εικονικό περιβάλλον. Επίσης, θα γίνει αναδιοργάνωση των υπηρεσιών με τέτοιο τρόπο για να διασφαλισθεί η ασφάλεια των συστημάτων, π.χ. μεταφορά όλων των εξυπηρετητών σε εσωτερικό δίκτυο και χρήση της DMZ για υπηρεσίες που είναι προσβάσιμες από εξωτερικά δίκτυα, διαχωρισμός υπηρεσιών υποδομής από τις υπηρεσίες που είναι διαθέσιμες στους φοιτητές για ανάπτυξη λογισμικού. Με την ολοκλήρωση του έργου, αναμένεται επίσης να ετοιμασθεί ένα γενικό πλαίσιο για την εγκατάσταση και διαχείριση των Windows εξυπηρετητών.

Υπάρχουσα κατάσταση

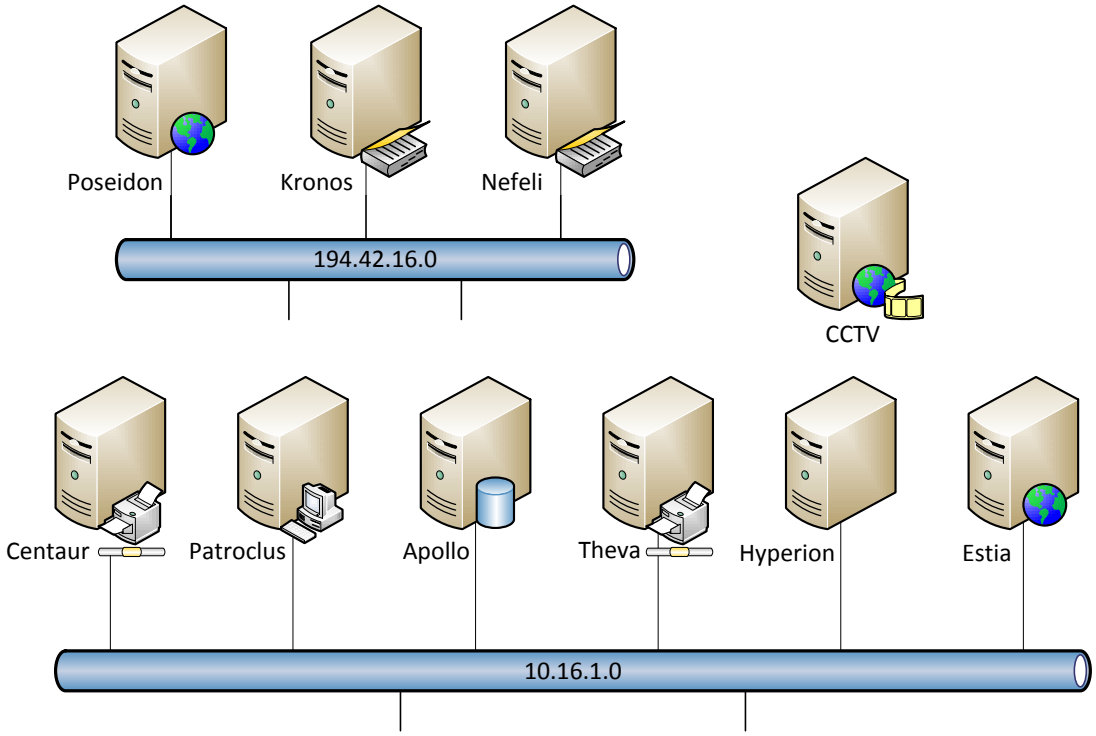
Στο Τμήμα σήμερα λειτουργούν 10 εξυπηρετητές με λειτουργικό σύστημα Windows Server. Στον πιο κάτω πίνακα αναγράφονται τα ονόματα των εξυπηρετητών, η έκδοση του λειτουργικού που χρησιμοποιούν, καθώς και οι υπηρεσίες που προσφέρουν.

