

Παραδοτέο

**Π3.2.1-α Πρώτη αναφορά καλής λειτουργίας των εγκαταστάσεων της
πλατφόρμας**

για το Υποέργο 1

**«Σχεδιασμός, ανάπτυξη και εγκατάσταση του πληροφοριακού συστήματος
και εργασίες τεχνικής συντήρησης»**

της Πράξης

**«Ενιαία Πλατφόρμα Δημιουργίας και Διάθεσης Ηλεκτρονικών
Συγγραμμάτων και Βοηθημάτων» με κωδικό MIS 389382**

Πίνακας Περιεχομένων

1	Οι εγκαταστάσεις της πλατφόρμας του Π.Σ. «Κάλλιπος»	3
1.1	Συνοπτική περιγραφή των διακομιστών των εγκαταστάσεων	4
1.1.1	Κύρια Εγκατάσταση.....	4
1.1.2	Εναλλακτική Εγκατάσταση	5
1.1.3	Δοκιμαστικό Περιβάλλον	5
1.1.4	Deployment περιβάλλον	5
1.1.5	Backup περιβάλλον.....	5
1.2	Συνοπτική περιγραφή του λογισμικού παρακολούθησης	6
2	Εργασίες για την εξασφάλιση της καλής λειτουργίας των εγκαταστάσεων.....	7
2.1	Τακτικές εργασίες για την καλή λειτουργία των εγκαταστάσεων	7
2.2	Επιπρόσθετες εργασίες για την καλή λειτουργία των εγκαταστάσεων.....	8
3	Αρχείο εργασιών για την εξασφάλιση της καλής λειτουργίας	9
3.1.1	Εργασίες 1 ^{ου} και 2 ^{ου} Τριμήνου 2013.....	9
3.1.2	Εργασίες 3 ^{ου} Τριμήνου 2013	10
3.1.3	Εργασίες 4 ^{ου} Τριμήνου 2013	12

1 Οι εγκαταστάσεις της πλατφόρμας του Π.Σ. «Κάλλιπος»

Για την καλή και απρόσκοπτη λειτουργία του Π.Σ. «Κάλλιπος» έχουν προβλεφθεί και έχουν τεθεί σε παραγωγική λειτουργία οι ακόλουθες εγκαταστάσεις διακομιστών:

- Κύρια Εγκατάσταση
- Εναλλακτική Εγκατάσταση
- Δοκιμαστικό περιβάλλον
- Deployment περιβάλλον
- Backup περιβάλλον

Η **Κύρια Εγκατάσταση** είναι η φάρμα διακομιστών που εξυπηρετεί την παραγωγική λειτουργία της πλατφόρμας, σε κανονικές συνθήκες. Αποτελείται από εικονικούς διακομιστές στην υπηρεσία ViMa του ΕΔΕΤ οι οποίοι φιλοξενούνται στο datacenter του ΕΔΕΤ στο Υπουργείο Παιδείας.

Η **Εναλλακτική Εγκατάσταση** είναι η φάρμα διακομιστών από όπου γίνεται παραγωγική λειτουργία της πλατφόρμας, σε περίπτωση που η Κύρια Εγκατάσταση τεθεί εξολοκλήρου εκτός λειτουργίας ή γίνει μη προσβάσιμη (π.χ. εάν καταρρεύσει το datacenter στο Υπ. Παιδείας). Αποτελείται από εικονικούς διακομιστές στην υπηρεσία ViMa του ΕΔΕΤ οι οποίοι φιλοξενούνται στο datacenter του ΕΔΕΤ στο Εθνικό Ίδρυμα Ερευνών.

Το **Δοκιμαστικό Περιβάλλον** είναι ένας διακομιστής (στο datacenter του ΕΔΕΤ στο Υπουργείο Παιδείας) που φιλοξενεί την νεώτερη έκδοση των εφαρμογών της πλατφόρμας. Χρησιμοποιείται για να γίνεται έλεγχος της καλής λειτουργίας των εφαρμογών (user acceptance testing) όταν η ομάδα ανάπτυξης τροποποιεί το λογισμικό των εφαρμογών.

Το **Deployment περιβάλλον** χρησιμοποιείται για το upload νέων εκδόσεων του λογισμικού των εφαρμογών από το περιβάλλον ανάπτυξης στην Κύρια Εγκατάσταση.

Το **Backup περιβάλλον** χρησιμοποιείται για την αποθήκευση των εφεδρικών αντιγράφων ασφαλείας των δεδομένων και των αρχείων των εφαρμογών, σε ασφαλή τοποθεσία εκτός του datacenter στο Υπ. Παιδείας.

1.1 Συνοπτική περιγραφή των διακομιστών των εγκαταστάσεων

1.1.1 Κύρια Εγκατάσταση

Η κύρια εγκατάσταση αποτελείται από 4 ζεύγη διακομιστών (8 στο σύνολο). Κάθε ζεύγος διακομιστών επιτελεί μία συγκεκριμένη λειτουργία ενώ ανάμεσα στους διακομιστές του ζεύγους έχουν υλοποιηθεί τεχνολογίες που επιτρέπουν την υψηλή διαθεσιμότητα της εφαρμογής. Συγκεκριμένα η κύρια εγκατάσταση αποτελείται από:

- 2 Firewall – Web Publishing Servers: Οι διακομιστές αυτοί ελέγχουν την δικτυακή κίνηση μεταξύ των υπόλοιπων διακομιστών καθώς και μεταξύ του συνόλου ΠΣ και του Internet. Επίσης είναι υπεύθυνοι για τον τερματισμό των https συνδέσεων στην εφαρμογή και το μοίρασμα του φόρτου εργασίας μεταξύ των application servers.
 - Λειτουργικό Σύστημα: Debian Linux
 - Λογισμικό: Haproxy, iptables, tinypoxy
 - Χαρακτηριστικά: 4 CPUs, 4GB RAM, 50GB storage
- 2 Application Servers: Οι διακομιστές αυτοί είναι υπεύθυνοι για την εκτέλεση της εφαρμογής web του ΠΣ.
 - Λειτουργικό Σύστημα: Microsoft Windows Server 2008 R2 Standard
 - Λογισμικό: Microsoft IIS 7.5, ASP.NET 4.5
 - Χαρακτηριστικά: 6 CPUs, 8GB RAM, 60GB storage
- 2 File Servers – Domain Controllers: Στους διακομιστές αυτούς αποθηκεύονται τόσο τα εκτελέσιμα αρχεία των εφαρμογών του ΠΣ όσο και τα αρχεία δεδομένων τους.
 - Λειτουργικό Σύστημα: Microsoft Windows Server 2008 R2 Standard
 - Λογισμικό: Microsoft Distributed File System, Active Directory.
 - Χαρακτηριστικά: 2 CPUs, 2GB RAM, 150GB storage
- 2 Database Servers: Στους διακομιστές αυτούς είναι εγκαταστημένο το Σύστημα Διαχείρισης Βάσεων Δεδομένων που χρησιμοποιείται από τις εφαρμογές.
 - Λειτουργικό Σύστημα: Microsoft Windows Server 2008 R2 Standard
 - Λογισμικό: Microsoft SQL Server 2012.
 - Χαρακτηριστικά: 8 CPUs, 8GB RAM, 150GB storage

1.1.2 Εναλλακτική Εγκατάσταση

Η εναλλακτική εγκατάσταση αποτελείται από έναν εξυπηρετητή στον οποίο έχει εγκατασταθεί όλο το απαραίτητο λογισμικό ώστε να εξυπηρετούνται πλήρως οι εφαρμογές του ΠΣ.