Α/Α	Εξυπηρετητής	Έκδοση Λειτουργικού	Υπηρεσίες
1	Kronos	Windows Server 2003	Active Directory Domain Controller, AD DNS
2	Nefeli	Windows Server 2003	Active Directory Domain Controller, AD DNS, Windows Server Update Services
3	Poseidon	Windows Server 2008 R2	Internet Information Services (IIS) 7.5
4	Apollo	Windows Server 2008 R2	Microsoft SQL Server 2008
5	Centaur	Windows Server 2003 R2	Primary Print Server, Sophos Antivirus
6	Patroclus	Windows Server 2003 R2	License Server for MATLAB, XILINX, MODELSIM
7	Theva*	Windows Server 2012	Secondary Print Server, License Server for OPNET
8	Hyperion*	Windows 2008	Symantec Endpoint Protection Manager
9	Estia*	Windows 2008 R2	Microsoft SharePoint
10	CCTV**	Windows Server 2008	CCTV Server using GeoVison GV-DVR

Πίνακας 1: Windows εξυπηρετητές στο Τμήμα Πληροφορικής

* Εικονικός εξυπηρετητής ** Δεν υπάρχει σύνδεση στο δίκτυο

Όπως διαφαίνεται από τον Πίνακα 1, οι περισσότεροι εξυπηρετητές τρέχουν λειτουργικό σύστημα Windows Server 2003. Το ότι η έκδοση είναι παλιά δεν δημιουργεί κενό ασφαλείας, αφού οι εξυπηρετητές ανανεώνονται συστηματικά.



Σχήμα 1: Υπάρχουσα συνδεσμολογία στο δίκτυο

Active Directory (AD)

Το μεγαλύτερο πρόβλημα που παρουσιάζεται με την υπηρεσία AD είναι ή ασφάλεια των εξυπηρετητών Kronos και Nefeli, αφού όπως φαίνεται από το Σχήμα 1 οι Domain Controllers βρίσκονται σε public δίκτυο. Ο εξυπηρετητής Nefeli φιλοξενεί την υπηρεσία WSUS που για την λειτουργία της χρειάζεται την ενεργοποίηση του ρόλου IIS, που δεν ενδείκνυται να ενεργοποιείται σε εξυπηρετητές που είναι Domain Controllers. Επίσης, η σχετικά παλιά έκδοση του AD δεν μας επιτρέπει να χρησιμοποιήσουμε κάποιες από τις νέες δυνατότητες των Windows 7/8 (π.χ. νέα Group Policies) που δεν υποστηρίζονται από την υφιστάμενη έκδοση των Active Directory Domain Controller μας.

Υπηρεσίες εκτυπώσεων

Οι εξυπηρετητές Centaur και Theva υποστηρίζουν τις υπηρεσίες εκτυπώσεων σε συνεργασία με το λογισμικό PaperCut, που διαχειρίζεται τους περιορισμούς. Πρόσφατα ο εξυπηρετητής Theva αναβαθμίστηκε σε Windows Server 2012 δίνοντας μας την δυνατότητα να υποστηρίζουμε οδηγούς εκτυπωτών 64-bit. Ο εξυπηρετητής Cenetaur δεν έχει αυτή την δυνατότητα και αυτό δυσκολεύει την διαχείριση των νέων υπολογιστών που τρέχουν 64-bit λειτουργικό.

Εφαρμογές ιστού

Η υπάρχουσα υποδομή για εφαρμογές ιστού υποστηρίζεται από τους εξυπηρετητές Poseidon (IIS) και Apollo (MSSQL). Στο πιο κάτω πίνακα καταγράφονται οι εφαρμογές ιστού που τρέχουν στον Poseidon.