- Λειτουργικό Σύστημα: Microsoft Windows Server 2008 R2 Standard
- Λογισμικό: Microsoft IIS 7.5, ASP.NET 4.5, Microsoft SQL Server 2012, Windows Firewall.
- Χαρακτηριστικά: 8 CPUs, 8GB RAM, 200GB storage

1.1.3 Δοκιμαστικό Περιβάλλον

Στο δοκιμαστικό περιβάλλον έχουν εγκατασταθεί σε έναν διακομιστή οι ίδιες εκδόσεις του λογισμικού το οποίο χρησιμοποιείται από την εφαρμογή ώστε να προσομοιάζει όσο το δυνατόν με το παραγωγικό περιβάλλον.

- Λειτουργικό Σύστημα: Microsoft Windows Server 2008 R2 Standard
- Λογισμικό: Microsoft IIS 7.5, ASP.NET 4.5, Microsoft SQL Server 2012, Windows Firewall.
- Χαρακτηριστικά: 4 CPUs, 6GB RAM, 100GB storage

1.1.4 Deployment περιβάλλον

Το deployment περιβάλλον αποτελείται από έναν διακομιστή στον οποίο έχει εγκατασταθεί η εφαρμογή web που χειρίζεται την ενημέρωση των εφαρμογών του ΠΣ με νέες εκδόσεις. Επίσης αποτελεί ένα σημείο μη διαχειριστικής ελεγχόμενης πρόσβασης του παραγωγικού συστήματος από τους developers.

- Λειτουργικό Σύστημα: Microsoft Windows Server 2008 R2 Standard
- Λογισμικό: Microsoft IIS 7.5, ASP.NET 4.5, Microsoft SQL Server 2012 Management Studio, Microsoft FTP Service.
- Χαρακτηριστικά: 1 CPUs, 3GB RAM, 200GB storage

1.1.5 Backup περιβάλλον

Στο Backup περιβάλλον αποθηκεύονται τα εφεδρικά αντίγραφα ασφαλείας όλων των στοιχείων του ΠΣ, δηλαδή τα εκτελέσιμα αρχεία των εφαρμογών, τα αρχεία δεδομένων των εφαρμογών και οι βάσεις δεδομένων.

- Λειτουργικό Σύστημα: Debian Linux
- Λογισμικό: Openssh.
- Χαρακτηριστικά: 1 CPUs, 1GB RAM, 700GB storage

1.2 Συνοπτική περιγραφή του λογισμικού παρακολούθησης

Η ενότητα αυτή παρουσιάζει το ειδικό λογισμικό Nagios που χρησιμοποιείται για την παρακολούθηση της καλής λειτουργίας των διακομιστών των εγκαταστάσεων από τους διαχειριστές συστημάτων της ομάδας ανάπτυξης και υποστήριξης του Π.Σ. Κάλλιπος.

Το λογισμικό Nagios είναι ένα ανοιχτό λογισμικό που αποτελείται από μία κεντρική υπηρεσία που συλλέγει και ελέγχει τα αποτελέσματα από scripts που επιστρέφουν δεδομένα σχετικά με την κατάσταση των διακομιστών την παρούσα χρονική στιγμή. Η κεντρική υπηρεσία του Nagios έχει τη δυνατότητα, ανάλογα με τα δεδομένα που λαμβάνει και τα όρια που έχουν ρυθμιστεί, να κρίνει αν ένα διακομιστής εμφανίζει κάποια δυσλειτουργία και αναλόγως να εντείνει τους ελέγχους ώστε να ανιχνευθεί αν πρόκειται για κάποια προσωρινό πρόβλημα ή για ένδειξη αστοχίας του συστήματος. Αν εντοπιστεί κάποιο πρόβλημα αποστέλλεται ειδοποίηση στους διαχειριστές με την αντίστοιχη ένδειξη αν πρόκειται για κάποια προειδοποίηση για πιθανά εξελισσόμενο πρόβλημα (π.χ. κάποιος δίσκος που κοντεύει να γεμίσει) ή για κρίσιμη ουσιαστική δυσλειτουργία του συστήματος (π.χ. κάποιος εξυπηρετητής έχει σταματήσει να αποκρίνεται).

Οι έλεγχοι που γίνονται στους διακομιστές έχουν να κάνουν με την απόδοσή τους (π.χ. χρήση επεξεργαστή ή μνήμης), την κατάστασή τους (π.χ. γεμάτος δίσκος ή ενημερώσεις ασφαλείας που πρέπει να γίνουν), τις υπηρεσίες που πρέπει να τρέχουν και το χρόνο απόκρισης των εφαρμογών. Για την πλειοψηφία των ελέγχων χρησιμοποιείται το πρωτόκολλο SNMP (Simple Network Management Protocol). Το πρωτόκολλο αυτό προτιμήθηκε καθώς υποστηρίζεται εγγενώς από τα λειτουργικά συστήματα των εξυπηρετητών συνεπώς δεν απαιτεί την εγκατάσταση επιπλέον agents που μπορεί να επιβαρύνουν τους διακομιστές ή να δημιουργήσουν άλλες δυσλειτουργίες.

2 Εργασίες για την εξασφάλιση της καλής λειτουργίας των εγκαταστάσεων

2.1 Τακτικές εργασίες για την καλή λειτουργία των εγκαταστάσεων

Περιγράφονται οι εργασίες που οι διαχειριστές συστημάτων της ομάδας ανάπτυξης και υποστήριξης του Π.Σ. Κάλλιπος εκτελούν σε τακτική, καθημερινή βάση για την εξασφάλιση της καλής λειτουργίας των εγκαταστάσεων του Π.Σ. Κάλλιπος.

- Έλεγχος καλή λειτουργίας και διαθεσιμότητας της εφαρμογής.
- Έλεγχος καλής λειτουργίας Nagios Monitoring system.
- Έλεγχος πιθανών alerts που έχουν προκύψει στο Nagios αλλά δεν έχει ληφθεί ή δεν έχει γίνει αντιληπτός ο σχετικός συναγερμός (αποστολή email). Συγκεκριμένα ελέγχονται:
 - Η χρήση CPU να μην είναι διαρκώς πάνω από 80%
 - Η χρήση μνήμης να μην είναι πάνω από 90%
 - Οι δίσκοι να έχουν διαθέσιμη χωρητικότητα
 - Οι σωστές υπηρεσίες είναι ενεργές σε όλους τους servers
- Εποπτεία και έλεγχος των logs. Ελέγχεται η παρουσία μη συνηθισμένων ή επαναλαμβανόμενων λαθών που είναι πιθανό να υποδεικνύουν πιθανά προβλήματα. Συγκεκριμένα ελέγχονται τα εξής log files:
 - Application Log σε όλους τους windows servers
 - System Log σε όλους τους windows servers
 - Security Log σε όλους τους windows servers
 - Syslog σε όλους τους Linux Server
 - IIS HTTPError Log
 - SQL Server Log
 - SQL Server Agent Log
 - iptables(firewall) error log
 - haproxy (web publishing) error log
- Έλεγχος ορθής λήψης των backups της προηγούμενης μέρας.
- Έλεγχος κατάστασης συγχρονισμού Distributed File System
- Έλεγχος κατάστασης Database Cluster

- Έλεγχος κατάστασης Firewall Cluster

2.2 Επιπρόσθετες εργασίες για την καλή λειτουργία των εγκαταστάσεων

Πέρα από τις τακτικές εργασίες για την εξασφάλιση της καλής λειτουργίας των εγκαταστάσεων της πλατφόρμας, οι διαχειριστές συστημάτων της ομάδας ανάπτυξης και υποστήριξης του Π.Σ. Κάλλιπος προβαίνουν σε μία σειρά από ελέγχους και εργασίες προκειμένου:

- Να αποκαταστήσουν προβλήματα που εντόπισαν οι ίδιοι κατά τους τακτικούς ελέγχους.
- Να ερευνήσουν και να αποκαταστήσουν προβλήματα που αναφέρθηκαν από την ομάδα ανάπτυξης ή από το Γραφείο Αρωγής της δράσης.
- Να προβούν σε ρυθμίσεις που οι ίδιοι έκριναν απαραίτητες, είτε μετά από ανακοινώσεις των προμηθευτών (π.χ. θέματα ασφαλείας των MS Windows Servers, θέματα του πρωτοκόλλου SSL), είτε με βάση δικές τους πρωτοβουλίες.