Α/Α	Εφαρμογή	Υπεύθυνος	Τύπος	Ημ. Λύξης
1	adaptiveweb	Γ. Σαμάρας	Ερευνητικό Πρόγραμμα	
2	adaptivewebmobile	Γ. Σαμάρας	Ερευνητικό Πρόγραμμα	
3	adaptivewebplus	Γ. Σαμάρας	Ερευνητικό Πρόγραμμα	
4	adaptivewebsystem	Γ. Σαμάρας	Ερευνητικό Πρόγραμμα	
5	bankdata		Διπλωματική Εργασία	
6	cardiacm	Κ. Παττίχης	Ερευνητικό Πρόγραμμα	
7	csresearchprograms		Διπλωματική Εργασία	
8	cyprusbusroutes	Π. Ευριπίδου	Διπλωματική Εργασία	12/2013
9	ditis3	Α. Πιτσιλλίδης	Ερευνητικό Πρόγραμμα	
10	ekpaideion	Γ. Σαμάρας	Ερευνητικό Πρόγραμμα	
11	ema			
12	epanag09	Γ. Πάλλης		05/2013
13	eumas09	Γ. Σαμάρας	Συνέδριο	
14	firewatch	Γ. Σαμάρας	Ερευνητικό Πρόγραμμα	
15	gymnasialikeia		Διπλωματική Εργασία	
16	ict2011	Α. Πιτσιλλίδης	Συνέδριο	
17	melco			
18	mesarch			
19	pads	Α. Φιλίππου	Διπλωματική Εργασία	
20	philotimo			
21	professor2student professor2studentWS	Γ. Καπιτσάκη	Διπλωματική Εργασία	09/2013
22	scrat	Γ. Σαμάρας	Ερευνητική Ομάδα	
23	smartag	Γ. Σαμάρας	Ερευνητικό Πρόγραμμα	
24	socialelectricity socialelectricitynew socialelectricityWSnew	Α. Πιτσιλλίδης	Ερευνητικό Πρόγραμμα	
25	task		Διπλωματική Εργασία	

Πίνακας 2: Εφαρμογές ιστού που τρέχουν στον Poseidon

Σημείωση: Ο λόγος που δεν είναι συμπληρωμένα όλα τα πεδία στον πιο πάνω πίνακα, είναι γιατί δεν ήταν διαθέσιμο το file που αποθηκεύονται οι αιτήσεις (το πιθανότερο να είναι στο γραφείο της Άντρης που απουσιάζει).

Η συγκεκριμένη υπηρεσία δεν παρουσίασε οποιαδήποτε λειτουργικά προβλήματα μέχρι σήμερα χωρίς να σημαίνει ότι δεν υπάρχουν περιθώρια βελτίωσης. Για παράδειγμα, τα αρχεία των πιο πάνω εφαρμογών αποθηκεύονται τοπικά στον Poseidon, και είναι προσβάσιμα με CIFS μόνο από το εσωτερικό δίκτυο. Η χρήση VPN δίνει την δυνατότητα απομακρυσμένης πρόσβασης είναι όμως σχετικά δύσκολο να ρυθμιστεί ο απομακρυσμένος υπολογιστής όταν δεν είναι μέλος του AD domain. Επίσης, δεν υπάρχει διαχωρισμός των εφαρμογών υποδομής (συνέδρια, ερευνητικά προγράμματα) από τις ασκήσεις των φοιτητών.

Βάσεις δεδομένων

Ο εξυπηρετητής Apollo είναι ο MS SQL του Τμήματος. Εκτός από τις βάσεις που εξυπηρετούν τις ανάγκες των εφαρμογών ιστού, χρησιμοποιείται και για την διδασκαλία του μαθήματος ΕΠΛ342, και γι' αυτό τον σκοπό δημιουργούνται περίπου 90-95 βάσεις. Στον πιο κάτω πίνακα αναγράφονται οι βάσεις που φιλοξενούνται στον εξυπηρετητή Apollo.