Οι σχετικές ρυθμίσεις και εργασίες έχουν κυρίως να κάνουν με θέματα που αφορούν:

- Την πρόσβαση στην πλατφόρμα (ρυθμίσεις στους firewalls των εγκαταστάσεων)
- Τις διαδικασίες upload νέων εκδόσεων της πλατφόρμας από την ομάδα ανάπτυξης
- Την ασφάλεια των δεδομένων των εφαρμογών.
- Τις επιδόσεις στα διάφορα επίπεδα της εγκατάστασης (database servers, web servers, application servers, file servers)
- Τη λήψη εφεδρικών αντιγράφων των δεδομένων
- Τη λήψη εφεδρικών αντιγράφων των αρχείων
- Την εξασφάλιση no-single-point-of-failure στην κύρια εγκατάσταση
- Τη μεταφορά των αντιγράφων των αρχείων και των δεδομένων σε εναλλακτική εγκατάσταση.
- Τις διαδικασίες disaster recovery, δηλαδή την εξασφάλιση ότι ολόκληρη η πλατφόρμα μπορεί να μεταφερθεί και να λειτουργήσει στην εναλλακτική εγκατάσταση, με την ελάχιστη δυνατή απώλεια σε δεδομένα και αρχεία, σε περίπτωση που η κύρια εγκατάσταση τεθεί εξολοκλήρου εκτός λειτουργίας.

3 Αρχείο εργασιών για την εξασφάλιση της καλής λειτουργίας

Στη ενότητα αυτή καταγράφονται οι επιπρόσθετες εργασίες που εκτέλεσαν οι διαχειριστές συστημάτων της ομάδας ανάπτυξης και υποστήριξης του Π.Σ. Κάλλιπος στο χρονικό διάστημα από την έναρξη της δράσης μέχρι και τις 31/12/2013.

3.1.1 Εργασίες 1^{ου} και 2^{ου} Τριμήνου 2013

Ρυθμίσεις στους διακομιστές των εγκαταστάσεων του πληροφοριακού συστήματος:

- Ανίχνευση καθυστέρησης στο χρόνο απόκρισης σε ορισμένες περιπτώσεις. Η δυσλειτουργία εντοπίστηκε στον ενίοτε αυξημένο χρόνο ανάκτησης στατικών αρχείων της εφαρμογής. Υλοποιήθηκε εναλλακτική μέθοδος ανάκτησης των αρχείων ώστε να παρακάμπτεται το πρόβλημα.
- Μελέτη, υλοποίηση και δοκιμή της δυνατότητας πρόσβασης των στατικών αρχείων της εφαρμογής με διαφορετικό URL, ώστε να ελαχιστοποιηθεί το φορτίο της εφαρμογής με τη μη χρήση security cookie για τα αρχεία για τα οποία δε χρειάζεται. Έγινε έλεγχος των παρενεργειών που μπορεί να προκύψουν από τη χρήση κρυπτογραφημένης σύνδεσης (https) υπό διαφορετικά URLs και υλοποιήθηκε λύση που τα παρακάμπτει.
- Ανίχνευση πιθανών δυσλειτουργιών στη λειτουργία του Shibboleth λόγω του δικτυακής αρχιτεκτονικής του συστήματος και της μη εμφάνισης της IP του client στους web servers όπου είναι εγκατεστημένο το shibboleth. Πειραματισμός με παραλλαγές της αρχιτεκτονική σε συνδυασμό με τις παραμέτρους checkAddress και consistentAddress του Shibboleth.
- Επιτάχυνση του χρόνου που απαιτείται για τη φόρτωση μίας εφαρμογής κατά το πρώτο request μετά από deployment. Απενεργοποιήθηκαν ορισμένοι μη χρήσιμοι έλεγχοι.
- Ρύθμιση παραμέτρων ασφαλείας στην έκδοση 2 του .NET Framework ώστε να είναι δυνατή η φόρτωση εκτελέσιμων αρχείων της εφαρμογής μέσω εσωτερικού δικτύου.
- Ρύθμιση παραμέτρων ασφαλείας σε επίπεδο File System ώστε να είναι δυνατή η φόρτωση βιβλιοθηκών που δεν είναι γραμμένες σε .Net Framework με τον ίδιο τρόπο και από την ίδια τοποθεσία με τα υπόλοιπα αρχεία των εφαρμογών.
- Δοκιμές και ρύθμιση connection rate per IP limits στο firewall ώστε να βρεθεί ισορροπία μεταξύ ασφαλείας και σωστής λειτουργίας της εφαρμογής.