Α/Α	Βάση	Υπεύθυνος	Τύπος	Ημ. Λύξης
1	adaptiveweb	Γ. Σαμάρας	Ερευνητικό Πρόγραμμα	
2	armes			
3	bankdata		Διπλωματική Εργασία	
4	bigpubs2000	Π. Ανδρέου	Διδασκαλία Μαθήματος	
5	cardiacm	Κ. Παττίχης	Ερευνητικό Πρόγραμμα	
6	csreasearchprograms		Διπλωματική Εργασία	
7	cyprusbusroutes	Π. Ευριπίδου	Διπλωματική Εργασία	12/2013
8	ditis3	Α. Πιτσιλλίδης	Ερευνητικό Πρόγραμμα	
9	dzeina	Δ. Ζεϊναλιπούρ	Προσωπική	
10	ecoactnow			
11	edrug			
12	epkaideion	Γ. Σαμάρας	Ερευνητικό Πρόγραμμα	
13	ema			
14	epl342	Π. Ανδρέου	Διδασκαλία Μαθήματος	
15	firewatch	Γ. Σαμάρας	Ερευνητικό Πρόγραμμα	
16	gymnasialikeia		Διπλωματική Εργασία	
17	iccloud			
18	insuarance	Γ. Καπιτσάκη	Εργασία Μαθήματος	02/2014
19	lawcs	Γ. Παπαδόπουλος	Εργασία Μαθήματος	06/2014
20	medicalRecords	Π. Ευριπίδου	Διπλωματική Εργασία	05/2014
21	melco			
22	mesarch			
23	philotimo			
24	professor2student	Γ. Καπιτσάκη	Διπλωματική Εργασία	09/2013
25	scrat	Γ. Σαμάρας	Ερευνητική Ομάδα	
26	scrumble			
27	smartag	Γ. Σαμάρας	Ερευνητικό Πρόγραμμα	
28	socialelectricity socialelectricitynew	Α. Πιτσιλλίδης	Ερευνητικό Πρόγραμμα	
29	SOPHOS45	ΟΤΥ	Sophos Antivirus	
30	SUSDB	ΟΤΥ	Windows Update Services	
31	task		Διπλωματική Εργασία	

Πίνακας 3: Εφαρμογές ιστού που τρέχουν στον Poseidon

Σημείωση: Οι βάσεις που δημιουργούνται για την διδασκαλία του ΕΠΛ342 δεν αναγράφονται, αφού έχουν διαγραφεί και θα δημιουργηθούν για τους νέους φοιτητές τον ερχόμενο Σεπτέμβρη.

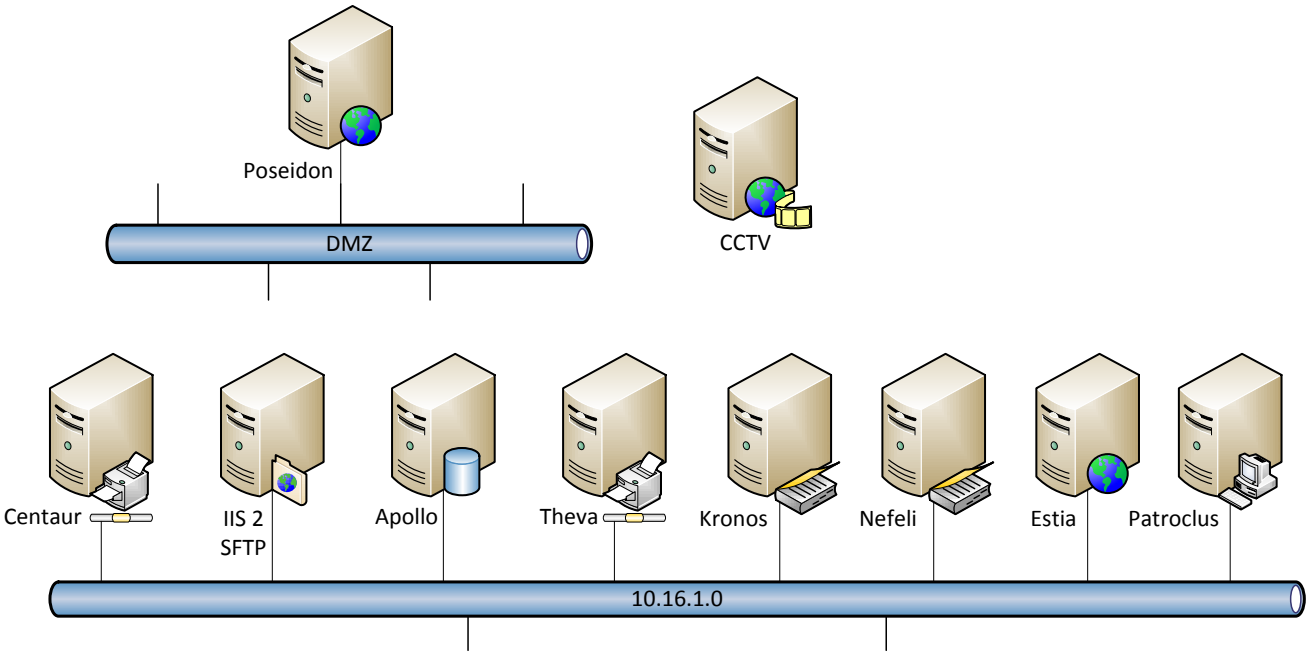
Microsoft SharePoint

Η συγκεκριμένη υπηρεσία τρέχει στον εξυπηρετητή Estia, που είναι η μοναδική εικονική μηχανή στο VMware vSphere. Η υπηρεσία ζητήθηκε από το προεδρείο για να καλύψει τις

ανάγκες διαμοιρασμού αρχείων και την ανάπτυξη λογισμικού στην συγκεκριμένη πλατφόρμα. Η υπηρεσία φαίνεται να χρησιμοποιείται σε περιορισμένο βαθμό για τον διαμοιρασμό αρχείων και καθόλου για την ανάπτυξη εφαρμογών.

Προτεινόμενη λύση

Πρωταρχικός σκοπός του έργου είναι η αναβάθμιση των εξυπηρετητών σε Windows Server 2012/R2 και η μεταφορά όσο το δυνατόν περισσότερων εξυπηρετητών σε εικονικό περιβάλλον για εξοικονόμηση πόρων. Επίσης, με τις αλλαγές που θα γίνουν θα βελτιωθεί η λειτουργικότητα των υπηρεσιών που προσφέρουμε. Το Σχήμα 2 περιγράφει τις αλλαγές που προτείνονται.



Σχήμα 2: Προτεινόμενη λύση

Οι σημαντικότερες αλλαγές που προτείνονται είναι:

- Μεταφορά Active Directory (Kronos/Nefeli) σε εσωτερικό δίκτυο
- Μεταφορά Poseidon στην DMZ
- Δημιουργία νέου εξυπηρετητή IIS, σε εσωτερικό δίκτυο, για την φιλοξενία εφαρμογών που είναι προσωρινές (π.χ. εργασίες μαθημάτων), και ενεργοποιήσει υπηρεσίας SFTP για την ανανέωση των αρχείων.
- Αναβάθμιση του monitoring, ώστε να μπορούμε να ελέγχουμε καλύτερα τους Windows εξυπηρετητές από τον Nagios, με την χρήση του NSClient ++.
- Δημιουργία κεντρικής σελίδας στο wiki με οδηγίες για τις σημαντικότερες ρυθμίσεις που αφορούν τους Windows εξυπηρετητές (παρόμοιο με το Linux installation).