3.1.2 Εργασίες 3^{ου} Τριμήνου 2013

Εργασίες αποκατάστασης της καλής λειτουργίας και ρυθμίσεις στους διακομιστές των εγκαταστάσεων του πληροφοριακού συστήματος, μετά από εντοπισμό των παρακάτω προβλημάτων κατά τη χρήση των εφαρμογών:

1. Επίλυση προβλήματος στην αυτοματοποιημένη διαδικασία επαναφοράς ενός αντίγραφου ασφαλείας μια βάσης δεδομένων και ενεργοποίησής της στο Always-On Availability Group του SQL Server. Εντοπίστηκε το πρόβλημα στις περιπτώσεις αντιγράφων βάσεων που δεν ήταν σε Full Logging Model, όπου και απαιτείται δημιουργία νέου αντιγράφου της Βάσης.
2. Αλλαγή των scripts αυτόματης λήψης backup των Βάσεων Δεδομένων ώστε να λαμβάνουν υπόψη τους ποιος από τους 2 Database Servers έχει πρωτεύοντα ρόλο στο Always On Availability Group και ποιος δευτερεύοντα, και να λαμβάνουν ολοκληρωμένα (full) backups μόνο από τον δευτερεύοντα και backups του log file μόνο από τον πρωτεύοντα.
3. Επίλυση προβλήματος στη διαδικασία Deployment των αρχείων των εφαρμογών. Συγκεκριμένα όταν νέες εφαρμογές γίνονταν enable για deployment τα σχετικά δικαιώματα δεν ενημερώνονταν στους web servers μέχρι να γίνει restart το Web Deployment service.
4. Ρύθμιση των παραμέτρων του firewall cluster ώστε να ανταποκρίνεται σωστότερα σε περιπτώσεις ταυτόχρονης απώλειας όλων των κόμβων του λόγω γενικής δυσλειτουργίας της υποδομής Virtualization. Αυξήθηκαν τα timeouts και ο χρόνος αναμονής για μετάπτωση των υπηρεσιών.
5. Έλεγχος δημιουργίας locks και υπέρογκων log files σε τρέξιμο query για τη συντήρηση εφαρμογής. Επιλέχθηκε η χρήση Cursor ώστε να αποφευχθεί το πρόβλημα.
6. Bulk εισαγωγή δεδομένων από CSV (comma separated values) αρχείο με ελληνικούς χαρακτήρες με ANSI Encoding. Έγινε με χρήση του bcp εργαλείου μετά από κατάλληλες μετατροπές στο αρχείο εισαγωγής.
7. Δημιουργία SQL Server Agent Jobs για τη ενημέρωση των reports των εφαρμογών. Λόγω του φόρτου των διαδικασιών ενημέρωσης των κατάλληλων πινάκων με συγκεντρωτικά στοιχεία

ελέγχθηκε ο χρόνος εκτέλεσης των queries, έγινε βελτιστοποίησή τους και επιλέχθηκε να εκτελούνται σε συγκεκριμένες χρονικές στιγμές σε περιόδους απουσίας φόρτου από τις εφαρμογές, χωρίς όμως να συμπίπτουν με τις διαδικασίες δημιουργίας αντιγράφων ασφαλείας.