Με το προτεινόμενο πλάνο ο διαμοιρασμός των υπηρεσιών θα γίνει ως ακολούθως:

Α/Α	Εξυπηρετητής	Έκδοση Λειτουργικού	Υπηρεσίες
1	Kronos	Windows Server 2012 R2	Active Directory Domain Controller, AD DNS
2	Nefeli	Windows Server 2012 R2	Active Directory Domain Controller, AD DNS
3	Poseidon	Windows Server 2012 R2	Internet Information Services (IIS) 8.5
4	Apollo	Windows Server 2012 R2	Microsoft SQL Server 2012
5	Centaur	Windows Server 2012 R2	Primary Print Server, Windows Server Update Services
6	IIS 2/SFTP	Windows Server 2012 R2	Internet Information Services (IIS) 8.5
7	Theva	Windows Server 2012	Secondary Print Server, License Server for OPNET, Symantec Endpoint Protection Manager
8	Estia*	Windows Server 2012 R2	Microsoft SharePoint for research
9	Patroclus**	Windows Server 2003 R2	License Server for MATLAB, XILINX, MODELSIM
10	CCTV	Windows Server 2008	CCTV Server using GeoVison GV-DVR

Πίνακας 4: Προτεινόμενος διαμοιρασμός υπηρεσιών

*Υπάρχει περίπτωση να μην εγκατασταθεί η συγκεκριμένη μηχανή σε περίπτωση που δεν υπάρχει ενδιαφέρον από τους ακαδημαϊκούς.

** Ο εξυπηρετητής δεν είναι εικονικός. Μετά από ελέγχους που έγιναν διαφάνηκε ότι δεν μπορεί να μεταφερθεί σε εικονικό περιβάλλον KVM το λογισμικό FLEXnet License Manager που υποστηρίζει τα προγράμματα XILINX, MATLAB, MODELSIM.

Active Directory

Με την αναβάθμιση του Active Directory στην έκδοση Windows Server 2012 μπορεί να μεταφέρουμε όλους τους Domain Controllers (Kronos, Nefeli) σε εικονικές μηχανές, κάτι που δεν ήταν δυνατό με τις προηγούμενες εκδόσεις. Υπάρχουν κάποια θέματα που χρίζουν περισσότερης διερεύνησης, π.χ. clock drift. Με την αναβάθμιση στην συγκεκριμένη έκδοση θα μπορούμε να χρησιμοποιήσουμε όλα τα group policies που αφορούν Windows 7/8, καθώς και την δημιουργία νέων λογαριασμών από οποιαδήποτε μηχανή χρησιμοποιώντας PowerShell.

Υπηρεσίες εκτυπώσεων

Με την αναβάθμιση του Centaur σε Windows Server 2012 θα μπορούν όλες οι Windows μηχανές που τρέχουν 64-bit λειτουργικό πρόγραμμα να χρησιμοποιούν τους οδηγούς που βρίσκονται στον εξυπηρετητή χωρίς να χρειάζεται να εγκαταστήσουν πρώτα τους οδηγούς εκτύπωσης στον υπολογιστή τους. Αυτή η δυνατότητα προσφέρεται ήδη από τον εξυπηρετητή Theva που τρέχει Windows Server 2012.

Εφαρμογές ιστού

Με την δημιουργία νέου IIS εξυπηρετητή θα μεταφερθούν όλες οι προσωρινές εργασίες των φοιτητών στον συγκεκριμένο εξυπηρετητή που δεν θα είναι προσβάσιμος από εξωτερικά δίκτυα. Η ίδια πρακτική χρησιμοποιείται ήδη στο Linux/Apache. Πρόσβαση στον συγκεκριμένο εξυπηρετητή θα επιτρέπεται μόνο με VPN. Επίσης στον νέο εξυπηρετητή θα ενεργοποιηθεί η υπηρεσία SFTP για να μπορούν οι φοιτητές να έχουν πρόσβαση στα web αρχεία τους χωρίς να χρειάζεται να είναι στο Τμήμα και να χρησιμοποιούν μηχανή εργαστηρίου. Ο ίδιος εξυπηρετητής θα χρησιμοποιείται για ανανέωση των αρχείων του web εξυπηρετητή που θα είναι στην DMZ. Για να μπορεί να γίνει αυτό θα πρέπει τα web αρχεία που μέχρι σήμερα αποθηκεύονταν τοπικά στον εξυπηρετητή να μεταφερθούν σε network share.