8. Επίλυση αδυναμίας χρήσης των γεωχωρικών βιβλιοθηκών του .NET Framework σε συνδυασμό με την εγκατάσταση του SQL Server. Επιλέχθηκε η απενεργοποίηση του light weight thread pooling στην εγκατάσταση του SQL Server.
9. Επίλυση προβλήματος στη διαχείριση (rotation) των αρχείων καταγραφής τους firewall που οδηγούσε στη δημιουργία μεγάλου αριθμού αντιγράφων των παλαιών αρχείων καταγραφής.
10. Ενεργοποίηση δυνατοτήτων HTTP PUT και DELETE για συγκεκριμένα services σε webserver και firewall.

3.1.3 Εργασίες 4^{ου} Τριμήνου 2013

Εργασίες ρυθμίσεων για την εξασφάλιση της καλής λειτουργίας του διακομιστή VM.demo2.kalliros (virtual server) όπου εγκαταστάθηκε η πιλοτική έκδοση του πληροφοριακού συστήματος kalliros:

- Δοκιμή ρυθμίσεων anti-click jacking (header X-FRAME-OPTIONS) ώστε να λειτουργούν σωστά τα pop up frames της εφαρμογής
- Ενημέρωση ρυθμίσεων anti-click jacking στο παραγωγικό περιβάλλον
- Επανεξέταση ρύθμισης anti-click jacking ώστε να λειτουργούν οι σελίδες των εφαρμογών που εμφανίζονται στο portal ως iframes
- Ρύθμιση του OAUTH για επικοινωνία με τα web services της ΓΓΠΣ
- Αναβάθμιση του διαθέσιμων resources (CPU, RAM) στο διακομιστή VM.demo2.kalliros
- Ρύθμιση αριθμού threads των εφαρμογών ώστε να λειτουργούν σωστά οι ασύγχρονες λειτουργίες των εφαρμογών
- Επίλυση προβλημάτων στο configuration της πιλοτικής εφαρμογής ώστε να λειτουργεί στο διακομιστή VM.demo2.kalliros
- Επίλυση προβλήματος στην αποστολή emails από τις εφαρμογές στο διακομιστή VM.demo2.kalliros
- Εγκατάσταση FTP Server στον διακομιστή VM.demo2.kalliros
- Έλεγχος προβλήματος στην επικοινωνία με το VM διακομιστή VM.demo2.kalliros λόγω αλλαγών στον Datacenter.
- Ενεργοποίηση δυνατότητας πρόσβασης στο διαχειριστικό περιβάλλον του IIS του διακομιστή VM.demo2.kalliros από μη διαχειριστικούς λογαριασμούς.
- Δημιουργία web εφαρμογής που επιτρέπει το recycling των application pools στον διακομιστή VM.demo2.kalliros από μη διαχειριστικούς λογαριασμούς.
- Δημιουργία φακέλου και ρύθμιση δικαιωμάτων για το ανέβασμα αρχείων μέσω των εφαρμογών στο διακομιστή VM.demo2.kalliros

Ρυθμίσεις για την εξασφάλιση της ασφάλειας και της υψηλής διαθεσιμότητας των διακομιστών της εγκατάστασης:

- **Web Publishing**

Για λόγους ασφαλείας και διασφάλισης της υψηλής διαθεσιμότητας των Application servers επιλέχθηκε να μην είναι άμεσα προσβάσιμοι από το διαδίκτυο. Εγκατέστησα το λογισμικό haproxy το οποίο και ανέλαβε το web publishing των εφαρμογών. Πιο συγκεκριμένα όλα τα αιτήματα προς τις εφαρμογές γίνονται προς το haproxy, το οποίο και στη συνέχεια αναλόγως με το αίτημα επιλέγει προς ποιον Application Server θα το προωθήσει. Ο Application server επιστρέφει την απάντηση στο αίτημα στον haproxy ο οποίος θα το παραδώσει στον πελάτη. Η μέθοδος αυτή με τον τρόπο που έχει υλοποιηθεί παρέχει τα εξής πλεονεκτήματα:

- SSL Offloading. Στην περίπτωση κρυπτογραφημένων συνδέσεων (https) ο haproxy αναλαμβάνει το σημαντικό φορτίο της αποκρυπτογράφησης του αιτήματος, απελευθερώνοντας έτσι πόρους στον Application Server για την εκτέλεση της εφαρμογής.
- Προστασία των Application Servers. Εκτός από το γεγονός ότι οι application servers δεν είναι πια άμεσα προσβάσιμοι από το διαδίκτυο, συνεπώς ένας επιτιθέμενος θα πρέπει πρώτα να προσπεράσει τον haproxy για να φτάσει στον application server, ο haproxy δίνει επιπλέον δυνατότητες κεντρικού και έγκαιρου φιλτραρίσματος των αιτημάτων σταματώντας έτσι κακόβουλες αιτήσεις πριν αυτές επεξεργαστούν από τον application server.
- Υψηλή διαθεσιμότητα των Application servers. Ο haproxy έχει τη δυνατότητα να ανακατευθύνει τα αιτήματα των χρηστών πότε στον έναν και πότε στον άλλο application server. Με τον τρόπο αυτό είναι δυνατόν όχι μόνο να χρησιμοποιούνται ταυτόχρονα περισσότεροι του ενός application servers αυξάνοντας έτσι τις συνολικές επιδόσεις του συστήματος, αλλά επιπλέον αν ένας application server αποτύχει ο haproxy το αντιλαμβάνεται, και τα αιτήματα ανακατευθύνονται προς κάποιον από τους

υπόλοιπους λειτουργικούς servers. Με τον τρόπο αυτό επιτυγχάνεται η υψηλή διαθεσιμότητα των application servers.

- **Υψηλή διαθεσιμότητα firewall και web publishing**

Για την υψηλή διαθεσιμότητα των συστημάτων αυτών εγκατέστησα δύο εξυπηρετητές που έχουν και οι δύο εγκαταστημένα τα παραπάνω λογισμικά. Τόσο ο haproxy όσο και το iptables δεν έχουν εγγενείς δυνατότητες υψηλής διαθεσιμότητας. Παρόλα αυτά και τα δύο υποστηρίζουν τη ρύθμιση τους και τη λειτουργία τους για IPs που δεν είναι ορισμένες στο λειτουργικό σύστημα (το iptables εγγενώς και ο haproxy μέσω της επιλογής transparent binding). Συνεπώς, και καθώς τα συστήματα αυτά δεν αποθηκεύουν αρχεία ή χρησιμοποιούν κάποιου άλλου είδους «μόνιμης» πληροφορίας, η μόνη απαίτηση για να γίνει μετάπτωση από τον έναν εξυπηρετητή στον άλλο είναι η μετάπτωση των IPs που χρησιμοποιούνται για τη λειτουργία τους.

Η μετάπτωση αυτή γίνεται μέσω του δημιουργία ενός Active-Passive cluster με χρήση του λογισμικού racemaker του Linux High Availability project. Ο racemaker χρησιμοποιεί εσωτερικά το corosync για να εντοπίσει αν όλα τα συστήματα είναι online και να αποφασίσει τελικά σε ποιο από τα δύο να εκχωρήσει τις εν λόγω IPs.