Βάσεις δεδομένων

Εκτός από την αναβάθμιση του λειτουργικού συστήματος και την αναβάθμιση του MS SQL στην τελευταία έκδοση δεν προτείνεται οποιαδήποτε αλλαγή στην συγκεκριμένη υπηρεσία.

Microsoft SharePoint

Όπως αναφέρθηκε και προηγούμενος το SharePoint υιοθετήθηκε για να καλύψει την ανάγκη διαμοιρασμού αρχείων και την ανάπτυξη εφαρμογών στην συγκεκριμένη πλατφόρμα. Για τον διαμοιρασμό αρχείων υπάρχει πλέον η υπηρεσία ownCloud που υπερκαλύπτει τις συγκεκριμένες ανάγκες. Επίσης, τα τελευταία δυο χρόνια που είναι εγκατεστημένο το SharePoint, δεν έγινε καμία ανάπτυξη λογισμικού στην συγκεκριμένη πλατφόρμα. Η άποψη μου είναι ότι δεν χρειάζεται πλέον να συντηρούμε την υπηρεσία. Προτού εισηγηθώ τον τερματισμό της υπηρεσίας, επικοινώνησα με το προεδρείο που ζήτησε αρχικά την εγκατάσταση του SharePoint, και εισηγήθηκα να μεταφέρουμε τα λίγα αρχεία που διαμοιράζονται στο ownCloud, κάτι που έγινε αποδεκτό. Το προεδρείο όμως ζήτησε όπως παραμείνει ζωντανή η πλατφόρμα για ανάπτυξη εφαρμογών. Με βάση τα πιο πάνω, μπορούμε να τερματίσουμε τον διαμοιρασμό αρχείων και σε συνεννόηση με του ακαδημαϊκούς να μεταφέρουμε τον εξυπηρετητή Estia σε περιβάλλον KVM σε περίπτωση που υπάρχει πραγματική ανάγκη για την υπηρεσία SharePoint.

Παρακολούθηση υποδομής Windows

Για την καλύτερη παρακολούθηση της υποδομής Windows, όλοι οι νέοι εξυπηρετητές θα παρακολουθούνται από την υπηρεσία Nagios, με την μέσω του λογισμικού NSClient++. Το συγκεκριμένο λογισμικό χρησιμοποιείται σε δοκιμαστική βάση τώρα στους εξυπηρετητές Apollo, Poseidon και Theva. Επίσης, θα διερευνηθεί ο τρόπος με τον οποίο θα γίνεται συλλογή των even logs από όλος τους Windows εξυπηρετητές σε κεντρικό σημείο.

Διαχείριση υποδομής Windows

Για την βελτίωση της διαχείρισης της υποδομής, θα δημιουργηθεί κεντρική σελίδα στο Wiki που θα καταγράφει την διαδικασία που πρέπει να ακολουθητέε για την εγκατάσταση και διαχείριση των Windows εξυπηρετητών.

Πλάνο αναβάθμισης

Ο πιο κάτω πίνακας απεικονίζει την σειρά με την οποία θα γίνει η αναβάθμιση και η μεταφορά των εξυπηρετητών στην προτεινόμενη μορφή:

Α/Α	Εξυπηρετητής	Χρόνοδιάγραμμα Αναβάθμισης
1	Centaur	Απρίλιος – Μάιος 2014
2	Kronos	Ιούνιος – Ιούλιος 2014
3	IIS 2/SFTP	Αύγουστος – Σεπτέμβριος 2014
4	Nefeli	Οκτώβριος – Νοέμβριος 2014
5	Poseidon	Δεκέμβριος 2014 – Ιανουάριος 2015
6	Apollo	Φεβρουάριος 2015 – Μάρτιος 2015